JOURNAL OF SCIENCE EDUCATION (JOSE) VOL. 18, NO. 1. 2024 (ISSN: 1118 - 1364)
Indexed in Google Scholar, School of Secondary Education (Science), Federal College of Education, Abeokuta, Nigeria.

A CRITIQUE OF USER AUTHENTICATION METHODS

[1]AGHOLOR S., [2]TIJANI R. A., [3]AGHOLOR A. O., [4]MAR'RUF-SOGEYINBO A. A., and [5]ADIGUN I.O.
Federal College of Education, Abeokuta
[1,2,4,5]Department of Computer Science,
[3]Registry Department

Abstract
There is a growing demand for user authentication technologies for both online and in physical systems. The major reason for authentication is to restrict access to account owner's information. Organizations have been facing difficulties in selecting the best authentication method that fits the security of their systems from the wide varieties of existing authentication methods. In this study, we explored the different methods of authentication using systematic literature review. The result of the review showed that authentication methods can be broadly classified into three. Furthermore, the result from the review showed the advantages and disadvantages of each of the three types of authentication methods. The requirements for implementing each were identified. Our aim is to give a guide to organizations in choosing the best option to use when implementing her authentication system.

Introduction
In any human society, identification of individuals has been a basic requirement for security purposes (Agholor, 2017). In small tribes and villages, it is an established fact that everyone knows and recognizes everyone else, hence, it is easier to detect a stranger or identify a potential breach of security. In today's larger and more complex society, it is not that simple. Similarly, as more and more interactions take place through the internet, it becomes very difficult to identify each person, hence the need to develop a method of identifying these online users. This method of identifying online users is often referred to as authentication.

Authentication, therefore, could be defined as one entity proving its identity to another (Forget, 2012). In a rhetoric question, Forget (2012) asked "but how can one entity always know that what another entity is claiming to be is true"? The answer to this question has remained unresolved for millennia years because of forgery/impersonation. For example, in the past centuries and till date, signatures have been used as an authentication system to prove our identity, despite numerous evidence that signatures can be forged (Forget, 2012).

This challenge of forgery/impersonation also exists in modern digital authentication systems as cybercriminals device various methods/techniques to break into a digital authentication systems. However, advances in technology have been made to reduce the incidences of forgeries/impersonation. This has led to the development of different authentication techniques/methods with each one claiming superiority over the other. In this study, we used a systematic literature review where twenty-eight articles were thoroughly reviewed, evaluated and analysed, bringing out the advantages and the disadvantages of the different types of authentication methods and leaving organizations with the liberty to choose the authentication system that best suits their security demands.

Statement of the Problem

The numerous authentication methods have put organizations in difficult situation in selecting the authentication method to be used as a result of one authentication method claiming superiority over the other. It is against this background that this paper did an independent analysis on the various authentication methods bringing out their merits and demerits so as to guide organizations in selecting the appropriate one that best suits her authentication needs.

Objectives of the Study

The objectives of this study are:

1. To give an independent assessment of the various authentication methods.
2. To provide a balanced independent assessment that will guide organizations in choosing the best option to use when implementing her authentication system.

Literature Review

Techniques for Authentication

The need to protect confidential information in the online space has become more essential nowadays, hence organizations and individuals are becoming more aware of the threats and the need for protecting their digital information. The bedrock on which the principles and techniques of authentication are built is the ability to distinguish between authorized and unauthorized users (Brostoff, 2004). The process by which this occurs is called user authentication. The user first declares his or her identity as a bona fide user. The system verifies the declared identity and if correct, grants access. Authentication is the most crucial elements when using the world wide web (Yıldırım and Mackie, 2019). According to Woods and Siponen (2019), there are several ways for users to authenticate themselves in the cyberspace.

The most used authentication form today are passwords, even though a few other authentication methods are being presented in the cyberworld (Agholor, 2021). Several studies indicate that even if the password is still being known as the most used authentication method, it is being used with risks, where users tend to store, log, and share their passwords in unsecured situations (Merdenyan and Petrie, 2022; Yıldırım and Mackie, 2019; Luna, 2018). The risks with passwords have been discussed in several fields ranging from information technology to behavioural science, where researchers have been questioning if the bad practice with passwords is being related to metacognitive beliefs (Agholor, 2017; Luna, 2022). Papathanasaki, Maglaras and Ayres (2022) did a comprehensive investigation of modern authentication schemes and found that password is still the most widely accepted authentication scheme. Depending on the length of the passwords, users tend to have difficulties remembering longer passwords (Bošnjak and Brumen, 2019). In an attempt to strengthen the security of passwords, systems administrators introduced stricter password management methods which have led to higher security (Agholor, 2017). However, it has been found by Merdenyan and Petrie (2022) that users tend to compromise security for usability. Despite the drawbacks of password as an authentication scheme, it is likely to remain the dominant authentication scheme (Aborisade *et al.*, 2013; McCarney *et al.*, 2012; Sodiya and Agholor, 2012; Shiva and Aggarwal, 2012; Preet and Gour, 2012; Florencio and Herley, 2010; Dell'Amico *et al.*, 2010; Zhang *et al.*, 2009; Wiedenbeck *et al.*, 2005).

