Journal Homepage: www.ijarpr.com ISSN: 3049-0103 (Online)

International Journal of Advance Research Publication and Reviews

Vol 03, Issue 10, pp 101-103, October, 2026

Comparative Analysis of Multi-Factor Authentication and Role-Based Access Control in Cloud Data Security

Vimalraj V[1], Dr. V. Maria Antoniate Martin[2]

[1]M.Sc. Computer Science, Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India.

[2]Assistant Professor, Department of Information Technology, St. Joseph's College (Autonomous), Tiruchirappalli, Tamil Nadu, India.

ABSTRACT

Cloud computing has made data storage and processing scalable and affordable, but it has also moved sensitive data outside an organization's physical perimeter. Identity has therefore become the main security boundary. Two controls are widely deployed to protect it: Multi-Factor Authentication (MFA), which verifies who is requesting access, and Role-Based Access Control (RBAC), which governs what an authenticated user may do. Although often discussed together, they address different threat classes and are seldom compared directly. This paper presents a qualitative, criteria-based comparative analysis of MFA and RBAC in cloud data security. Both are evaluated against six criteria: threat coverage, protection against credential compromise, protection against insider misuse, usability, administrative overhead, and regulatory alignment. The analysis shows that MFA is most effective against external credential-based attacks, while RBAC is most effective at limiting damage from insider misuse and over-privileged accounts. Neither is sufficient alone. A layered model combining both, supported by periodic access reviews, gives the strongest protection.

Keywords: Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), Cloud Security, Authentication, Authorization, Data Protection, Least Privilege

Introduction

Organizations increasingly host critical data on public, private and hybrid cloud platforms. NIST describes cloud computing as on-demand network access to a shared pool of configurable resources that can be rapidly provisioned with minimal management effort [1]. This model brings flexibility, but data is now reachable over the internet from anywhere, so a single stolen password can expose large volumes of information.

MFA answers the first question by requiring two or more independent proofs of identity, typically something the user knows (password), has (phone, hardware token) or is (biometric) [2]. RBAC answers the second by assigning permissions to roles rather than to individuals, and then assigning users to roles [3][4].

Both controls are recommended in security guidance, yet organizations often treat them as interchangeable "access security" measures. This is a misconception: they protect different points in the access lifecycle and fail in different ways.

Literature Review / Related Works

Passwords and their weaknesses. Bonneauetal. evaluated many alternatives to passwords against usability, deployability and security criteria, and found that no single scheme beats passwords on all fronts, which explains why passwords persist and why they must be supplemented [5]. Weak, reused and phished passwords remain a leading cause of account compromise, which motivates additional authentication factors.

Multi-factor authentication. Ometov et al. surveyed MFA technologies, covering knowledge, possession and inherence factors, and discussed the trade-offs between security and user convenience [2]. NIST's Digital Identity Guidelines define authenticator assurance levels and note that some factors (such as SMS codes) are weaker than cryptographic authenticators [6]. Studies of mobile two-factor schemes have also shown that implementation flaws can weaken an otherwise sound design [7]. MFA is therefore a strong control, but its strength depends on the factor type and implementation.

Role-based access control. Sandhu et al. formalized a family of RBAC models covering core roles, role hierarchies and constraints such as separation of duty [3]. Ferraiolo et al. then proposed the NIST RBAC standard, unifying these ideas into a reference model [4]. RBAC's key advantages are simplified administration and support for the principle of least privilege.

Beyond RBAC. Attribute-Based Access Control (ABAC) makes decisions using user, resource and environment attributes, offering finer granularity than fixed roles [8]. It is often cited as a response to "role explosion" in large systems, but it is more complex to design and audit.

Research gap. Much of the literature studies MFA and RBAC separately, one under authentication and the other under access control. Fewer works compare them side by side on shared criteria for cloud data security. This paper addresses that gap.

Methodology

This study uses a qualitative comparative analysis based on documented standards and published literature. No new experimental measurements were collected.

Step 1: Scope definition. The analysis considers a typical cloud deployment in which users access stored data and services through a web console or API.

