ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

Passwordless Authentication Using FIDO Server

Anvesh Gunuganti

USA

ABSTRACT

The emphasis of the discussion will be on a passwordless login approach using the FIDO protocol and Ping Federate standard to resolve the security consequences linked to the password-based authentication. The paper covers the FIDO efficacy in the business realm, the security benefits of FIDO password-less authentication, and the impact of FIDO on enterprises user experience and security. Passwordless login options which are based on biometrics, hardware tokens, or connected mobile devices, make security and user authentication easier. The main security functionality comprises lower risk of fraud, quick login for the user, automated operations, compatible with reporting guidelines, and cutting-edge future-proof security features. This paper offers using FIDO2's passwordless authentication techniques as a remedy for cyberattacks determined factors as well, advises to educate both users and management of organization, in order to maximize and increase security.

***Corresponding author**

Anvesh Gunuganti, USA.

Received: January 08, 2024; **Accepted:** January 16, 2024; **Published:** January 19, 2024

Keywords: Passwordless Authentication, FIDO Protocol, Ping Federate, Biometrics

Introduction

In an era that has been denoted by worsening cyber threats and the unending exposures of traditional password-based authentication, organizations have been greatly compelled to adopt Inventive measures like passwordless authentication so as to enhance their security position [1]. This article is concerned with how the FIDO protocol and the Ping Federate identity and access management functionality are implemented to solve the problem of password authentication. Through this study we aim to solve some of the challenges that have been posed by conventional authentication systems without compromising the security and performance of the system integration within organizational environments.

Background and Motivation

The statistics on significant security breaches emphasize how vital it is to fix password limitations and look into alternate forms of authentication. The traditional password system is vulnerable to various threats, such as phishing, credential stuffing, as well as password reuse. These threats could lead to major security problems for organizations if they are neglected [2].

The notion of this research work is in line with the progress of leaving behind the password-based authentication method in place of something which is more secure and user-friendly. FIDO protocol that uses biometric or hardware tokens-based authentication provides an efficient mechanism that ends the use of passwords and thus magnifies the online security.

Problem Statement and Research Objectives

This study aims to tackle one critical deficiency in traditional password-based authentication system which is insecurity. When numerous accounts and workplaces use weak passwords and the hits of credential theft are on the rise, that is a good reason to implement secure and user-friendly authentication mechanisms universally. The research objectives of this study include:

- Evaluating the viability of using FIDO in a workplace context.
- Discussing the security benefits of operations systems that are enforced by using passwordless authentication.
- Investigating the influence of passwordless verification on user experience as well as the security posture of the organization.

Significance of Passwordless Authentication

Passwordless authentication offers compelling benefits over traditional methods:

- **Enhanced Security:** The credential theft risks and phishing attacks are greatly reduced due to the usage of the robust authentication toolsets such as biometrics and hardware tokens [3].
- **Improved User Experience:** With the authentication of advanced authentication technology, quick sign-in will be easy, and there will be no need to remember complex passwords.
- **Reduced Operational Overhead:** Reduces password use complexity and lowers IT support costs.
- **Compliance and Regulatory Alignment:** The benefits include meeting the requirements of privacy laws and principles.
- **Future-Proof Security Strategy:** The dynamic nature of the cyber-security landscape is reflected in the quick response to threats. Sticking to user-centered approach to cyber-security is a priority.

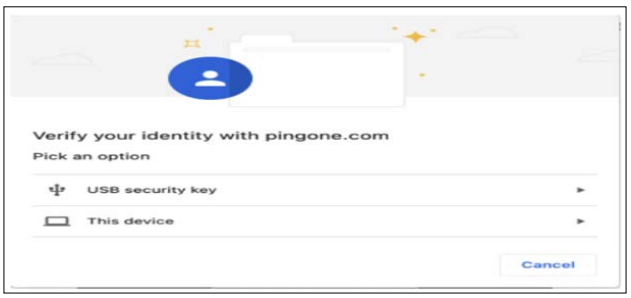

Figure 1: Passwordless Login Screen [4].

Overview of FIDO Protocol and Ping Federate

The FIDO protocol and Ping Federate are key components enabling passwordless authentication solutions. FIDO leverages open standards and robust authentication methods like biometrics and hardware tokens, enhancing security without transmitting sensitive user credentials over networks. Meanwhile, Ping Federate provides strong identity management and streamlined single sign-on features, supporting industry standards like SAML, OAuth, and OpenID Connect for secure access to cloud, mobile, and enterprise applications. Together, they simplify identity federation and enhance authorization controls across various platforms.