However, there are other existing authentication methods such as biometrics, which can be divided into physical and behavioral biometrics. The physical is concerned with traits from the person's identity, such as fingerprint or face recognition, while behavioral biometrics is concerned with the person's behavior such as how they walk. Biometrics are also prone to

vulnerabilities, such as finding a picture of someone's face to identify them with face recognition or forging the victims' fingerprint. Behavioral biometrics are more demanding for an attacker but would be difficult to implement in systems and with devices that are being used (Syed and Salil, 2019).

Another authentication method that could be used is smart card authentication, which is identified as something that the user has. The smart card is a card similar to a credit card, which involves a memory card with a chip for identification. In addition, the user also needs to provide a pin number to authenticate themselves. These smart cards are in general encrypted (Farik et. al, 2016). In addition, security tokens can be used to authenticate users. It is a hardware device that generates a dynamic One-Time password (OTP). Similar to the previous authentication methods, these are subject to drawbacks. Examples of such drawbacks are that a user needs to carry the device and it could be burdensome and an expensive solution for the provider (Syed and Salil, 2019). These alternatives to passwords are slightly more consuming and costly to deploy than passwords, which is the main reason why there are no such alternatives for many systems.

Another form of authentication is the Multi-Factor Authentication method. Multi-Factor Authentication (MFA) is a combination of different authentication factors, and it is a concept that is becoming more known in society. Multi-Factor Authentication is also known as two-factor authentication (Syed and Salil, 2019). The research finding of Papathanasaki, Maglaras and Ayres (2022) showed that MFA is one of the most secure ways of authentication.

Methodology

We used a systematic literature review by exploring studies related to the research topic. Twenty-eight articles were reviewed, evaluated, and analysed after the eligibility process. The search was thoroughly done according to the objective of this study, which is to examine the current types of authentication methods. These studies were classified into relevant themes by using qualitative synthesis. This was done by reading the title, abstract, and keywords of each study. Furthermore, a thematic analysis was performed to classify themes related to type of authentication method. Through an article review process, relevant groups were identified. Finally, we relied on Farik, et.al. (2016) and Syed and Salil (2019) to classify the different authentication methods found in literature into three; ‘something you know’, ‘something you have’, and ‘something you are’. The first one, “Something you know” can be identified as passwords or Personal Identification Numbers (PIN). “Something you have” is known as smart cards and tokens and “something you are” is biometrics methods such as fingerprints. The results of the systematic literature review on the three selected authentication methods are further summarized in the next section.

Results

The three selected authentication methods are discussed below.

The Password Authentication

A password is a character or sequence of characters used to determine that a device user requesting access to a system is really that particular user (Agholor, 2012).

Advantages of Password Authentication

The advantages of password authentication method as stated by Forget (2012), Gayathiri (2013) and Agholor (2017) are:

1) They are easy to learn how to use them.
2) They do not require any special hardware for implementation (cost effectiveness).
3) They can easily be changed if compromised or forgotten.

4) They provide adequate security to end-user's data, although there are some concerns about weak passwords which can lead to weak security.
5) Its simplicity and familiarity to all users makes it a good candidate to the end-user (Gayathiri, 2013).

Disadvantages of Password Authentication

The disadvantages of password authentication method according to Agholor (2017), Bošnjak and Brumen (2019, Merdenyan and Petrie (2022) and Andrew (2024) are:

1) Memorability Issue

This is the greatest problem with the use of password. The more we try to make it easy to remember, the less secure is the password. Thus, to aid recall memory, users usually write them down or use the same password on multiple sites which make them less secure.

2) Security Issue

This is another big problem associated with the use of password. The more we try to make it strong, the more difficult it is to remember. In an attempt to make passwords more secure, users are asked to make them more complex by using numbers, uppercase letters, lowercase letters, and special characters. This makes them hard to remember and as a result user resort to self-help by writing it down somewhere, sharing it with friends, or even use the same password on multiple accounts.

3) Balancing security and usability

This is very difficult to achieve because experienced has shown that a memorable password is insecure, but a secure password is hard to remember. However, this problem is gradually being addressed by the use of password manager.

4) Password Attacks/Hacking/Cracking

While passwords are at risk from brute force attacks and social engineering, simple guessing is also an effective tool to crack a password and gain access to the owners's account.

Biometric Authentication

Biometric authentication is a *security process that relies on the unique biological characteristics of individuals to* verify they are who they say they are.

