Volume-08 Issue 12, December-2024 ISSN: 2456-9348
Impact Factor:7.936

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

TRANSITIONING TO PASSWORD LESS SECURITY: IMPLEMENTING ADVANCED AUTHENTICATION STRATEGIES IN THE ZERO-TRUST LANDSCAPE

Sairam Durgaraju
Sr Security Architect
The Cigna Group
Liberty Place, 50 S 16th St, Philadelphia, PA 19192

ABSTRACT
This research examines the transition to passwordless security under the security model of Zero Trust, the failure of the classical methods based on passwords, and the advantages of more sophisticated authentication processes. Focuses on its weaknesses, when used, one is likely to fall a victim of a phishing attack, or else make a simple mistake and the account is compromised, then it recommends better means such as the biometric, hardware tokens, and one-time passcodes (OTPs). When these are implemented with Zero-Trust model, the benefits get supplemented with strong security since there is constant checks and verification of users and devices. The improvements to the user experience of security as well as the lower administrative costs are also mentioned in the study. Of course, changing to pass less security has its benefits, and it needs planning, checking compatibility, and tutorials. This is because biometric data require special protection and the management of the hardware tokens also present other risks that need be solved by security measures. Thus, the research supports the notion that passwordless security is one of the measures that, when implemented, makes it possible to prevent the emerging cyber threats.

Keywords:
Passwordless, Security, Cybersecurity, Advanced Authentication, Transition.

INTRODUCTION

In the current era, a direct dependency on passwords is seen as a primary method of authentication is becoming an increasingly important problem as a result of the dynamic growth of contemporary threats to information security. The contemporary evolution of improved types of cyber threats and vulnerabilities, in conjunction with the weaknesses of password-based systems, which include falling for phishing scams, misusing the same passwords for multiple profiles, and general user mistakes such as typos, have necessitated a shift in gears in the enhancement of security (Kak, 2022). This method of security is known as passwordless security, and it is consistent with the majority of the fundamentals of Zero-Trust architecture.

Through the implementation of passwordless security, a revolutionary transformation is brought about in which passwords are no longer an essential component of the authentication process (Kak, 2022). On the contrary, it carries out a number of high-level authentications that not only strengthen the protection strategy but also increase the degree of satisfaction experienced by customers. There is a significant role that biometrics, such as fingerprint scanning and facial recognition, hardware tokens, and one-time passcodes (OTPs), play in this shift (Furuberg and Øseth, 2023). These approaches provide more secure methods to authenticate users, in contrast to the easy methods that are often used, which are prone to compromise and assault.

Both passwordless approaches and the Zero-Trust security model, which is based on the assumption that no one, including employees and endpoints within a network or any third party, should be automatically trusted, are complementary to one another. Due to the fact that Zero-Trust is based on the assumption that risks could exist both inside and outside of the conventional border, it places an emphasis on the continuous validation of both users and devices (Kak, 2022). As a result, we are able to draw the conclusion that the use of passwordless authentication within a Zero-Trust framework can assist organisations in enhancing the level of security around their environment. Additionally, it ensures that the security of the sensitive resource is evaluated at regular intervals using both identity-aware and context-based security policies. This is done in order to guarantee that the resource is protected.

Research Aim

The aim of the research is on analysing the transition towards the password less security with the implementing of the advanced authentication strategies in the Zero-Trust Landscape.

Research Objectives

The objectives of the research are as follows:

1. To analyse the transition towards the password less security.
2. To understand the advanced automation strategies in the Zero-trust landscape.
3. To access the influence of password less security with authentication strategies in the Zero-trust landscape.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Research Question

The core research questions the paper will address is how the transitioning to password less security with the implementation of advanced authentication strategies in the Zero-Trust Landscape?

