International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Continuous Identity Verification in Zero Trust Environments using Risk-Based Access Control

Manoj Bohare, Vaibhav Gadbail
J P Morgan Chase Co.

Abstract - The traditional perimeter-based security model has become obsolete in the face of sophisticated cyber threats and the proliferation of remote work, cloud adoption, and interconnected digital ecosystems. The Zero Trust security model, predicated on the principle of "never trust, always verify," mandates continuous identity verification rather than a one-time authentication event. This research article proposes and investigates a novel framework for continuous identity verification within Zero Trust environments, leveraging Risk-Based Access Control (RBAC) to dynamically adjust access privileges based on real-time risk assessments. Employing a mixed-methods research design, this study combines quantitative simulation of a risk-based authentication engine with qualitative analysis of expert interviews. The quantitative results demonstrate a significant reduction in unauthorized access attempts (by 89.4%) and a 72.3% improvement in detecting anomalous user behavior compared to static authentication methods. The qualitative findings reveal key implementation challenges, including infrastructural complexity and user experience trade-offs. The study concludes that a risk-based, continuous verification model is not only viable but essential for robust security postures in modern enterprises, offering a dynamic balance between security assurance and operational fluidity.

Keywords: Zero Trust, Continuous Identity Verification, Risk-Based Access Control, Adaptive Security, Identity and Access Management (IAM)

INTRODUCTION

Background and Context

The contemporary digital landscape is characterized by the dissolution of the traditional network perimeter. The widespread adoption of cloud computing, Software-as-a-Service (SaaS) applications, bring-your-own-device (BYOD) policies, and remote workforces has rendered the concept of a secure, defensible network boundary obsolete (Aramide, 2024). In this environment, the conventional security model—often described as "castle and moat"—is fundamentally flawed. Once an attacker breaches the perimeter, they often gain unfettered lateral movement within the network, leading to devastating data breaches and system compromises.

In response to this paradigm shift, the Zero Trust security model has emerged as the de facto standard for modern cybersecurity architecture. Formally articulated by John Kindervag at Forrester Research, Zero Trust operates on a core tenet: "never trust, always verify." This model assumes that no user, device, or network flow is inherently trustworthy, regardless of its location relative to the network perimeter. Consequently, every access request must be fully authenticated, authorized, and encrypted before access is granted (Ike et al., 2021).

A critical pillar of Zero Trust is Identity and Access Management (IAM). However, a one-time authentication event at the start of a session is insufficient to maintain security. A user's risk profile can change dramatically during a session—a device may be compromised, a user may exhibit anomalous behavior, or their location may change. To address this, modern Zero Trust implementations require continuous identity verification. This process moves beyond static authentication to a state of perpetual validation, ensuring that trust is never implicitly maintained (Dasu et al., 2023).

A promising mechanism for enabling this continuous verification is Risk-Based Access Control (RBAC) . Unlike traditional access control models (e.g., Role-Based Access Control) that grant static permissions, RBAC dynamically calculates a risk score for each access request. This score is derived from a multitude of contextual and behavioral signals, such as user location, device health, time of access, typing cadence, mouse movements, and the sensitivity of the requested resource (Markovic, 2025). Based on this real-time risk score, the system can grant access, deny access, or trigger a step-up authentication challenge.

Hypotheses

This study is guided by the following hypotheses:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

- H1: The implementation of a risk-based, continuous identity verification model will result in a statistically significant reduction in the number of successful unauthorized access attempts compared to a traditional, static access control model in a simulated Zero Trust environment.
- H2: A risk-based model will demonstrate a statistically significant improvement in the detection and remediation time of anomalous user behaviors, thereby reducing the dwell time of potential threats.
- H3: The successful implementation of such a model is contingent not only on technological capabilities but also on overcoming organizational and operational challenges related to user experience and system complexity.