Step 2: Selection of criteria. Six criteria were chosen to reflect both security and practical concerns:

Step 3: Threat scenarios. Four common cloud threat scenarios were used to test each control conceptually: (a) phishing-based credential theft, (b) brute-force or credential-stuffing attacks, (c) a malicious or careless insider, and (d) an over-privileged account compromised by an attacker.

Step 4: Scoring. For each criterion, each control was rated Low (1), Medium (2) or High (3) based on how the cited standards and literature characterize it. These ratings are analytical judgments, not measured values, and are intended to support structured comparison rather than precise ranking.

Limitations. Ratings depend on implementation quality (for example, SMS-based MFA rates lower than hardware keys). Results are therefore indicative and should be validated in specific environments.

Results and Discussion

Scenario analysis

ScenarioMFA effectRBAC effectOutcome

- Phishing steals password Attacker lacks second factor, so login is blocked (unless the factor itself is phished)No effect on the login itself MFA is the primary defense
- Brute force / credential stuffingStrongly reduces successNo direct effectMFA is the primary defense
- Malicious or careless insider No effect, since the user authenticates legitimately Limits accessible data to the role's permissions RBAC is the primary defense
- Over-privileged account compromisedMay prevent the compromiseLimits blast radius only if privileges are well designedBoth needed

Discussion

MFA protects the door; RBAC controls the rooms. MFA reduces the chance that an unauthorized person gets in. Once inside, it offers no further limitation. RBAC does the reverse: it says nothing about whether the person is genuine, but it constrains what any authenticated identity can touch.

Failure modes differ. MFA can be weakened by SIM-swapping, push-notification fatigue and real-time phishing proxies, and by weak account-recovery paths [2][6][7]. RBAC commonly fails through privilege creep (users accumulating roles over time), role explosion (too many narrowly defined roles) and poorly reviewed role assignments [3][8]. Each weakness is addressed only by better implementation and governance, not by the other control.

Usability and cost. MFA imposes a small per-login burden, which can lead users to seek workarounds if poorly designed. RBAC is nearly transparent to users but demands upfront effort to map job functions to permissions and ongoing effort to keep roles accurate.

Complementary design. A robust cloud design applies MFA at authentication (with stronger factors for privileged roles), RBAC at authorization with least privilege and separation of duty, and periodic access reviews and logging. Where fine-grained context is needed, ABAC can extend RBAC [8].

Conclusion

This paper compared Multi-Factor Authentication and Role-Based Access Control in the context of cloud data security using a criteria-based, scenario-driven analysis. MFA is the stronger defense against external attacks that rely on stolen or guessed credentials, while RBAC is the stronger defense against insider misuse and excessive privileges. Because they operate at different stages of the access lifecycle, neither can replace the other. Organizations should deploy them together, choose phishing-resistant factors for high-privilege accounts, keep roles aligned with the principle of least privilege, and review access regularly.

Future work. The qualitative ratings here could be strengthened by empirical studies, such as simulated attack testing in a cloud sandbox, user-experience surveys on MFA friction, and measurements of privilege creep in real role structures. Comparison with ABAC and zero-trust architectures is another promising direction.

References

- P. Mell and T. Grance, "The NIST Definition of Cloud Computing," NIST Special Publication 800-145, National Institute of Standards and Technology, 2011.
- A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," Cryptography, vol. 2, no. 1, art. 1, 2018.
- R. S. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, "Role-Based Access Control Models," IEEE Computer, vol. 29, no. 2, pp. 38–47, 1996.
- D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn and R. Chandramouli, "Proposed NIST Standard for Role-Based Access Control," ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 224–274, 2001.
- J. Bonneau, C. Herley, P. C. van Oorschot and F. Stajano, "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," in Proc. IEEE Symposium on Security and Privacy, 2012, pp. 553–567.
- P. A. Grassi et al., "Digital Identity Guidelines: Authentication and Lifecycle Management," NIST Special Publication 800-63B, 2017 (and subsequent revisions).
- A. Dmitrienko, C. Liebchen, C. Rossow and A.-R. Sadeghi, "On the (In)Security of Mobile Two-Factor Authentication," in Financial Cryptography and Data Security, 2014.
- V. C. Hu et al., "Guide to Attribute Based Access Control (ABAC) Definition and Considerations," NIST Special Publication 800-162, 2014.