Literature Review

According to George, (2024), when it comes to the Zero-Trust models, the implementation of passwordless security requires a significant amount of planning and the implementation of effective techniques in order to be successful. When it comes to the security of identities, it mandates that businesses deploy multi-factor authentication (MFA) solutions, make use of the most recent identity verification technologies, and ensure compatibility across all systems and devices (George, 2024). Therefore, it is necessary to establish a culture within organisations that encourages users to place a high level of importance on security. Adopting the notion of a password-less security system as a component of the Zero-Trust model is one of the most proactive and necessary steps that can be taken to enhance the security mechanism and protect the key data in this era of advanced digitalization. This is because the risks that exist in the cyber world are continuously increasing.

The Trend of Passwordless Authentication: The New Wave

According to Muhammad, et al., (2022), mentioned that by eliminating the need for passwords, which are susceptible to being exploited by phishing, brute force attacks, and reused passwords, the use of passwords is reduced (Muhammad, et al., 2022). Instead, it employs methods such as cryptography, biometrics, and device identification in order to successfully verify the identities of its users. A number of advantages can be gained from utilising passwordless authentication, including a higher level of security, increased levels of user happiness, and reduced expenses associated with password administration (Muhammad, et al., 2022). The Foundation for Secure Access is the name of the Zero Trust Architecture, and the middle of the cheque is written in capital letters to emphasise the importance of the term.

According to the Zero Trust landscape, which operates under the principle of "never trust, always verify," access to any resource is continuously reviewed based on a variety of variables including the User, the System, and the Network of the organisation (Furuberg and Øseth, 2023).

As mentioned by Furuberg and Øseth (2023), it is stated that through the implementation of the Zero Trust model, the access to information is strictly regulated, as are the movements of the intruder within the network. This results in a considerable reduction in the risks of a breach, attacks on different levels, and lateral movement (Furuberg and Øseth, 2023). Within the framework of zero trust, the following are some examples of sophisticated authentication mechanisms that are considered available: Multi-Factor Authentication (MFA) is a multi-factor authentication system that combines two or more authentication elements, such as passwords, fingerprints, smart cards, or tokens, in order to increase the level of security within an organisation. By improving the protection level and minimising the organization's exposure to threats based on credentials, multi-factor authentication (MFA) adds to the organization's overall security. The requirements for authentication can be changed through the use of adaptive authentication, which, on the other hand, makes use of data regarding a user's behaviour, location, and device attributes in order to make the necessary adjustments. Using this technique, organisations are able to build a security measure that is user-friendly. This is accomplished by installing an authenticating measure that is based on the levels of risk that are involved in accessing the system.

As per Furuberg and Øseth, (2023), mentioned that in order to verify the identities of users and devices within a network, the Public Key Infrastructure (PKI) employs two keys that are distinct from one another but are associated to one another. In its role, public key infrastructure (PKI) offers assurance to individuals and applications by means of the issuing of digital certificates and the confirmation of their authenticity, particularly in circumstances where the systems were dispersed (Furuberg and Øseth, 2023). Fingerprints, facial recognition, and even voice recognition are all examples of biometric identification methods that are used to verify a identify. These methods are derived from a person's physical traits and are used to confirm a person's identity. In spite of the fact that the usage of biometric identifications is thought to be relatively secure and convenient from an operational standpoint, there have been some concerns raised about privacy, accuracy, and spoofing attacks by some individuals (Kingo and Aranha, 2023).

Zero-Trust Security Model

According to Chowhan and Tanwar, (2019), Zero-Trust Security Model enforces the idea that one should not trust any entity by default both in the network perimeters and out of them and every access request should be validating continuously. Some of the primary principles that embrace zero-trust architecture are identity assurance at every level, using the minimum level of access control, segmenting the networks into tiny parts, and perpetual check (Chowhan and Tanwar, 2019). End User Identity Probing; Identity checking is an uninterrupted process to validate the user's identity with high levels of precision and accredit it on the MFA and context-sensitive access control mechanisms. The principle of least privilege restricts users' capabilities to the barest minimum required for them to perform their tasks, thereby limiting the probability of transferable attacks in the network (Casey, et al., 2020). Micro-segmentation of the network implies dividing it into several small segments that are independent and hence will not allow any leak to spread to the entire network while on the other hand continuous monitoring carries out analysis on users' behaviour and the traffic in the network to detect any irregularities and signs of potential threats (Chowhan and Tanwar, 2019). When passwordless authentication is incorporated into a zero-trust environment, an organisation gains more security as it enforces strong authentication of all access requests.

