RESEARCH ARTICLE OPEN ACCESS

Evaluating the Effectiveness of Multi-Factor Authentication (MFA) Mechanisms in Mitigating Security Risks in Cloud Services

RACHANA C R
Associate Professor and Head
DoS in Computer Science, PG Wing of SBRR Mahajana First Grade College, KRS Road, Metagalli, Mysuru-570016.

ABSTRACT

Multi-factor authentication (MFA) enhances the security of cloud resources by requiring multiple forms of verification, thus mitigating risks associated with single-factor authentication vulnerabilities. As organizations increasingly adopt cloud computing for its scalability and efficiency, the accompanying security vulnerabilities have prompted the need for robust authentication solutions. MFA enhances security by requiring multiple verification methods—such as knowledge-based factors (passwords), possession-based factors (smartphones or tokens), and inherent factors (biometrics)—before granting access to sensitive data and applications. SMS-based Multi Factor Authentication is about sending a one-time code via text message, which, despite its widespread use, is susceptible to interception. App-based Multi Factor Authentication generates Time-based One-Time Passwords (TOTPs), offers a higher level of security as it is less vulnerable to interception compared to Short Messaging Service. This relies on users having access to their mobile devices, as well as the app. Hardware token-based Multi Factor Authentication employs physical devices such as USB tokens or smart cards, provides robust protection by generating one-time codes or by using cryptographic methods that are difficult to replicate or intercept. This paper compares the effectiveness of various MFA techniques—specifically SMS-based, app-based, and hardware token-based methods—in protecting cloud resources.

Keywords: App-based, Authentication, Cloud Security, Multifactor, OTPs, SMS.

I. INTRODUCTION

In the rapidly evolving digital landscape of India, securing online resources and personal information has become increasingly critical. In the traditional methods, a system that requires authentication challenges the user for a secret, typically a pair of username and password. The entry of the correct pair grants access to the system's services or resources. [6]

More precisely, According to the fundamental work in [9], authentication is a process where a "user identifies himself by sending x to the system; the system authenticates his identity by computing F(x) and checking that it equals the stored value y". Whether the user is Online or offline, Authentication remains a fundamental safeguard against illegitimate access to the device or any other sensitive application. [10-12]

As organizations store and process large volumes of data in the cloud, ensuring data security and privacy becomes crucial[1]. Cloud-based big data environments need robust security measures, including authentication, access controls, encryption, and data governance practices, to protect sensitive information and comply with relevant regulations.

Cloud-based authentication is the need of the hour and it can reduce overhead and improve cost efficiency by distributing systems across large, interconnected networks made up of various devices [3]. Cloud-based security features enable enhanced countermeasures to be deployed across complex environments.

Authentication involves multiple cryptographic approaches in developing MFA techniques, which can be integrated into healthcare-related IoT devices, enabling medical professionals and patients to protect critical medical information. [4]

Authentication factors are used to verify the identity of a user trying to access a system. The fundamental types of authentication factors are:

Something You Know: The information that only the user should have knowledge of such as Passwords, PINs, or answers to security questions.

Something You Have: They are the physical objects in one's possession, such as a security token, smart card, or mobile device with an authentication app.

Something You Are and Do: This is based on the unique physical characteristics of the user, the biometric factors such as fingerprints, facial recognition, or iris scans. Also, the user's behavior as a way to authenticate is looked at. That includes the behavioural biometrics, like typing patterns or the way the mouse is used by the user.

Somewhere You Are: This factor involves the physical or network location from which the user is trying to access the system, often verified through IP addresses or GPS data.

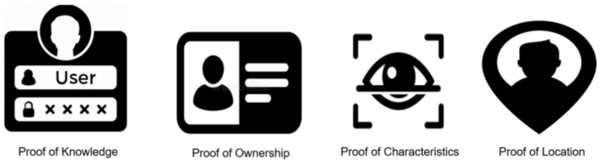

Fig. 1: Fundamental Authentication Factors.

With the rise of cloud computing and digital services, the need for robust authentication mechanisms to protect sensitive data is more pressing than ever. Multi-Factor Authentication (MFA) has emerged as a crucial tool in this context, adding layers of security beyond traditional username and password combinations.

II. MULTI- FACTOR AUTHENTICATION

Multi Factor Authentication includes various authentication principles associated with the login process of a system through devices by gathering enough evidence to verify a user is who they claim to be. Multifactor authentication methods, properly designed and implemented, are more reliable and stronger fraud deterrents [7]. Passwords are used in combination with two-factor authentication (2FA) or MFA, that is, two or more factors of authentication are used to enhance the security of the credentials being used. A few examples of 2 Factor Authentication are passwords, PIN codes, biometric traits, and memory cards, each belonging to their own respective categories based on the 'type' of factor[5].

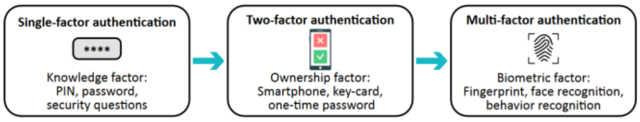

Fig. 2: Evolution of authentication methods from SFA to MFA.

