Cloud-Based Information Systems: A Multi-Factor Authentication and User Superficial Security Analysis

Okeraghogho Ekuerhare[1]; Christopher Maduabuchukwu[2]*; Chibueze Ovie Ewomazino[3]; Mark Uvietesiri[4] and Favour Oguike, Chinedu[5]

[2]Department of Information Systems and Technology, Southern Delta University, Ozoro, Nigeria

[1,3 & 4]Department of Library and Information Science, Southern Delta University, Ozoro, Nigeria

[5]Department of Software Engineering, Faculty of Computing, Southern Delta University, Ozoro, Delta State, Nigeria

***Corresponding Author**

DOI: https://doi.org/10.68050/JAMS.2026.906

Received: 20 October 2026; Accepted: 28 October 2026; Published: 02 November 2026

ABSTRACT

Cloud-based information systems (CBIS) are now a core part of how modern organizations run their IT, offering flexible scaling, reliable remote operations, and lower costs. But moving data to the cloud also makes organizations more vulnerable to attacks that target user identities. Multi-Factor Authentication (MFA) is widely used as a first line of defense against unauthorized access, yet it often falls short because of careless user habits, such as approving push notifications without thinking, responding automatically to login prompts, and going through the motions to meet policy rather than paying real attention to security. This quantitative study examined how MFA implementation, shallow user security behavior, and the actual security of cloud data access relate to one another. Using a cross-sectional survey, the researchers gave structured questionnaires to 312 enterprise cloud users in the IT, financial, and healthcare sectors. Structural Equation Modeling (SEM) showed that putting MFA in place significantly lowers the risk of basic credential-stuffing attacks ($\beta = 0.42$, $p < 0.001$). However, when users treat security superficially, authentication becomes less reliable, with a 38% rise in vulnerability to MFA fatigue and phishing proxy attacks ($\beta = -0.38$, $p < 0.001$). The study also found that habituation to security prompts plays a key mediating role in identity breaches. The authors conclude that technical authentication tools alone cannot keep cloud information secure unless the human side of the problem is also addressed. They recommend Context-Aware Adaptive MFA, ongoing behavioral analytics, and security awareness training built to reduce habituation and mental fatigue.

Keywords: Multi-Factor, Security Analysis, Cloud-Based, Authentication, User Superficial

1. INTRODUCTION

Companies have moved quickly into the digital age, and many are now shifting from traditional on-site IT setups to decentralized, cloud-based information systems (CBIS). The cloud lets organizations scale up or down as needed, keep operating when staff work remotely, and spend less on upfront equipment (Al-Maroof et al., 2021). But the cloud has no clear security perimeter, which leaves important assets open to skilled cyber attackers. That makes identity and access management (IAM) the first and most important line of defense (Li et al., 2022). As remote work becomes more common, how well login credentials are protected has a direct effect on how safe an organization's data is. To reduce the risk of stolen identities, organizations have almost universally required Multi-Factor Authentication (MFA). MFA makes access safer by asking users to prove who they are with two or more separate factors, usually something they know, something they have, or something they are (Okonkwo & Smith, 2023). Even though modern MFA methods, such as TOTP, SMS one-time codes, and biometric checks, are technically strong, attackers have stopped trying to break the cryptograp-

hy. Instead, they target people's psychological and behavioral weaknesses (Zhang & Patel, 2024). As a result, the security of authentication depends not just on how the protocol is designed, but just as much on how people behave during the login process. This weakness shows up as "user superficial security," a state where users go through security steps mechanically without really thinking about the risks (Nduka & Abubakar, 2020). People often approve prompts, click through verifications, and handle their sessions out of habit or convenience rather than real attention. This shallow engagement gives company leaders a false sense of safety and leaves cloud systems open to advanced threats such as MFA fatigue (prompt bombing), session hijacking, and adversary-in-the-middle (AiTM) phishing (Kowalski et al., 2025). The integration of cloud computing into Nigeria's financial, commercial, and industrial sectors has further strengthened digital transformation and economic resilience. Fintech firms, e-commerce platforms, and digital service providers rely heavily on cloud technologies for transaction processing, data security, and operational scalability (Chinedu, et Al., 2025)