Advantages of Passwordless Authentication System in Zero-Trust Architecture

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

According to Parmar, et al., (2022), Passwordless authentication has many advantages when used in a zero-trust environment when it has been incorporated. First, it increases security because of inherent resistance to more general attack methods like phishing, brute force, and credential stuff. Better than passwords are biometric data, as well as permanently connected hardware tokens and numerous cryptographic features, which are much more difficult to hack by the perpetrators (Parmar, et al., 2022). Secondly, passwordless methods enhance the end users' experience since there will be no need to remember many secured passwords, resulting in a generally less complicated login process in this methodology. According to Zhu, et al., (2014), it is mentioned that passwordless methods impact credential management costs as they lower the need for administrative work and resources required for carrying out password resets and Helpdesk services. According to Oesch and Ruoti, (2020), it is stated that the use of enhanced forms of identification also ensures that an organization meets all the legal standards set on data protection and security, thereby improving the risk management capabilities and reduce exposure to possible threats (Oesch and Ruoti, 2020).

Challenges and Considerations

According to Zhu, et al., (2014), the move to passwordless authentication within the zero-trust security model come with the following difficulties (Zhu, et, al., 2014). In the case of passwordless systems, there are issues of complexity during implementation because the changes that need to be made in terms of infrastructure are massive, and one might need to invest in new technology altogether (Chowhan and Tanwar, 2019). According to Casey, et al., (2020), it is mentioned that compatibility with older systems is also a problem that needs to be solved. User adoption can also be a problem; thus, an extensive training and sensitization program has to be carried out to make the users understand the importance of passwordless authentication and how to go about it (Casey, et al., 2020). Because of the methods that may be used in the storage and management of the biometric data, there are great risks that the biometric data may be hacked or breached hence the necessity of putting in place strong security measures to ensure that the biometric data is not exposed (Oesch and Ruoti, 2020).

Real World

Fortunately, there are several organizations that have adopted passwordless authentication, therefore, giving real-life experience on how it works (Casey, et al., 2020). For instance, Microsoft synchronously implemented passwordless authentication system by activating Windows Hello and the FIDO2 standards to improve the overall security of its operating system for a large population of users. Google's Advanced Protection Program uses HSK for the most endangered personnel; the use of HT contributes significantly to protecting sensitive accounts (Parmar, et al., 2022). The using of the biometric technology has been practiced in the finance sector; whereby the banks and other financial institutions have integrated the biometric in the mobile banking applications; enabling customers control through the biometric data so as to offer secured access as well as to increase the trust in mobile banking (Horsch, et al., 2015).

RESEARCH METHODOLOGY

The research methodology shows all the tools, methods and techniques that are used in the research paper to attain the outcomes and gain valuable insights.

Research Data Collection

The data is collected from the secondary sources which include the data collection from already published journals, researches, articles and other validated sources to get relevant, reliable, and authenticate data. Secondary data is already published and validated data which makes the data collection real, and authentic.

Research Data Analysis

The qualitative analysis of the secondary data is done, to get the insights of the research data collected and to gain the valuable outcomes of the data. The qualitative analysis makes the research work more justified and the outcomes driven to gain the valuable insights of the data and deliver the outcomes about how the transition towards the passwordless security is leading to advanced authentication.

Research Ethics

The entire research work is done ethically within the research code of conduct to stay within the preview of the research norms. No specific group is targeted or none of the sentiments are hurt with the research. All the ethical means and followed throughout by the researcher.