Initially, only one factor was employed to authenticate the user. Single-Factor Authentication (SFA) was mostly adopted by the user community due to its simplicity and user friendliness [13, 14]. Further, it was realized that authentication with just a single factor is not reliable to provide adequate protection due to a number of security threats [15]. As an intuitive step forward, Two-Factor Authentication (2FA) [16–18] was proposed that couples the representative data (username/password combination) with the factor of personal ownership, such as a smartcard or a phone [19, 20].

In India, the adoption of MFA is growing as businesses and individuals become more aware of the risks associated with cyber threats and data breaches. Despite its benefits, the effectiveness of various MFA techniques—such as SMS-based, app-based, and hardware token-based methods—varies significantly, and each comes with its own set of advantages and challenges. [21]

III. COMPARISONS OF THE TECHNIQUES:

Comparing the effectiveness of different Multi-Factor Authentication (MFA) techniques—SMS-based, app-based, and hardware tokens—in protecting cloud resources involves assessing several factors such as security, usability, cost, and resistance to specific types of attacks.

How they work is illustrated as in [22, 23]

SMS-Based MFA: This method sends a one-time code through an SMS to the user's registered mobile number. The user enters this code into the login form. The authentication server verifies the OTP. If it matches the code sent via SMS, the user is granted access.

Mobile App MFA: The user installs an authenticator app on their smartphone. During the initial step, the app is linked to the user's account usually by scanning a QR code provided by the service. These apps generate time-based one-time passwords (TOTP) or push notifications for user verification. TOTP codes are generated every 30 seconds and are based on a shared secret key and the current time. The user opens the authenticator app, retrieves the current OTP, and enters it into the login form. The authentication server verifies the OTP against the expected value, if it matches, access is granted.

Hardware Tokens: The user is provided with a physical hardware token, which may generate OTPs or require physical interaction. Although these devices are used to represent an increased level of security for the user's accounts, they are generally not useful without the account credentials with which they are associated, the user must remember the credentials to safeguard them [24]

IV. CONCLUSION

If providing highest Security to data is the priority then, Hardware Tokens are the most secure but it is least convenient [2] . Biometrics can be convenient but there are potential vulnerabilities. SMS-based MFA is widely used due to its simplicity. However, it is vulnerable to attacks such as SIM swapping and phishing, which can compromise user security. App-based MFA, leveraging mobile applications to generate Time-based One-Time Passwords (TOTPs), offers a more secure alternative but requires users to have access to both their devices and the authentication app. On the other hand, hardware token-based MFA, though highly secure, involves higher costs and logistical challenges, making it less accessible for some segments of the Indian population. Using a combination of these factors enhances security by providing multiple layers of verification, which makes unauthorized access more difficult. Organizations should evaluate their specific security risks and needs before selecting a Multi Factor Authentication method. Any form of MFA is more secure than single-factor authentication, and would represent an important step forward in a cloud-based organization's security journey.

REFERENCES

[1] Saroj Mali, Assessing the Effectiveness of Multi-Factor Authentication in Cloud-Based Big Data Environments, Science Publishing Group, 6 August 2024.

[2] Srihari Subudhi, Comparative Analysis of Multi-Factor Authentication Mechanisms In Enhancing Cloud Security, International Research Journal of Modernization in Engineering Technology and Science, July 2024.

[3] Al Nafea R, Almaiah MA. Cyber security threats in cloud: literature review. In: 2021 international conference on information technology (ICIT), Amman, Jordan, 14–15 July 2021, pp.779–786. IEEE.

[4] Malakreddy B. ECC Based multifactor authentication and key generation system for IoT healthcare. Turk J Comput Math Educ 2021; 12: 5026–5032.

[5] Sharma NA, Farik M. Security gaps in authentication factor credentials. Int J Sci Technol Res 2016; 5: 116–120.

[6] Abhishek, K., Roshan, S., Kumar, P., Ranjan, R. (2013). A Comprehensive Study on Multifactor Authentication Schemes. In: Meghanathan, N., Nagamalai, D., Chaki, N. (eds) Advances in Computing and Information Technology. Advances in Intelligent Systems and Computing, vol 177. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-31552-7_57

[7] Authentication in an Internet Banking Environment, Federal Financial Institutions Examination Council, http://www.ffiec.gov/pdf/authentication_guidance.pdf

[8] Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy, Y. Multi-Factor Authentication: A Survey. Cryptography 2018.

[9] Lamport, L. Password authentication with insecure communication. Commun. ACM 1981, 24, 770–772.

[10] Boyd, C.; Mathuria, A. Protocols for Authentication and Key Establishment; Springer: Berlin, Germany, 2013.

[11] Mohsin, J.; Han, L.; Hammoudeh, M.; Hegarty, R. Two Factor vs. Multi-factor, an Authentication Battle in Mobile Cloud Computing Environments. In Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, UK, 19–20 July 2017; ACM: New York, NY, USA, 2017; p. 39.