Advantages of Biometric Authentication

According to M2sys (2024), the advantages of biometric authentication are:

1) Quicker Authentication

It makes authentication process quick and easy.

2) Memorability Issue

The need to memorize passwords is eliminated.

3) Security Issue

Since it is very difficult to forge fingerprints, the system is good for protecting sensitive data. However, there are some concerns that a like image of the account's owner can be used to login. Hence, security issue is also discussed under disadvantage in order to give it a balance analysis.

4) Maximizes Convenience

It is a convenient method of tracking each employee in an organization through the process of sign-in and sign-out. This helps Human Resource Officers in data organization and analysis.

Disadvantages of Biometric Authentication

According to Syed and Salil (2019 and M2sys (2024), the disadvantages of biometric authentication are:

1) Security Issue

Face recognition is less secure because there is possibility that someone who looks like you or who uses an image of your face could unlock your account.

2) Physical Disabilities/Fake Negatives

It only recognizes traits that were entered during enrolment without putting into consideration of changes in physical traits of the enrollee. For instance, a burnt or damaged finger, a retina transplant, tattooed hands, etc may give room for slight changes which the authentication system will not recognize.

3) Expensive to implement

While the system is reliable and handy, the cost for its implementation is high because it requires special hardware, unlike passwords. However, the issue of special hardware is gradually being addressed. For example, smartphones users do not require special hardware to capture their biometrics for the purpose of using it for authentication mechanism.

4) Difficulty in changing physical traits during Security Breaches

If there is a breach of data, the account's owner cannot change his/her physical identification traits thereby allowing the impostor to continue to access the account.

5) Fake Positives

The case of fake positives arose when a stolen data was manipulated to look like the biometric of the original account owner and used to gain access to the account, (Agholor, 2017).

Multi Factor Authentication (MFA)

It is a good security measure that is used to protect user accounts from hackers and other cybercriminals. It uses a combination of two or more authentication factors for logging-in, which offers extra layer of protection to account's owner confidential information.

Advantages of Multi-Factor Authentication

According to Papathanasaki, Maglaras and Ayres (2022) and Nicole (2023), the advantages of biometric authentication are:

1) Increased Security

With MFA, even if someone knows your login credentials, they cannot access your account without also having access to the second factor, such as a physical token or code sent to your email or mobile phone.

2) Less Risk of Compromised Passwords

Using a second form of authentication makes it much more difficult for hackers to obtain your login credentials and gain access to your account.

3) Easy to Use

MFA is simple to set up and use, and does not require any special hardware or software. All that is needed is the user's phone, and the system can be configured in minutes. MFA is becoming increasingly commonplace, and is being adopted by organizations of all sizes and in all industries.

4) Reduce Phishing Risk

Multi-factor authentication provides additional protection against phishing scams that attempt to extract sensitive data from users. Even if hackers steal your password, multi-factor authentication reduces the risk that they can access your account.

Disadvantages of Multi-Factor Authentication

According to Nicole (2023), the disadvantages of biometric authentication are:

1) Fragmented User Experience.

Multi-factor authentication can be a hassle for users who must remember and type in extra codes and answer security questions each time they want to log in. As the number of authentication steps increase, so does the degree of complexity, making it more difficult for users to move from one step to the next. As a result, user experience is often fragmented.

2) Cost.

Another drawback of multi-factor authentication is the cost associated with implementing it. Unless you use something like a free two-factor authentication app, you may need to buy out-of-band hardware like USB tokens, smart cards, or mobile devices in order to provide authentication with an extra layer of security.

Conclusion

This study will contribute to educating users and systems administrators on the strengths and weaknesses of the different authentication methods. This become necessary as the study of Trnka et al. (2022) showed that common practices and models are used for authentication and authorization.

Recommendation

We recommend this paper to software developers who are interested in implementing one authentication method or the other for their clients.

References

Aborisade, D. O., Alowosile, O. Y., Odunlami, K. O. and Odumosu, A. (2013). A Cloud Based Password Manager for Multiple Transaction Accounts. In: Uwadia, C. O., Aderounmu, A., Sodiya, A. (eds) Proceedings of the 11th International Conference on e-Governmant and National Security. NCS, Iloko, Nigeria, pp4-11.

Agholor, S. (2021). Design and Evaluation of a Password Quality Assessment Model. *International Journal of Basic Science and Technology*. Vol. 7, no. 2, pp. 95-103.

Agholor, S. (2017). An Improved Approach for Managing Multiple Passwords. An unpublished Ph.D. thesis submitted to the Department of Computer Science, Federal University of Agriculture, Abeokuta, Nigeria. 291pp.