Findings and Analysis

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

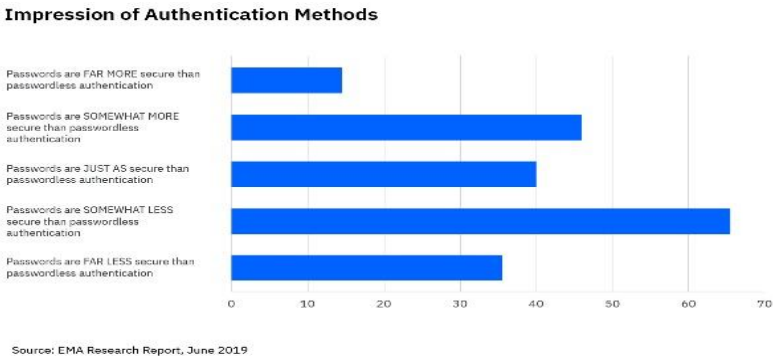

Figure 1: The path to passwordless authentication is shorter

Source: (Billings, 2019)

A significant number of organisations, specifically 64 percent, rely on passwords as their primary method of authentication, according to the findings of the research (Billings, 2019). In addition, it was discovered that passwords are problematic, since ninety percent of organisations reported that they had discovered a substantial violation of their password policy within the past month (Billings, 2019).

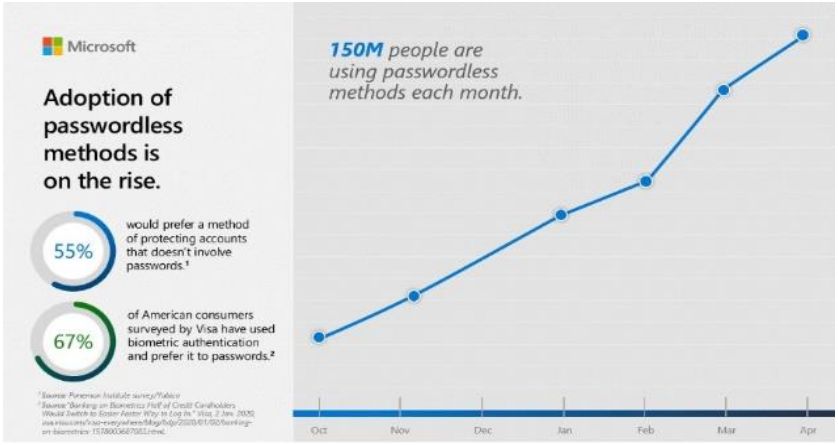

Figure 2: Adoption of passwordless methods is on the rise

Source: (Microsoft Stories Asia, 2020)

As an additional aspect, Microsoft Stories Asia (2020), stated that sixty percent of significant and multinational organisations as well as ninety percent of mid-size businesses will have deployed passwordless solutions in more than fifty percent of use cases. According to a survey that was carried out by Microsoft, it is anticipated that the utilisation of biometric work accounts will enhance by a factor of two throughout the course of this year. According to the poll, around one quarter of organisations are either utilising biometrics or are going to implement them in the near future (Parmar, et al., 2022). This information was also received.

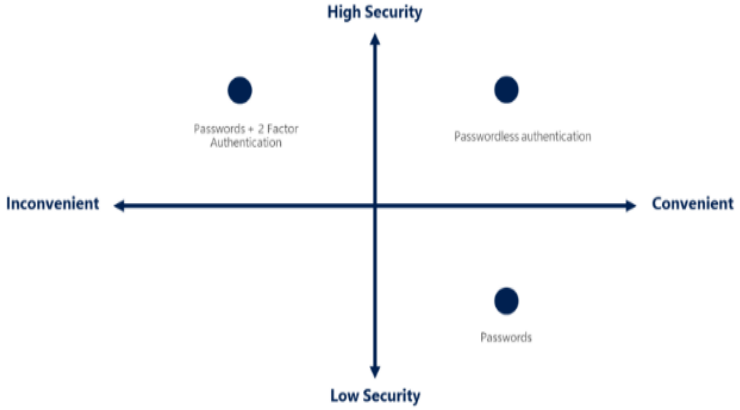

Figure 3: Convenience of passwordless authentication

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

Source: (Microsoft Stories Asia, 2020)

