Research Essay

Name	Vignesh Maneesh Kumar
Student ID	202442363
AES Class	Pre-Masters For Sciences and Engineering
AES Tutor	Katrin Schmid
Essay Title	To what extent are passkeys viable solution for passwords among everyday users? Is a password-less future realistic?
Assignment deadline	23rd May 2025
Word Count	1457

It is very important that any work you present as yours must in fact be your own work and not taken from another place or done by another person. Cheating, collusion (working together with another person on an assessment which is not intended to be collaborative) and copying from unacknowledged sources (plagiarism) are all serious offences and must be avoided.

DEFINITION OF ACADEMIC IMPROPRIETY

Academic impropriety is a term that covers cheating, attempts to cheat, plagiarism, collusion and any other attempts to gain an unfair advantage in assessments. Assessments include all forms of written work, presentations and all forms of examination. Academic impropriety, in any form, is a serious offence and the penalties imposed would reflect this.

DECLARATION

By entering my Student ID below, I confirm that this piece of work is a result of my own work except where it forms an assessment based on group project work. In the case of a group project, the work has been prepared in collaboration with other members of the group. Material from the work of others not involved in the project has been acknowledged and quotations and paraphrases suitably indicated. Furthermore, I confirm that I understand the definition of Academic Impropriety that is used by Strathclyde University International Study Centre.

Student ID: 202442363	**Date: 23-04-2025**

To what extent are passkeys viable solution for passwords among everyday users? Is a password-less future realistic?

Security on the internet has never been more vital in today's day and age, especially with many essential services such as banking, email, government services and healthcare, being online. To be able to access these services, a combination of an account and password is usually required to authenticate the user. Passwords are currently the most common method of authentication in this digital age (Dasgupta, Roy and Nag, 2017). However, passwords are increasingly being compromised due to data breaches, phishing attacks, and brute-force attacks. According to George (2024), over 1.1 billion passwords have been compromised at companies like Uber and X (formerly known as Twitter) in 2024. Passkeys are an alternative method of authentication that is based on public-private key cryptography. It is usually tied to biometric verification on the user's device. Unlike passwords, they are not susceptible to phishing, password theft, or brute-force attacks (George, 2024). Tech companies like Apple, Google, and Microsoft have started implementing passkeys in their platforms and are endorsing them to users (Lassak *et al.*, 2024) due to the positive impacts on user experience. User experience when it comes to technology is a term commonly used to describe all the interactions a user has with a feature, product or service (Norman and Nielsen, 1998). This trend highlights its growing momentum towards a password less future. This essay assesses the viability of passkeys as a replacement for passwords for everyday users. It examines their effectiveness in terms of security, usability, and accessibility. The central argument of this essay is that passkeys have the potential to replace passwords, which will improve the overall user experience and security of authentication.

Understanding what passkeys are and how they work is important to evaluate if they are a viable replacement to passwords. As cyber breaches and attacks are becoming more advanced, passkeys provide a more secure authentication method than passwords. Using passkeys rule out common vulnerabilities such as phishing, brute-force attacks, and password reuse. It uses the technology of public-private key cryptography. When an account is created with passkey as the main method of authentication, a unique key pair is generated. The private key is securely stored on the user's device and is never transmitted to the server while the public key is stored server side (Matzen *et al.*, 2025). Furthermore, authentication between these keys occur via biometric verification such as fingerprint or Face-ID. This approach makes sure that if the server is compromised, user credentials remain safe. Wang *et al.*, (2017) support this as they report that more than 2000 breaches in 2016 resulted in billions of user records, such as account details and passwords, being leaked. This highlights the need for a more secure system. By eliminating the need for centralised storage of passwords, passkeys offer a more robust method of authentication for everyday users who are more vulnerable to these attacks.

Apart from increased security, passkeys bring greater improvements in user experience compared to plaintext passwords. Most users reuse passwords because it is more convenient than trying to remember different passwords across different platforms. This is known as password fatigue (Dasgupta, Roy and Nag, 2017). Wang *et al.* (2017) reports that 38% of users reuse the same passwords for different platforms and 20% of the users modify existing passwords to create new ones. Another downside to passwords is that they are highly vulnerable to phishing attacks, where attackers trick users into inputting their credentials on illegitimate websites. This is one of the most common methods for compromising account credentials (Muir, Brown and Girma, 2024). An example of an incident involving passwords would be the Advanced Computer Software Group in 2022 (Landi, 2025). Landi (2025) reports that in 2022, hackers were able to illegally gain access to some systems of the health and care division of Advanced Computer Software Group. They were able to do so as they hijacked a customer's account since it only had a single layer of security which was a password (Landi, 2025). The consequences that this incident caused was dire as it affected both Advanced Computer Software Group and the NHS. Some of these consequences were the significant disruptions of services to critical NHS infrastructure such as the NHS 111. Additionally, the hackers were also able to obtain personal information of 79,404 people (Landi, 2025). Usually, stolen credentials like these are usually placed on the internet by hackers in databases such as Collection #1-5 which contains 3 billion compromised log-in credentials (Grimes, 2021). Passkeys eliminate these limitations by linking its authentication process to the user's

device and enabling biometric or PIN-based login (George, 2024). This further removes the need for frequent password changes and account recovery due to forgotten credentials. Passkeys offer a simple and more straightforward user experience while maintaining high security, making them an attractive option for authentication.

