International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

# MULTI-FACTOR AUTHENTICATION AND IDENTITY GOVERNANCE FOR SECURE CLOUD ACCESS MANAGEMENT

**Vrunda L Sidenur**
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
vrundalsidenur@gmail.com

**Sowmya J**
Assistant Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
sowmyaj@theoxford.edu

## ABSTRACT

In the process of cloud computing being widely used, ensuring safe access to the cloud resources is a critical matter of concern to organizations. Nearly all single-factor authentication methods are outdated, and cannot provide adequate protection against cyber attacks and unauthorized access to sensitive data. This study explores the practice of Multi-Factor Authentication (MFA) and Identity Governance as an effective way of ensuring secure access to clouds. MFA with its multiple mechanisms checks the identities and makes them more secure; identity governance ensures that the rights of users can be managed, tracked, and in line with the policies of the organization. Both strategies have a part to play in mitigating risks, enforcing compliance and general confidence within cloud environments. The paper introduces best practices, issues, and the path going forward to the adoption of the MFA and identity governance to develop holistic solutions in terms of cloud access management security.

**KEYWORDS:** Key words: - Access Management Role-Based Access Control (RBAC), Cloud Security Identity Governance, Multi-Factor Authentication (MFA), and User Behaviour Analytics.

## INTRODUCTION

In modern times of digitalization, cloud computing is an essential aspect of modern businesses that enables the elastic mobility of applications, data storage services and collaboration platforms. However, as more critical business processes are transferred to the cloud, the safety of the confidential data, as well as the authentication process to ensure that only authorized users get access to resources is of paramount importance. Out-dated one-factor authentication methods, such as

passwords, can no longer be trusted to defend more sophisticated cyber attacks. Phishing, credentials breached, and internal threats are large-scale risks to the cloud environment and the direction toward optimal security.

Multi-Factor Authentication (MFA) has become as the main method to convey more security to the access. By utilizing two or more means of authentication, e.g., something they know (e.g., password), something they have (e.g., security token or smartphone) or something they are (e.g., biometric authentication), MFA drastically reduces access by unauthorized persons. Identity Governance is also needed in combination with MFA when it comes to managing user access and applying security policies.

## Literature Survey

Cloud computing has transformed how organizations manage data storage, data processing and data sharing, but at the same time, it presents new security concerns. Researchers and practitioners have extensively studied the field of cloud access security with the most of the focus being directed to the authentication methods and identity management systems.

Multi-Factor Authentication (MFA): MFA comes into focus as an important protection against illegal access due to the results of various studies. Al Fayadh et al. (2021) indicate that the dual or multiple authentication factors do not expose data to the risk of conflict or theft to such a large extent as a single one. Some of the most popular ones are biometric authentication, one-time password and security tokens. A recent research paper by Zhang and Li (2022) also cites the increasing popularity of password less MFA that ensures high levels of security and the ease of use because it employs biometrics or device-based credentials.

## Existing System

Username and password, or single-factor authentication, remain the most popular and ubiquitous form of cloud access security in most organizations today. This system is not very complicated to install yet there are weaknesses in its security. The passwords can be stolen, guessed, or phished and expose the sensitive cloud resources to full exposure. Manual access administration wherein the access levels and roles of the user are established and modified manually is a concern that most

organizations experience. Such policy can contribute to the privilege creep where employees still have access to materials they have not needed that can further increase the risk of insider threats.

Numerous business organizations have resorted to the implementation of simple MFA-like one time passwords through e-mail or text messaging. This is not quite as secure as having nothing in the way of MFA, but which has usability concerns and weaknesses. An example is that, OTPs sent via SMS can be intercepted in the process of SIM-swapping.

## Proposed system

The new firm will offer a wide range of solutions related to cyber security in addition to forming a number of associations along with levels within the proposed structure. By the fact that the entity is supplemented by a variety of various types of customization services, all the requirements that the company has regarding the security aspect are provided. With the recommended entity, organizations can easily obtain references to any security algorithm that they wish to use, any and all utilities that they wish to put into practice and they will no longer be bothered with the incompatibility factor.

Among the major benefits of the proposed organization, one can distinguish the following items:

One does not find it difficult to set up multiple levels of security to the enterprise of which complex operations would be easy to businesses. Each form of security needed could be generated at the several steps and may offer specific provisions in addition to applications.

