International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Authentication and Authorization Techniques – A Case Study on Multifactor Authentication with AWS IAM

Hareesh Kumar Rapolu

hareeshkumar.rapolu@gmail.com

Abstract

The research paper has appropriately evaluated the importance of multifactor authentication with AWS IAM. It has further identified the ways in which this service is implemented by individuals and organizations alike. In addition, the research paper has also highlighted the various benefits that can be experienced by using multifactor authentication with AWS IAM. The different drawbacks are also properly listed within the research paper. A few recommendations have also been provided in order to mitigate the challenges that are posed by the multifactor authentication with AWS IAM.

Keywords: AWS IAM, AWS MFA, Multifactor authentication, Password, MFA Token

I. INTRODUCTION

The research paper will critically analyse the significance of multifactor authentication with the help of AWS Identity and Access Management (IAM) in the digital world. The paper will appropriately explore the different ways in which multifactor authentication of AWS IAM is applied by individuals and businesses alike. The research paper will further highlight the different merits of using multifactor authentication of AWS IAM. Finally, a few drawbacks and mitigation strategies will be provided in the paper that can allow AWS IAM to revamp their protocols and grant special kind of protection against online perpetrators to users in the digital world.

II. OVERVIEW OF MULTIFACTOR AUTHENTICATION WITH AWS IAM

AWS IAM is a web service that is provided by one of the largest technological giants in the industry. In the digital era, despite the multiple advantages, there is a constant threat of important data getting stolen by unauthorized users. Therefore, multifactor authentication helps users in this regard by securing the system[1]. In order to access the system, the user is required to have more than one kind of identification to prove their identity. The user cannot override it unless they fulfil the identity requirement. Multifactor authentication in AWS IAM helps a user control access to the different AWS resources[2]. The available methods for multifactor authentication with AWS IAM include passkeys and security keys, virtual

authenticator apps, hardware TOTP tokens and hardware TOTP tokens. If the server in AWS IAM properly verifies the credentials of the user, it grants access to the user.

Figure 1: Depicting multifactor authentication with AWS IAM

III. WAYS IN WHICH MULTIFACTOR AUTHENTICATION WITH AWS IAM IS IMPLEMENTED

There are a number of different ways in which the multifactor authentication service within AWS IAM is implemented by different users. It is used with the help of Virtual MFA devices, physical security keys like FIDO U2F and text messages. Various inherent equations are used for successful multifactor authentication by AWS IAM. The formula for the general multifactor authentication equation is Authentication Success=f(Password, MFA Token). Additionally, the formula for multifactor authentication by AWS IAM is Authentication Success=True, if the Password is valid∧MFA Token is valid and Authentication Success=False, otherwise.

IV. EXPLORING THE MAIN ADVANTAGES OF USING MULTIFACTOR AUTHENTICATION WITH AWS IAM

Enhanced security

The multifactor authentication with AWS IAM helps different users protect their sensitive data against hackers. Particularly, it provides superior protection against phishing attempts where the user mistakenly shares their credentials with others[3]. The extra layer of encryption and identity requirement is important for mitigating online threats.

Compliance with regulations

A number of industries have made it mandatory for users and businesses to use multifactor authentication for the purpose of enhanced security. Therefore the multifactor authentication service provided by AWS IAM is quite significant for properly meeting the established industry standards.

Granular access control

The user of multifactor authentication of AWS IAM gets to control access to their sensitive data in an efficient manner. This fine-grained control over critical information enables them to carry out their operations without any hindrances or influences of online threats in the digital era[4].

Enhanced user trust

The state-of-the-art level of security provided by the multifactor authentication by AWS IAM helps to improve trust among the users. Furthermore, it is very easy to set up, which further enhances the reliability.

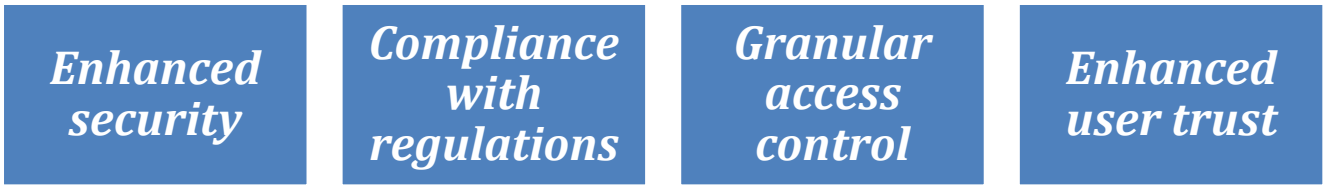

Figure 2: Advantages of using multifactor authentication with AWS IAM

V. ANALYSING THE DRAWBACKS OF MULTIFACTOR AUTHENTICATION WITH AWS IAM

Role misconfigurations

If the different layers of trust policies are inherent within the operations of the multifactor authentication of AWS IAM, it can lead to security disasters. In this manner, this problem can be leveraged by the online perpetrators to gain access to roles having elevated privileges, which can lead to infiltration within a user's system[5].