[12] Pathan, A.S.K. Security of Self-Organizing Networks: MANET, WSN, WMN, VANET; CRC Press: Boca Raton, FL, USA, 2016.

[13] Konoth, R.K.; van der Veen, V.; Bos, H. How anywhere computing just killed your phone-based two-factor authentication. In Proceedings of the International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, 22–26 February 2016; Springer: Berlin, Germany, 2016; pp. 405–421.

[14] Kim, J.J.; Hong, S.P. A method of risk assessment for multi-factor authentication. J. Inf. Process. Syst. 2011, 7, 187–198.

[15] Gunson, N.; Marshall, D.; Morton, H.; Jack, M. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. Comput. Secur. 2011, 30, 208–220.

[16] Schneier, B. Two-factor authentication: Too little, too late. Commun. ACM 2005, 48, 136.

[17] Petsas, T.; Tsirantonakis, G.; Athanasopoulos, E.; Ioannidis, S. Two-factor authentication: Is the world ready?: Quantifying 2FA adoption. In Proceedings of the 8th European Workshop on System Security, Bordeaux, France, 21 April 2015; ACM: New York, NY, USA, 2015; p. 4.

[18] Wang, D.; He, D.; Wang, P.; Chu, C.H. Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. IEEE Trans. Dependable Secur. Comput. 2015, 12, 428–442.

[19] Sun, J.; Zhang, R.; Zhang, J.; Zhang, Y. Touchin: Sightless two-factor authentication on multi-touch mobile devices. In Proceedings of the Conference on Communications and Network Security (CNS), San Francisco, CA, USA, 29–31 October 2014; pp. 436–444.

[20] Bruun, A.; Jensen, K.; Kristensen, D. Usability of Single- and Multi-factor Authentication Methods on Tabletops: A Comparative Study. In Proceedings of the International Conference on Human-Centred Software Engineering, Paderborn, Germany, 16–18 September 2014; Springer: Berlin, Germany, 2014; pp. 299–306.

[21] https://blog.scalefusion.com/what-is-multi-factor-authentication-mfa/

[22] https://instasafe.com/glossary/what-is-cloud-mfa/

[23] https://www.onelogin.com/learn/mfa-checklist

[24] Jason Andress, in The Basics of Information Security (Second Edition), *2014*

[25] https://www.cloudflare.com/learning/access-management/what-is-multi-factor-authentication/

V. STRUCTURED COMPARISON:

TABLE 4.1

METHOD	SMS-Based MFA	App-Based MFA	Hardware Tokens
PROS	**Ease of Use**: Simple to implement and use; users receive a code via SMS which they enter to authenticate. **Accessibility:** Requires only a mobile phone capable of receiving text messages.	**Enhanced Security:** Uses time-based one-time passwords (TOTP) or HMAC-based one-time passwords (HOTP), which are more secure than SMS. Codes are generated on the user's device and	**Strong Security**: Provides high security by generating codes or using cryptographic methods that are difficult to spoof. Hardware tokens can use various mechanisms, including

		are not transmitted over the network. **Offline Capability**: Does not require an internet connection to generate the authentication code once the app is set up.	one-time passwords (OTPs) and public key cryptography. **Resistance to Phishing**: Hardware tokens often require physical interaction, making them resistant to remote phishing attacks.
CONS	**Vulnerability to Attacks:** Susceptible to SIM swapping and interception attacks. Attackers can potentially intercept SMS messages or trick mobile providers into transferring a victim's phone number. **Dependence on Mobile Network**: Requires reliable cellular service, which can be problematic in areas with poor reception.	**Device Dependency:** Requires a smartphone or tablet; if the user loses their device, they may face difficulties in accessing their accounts. **Complexity in Backup:** Users must manage and securely backup their app configurations to avoid being locked out if their device is lost or replaced.	**Cost:** Generally more expensive than SMS or app-based solutions. Organizations need to purchase and distribute tokens. **Usability Issues**: Users need to carry the physical token, which can be lost or forgotten. There's also the need to ensure compatibility with all systems and devices.
Effectiveness:	**Moderate:** Provides a layer of security but is less secure compared to other MFA methods due to the risk of interception and social engineering attacks.	**High:** Generally considered more secure than SMS-based MFA, as the codes are generated locally and are less vulnerable to interception.	**Very High:** Offers one of the highest levels of security among MFA options, particularly effective in preventing unauthorized access even if login credentials are compromised.
Security	Least secure, as it is vulnerable to various forms of interception and social engineering attacks.	Generally, more secure than SMS-based MFA due to the lack of transmission over potentially insecure channels.	Highest security due to their physical nature and resistance to remote attacks.
Usability	SMS-Based MFA is the most convenient and requires minimal setup, but at the cost of security.	App-Based MFA provides a balance between security and convenience, though it requires a smartphone.	Hardware Tokens can be less convenient but are very secure.
Cost	Cheapest in terms of setup, with minimal infrastructure costs.	Low-cost, especially if using free apps.	Higher upfront cost due to the purchase of physical devices.