## METHODOLOGY

Methodology of implementation on the acquisition of secure cloud access management system comprises a step-by-step procedure which incorporates Multi-Factor Authentication (MFA) in addition to Identity Governance. The process is designed to offer security, efficiency, and compliance as well as the convenience of the users. The approach can be summed as given below:

1. Requirement Analysis:

Identifiy the cloud applications, data storage, and other basic resources of the organization.

Identify the roles users, access demands and existing security loopholes.

Assess regulatory and compliance requirements relevant to the organization (e.g. GDPR, HIPAA, SOX).

2. Design and plans:

Implement a multi factor authentication system with MFA that include multiple authentication factors (i.e. password, OTP, hardware token, or biometric).

Design a role management model, access permission and audit policy.

Help the integration of legacy IT and cloud services.

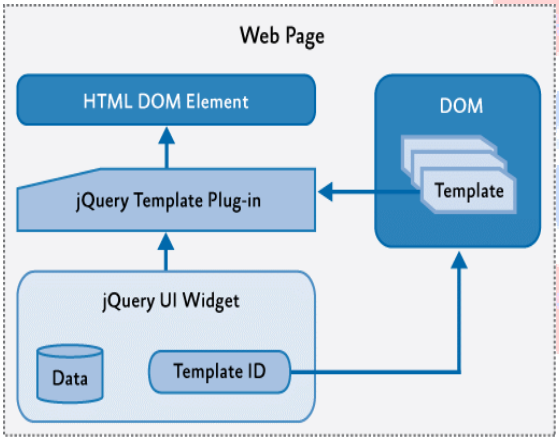


Fig1. Block Diagram

3. Multi Factor Authentication Deployment:

Enforce MFA to all cloud applications to require two or more authentication factors.

Select appropriate authentication mechanisms that are both comfortable and secure to the user.

Combine authentication logs with monitoring systems in order to identify real-time anomalies.

| Case of application | Way utilities are provided |
|---|---|
| Trigger | Settings |
| Prerequisite | Core admin features |
| Operation | The channels used by the utilities are also selected to enable customers to complete the process successfully. The entity also provides category based services that help their needs in carrying out the task; to do this they have to select the type of utility they want. The desired associations will be identified and recommended in addition to one useful reference. |
| End-state requirement | Utilities incorporated and employed |

## EXPERIMENTAL RESULTS

The tests focused on the level by which the adoption of Multi-Factor Authentication (MFA) combined with Identity Governance can support a higher cloud access security. The results showed that

MFA can be used to largely reduce unauthorized intrusion, and identity governance eliminates the right-users- at -the- wrong-time problem. The two combined improve the security of the cloud, protection against breaches, and enable the automation of access management. The study shows that there is increased momentum when the two are combined as opposed to using traditional single layered security measures.