Scalability limitations

The authentication techniques that are used within AWS IAM have limited scalability options. Therefore, if the multifactor authentication technique is not regularly updated by AWS, an online attacker can make use of it to get into a user's system and steal relevant information[6].

Inconsistent multifactor authentication enforcement

In an organisational context, it can be quite difficult to implement multifactor authentication across all the different users, roles and federated accounts. It can create loopholes for the attackers to exploit, get into a system and gather sensitive information.

VI. RECOMMENDATIONS

Implementing the principle of least privilege

The principle of least privilege can help to monitor the access of different individuals for a particular AWS resource. If minimum permissions are granted to the individuals, it can mitigate the problem of impersonation or unauthorised access[7]. AWS IAM Access Analyser can be utilised to find out if there are any kind of unused or excess permissions within the system.

Proper monitoring of service limits

The different kinds of service limits need to be regularly monitored in regard to IAM. It can be beneficial for bypassing the limitations effectively.

Training the employees

In an organisation, appropriate training needs to be provided to the employees about the significance of multifactor authentication. It can significantly improve their ways of operation and enhance productivity.

Abbreviations and Acronyms

- AWS - Amazon Web Services
- IAM - Identity and Access Management
- MFA - Multifactor authentication

Units

- Password length - Characters
- Password complexity - Boolean/conditions
- MFA token - 6-digit number
- Token validity - Seconds
- Authentication - Binary (0 or 1)

Equations

- General multifactor authentication equation - Authentication Success=f(Password, MFA Token).
- Multifactor authentication by AWS IAM - Authentication Success=True, if the Password is valid∧MFA Token is valid.
- Multifactor authentication by AWS IAM - Authentication Success=False, otherwise.

VII.CONCLUSION

From the above discussion, it can be properly concluded that the multifactor authentication service provided by AWS IAM is really helpful in protecting the confidential data of the users. The enhanced security can also be really beneficial for managing the overall resources within the AWS system. In the digital era, the increase in phishing attempts has exposed personal information. The security credentials of the users are properly verified by the authentication service of AWS IAM. Subsequently, the user is granted permission with proper access to the different resources. However, it needs to be mentioned that AWS needs to keep improving its multifactor authentication services within IAM in order to keep the online perpetrators at bay.

REFERENCES

[1] A. M. Mostafa *et al.*, "Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication," *Applied sciences*, vol. 13, no. 19, pp. 10871–10871, Sep. 2023, doi: https://doi.org/10.3390 /app131910871.

[2] E. Putra, UbaidiUbaidi, AchmadZulfikri, Goffal Arifin, and Revi Mario Ilhamsyah, "Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study," *Brilliance Research of Artificial Intelligence*, vol. 4, no. 1, pp. 413–421, Aug. 2024, doi: https://doi.org/10.47709/brilliance.v4i1 .4357.

[3] M. I. Hussain *et al.*, "AAAA: SSO and MFA Implementation in Multi-Cloud to Mitigate Rising Threats and Concerns Related to User Metadata," *applied sciences,* vol. 11, no. 7, doi: https://doi.org/10.3 390/app11073012.
[4] O. R. Arogundade, "Network security concepts, dangers, and defense best practical," *Computer Engineering and Intelligent Systems,* vol. 14, no. 2, Mar. 2023, doi: https://doi.org/10.7176/ceis/14-2-03.
[5] S. Talluri and S. T. Makani, "Managing Identity and Access Management (IAM) in Amazon Web Services (AWS)," *Journal of Artificial Intelligence & Cloud Computing*, vol. 2, no. 1, Feb. 2023, doi: https://doi.org/10.47363/JAICC/2023(2)147.
[6] Y. Fei, J. Yin, and L. Yan, "MFF-IoT: A Multi-Granularity Formal Framework of User Authentication for IoT," *electronics,* vol. 12, May 2023, doi: https://doi.org/10.3390/electronics12112356.
[7] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, "Phishing Attacks: a Recent Comprehensive Study and a New Anatomy," *Frontiers in Computer Science,* vol. 3, no. 1, pp. 1–23, Mar. 2021, doi: https://doi.org/10.3389/fcomp.2021.563060.