Because the password is removed and replaced with something people have, something people are, or something people know, verification techniques that do not require a password are more convenient and less time-consuming (Oesch and Ruoti, 2020). Among the potential solutions that individuals and organisations should take into consideration are as Direct access to the personal computer through the use of biometric or personal identification numbers (PIN), which prevents anybody other than the owner from accessing the device. To facilitate a seamless sign-in process, this solution enables the user to make use of his or her own unique IDs. Additionally, this solution can be integrated with single sign-on (SSO) systems (Parmar, et al., 2022). This method allows users to sign in to resources without having to use a login or password. A platform key or an external security key that is incorporated into a device is utilised in this technology. If an organisation is extremely concerned about security, or if it has situations or workers who are unwilling or unable to utilise their phone as a second factor, this is an excellent choice for them (Zhu, et al., 2014).

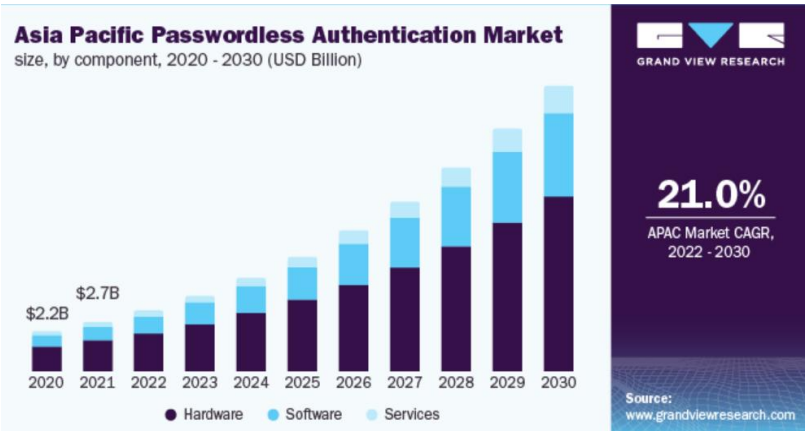

Figure 4: Asia Pacific Passwordless authentication market 2020-2030

Source: (Grand View Research, 2023)

The underlying security architecture is altered by passwordless technology since it transfers verification to the device itself rather than passing it across an internet connection (Grand View Research, 2023). Traditional multi-factor authentication (MFA) is superior in terms of both security and ease when it comes to the authentication procedure. This is despite the fact that passwordless solutions offer a higher level of sophistication (Zhu, et al., 2014). There are many instances in which firms attempt to manage supply chain security, which is essential for B2B financial infrastructure, while concurrently attempting to strike a balance between workforce access security and user experience (Microsoft Stories Asia, 2022).

Even in the modern business world, these safety precautions continue to be indispensable. Numerous companies are continuing to focus their efforts on finding solutions to the problems that small and medium-sized enterprises (SMEs) face in relation to digitization and financial infrastructure (Grand View Research, 2023). For instance, in June of 2022, SecureAuth Corporation, a provider of identity access management security solutions, announced Arculix, a following-generation passwordless authentication and identity orchestration platform. Arculix was designed to facilitate the management of identities. With the assistance of the new platform, businesses are able to create ID experiences that are both secure and frictionless on a global scale (Grand View Research, 2023).

According to Grand View Research, (2023), it is mentioned that Verizon's data breach investigations reports (DBIR) for the month of June 2022, approximately 81% of hacking-related breaches are caused by passwords that are either too weak or too similar to one another. The banking sector is moving towards passwordless authentication as an additional layer of protection for their customers' accounts. This is due to the fact that more than ninety percent of users reuse passwords between their personal and business accounts. Professional security specialists focus the majority of their attention on this aspect, however there are additional ways that information technology can reduce risk. Considering how easily passwords may be stolen, the banking industry is increasingly turning to passwordless authentication solutions. This is due to the fact that authentication is not very strong.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