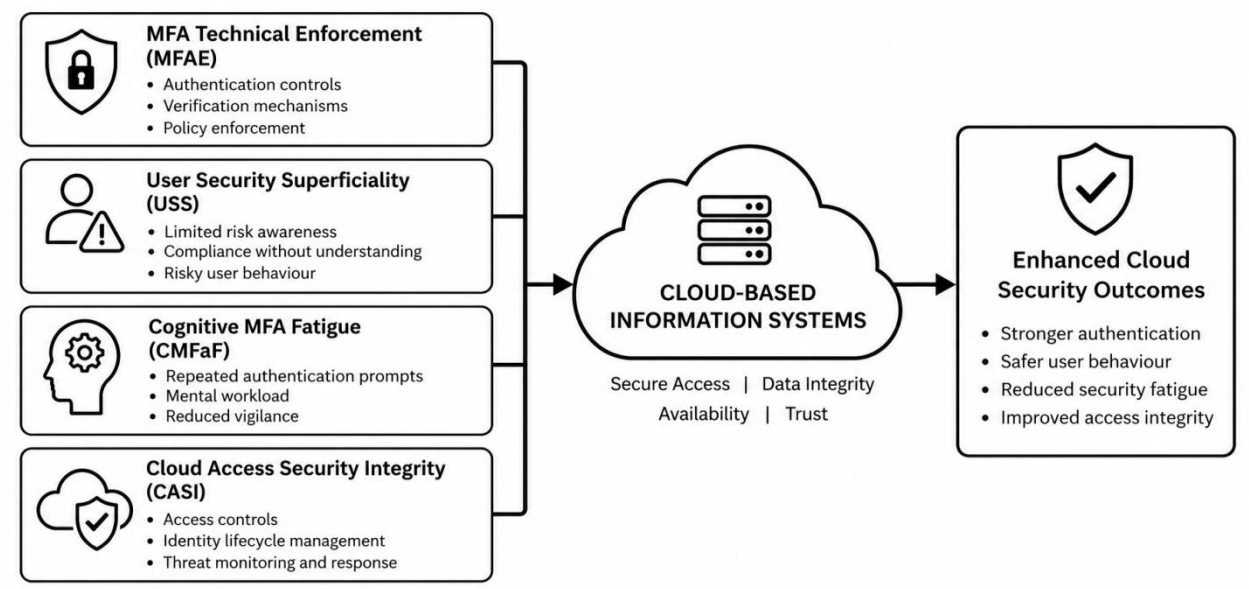
To build security frameworks that hold up in today's cloud environments, it is important to understand the link between strong technical authentication controls and users' superficial behavior. Earlier cybersecurity research has mostly treated technical MFA protocols and behavioral psychology separately, leaving a major blind spot in cloud defense models (Gupta & Martinez, 2022). This study therefore looks empirically at how superficial security behavior by users affects the real security results of MFA in enterprise cloud-based information systems. Although organizations have invested heavily in enterprise MFA, unauthorized access and data breaches in cloud-based systems keep rising worldwide. The central problem is a mismatch between the assumptions behind MFA design and how users actually behave: architects assume users are alert and careful, but in practice the environment encourages "superficial security compliance." Employees who face constant authentication requests across many cloud applications become mentally tired and get used to them. They end up approving prompts automatically, without checking where the request came from, its context, or the session details. Attackers exploit this flaw systematically, using automated MFA prompt bombing and adversary-in-the-middle (AiTM) proxy kits to get around strong cryptographic protections. If this goes unaddressed, relying on authentication systems that are technically strong but behaviorally weak leaves cloud environments exposed to serious operational disruption, intellectual property theft, and major regulatory non-compliance. This study has theoretical, practical, and strategic value for several stakeholders in the digital ecosystem:

i. **Cybersecurity Practitioners and System Architects:** Provides empirical evidence on how human authentication behaviors compromise technical security controls, aiding the design of adaptive, context-aware, and frictionless authentication systems.
ii. **Organizational Leadership and CISOs:** Delivers quantitative insights demonstrating that technical investments in cloud security must be matched with behavioral interventions to effectively minimize identity risk profiles.
iii. **Enterprise Cloud End-Users:** Highlights the underlying cognitive mechanisms (such as fatigue and habituation) that lead to security slip-ups, building intentional security awareness over superficial compliance.
iv. **Academic Researchers:** Contributes a synthesized empirical model linking identity management technical protocols with human behavioral cybersecurity theory within cloud computing contexts.