Research Question

- How does passwordless authentication using the FIDO protocol enhance security compared to traditional password-based methods?

Literature Review

Traditional Password-Based Authentication Challenges

The conventional password-based authentication systems face a lot of problems that undermine the security, usability, and efficiency of the systems. Some of the security problems that need to be tackled include the possibility of being hacked using phishing attacks, which trick users into revealing their credentials, as well as brute force attacks where all the password options are tried systematically. Likewise, credential stuffing, exploitation of stolen credentials and data breaches, also aggravate logging vulnerabilities. The user experience gets worse because of the complicated password requirements, which leads to the use of weak passwords and the need to reset them frequently, which is frustrating and the cause of many support requests. Businesses are required to bear the burden of managing password policies, securities, and support enquiries such as resets and lockouts that take significant time and resources. Moreover, it is mostly the case that adherence to the changing data security rules will result in tighter authentication methods to preserve this information.

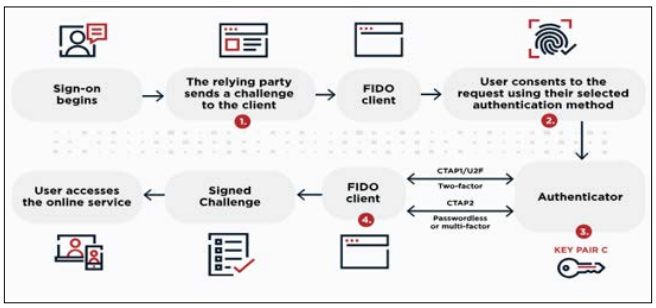

Figure 2: FIDO Authentication [5].

System Architecture

Client Access to Service Provider (SP) Server: When a user uses a client application to connect to the service provider (SP) server, authentication starts. First, the client contacts the service provider to see if there is already a session in progress. In the event that the client cannot locate an authorized username (session cookie), it will reroute towards the Ping Federate server.

Ping Federate Server Handling: When the Ping Federate server gets a redirection, it decides whether to use authentication or just continue with the client's session status test. For the first time or unverified session, after redirecting the client to the Ping Federate server, the next step involves redirecting the client to the FIDO server to initiate the authentication process.

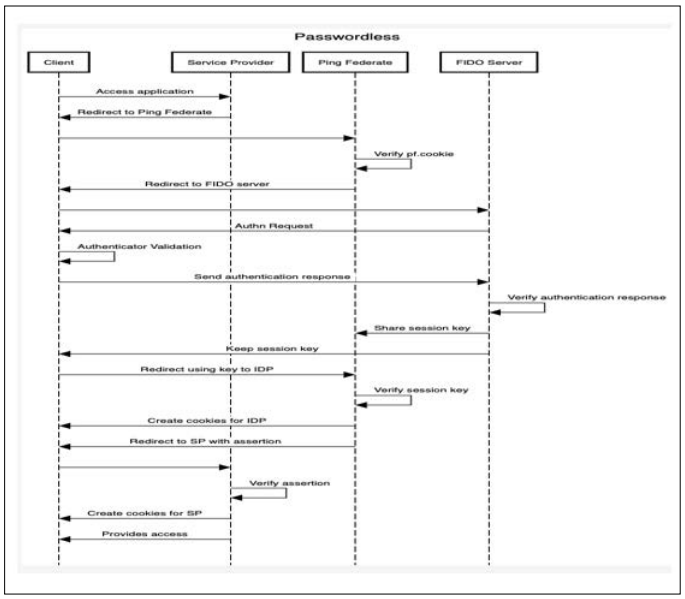

Figure 3: FIDO System Architecture [6].

FIDO Server Authentication Process: The FIDO server now interferes with the client by doing an authentication. The client is challenged FIDO2 and completes the local authentication with their preferred modality (e.g., fingerprint or FaceID, biometrics, PIN). Clients will authenticate themselves locally. Then, the client sends the internet address of the local host to the FIDO server.

Session ID Generation and Communication: The FIDO server is inclined to provide a session ID to the authenticator when the verification of the results is accurate. This session ID then forms part of an expression that is communicated back to the Ping federate server.

Attribute Retrieval and SP Server Access: PingFederate is the service that gets the requisite elements because of the user identity by making the usage of the session identifier. By means of this identification, the data which is being linked with the session is being sent to the SP server, completing the identification process and giving secure access to the requested online service.