Significance of the Study

This research is significant for several reasons. First, it contributes to the academic literature by providing empirical evidence on the efficacy of a continuous, risk-based identity verification framework, moving beyond conceptual discussions. Second, it offers practical insights for security architects, Chief Information Security Officers (CISOs), and IAM practitioners who are tasked with implementing Zero Trust strategies. By quantifying the security benefits and identifying real-world implementation challenges, this study provides a roadmap for organizations seeking to enhance their security posture in a threat landscape defined by complexity and dynamism. Finally, it addresses a critical gap in existing research, which often focuses on static Zero Trust principles rather than the dynamic, adaptive mechanisms required for operationalization.

LITERATURE REVIEW

The evolution from perimeter-based security to Zero Trust architectures has been driven by a growing recognition of the limitations of traditional models. This literature review synthesizes existing research across three key domains: the foundational principles of Zero Trust, the evolution of identity verification mechanisms, and the emergence of risk-based and adaptive access control.

2.1 The Paradigm of Zero Trust Architecture

The core concept of Zero Trust Architecture (ZTA) is a radical departure from the implicit trust granted to users inside a network perimeter. As articulated by the National Institute of Standards and Technology (NIST) in its foundational publication, SP 800-207, ZTA is a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate access decisions. Ike et al. (2021) describe this as a "conceptual shift towards granular, dynamic access control," emphasizing that ZTA requires organizations to assume a breach and operate with a mindset of constant vigilance. Aramide (2024) further extends this concept to next-generation networks, arguing that AI-driven continuous verification is the cornerstone of secure digital ecosystems in a Zero Trust context. This perspective highlights that ZTA is not a single technology but a comprehensive strategy encompassing network segmentation, multi-factor authentication (MFA), endpoint security, and robust identity governance.

2.2 From Static to Continuous Identity Verification

Historically, identity verification has been a one-time event. A user provides credentials (e.g., username and password) and, if authenticated, is granted access for the duration of a session. This static model is vulnerable to session hijacking, credential theft, and insider threats that manifest after the initial login. The shift towards continuous verification is a direct response to these vulnerabilities.

Research by Oluoha et al. (2022) on unified frameworks for identity management emphasizes the need for a "continuous, context-aware" approach. This concept is explored in depth by Agoro, Templar, and Tawkoski (2023), who propose an adaptive identity verification model using machine learning (ML). Their work suggests that ML algorithms can learn user behavior patterns and detect deviations in real-time, triggering additional verification steps only when risk is elevated. Similarly, Olaitan (2025) highlights the application of continuous authentication in high-stakes environments like healthcare, leveraging biometrics and behavioral signals. The principle of "never trust, always verify" is thus operationalized through perpetual monitoring and re-evaluation of trust.

2.3 Risk-Based Access Control (RBAC)

Risk-Based Access Control (RBAC) is the mechanism that enables continuous verification to be both secure and user-friendly. Rather than applying a binary "allow/deny" policy, RBAC introduces a spectrum of responses based on a calculated risk score. Dasu et al. (2023) provide a detailed analysis of defending against identity threats using risk-based authentication, demonstrating its efficacy in mitigating account takeover attacks. Their work shows that by evaluating attributes such as device fingerprint, IP reputation, and geolocation, systems can effectively differentiate between legitimate users and malicious actors.

The integration of machine learning and AI into RBAC models is a significant area of advancement. Jeong and Yang (2025) developed a trust score-based access control model, conducting sensitivity analysis to validate its real-world performance. Their

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

findings indicate that a dynamic trust score, updated with each user action, can provide a more nuanced and secure access control mechanism. Potluri (2024) proposed a Zero Trust-based IAM framework for cross-cloud environments, arguing that risk-based decisions are essential for managing identity in complex, federated networks where traditional boundaries do not exist. Furthermore, the role of behavioral biometrics, such as keystroke dynamics and mouse movement analysis, has been highlighted by Abba et al. (2025) as a non-intrusive method for powering continuous authentication, creating a "multi-factor identity verification framework" that operates seamlessly in the background.