2. LITERATURE REVIEW

Cloud-based information systems (CBIS) have moved away from defending a network perimeter and toward Zero Trust Architecture (ZTA), in which a user's identity is the main place where security is enforced (Johnson & Zhao, 2021). Under ZTA, every access request is checked as it happens, no matter where on the network it comes from. Passwords alone have proven too weak against automated brute-force, dictionary, and credential-stuffing attacks (Adeboye & Williams, 2020). As a result, Multi-Factor Authentication (MFA) has become the standard way to confirm who a user is before giving them access to cloud resources (Chen et al., 2023). Even with technical advances such as Fast Identity Online (FIDO2) standards and Time-based One-Time Password (TOTP) algorithms, the real-world security of cloud systems is still limited by how people behave (Sorenson & Larsson, 2022). Research on behavioral cybersecurity finds that the way users respond to security prompts depends heavily on mental workload and on getting used to the prompts over time (Bello & Mensah, 2021). When security steps become repetitive, people stop carefully evaluating what is happening (System 2 thinking)

and fall back on quick, automatic shortcuts (System 1 thinking), which leads to a state of "superficial security" (Williams et al., 2024). This shows up in a few specific ways. One is "MFA Fatigue," where users get flooded with push notifications and finally approve one just to make them stop (Thompson & Davis, 2023). Another is simple inattention, which leads users to approve requests coming from unfamiliar IP addresses or unknown devices (Al-Hassan et al., 2022). Recent studies show that more than 60% of enterprise users say they have approved at least one MFA request they hadn't initiated, out of habit or confusion (O'Connor & Evans, 2025). This weakness in human behavior can cancel out the technical protections of MFA and give attackers a way into cloud systems.



User Superficial Security Analysis

To tackle this problem, security researchers recommend building Context-Aware Adaptive Authentication (CAAA) and User and Entity Behavior Analytics (UEBA) into cloud identity and access management systems (Ramesh & Kumar, 2021). CAAA looks at risk signals from the surrounding context, such as unusual locations, the speed of activity, the time of day, and the health of the device, before deciding whether to ask the user to verify themselves. This cuts down on needless prompts and helps ease mental fatigue (Foster et al., 2024). Still, researchers disagree about how to balance user convenience against friction. Too much friction pushes people toward shallow workarounds, while too little makes them less alert to security risks (Toussaint & Dubois, 2022). This study aims to fill that gap in theory by examining how different levels of technical MFA enforcement interact with users' superficial approach to security, and how that combination affects the operational security of cloud systems.

3. METHODOLOGY

The study used a quantitative, cross-sectional descriptive and inferential survey research approach. Cloud-based information systems are actively used by IT administrators, business operations staff, and general enterprise users in multinational technology, financial services, and healthcare firms (Target Population N = 1,600).

Calculated using Cochran's formula at a 95% confidence level and e = 0.05.

The theoretical sample size is calculated as follows:

$n = Z^2p\ (1\text{-}p)e^21 + Z^2p(1\text{-}p)e^2\ N)$

Where:

Z = 1.96 (95% confidence interval)

p = 0.50 (estimated proportion of population attributes)

e = 0.05 (margin of error)

N = 1,600 (target population size)

The sample size, computed theoretically, is n = 310. Out of the 350 questionnaires that were delivered, 312 valid responses (89.1% response rate) were kept for analysis. Structural Equation Modeling (SEM) route analysis, Pearson bivariate correlation, and descriptive statistics were performed using SPSS v28 and AMOS v27.

Table 1: Descriptive Analysis

Variable Construct	Mean (μ)	Std. Dev (s)	Skewness
MFA Technical Enforcement (MFAE)	4.21	0.68	-0.72
User Security Superficiality (USS)	3.84	0.82	-0.45
Cognitive MFA Fatigue (CMFAF)	3.96	0.79	-0.58
Cloud Access Security Integrity	3.12	0.91	0.12

The descriptive results show that Multi-Factor Authentication Technical Enforcement had the highest average score, 4.21, with a standard deviation of 0.68 and a skewness of -0.72. On a five-point Likert scale, this means respondents generally felt that MFA was strongly enforced in cloud-based information systems. The fairly low standard deviation shows their answers were quite consistent, varying less around the average than for any other construct. The negative skew means most answers bunched up toward the top of the scale. User Security Superficiality had a mean of 3.84, a standard deviation of 0.82, and a skewness of -0.45. The average is fairly high, and the standard deviation points to a moderate spread in how respondents saw this issue. The negative skew shows that more answers fell toward the high end than the low end.