Evolution and Adoption of Passwordless Authentication

The progression and adaptation of passwordless verification methods have been fueled by the weaknesses of traditional password-based authentication techniques. Biometric authentication, which uses technologies like fingerprints, facial recognition, and iris scanning, has a higher level of security and user convenience than passwords and eliminates the need for memorization. Hardware tokens, including the cards that generate one-time codes and the cards that use cryptographic signatures, make the authentication process more secure, and, in doing so, they reduce the reliance on static passwords and, therefore, improve

application security. Passwordless authentication puts an emphasis on security while having the ability to enhance user experience thus making it an increasingly common method used in many industries.

Overview of FIDO2 Protocol and Its Security Features

The FIDO2 protocol revolutionizes passwordless authentication with key security features: It uses public key cryptography to ensure safe logins without the need to send passwords over networks, but instead utilizing the critical keys stored on the user's device. The FIDO2 allows for the local authentication of users with biometric use. g., (e.g., passwords and PINs) and hardware tokens (for example, smart cards and key fobs). g., (security keys) stored on the device, the risks of unauthorized access are reduced. It provides a stronger phishing resistance by verifying authentication requests through local verification without sending the data over the networks. With its slim standards, FIDO2 allows for identity verification of users both through native applications and third-party applications, thus promoting its acceptance and the widespread adoption of passwordless identity authentication.

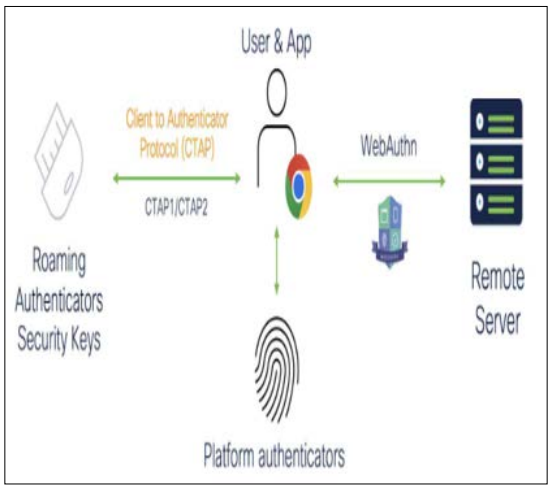

Figure 4: Passwordless Authentication [7].

Research Methodology

Case Study Approach

This research utilizes a case study to investigate the implementation and effect of passwordless authentications with FIDO set about in organizational entities. Case studies provide an epistemological tool to investigate actual cases showcasing how specific adoption of recent authentication methods influence practice and reality.

Selection Criteria for Case Studies

The case studies will be selected based on their relevance to the companies which are implementing FIDO-based passwordless authentication solutions, covering different industries in order to show the diversity of implementation scenarios and security needs. We will explore cases of varying scales that adhere to security protocols and regulations, with a particular focus on models that demonstrate flawless compliance. Comprehensive data availability covering not only implementation details but also challenges, success criteria, and feedback from users would be critically taken into account for inclusion in the analysis.

Case Study Analysis

Summary of Case Study 1

In the paper at hand the scholars explore the possibility of FIDO2 passwordless authentication supplanting textual passwords as the primary authentication method while on the web [8]. FIDO2, co-invented by the FIDO Alliance and the W3C, brings in the different approach of developing secure and convenient authentication while inheriting the characteristics. The main goal of the research is to evaluate the feedback concerning FIDO2 single-factor authentication using security keys which is its acceptability, usage concerns, and end-users' perceptions. As this criterion is met, the authors have a big lab-based usability research on hand where various tasks are assigned to participants to deal with FIDO2 security keys. Different participants will experience and understand passwordless authentication in different ways. The survey will collect their experiences and attitudes, and the analysis will be performed on them.

The study showed that users, in a vast majority, are ready to adopt security keys as a new method to replace passwords on single-factor authentication models which are widely used. This favorable reception hints at a passage of the proverbial industry locomotive from password-based authentications to secure passwordless methods, and this is what the industry should be working hard to achieve. Nevertheless, together with the stated issues the research highlights the problem areas that may make FIDO2 the less attractive and potentially the less popular alternative to password-based authentication. Besides convenience issues associated with device compatibility problems as well as interface usability problems during the first-time use and everyday usage of security keys, there is also a widespread skepticism that is seen across the world among users who are not used to security keys and hence they often struggle with these new methods and often abandon the new technologies.

Summary of Case Study 2

This research will uncover the main difficulties preventing the adoption of the FIDO2 standard, an authentication technology without passwords, developed by the FIDO Alliance to make the process more secure and convenient [9]. Even though FIDO2 proves to have higher safeness in comparison with traditional password authentication, this approach has not been widely adopted, despite major tech companies like Apple, Google, and Microsoft that have been announced to be supporters of FIDO2 protocol.