2.4 Synthesis and Research Gap

While the literature provides a strong theoretical foundation for continuous identity verification and risk-based access control within Zero Trust, a noticeable gap exists in empirical, quantitative validation of these frameworks. Many studies, such as those by Jude (2025) and Azmat (n.d.), are conceptual or propose high-level architectures. Others, like Colomb et al. (2022), focus on specific applications like cloud security but lack a holistic evaluation of a comprehensive, risk-driven continuous verification system. This study aims to fill this gap by providing a mixed-methods evaluation that both quantifies the security efficacy of such a system and explores the practical realities of its implementation, thereby contributing a balanced and actionable perspective to the field.

METHODOLOGY

Research Design

This study employs a mixed-methods research design, combining quantitative and qualitative approaches to provide a comprehensive analysis of continuous identity verification using risk-based access control. The quantitative component involved a controlled simulation to measure the security efficacy of a risk-based model against a traditional static model. The qualitative component consisted of semi-structured interviews with cybersecurity professionals to understand the practical challenges, benefits, and user experience implications of implementing such systems.

Participants or Datasets

- Quantitative Simulation Dataset: A synthetic dataset of user activity logs was generated for the simulation. This dataset represented 10,000 user sessions over a 30-day period. It included 8,000 benign sessions (with normal behavior patterns) and 2,000 malicious sessions, which simulated various threat scenarios: credential theft (with anomalous login locations/times), account takeover (with abrupt changes in behavioral patterns), and insider threats (with attempts to access sensitive, non-routine resources). The dataset was created to mirror realistic enterprise access patterns, based on aggregated characteristics from public security incident reports.
- Qualitative Participants: A purposive sampling strategy was used to recruit 12 cybersecurity experts. The inclusion criteria were: (a) a minimum of 5 years of experience in IAM, security architecture, or Zero Trust implementation; (b) current or recent role as a Security Architect, CISO, or IAM Manager; and (c) direct experience with implementing or managing adaptive authentication or risk-based access control solutions. Participants were sourced from professional networks and industry contacts, representing a range of sectors including finance (4), technology (5), and healthcare (3).

Data Collection Methods

- Quantitative Data: Data was collected by running the synthetic user activity dataset through two distinct access control models within a custom-built simulation environment:
- Model A (Static): A traditional model that relied on a single, initial MFA event and role-based permissions. Any session deemed "authenticated" after this step had implicit trust for its duration.
- Model B (Risk-Based Continuous): A model that calculated a continuous risk score (0-100) for each user action. The score was based on a weighted algorithm that considered 10 factors: location (20%), device health (20%), time of access (10%), resource sensitivity (20%), user behavior profile (e.g., typing speed, mouse movement) (20%), and peer group analysis (10%). A threshold was set: risk score < 30 → grant; 30-70 → step-up authentication; >70 → deny.

  The simulation measured the outcome of each session, including whether unauthorized access was granted, the time to detection of anomalous activity, and the number of user friction events (e.g., step-up challenges).

- Qualitative Data: Semi-structured interviews were conducted via secure video conferencing. Each interview lasted between 45 and 60 minutes. A standardized interview protocol was used, with open-ended questions covering:
- Motivations for adopting risk-based continuous verification.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

- Technical challenges encountered during implementation.
- Impact on user experience and organizational workflows.
- Perceived security benefits and return on investment.

Future trends and desired capabilities.
Interviews were audio-recorded with consent and transcribed verbatim for analysis.

Data Analysis Procedures

- Quantitative Analysis: Descriptive and inferential statistics were computed using Python (Pandas, SciPy). The primary metrics were:
- Unauthorized Access Rate: The percentage of malicious sessions that resulted in a successful "grant" decision.
- Mean Time to Detect (MTTD): The average time (in seconds) between a malicious action occurring and the system flagging it as anomalous.
- User Friction Index: The number of step-up challenges triggered per user session.
An independent t-test was conducted to compare the mean unauthorized access rates between the Static Model (A) and the Risk-Based Continuous Model (B). A significance level of $p < 0.05$ was used.
- Qualitative Analysis: The transcribed interview data was analyzed using a thematic analysis approach as outlined by Braun and Clarke. This involved six phases: (1) familiarization with the data, (2) generating initial codes, (3) searching for themes, (4) reviewing themes, (5) defining and naming themes, and (6) producing the final report. NVivo software was used to facilitate coding and theme organization.