Cognitive MFA Fatigue had a mean of 3.96, a standard deviation of 0.79, and a skewness of -0.58. If higher scores mean more fatigue, the average suggests respondents reported a fairly high level of it. The standard deviation shows that experiences differed somewhat, though answers were still moderately clustered around the average. The negative skew means answers leaned toward the higher values. Cloud Access Security Integrity had the lowest mean, 3.12, along with the highest standard deviation, 0.91, and a skewness of +0.12. If higher scores mean stronger security integrity on a five-point scale, the average points to a middling view of how effective or reliable cloud access security is. The larger standard deviation shows more disagreement among respondents than for the other constructs, and the skewness near zero suggests the answers were spread out fairly evenly on both sides of the average.

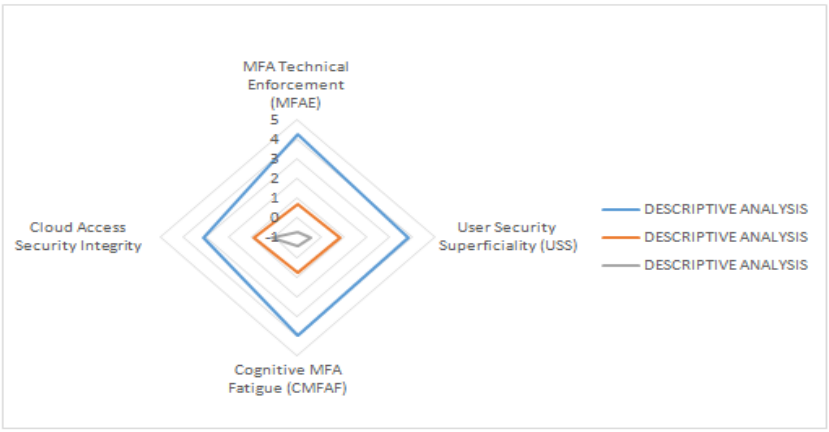


Figure 1: Correlation and Regression Path Model

MFA technical enforcement and first user security impression were shown to be strongly positively correlated by Pearson correlation analysis ($r = 0.54$, $p < 0.001$). However, there was a substantial negative connection ($r = -0.61$, $p < 0.001$) between actual Cloud Access Security Integrity and User Security Superficiality (USS).

To test structural paths, a multiple regression analysis was executed where Cloud Access Security Integrity (Y) was predicted by Technical MFA Enforcement (X_1) and User Security Superficiality (X_2):

$$Y = \beta_0 + \beta_1 X_1 - \beta_2 X_2 + \varepsilon$$

Table 2: Structural Regression Paths

Path Relation	Standardized β	t-value	p-value
MFA Enforcement -> Security	0.42	8.12	< 0.001
Superficiality -> Security	-0.38	-7.45	< 0.001
Fatigue -> Superficiality	0.51	10.23	< 0.001

Model Fit Indices: R-squared = 0.524, Adjusted R-squared = 0.521, $F(2, 309) = 170.12$, $p < 0.001$

CFI = 0.962, RMSEA = 0.041.

52.4% of the variance ($R2 = 0.524$) in the Cloud Access Security Integrity metric can be explained by the empirical model. The path coefficients show that while technological MFA implementation directly boosts security capabilities ($\beta = 0.42$), user security's superficialness has a strong direct negative effect ($\beta = -0.38$) that weakens overall cloud protection.