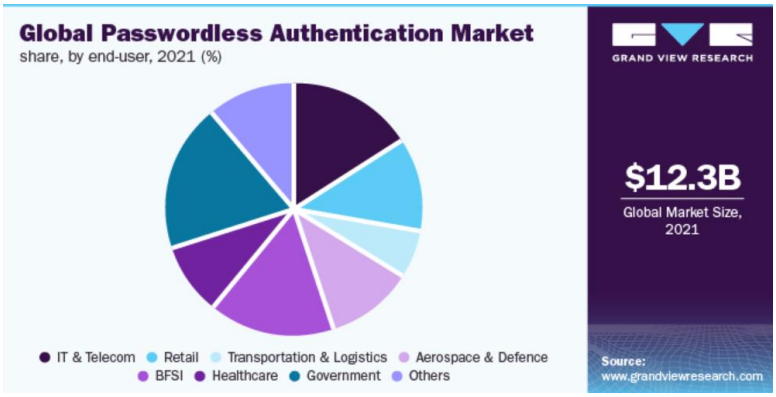

Figure 5: Global passwordless authentication market

Source: (Grand View Research, 2023)

During the course of the years that are being forecasted, it is anticipated that the BFSI industry will experience a significant amount of growth. The ability of financial institutions to push their passwordless authentication to greater heights can be achieved by granting customers access to additional data that was previously protected by a password. Consequently, this leads to increased production per worker in addition to increased accessibility for a larger audience (Grand View Research, 2023).

CONCLUSION

The adoption of password-less technology in Zero Trust system shows change in the modern-day security solutions. This research shows all the vices that are associated with the use of password such as phishing attacks, reuse of password as well as incompetence that are associated with use of password baseline systems. To strengthen an organization's security the best authentication approaches that should be employed include biometrics, hardware tokens and one-time passcode devices (OTPs). These methods afford high levels of security to simple interception and cyber-attacks, which is paradigm to the Zero-Trust model where validation is ceaseless and trust minimal.

Besides, the Zero-Trust model that supposes that risks are inside and outside the conventional perimeters dovetails passwordless security since it constantly checks users and their devices for authentication. The infosphere conceives of a protective model whose security policy is both identity and context-conscious, guaranteeing the ongoing safeguarding of pertinent resources. The application of Multi-Factor Authentication (MFA) within this framework is also beneficial in as much as it provides easy ways to ensure that various kinds of risks especially those that are associated with credential-based attacks are reduced by virtue of the fact that authentication requires several factors.

Thus, the study makes it clear that going for passwordless security increases users' satisfaction as well as security since the inconveniences that resulted from having to remember different password is removed. Also, the lower rates for password-related administrative expenses make the necessary transformations more understandable from the economic point of view. Improved methods of cryptographic techniques and increased use of biometric authentication are also helpful in passwordless security because they provide more effective and comfortable ways of user identification. However, passwordless security entails a comprehensive set of changes that needs to be made and therefore must be introduced carefully. This means embracing the cross-platform compatibility or investments in compatible infrastructures with the systems and devices of the organizations and also the promotion of the new methods of authentication to the users of the organizations. Also, the protection of biometric data and the handling of hardware tokens pose other issues that should be solved by strong security measures and efficient managing.

Recommendations

Thus, to implement transition to the use of passwordless security, organizations need to focus on training to ensure that all users are informed about the changes made to the authentication system and the new methods of protection. They have to assess and modernize older ones to be compatible and fully integrate with passwordless solutions. To ensure the privacy and security of biometric data, special measures such as encrypting the data and storing the biometrical data securely should be used. The management of these tokens should be well policed when it comes to distribution in addition to the recovery of the hardware tokens. Last but not the least, structuring the plan into phases enables a step-wise deployment process that allows for easy detection and rectification of issues before going mass, hence making it very efficient.