Andrew, B (2024). The End of the Password, retrieved on 13/3/2024 from www.iproov.com/reports/the-end-of-the-password

Bosnjak, L., and Brumen, B. (2019). Rejecting the death of Passwords: Advice for Future. *Computer Science and Information Systems.* Vol. 16, no. 1, pp. 313-332.

Brostoff, A. 2004. Improving Password System Effectiveness. Unpublished Ph.D. Thesis submitted to Department of Computer Science, University College London. 313pp.

Dell'Amico, M., Michiardi, P. and Roudier, Y. (2010). Password Strength: An Empirical Analysis. In: Chuah, M. C., Cohen, R., Xue, G. (eds) Proceedings of INFOCOM, San Diego, CA, pp. 983–991.

Farik, M., Lal, A. N., and Prasad, S. (2016). A Review of Authentication Methods. *International Journal of Scientific & Technology Research.* Vol. 5, no. 11, pp. 246-249.

Florencio, D. and Herley, C. (2010). Where Do Security Policies Come From? In: Cranor, L. F. (ed) Proceedings of 6th Symposium on Usable Privacy & Security, (SOUPS). ACM, Redmon, WA, USA, pp. 102-114.

Forget, A. 2012. A World with Many Authentication Schemes. An Unpublished Ph.D. thesis submitted to the Faculty of Graduate and Postdoctoral Affairs, School of Computer Science, Carleton University, Ottawa, Ontario, Canada. 244pp.

Gayathiri, C (2013). Text Password Survey: Transition from First Generation to Second Generation, retrieved on 13/3/2024 from www.b;ogs.ubc.ca/../

Linak, K. (2018). If it is easy to remember, then it is not secure: Metacognitive beliefs affect password selection. *Applied Cognitive Psychology.* Vol. 33, no. 5, pp. 544-558.

M2ysys (2020). Top 8 Advantages and Disadvantages of Biometric Authentication, retrieved on 13/3/2024 from www.m2sys.com

McCarney, D., Barrera, D., Clark, J., Chiasson, S. and Van'Oorschot. (2012). TAPAS: Design, Implementation and Usability Evatuation of a Password Manager. In: Schuba, C. (eds) Proceedings of the 28th Annual Computer security Applications Conference, Orlando, Florida, USA, pp. 89-98.

Merdenya, B., and Petrie, H. (2022). Two studies of the Perception of Risks, Benefits and Likelihood of Undertaking Password Management Behaviours. *Behaviour & Technology.* Available at: https://doi.org/10.1080/0144929X [24-01-2024].

Nicole, V (2023). Multi Factor Authentication Advantages and Disadvantages retrieved on 13/3/2024 from www.logmeonce.com/multi-factor-authentication-advantages-and-aisadvantages

Papathanaski, M., Maglaras, L. and Ayres, N. (2022). Modern Authentication Methods: A Comprehensive Survey. *AI, Computer Science and Robotics Technology*. PP. 1-24.

Preet, I. S. and Gour, S. M. T. (2012). Enhanced Password Based Security System Based on User Behaviour using Neural Networks. *International Journal of Information Engineering and Electronic Business.* Vol. 2, pp. 29-35.

Sodiya, A. S. and Agholor, S. (2012). Users' Password Selection and Management Methods: Implications for Nigeria's Cashless Society. In: Uwadia, C. O., Aderounmu, A., Sodiya, A. (eds) Proceedings of the 24th National Conference on Towards a Cashless Nigeria: Tools and Strategies. NCS, Uyo, Nigeria. Vol. 23, pp. 39-47.

Shiva, H. Y. and Aggarwal, S. (2012). Building Better Passwords using Probabilistic Techniques. In: Schuba, C. (ed) Proceedings of the 28th Annual Computer security Applications Conference, Orlando, Florida, USA, pp. 109-118.

Syed, W. S., and Salil, S. K. (2019). Recent Trends in User Authentication-A Survey. IEEE Access. Available at: 10.1109/ACCESS.2019.2932400 [25-02-2023]

Trnk, M., Abdelfattah, A. S., Shrestha, A., Coffey, M. and Cerny, T. (2022). Systematic Review of Authentication and Authorization Advancements for the Internet of Things. *Sensors*. Vol. 22, pp. 1-24.

Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A. and Memon, N. (2005). Passpoints: Design and Longitudinal Evaluation of Graphical Password System. *International Journal of Human-Computer Studies.* Vol. 63, pp. 42-49.

Woods, N., and Siponen, M. (2019). Improving Password Memorability, while not inconveniencing the user. *International Journal of Human-Computer Studies.* Vol. 128, pp. 61-71.

Yildrim, M., and Mackie, I., (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security.* Vol. 18, pp. 741-759.

Zhang, J., Luo, X., Akkaladevi, S. and. Ziegelmayer, J. (2009). Improving Multiple-Password Recall: An Empirical Study. *European Journal of Information Systems.* Vol. 8, pp. 165-176.