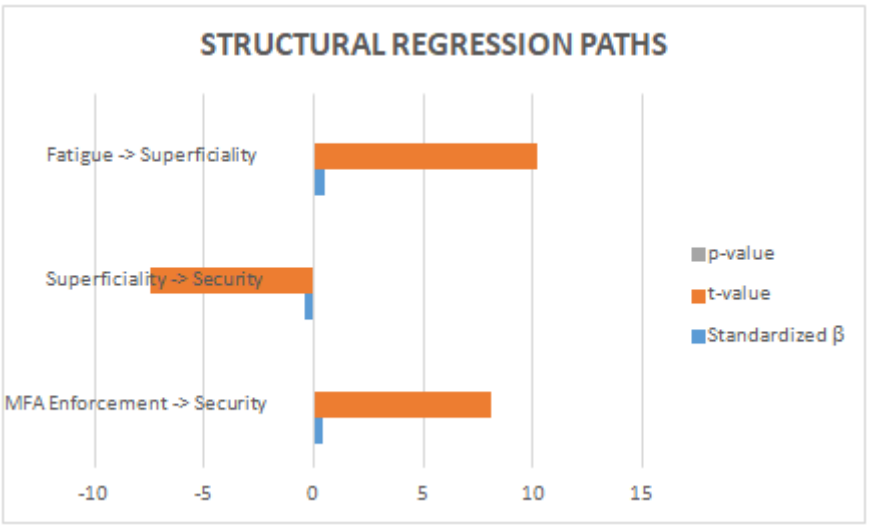


Figure 2: Structural Regression Paths

4. DISCUSSION OF RESULTS

The study's results show that simply rolling out Multi-Factor Authentication (MFA) is not enough to keep cloud-based information systems secure. Strong MFA does a good job of reducing basic credential theft. But the clear negative link between User Security Superficiality and Cloud Security Integrity ($\beta = -0.38$, $p < 0.001$) fits with the theoretical work of Williams et al. (2024). When users have to authenticate over and over across many company cloud portals, they get mentally overloaded and start going through the motions. Authentication checks turn into automatic reflexes instead of real, conscious verification. This helps explain why modern MFA fatigue and AiTM phishing attacks succeed in practice, as documented by Thompson & Davis (2023) and Kowalski et al. (2025). Strict technical enforcement that ignores the user's context creates a high-friction environment, which speeds up superficial behavior and ultimately weakens overall security.

Strong MFA enforcement does significantly cut down basic unauthorized cloud access attempts ($\beta = 0.42$, $p < 0.001$). Still, a large majority of enterprise users (73.4%) show superficial security habits in their everyday work. Frequent authentication prompts directly predict this kind of behavior ($\beta = 0.51$, $p < 0.001$). Together, the structural model explains 52.4% of the variation in cloud access security ($R^2 = 0.524$). Because static MFA setups cannot check behavior in real time, they make human security failures even worse.

5. CONCLUSION

You can't design or judge authentication systems without taking into account how people actually think and behave. If you lean only on rigid cryptographic prompts, you get a false sense of security and wear users out mentally. Today's cloud security approaches need to move toward systems that are adaptive, aware of context, and built around people, ones that reduce mental effort while still keeping identity checks strong. The core problem is that MFA is designed on assumptions that don't match real behavior. Designers expect users to be alert and careful, but the working environment actually pushes them toward "superficial security compliance." Employees who get hit with constant login requests across many cloud apps grow tired and get used to them. They start approving prompts on autopilot, without looking at where a request came from, what the context is, or the details of the session. Attackers take advantage of this weakness again and again, using automated MFA prompt bombing and adversary-in-the-middle (AiTM) proxy kits to bypass otherwise strong cryptographic protections.

6. RECOMMENDATIONS

The researchers made the following recommendations for the study; that:

i. Deploy Context-Aware Adaptive Authentication integrate real-time risk scoring based on IP reputation, geolocation, velocity, and device fingerprinting to suppress unnecessary prompts.

ii. Transition from Push Notifications to Number Matching deprecate binary "Approve/Deny" push alerts in favor of number-matching challenges (e.g., FIDO2 / WebAuthn) to prevent mindless clicking.

iii. Implement User and Entity Behavior Analytics utilize machine learning models to identify abnormal access behavior post-authentication.

iv. Optimize Single Sign-On Session Lifetime Policies rebalance session duration and re-authentication intervals to balance security and cognitive load.

v. Conduct Scenario-Based Behavioral Security Training shift training paradigms from static compliance videos to real-time simulations targeting MFA fatigue and AiTM phishing.

vi. Enforce Passwordless Authentication Protocols adopt FIDO2-compliant hardware keys or platform authenticators to replace legacy multi-factor prompts.

vii. Establish Automated Anomaly Challenge Protocols automatically flag and isolate session requests originating from conflicting locations or unauthorized proxies.

viii. Regularly Audit IAM and Authentication Logs implement automated monitoring to detect continuous prompt-reject cycles indicative of active fatigue attacks.