So, obstacles were examined by executing usability tests and interviewing ten participants of the study. Users of web showed a very low familiarity with passwordless authentication; among them most were enthusiastic about how passwordless authentication might work out but they were rather worried regarding the manual changing of security settings and they were willing to see a smoother process of the shift. These findings are again an evidence of user knowledge and FIDO2 implementation options that involve a user-friendly authentication technology.

Comparative Analysis of Case Studies

User-centric examinations would look at the acceptance of passwordless security standards, while also emphasizing the implementation with FIDO2 standards. The first report from S. GhorbaniLyastani et al, presents end-user perceptions of and reticence to use FIDO2 single-factor authentication via security bar among end-users. Results show most respondents in favor of using security keys to replace the old-fashioned text passwords, but also thoughts about what is to keep the possible adoption universal.

While the former test proves the presence of difficulties implementing FIDO2, the later research underlines the usability and the user knowledge issues. While this study acknowledges

the positive aspects of FIDO2 as a security protocol, it expresses concerns about the manual change of the security settings and the transformation of the process into a seamless switch between protocols. These studies also support the fact that user training and simplified deployment are the solutions for these challenges and the move towards the adoption of passwordless approaches such as FIDO2 by commercial services.

Findings and Discussion

The key learning and takeaways from the case study reflect at your research question by clearly exhibiting the advantages the FIDO protocol confers to passwordless authentication against the conventional password-based authentication. Built-in FIDO2 security keys and biometrics offspring diminishes the hazard of passwords breaches, ensuring a robust authentication mechanism that effectively minimizes security threats. Based on this, FIDO2 not only boosts user awareness and provides a common platform for collaboration within the authentication sector, but it also has a positive impact on the security and user experience in the authentication ecosystem; which is a match to your research that is aimed at improving authentication through innovative approaches. It is evident that this research provides the formula that can help in improving the implementation of passwordless authentication in cyber strategies utilized by people. This can be achieved by ensuring success and a better user experience.

Security and Operational Implications

Security Benefits of Passwordless Authentication

FIDO2 technology offers a robust solution to eliminate password-related security issues by leveraging advanced authentication methods like security keys and biometrics. Passwordless authentication, such as FIDO2, mitigates threats associated with password reuse, phishing attacks, and credential stuffing, enhancing overall security [10]. These methods employ strong cryptographic techniques and hardware-based security, reducing the risk of identity theft and unauthorized access. Moreover, passwordless authentication eliminates vulnerabilities to phishing attacks since there are no passwords to steal, making systems more secure even in cases of device theft or credential exposure.

Operational Challenges and Mitigation Strategies

Although passwordless systems provide several security advantages, companies may have difficulties in creating and deploying them, such as adjusting to different user profiles and device types. To ensure a seamless transition towards passwordless authentication methods, mitigation tactics include explicit communication of incentives, thorough user training, and the availability of user-friendly tools [11]. For flawless operation across all devices, interoperability must be achieved through agreements among device manufacturers and industry standards like FIDO2. Passwordless authentication solutions can further reduce the risk of device loss or failure by implementing secure recovery techniques, educate users on secure password usage, and conducting routine backups and recovery procedures.

User-Centric Authentication Solutions

To ensure effective and smooth running of the operations, user-centric sign-in methods should be emphasized along with security processes. First, user-driven solutions in the realm of authentication prioritize ease of use and conveniences [11]. The aim behind this strategy is to facilitate acceptance and adoption of these solutions among the users. Creating intuitive user interfaces and keeping user friction to minimum promote a positive authentication experience and expand the adoption of passwordless solutions. Secondly, adopting an identity assurance method that needs the users two or even more elements and proof of their identity, in addition to passwordless methods like those FIDO2 offers, will both make the system harder to crack and make it more user friendly. These devices create a possession-based technology by allowing different authentication factors (e.g., pin, photo, fingerprint, etc.). It makes it harder to forge a user's identity and use biometrics and security keys. Organizations can seek security and user experience, giving strong security that will protect against unauthorized access.

User-centric authentication solutions cater to target consumers and require constant feedback and regular adaptability to changing environment models of security threats. Therefore, it is vital to consider agility and adaptability in changing user authentication systems, preferably to match the varying needs and security levels. Additionally, this will help nurture an ecosystem that is not only secure but also user-friendly.