Future Directions

The combination of artificial intelligence or AI and machine learning can transform the authentication process because the programs learn the users' behaviour and notice discrepancies immediately. Fourth, blockchain solutions can improve the identities' protection and the decentralization of identification services, increasing the reliability of the authentication systems. Given the steady progress in the application of quantum computing, there is a need to build post-quantum cryptographic systems for use in post-quantum authenticity. Further study and development in these fields will be crucial for further effective protection readiness against new types of cyber threats techniques within a more digital-oriented world.

iJETRM
International Journal of Engineering Technology Research & Management
Published By:
https://www.ijetrm.com/

REFERENCES

1. Kak, S. (2022). *Zero Trust Evolution & Transforming Enterprise Security* (Doctoral dissertation, California State University San Marcos). https://scholarworks.calstate.edu/downloads/7s75dj998
2. George, A. S. (2024). The Dawn of Passkeys: Evaluating a Passwordless Future. *Partners Universal Innovative Research Publication*, *2*(1), 202-220. https://puirp.com/index.php/research/article/view/44
3. Muhammad, T., Munir, M. T., Munir, M. Z., & Zafar, M. W. (2022). Integrative Cybersecurity: Merging Zero Trust, Layered Defense, and Global Standards for a Resilient Digital Future. *International Journal of Computer Science and Technology*, *6*(4), 99-135.
4. Furuberg, I. L., & Øseth, M. (2023). *From Password to Passwordless: Exploring User Experience Obstacles to the Adoption of FIDO2 Authentication* (Master's thesis, NTNU). https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3093908
5. Kingo, T., & Aranha, D. F. (2023). User-centric security analysis of MitID: the Danish passwordless digital identity solution. *Computers & Security*, *132*, 103376. https://www.sciencedirect.com/science/article/pii/S0167404823002869
6. Chowhan, R. S., & Tanwar, R. (2019). Password-less authentication: methods for user verification and identification to login securely over remote sites. In *Machine Learning and Cognitive Science Applications in Cyber Security* (pp. 190-212). IGI global.
7. Casey, M., Manulis, M., Newton, C. J., Savage, R., & Treharne, H. (2020). An interoperable architecture for usable password-less authentication. In *Emerging Technologies for Authorization and Authentication: Third International Workshop, ETAA 2020, Guildford, UK, September 18, 2020, Proceedings 3* (pp. 16-32). Springer International Publishing.
8. Parmar, V., Sanghvi, H. A., Patel, R. H., & Pandya, A. S. (2022, April). A comprehensive study on passwordless authentication. In *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)* (pp. 1266-1275). IEEE. https://www.researchgate.net/profile/Harshal-Sanghvi/publication/360229809_A_Comprehensive_Study_on_Passwordless_Authentication/links/627300c43a23744a726495bb/A-Comprehensive-Study-on-Passwordless-Authentication.pdf
9. Zhu, B., Fan, X., & Gong, G. (2014, April). Loxin—A solution to password-less universal login. In *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 488-493). IEEE. https://about.bozhu.me/paper/loxin.pdf
10. Horsch, M., Hülsing, A., & Buchmann, J. (2015, August). PALPAS--PAssword Less PAssword Synchronization. In *2015 10th International Conference on Availability, Reliability and Security* (pp. 30-39). IEEE. https://arxiv.org/pdf/1506.04549
11. Oesch, S., & Ruoti, S. (2020, August). That was then, this is now: A security evaluation of password generation, storage, and autofill in browser-based password managers. In *Proceedings of the 29th USENIX Conference on Security Symposium* (pp. 2165-2182). https://www.usenix.org/system/files/sec20-oesch_0.pdf
12. Billings, L. (2019). The path to passwordless authentication is shorter than we thought. Security Intelligence. https://securityintelligence.com/posts/the-path-to-passwordless-authentication-is-shorter-than-we-thought/
13. Microsoft Stories Asia. (2020). Going passwordless for smarter and better protection. Microsoft. https://news.microsoft.com/apac/2020/06/02/going-passwordless-for-smarter-and-better-protection/
14. Grand View Research. (2023). Passwordless authentication market size, share & trends analysis report by component, by product type, and segment forecasts, 2022-2030. https://www.grandviewresearch.com/industry-analysis/passwordless-authentication-market-report