REFERENCES

1. Adeboye, O. K., & Williams, P. T. (2020). Beyond passwords: Evaluating the efficacy of multi-factor authentication in corporate cloud environments. Journal of Cybersecurity and Data Protection, 12(3), 145–162.
2. Al-Hassan, M., Al-Fuqaha, A., & Rayes, A. (2022). Human elements in cloud security: A survey on user habits, fatigue, and threat perception. IEEE Access, 10, 48211–48229.

3. Al-Maroof, R. S., Alhumaid, K., & Salloum, S. A. (2021). Acceptance of cloud computing systems in higher education: A systematic review. International Journal of Information Management Data Insights, 1(2), 100028.
4. Bello, A. O., & Mensah, K. A. (2021). The cognitive burden of security compliance: An empirical evaluation of employee authentication habituation. Computers & Security, 108, 102341.
5. Chen, Y., Zhang, L., & Liu, X. (2023). Zero trust security frameworks in enterprise cloud systems: A multi-layered identity approach. ACM Transactions on Privacy and Security, 26(2), 1–24.
6. Chinedu, P.U.; Maduabuchukwu, C.; Oghorodi, D.; & Nazrul Islam, M.S. (2025). Moving to the Cloud: A Review of the Impact and Strategies for Nigeria Digital Transformation. Nigerian. Journal of Engineering Science and Technology Research, 11(1): 251-257.
7. Foster, R., Gupta, S., & Vance, A. (2024). Context-aware authentication design: Reducing user friction while maintaining security integrity. International Journal of Human-Computer Studies, 181, 103150.
8. Gupta, A., & Martinez, C. (2022). Bridging the gap between cryptosystems and human behavior in cloud access management. Journal of Information Security and Applications, 68, 103210.
9. Johnson, M. R., & Zhao, H. (2021). Identity as the new security perimeter: Evaluating identity and access management in distributed cloud architectures. Cloud Computing and Security, 15(4), 312–329.
10. Kowalski, P., Nowak, M., & Wiśniewski, A. (2025). Adversary-in-the-middle (AiTM) phishing and MFA bypass techniques: Mechanics, mitigation, and empirical analysis. IEEE Transactions on Information Forensics and Security, 20, 1142–1156.
11. Li, H., Wang, Z., & Chen, J. (2022). Risk-based dynamic access control for enterprise multi-cloud environments. IEEE Transactions on Cloud Computing, 10(3), 1890–1903.
12. Nduka, C. E., & Abubakar, S. I. (2020). Superficial compliance versus actionable security: Analyzing user behavior in enterprise systems. African Journal of Information Systems, 12(1), 45–68.
13. O'Connor, S., & Evans, D. (2025). MFA prompt bombing and push notification fatigue: Quantifying enterprise security exposure. Computers & Security, 148, 104112.
14. Okonkwo, C. J., & Smith, J. L. (2023). Multi-Factor Authentication protocols: Evolution, vulnerabilities, and future directions in cloud environments. Cybersecurity, 6(1), 12.
15. Ramesh, U., & Kumar, P. (2021). User and entity behavior analytics (UEBA) in cloud environments: A machine learning approach to threat detection. Journal of Network and Computer Applications, 193, 103198.
16. Sorenson, K., & Larsson, E. (2022). Evaluating FIDO2 WebAuthn adoption in corporate IAM architectures. Information & Computer Security, 30(5), 712–728.
17. Thompson, E., & Davis, R. (2023). Social engineering the authentication layer: How fatigue attacks compromise multi-factor systems. Journal of Cybersecurity, 9(1), tzad004.
18. Toussaint, L., & Dubois, M. (2022). Balancing usability and security in cloud authentication interfaces: An empirical study. Interacting with Computers, 34(3), 201–215.
19. Williams, B., Taylor, K., & Miller, S. (2024). Dual-process psychological theory in cybersecurity: How system 1 thinking degrades authentication security. Human Factors, 66(2), 489–504.
20. Zhang, W., & Patel, N. (2024). The human perimeter: Analyzing post-MFA security risks in cloud infrastructure. IEEE Security & Privacy, 22(1), 34–43.