Conclusion

Studies of FIDO2-based passwordless authentication examine user acceptance, underlying security advantages and operational drawbacks. Users are positive about passwordless authentication, especially FIDO2, as they think it really decreases the security risks and improves the comfort. Just like the experience of EVs into the regular road-users, educating and implementation efforts can lead to a broad acknowledgement of the technology. The implementation of Passwordless authentication with the help of FIDO2 eliminates the leakage of passwords and combines different authentication mechanisms such as security keys and biometrics. The issues of user onboarding, device compatibility, and backup recovery are very important when it comes to the integration and the best use of passwordless authentication technology in the security policy. Although not completely secure, passwordless authentication has a drastic impact on the phishing and credential theft vulnerabilities that are usually associated with password-based methods, among other things, which enhance users' ability to defend against cyberattacks.

Recommendations for Future Research and Practice

Encouraging the routine use of these technologies themselves is the main element of promoting adoption and enhancing password-free authentication. Next, the research objective and the future practice issues should address them with high priority. With user education being enhanced and awareness campaigns being developed, passwordless authentication became to be regarded as natural and has been introduced to the majority of people. Integration of using software through simplified integration, ubiquitous devices, and easily aware user interfaces, will be the key of whether the audiences leave the app or not. The continued assessment, majoring on user feedback and the dynamic development of security threats will improve the authentication technology further to optimize it for the best performance and effectiveness. Promoting the undertaking of standardization and interoperability efforts will enable easy access and usage of passwordless authentication across multiple platforms and services thereby tightening the cybersecurity strategy through addressing user experience [12-14].

References

1. Parmar V, Sanghvi HA, Patel RH, Pandya AS (2022) A Comprehensive Study on Passwordless Authentication. 2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS) https://ieeexplore.ieee.org/document/9760934.

2. Arabo A, Tunde Oduguwa (2023) A Review of Password-less User Authentication Schemes. Authorea https://www.authorea.com/users/701847/articles/688072-a-review-of-password-less-user-authentication-schemes?commit=3441addcc282ec7bfb7c8bb1820648a4f0f40033.
3. Assumpta Ezugwu, Elochukwu Ukwandu, Celestine Ugwu, Modesta Ezema, Comfort Olebara, et al. (2023) Password-based authentication and the experiences of end users. Scientific African 21: e01743.
4. We're here to help. docs.pingidentity.com https://docs.pingidentity.com/r/en-us/solution-guides/bp_workforce_passwordless_journey.
5. FIDO (Fast Identity Online). www.pingidentity.com https://www.pingidentity.com/en/resources/identity-fundamentals/authentication/passwordless-authentication/fido.html.
6. (2015) From Theory to Practice: Adding Two-Factor Authentication to Node.js. Auth0 - Blog https://auth0.com/blog/from-theory-to-practice-adding-two-factor-to-node-dot-js/.
7. (2021) WebAuthn, Passwordless and FIDO2 Explained - Duo Blog. Duo Security https://duo.com/blog/webauthn-passwordless-fido2-explained-componens-passwordless-architecture.
8. Ghorbani Lyastani S, Schilling M, Neumayr M, Backes M, Bugiel S (2020) Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. 2020 IEEE Symposium on Security and Privacy (SP) https://ieeexplore.ieee.org/document/9152694.
9. Furuberg IL, Øseth M (2023) From Password to Passwordless: Exploring User Experience Obstacles to the Adoption of FIDO2 Authentication. ntnuopen.ntnu.no https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3093908?locale-attribute=en.
10. A Zhidovich, A Lubenko, I Vojteshenko, A Andrushevich (2023) Semantic approach to designing applications with passwordless authentication according to the FIDO2 specification. libeldoc.bsuir https://libeldoc.bsuir.by/handle/123456789/51307.
11. M Kepkowski, Maciej Machulak, I Wood, Dali Kaafar (2023) Challenges with Passwordless FIDO2 in an Enterprise Setting: A Usability Study. IEEE Xplore https://ieeexplore.ieee.org/document/10305624.
12. I Gordin, A Graur, S Vlad, C I Adomniței (2021) Moving forward passwordless authentication: challenges and implementations for the private cloud. IEEE Xplore https://ieeexplore.ieee.org/document/9638271/.
13. Emin Huseynov (2022) Passwordless VPN using FIDO2 Security Keys: Modern authentication security for legacy VPN systems. IEEE Xplore https://ieeexplore.ieee.org/document/9984888.
14. J Kunke, S Wiefling, M Ullmann, L Iacono (2021) Evaluation of Account Recovery Strategies with FIDO2-based Passwordless Authentication. arXiv.org https://arxiv.org/abs/2105.12477.