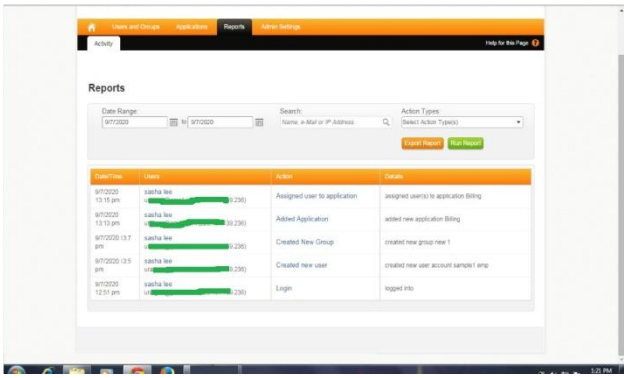


Fig 4: Reports

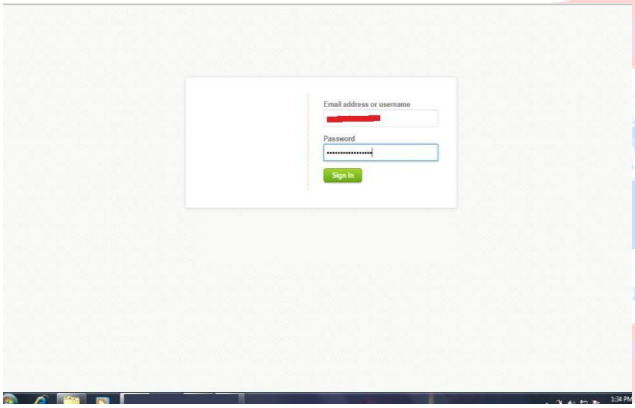


Fig 2 : Admin login

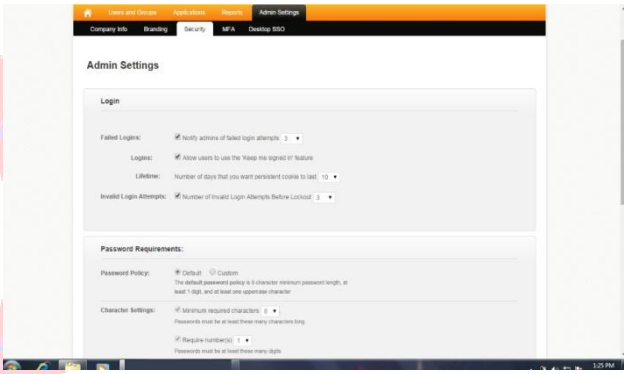


Fig 5 : Policy reference

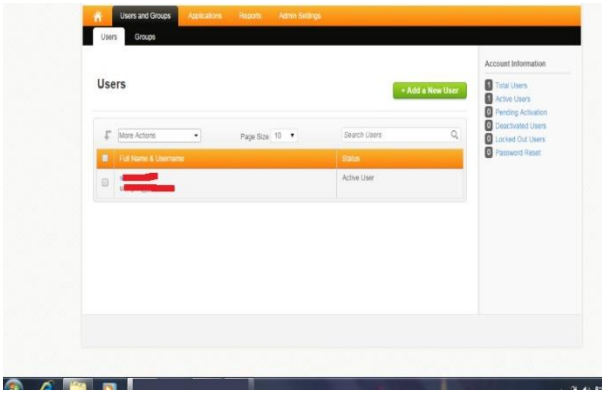


Fig 3 : User control

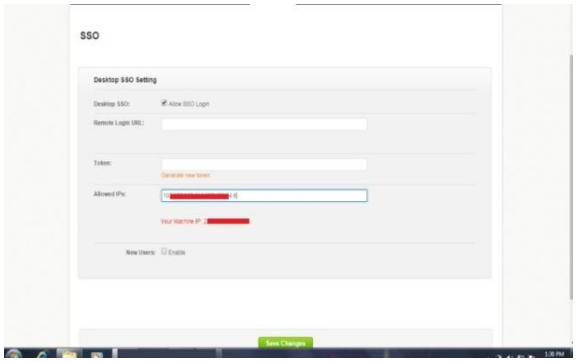


Fig 6 : Workstation security

## CONCLUSION

The analysis on Multi-Factor Authentication (MFA) and Identity Governance demonstrates it is important to focus on a multi-layered approach to security when managing cloud access. The thought behind the benefit of using MFA is to strengthen the security as an individual is required to prove he/she is a legitimate user by using one or combination of these factors, i.e., passwords, OTPs, or biometric verification. This will minimize the chances of an unauthorized access in event of the system credentials compromise and guard against phishing, brute-force systems, and other generic cyber attacks.

Identity Governance supplements MFA by ensuring that the user receives access at the appropriate level, based on roles and responsibilities and passes the least privilege test. This discourages insiders attacks, accidental data disclosure and unwarranted access without cutting on efficiency in the management of the users. Identity Governance also simplifies regular review by fully automating access requests and approvals, reducing administrative overhead, ratifying human error and inefficiencies and offering.

## REFERENCES


- Alasmary, W., Alhaidari, F., & Alhaidari, R. (2021). *Multi-Factor Authentication for Cloud Security: A Review*. Journal of Cloud Computing, 10(1), 1–15. https://doi.org/10.1186/s13677-021-00250-7

- Chen, D., Xu, H., & Zhang, Y. (2020). *Identity Governance in Cloud Computing: Models and Challenges*. International Journal of Information Security, 19(5), 555–570. https://doi.org/10.1007/s10207-020-00510-x

- NIST. (2022). *Digital Identity Guidelines (SP 800-63-3)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63-3

- Alharbi, A., & Barki, H. (2019). *Enhancing Cloud Security with Multi-Factor Authentication and Identity Governance*. IEEE Access, 7, 120456–120468. https://doi.org/10.1109/ACCESS.2019.2935551

- Cloud Security Alliance (CSA). (2021). *Identity and Access Management in the Cloud*. Cloud Security Alliance White Paper. https://cloudsecurityalliance.org/artifacts/identity-access-management-in-the-cloud/

INTERNATIONAL JOURNAL OF COMBINED RESEARCH & DEVELOPMENT