While passkeys may be considered more secure and user-friendly, traditional passwords still offer advantages which show why they continue to be the primary method of authentication. On the one hand, passwords have an advantage in terms of portability, where they can be used on any device. On the other hand, passkeys need to be registered again on every new device the user uses. Tech companies like Apple and Google use the iCloud Keychain and Google Passwords respectively as a workaround for this. They share the passkeys to every device linked with the user's account which mostly avoids the above-mentioned limitation (George, 2024). However, not all devices belong to Apple or Google's ecosystem, thus this should not be considered as a viable fix. In interviews conducted by Lassak et al., 2024, some of the participants were concerned about how cloud synchronisation may be required and the lack of cross-platform support. Even though QR codes could be used to transfer these passkeys to different devices, users may find the process confusing. In conclusion, these drawbacks show that despite the increased security of passkeys, many users continue to use traditional passwords due to usability limitations.

Furthermore, adoption of passkeys and completely replacing passwords by everyday consumers may not be as quick and straightforward as accessibility limitations may need to be addressed. Passwords are supported on many IoT (Internet of Things) devices, but passkeys depend on hardware that supports biometric verification and secure credential storage (George, 2024). As a result, users with older smartphones, shared devices, or older operating systems may not be able to use passkeys. The findings of Matzen *et al.* (2025) align with this as they highlight that there are interoperability issues with legacy hardware and systems when it comes to passkey implementation. This may lead to a digital divide where only users with modern technology are able to benefit from the improved security. Therefore, this shows that a complete transition to passkeys will take time, and passwords will still be used despite their limitations.

Finally, beyond technical limitations, digital literacy of users plays a very crucial role when it comes to the adoption of new technologies like passkeys among everyday users. Kovalan *et al. (*2021) highlight that widespread adoption of passkeys depends on the consumer's digital literacy. Their level of literacy can vary according to age, income, and region. For example, older users may be less familiar and may face difficulties with biometric authentication and cloud synchronisation across different devices which may lead to hesitance in adopting passkeys. The findings of Lassak *et al.* (2024) align with this during their research, some participants regardless of the demographics were not aware of what passkeys were and others expressed that they were uncomfortable about cloud synchronisation due to privacy concerns. Meanwhile, tech giants like Apple, Google and Microsoft have already started implementing passkeys into their respective ecosystems (Lassak, 2024). Moreover, Microsoft announced that they would make passkeys the default method of signing in for new Microsoft accounts and recommend existing users to create passkeys for their accounts on supported devices (Microsoft, 2025). However, the rate of adoption of this technology is quite varied (Lassak, 2024) which shows that even those with compatible devices may hesitate to use technology that is unfamiliar to them, especially when it comes to authentication.

In conclusion, while passkeys may offer a more secure and user-friendly alternative, a passwordless future remains years away. Passkeys have the potential to replace passwords as the primary method of authentication. They could help in reducing security risks and may provide an enhanced user experience with the use of biometric authentication. However, factors like accessibility, hardware compatibility, digital literacy, and standardisation of various aspects such as account recovery and cloud synchronisation need to be addressed. Across all the research, passwords are likely to be the primary method of authentication despite their known limitations for the foreseeable future.

References

Dasgupta, D., Roy, A. and Nag, A. (2017) 'Advances in User Authentication'. Available at: http://dx.doi.org/10.1007/978-3-319-58808-7.

George, A.S. (2024) 'The Dawn of Passkeys: Evaluating a Passwordless Future', 02 pp. 202-220. Available at: http://dx.doi.org/10.5281/zenodo.10697886.

Grimes, R.A. (2021) 'Hacking Multifactor Authentication'. Available at: http://dx.doi.org/10.1002/9781119672357.

Kovalan, K., Omar, S.,Tang, L., Bolong, J., Rusli, A., Akmar H., Ghazali P., and Muhammad A. (2021) 'A Systematic Literature Review of the Types of Authentication Safety Practices among Internet Users', International Journal of Advanced Computer Science and Applications, 12 (7). Available at: http://dx.doi.org/https://doi.org/10.14569/IJACSA.2021.0120792.

Lassak, L., Pan, E., Ur, B., and Golla, M. (2024) 'Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication' Available at: https://www.usenix.org/conference/usenixsecurity24/presentation/lassak. Accessed: 7th March 2025)

Landi, M. (2025) Software provider fined £3m over ransomware attack that hit NHS services. Available at: https://www.independent.co.uk/news/business/software-provider-fined-ps3m-over-ransomware-attack-that-hit-nhs-services-b2722293.html (Accessed: 23 May 2025)

Matzen, A., Rüffer, A., Byllemos, M., Heine, O., Papaioannou, M., Choudhary, G., and Dragoni, N., (2025) 'Challenges and Potential Improvements for Passkey Adoption—A Literature Review with a User-Centric Perspective', Applied Sciences, 15 (8). Available at: http://dx.doi.org/10.3390/app15084414.

Microsoft (2025) 'Pushing passkeys forward: Microsoft's latest updates for simpler, safer sign-ins', Microsoft Security Blog, 1 May. Available at: https://www.microsoft.com/en-us/security/blog/2025/05/01/pushing-passkeys-forward-microsofts-latest-updates-for-simpler-safer-sign-ins/ (Accessed: 23 May 2025).

Muir, A., Brown, K. and Girma, A. (2024) 'Reviewing the Effectiveness of Multi-factor Authentication (MFA) Methods in Preventing Phishing Attacks', 1157. Available at: http://dx.doi.org/10.1007/978-3-031-73128-0_40.

Norman, D. and Nielsen, J. (1998) The Definition of User Experience (UX). Available at: https://www.nngroup.com/articles/definition-user-experience/ (Accessed: 7th March 2025).

Wang, C. et al. (2017) 'Empirical Analysis of Password Reuse and Modification across Online Service', arXiv.org. Available at: https://doi.org/10.48550/arXiv.1706.01939.