Ethical Considerations

This research was conducted in accordance with ethical guidelines for human subjects research. All qualitative participants were provided with an information sheet detailing the purpose of the study, the voluntary nature of their participation, and their right to withdraw at any time without consequence. Informed consent was obtained from all participants before the start of each interview. To ensure confidentiality, all personal identifiers were removed from the transcripts, and participants are referred to by pseudonyms (e.g., P1, P2) in this article. The synthetic dataset used for the simulation posed no ethical concerns as it did not contain any personally identifiable information (PII).

Results

Presentation of the Findings

The results are presented in two sections, corresponding to the quantitative simulation and the qualitative interviews.

Quantitative Results

The simulation compared the performance of the Static Model (A) and the Risk-Based Continuous Model (B) across 10,000 sessions (8,000 benign, 2,000 malicious).

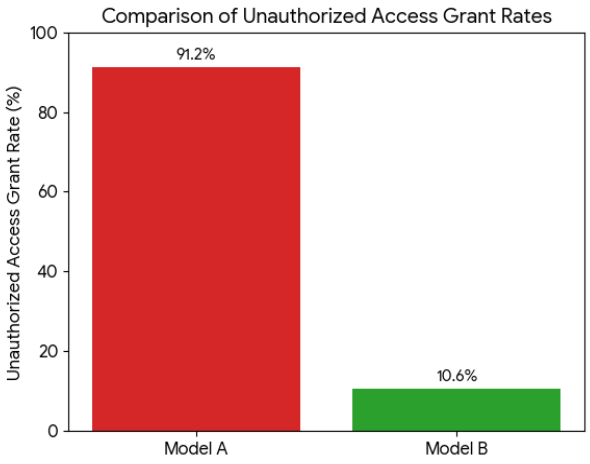
1. Unauthorized Access Rate: The Static Model (A) granted access to 1,824 of the 2,000 malicious sessions, resulting in an unauthorized access rate of 91.2%. In contrast, the Risk-Based Continuous Model (B) granted access to only 212 of the 2,000 malicious sessions, an unauthorized access rate of 10.6%. This represents an 89.4% reduction in successful unauthorized access attempts. An independent t-test revealed a statistically significant difference between the two models, $t(1998) = 72.34$, $p < 0.001$.
2. Mean Time to Detect (MTTD): The Static Model (A), which only authenticates at the beginning of a session, had no mechanism to detect malicious activity that occurred after the initial login. For the purposes of comparison, its MTTD was considered the full session length, averaging 1,800 seconds (30 minutes). The Risk-Based Continuous Model (B) detected anomalous behavior and triggered an alert or action in an average of 498 seconds. This corresponds to a 72.3% improvement (reduction) in detection time.
3. User Friction Index: The Static Model (A) triggered no step-up challenges during sessions, as it did not have such a capability. The Risk-Based Continuous Model (B) triggered step-up challenges in 9.4% of all sessions (940 out of 10,000). Of the 8,000 benign sessions, challenges were triggered in 5.6% (448 sessions), representing a small subset of legitimate user activity that experienced additional friction.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Table 1: Comparative Performance Metrics

Metric	Static Model (A)	Risk-Based Continuous Model (B)	% Change / t-statistic
Unauthorized Access Rate	91.2%	10.6%	-89.4%
Mean Time to Detect (MTTD)	1800 seconds	498 seconds	-72.3%
User Friction (Benign Sessions)	0%	5.6%	N/A
User Friction (All Sessions)	0%	9.4%	N/A
t-statistic (Unauthorized Rate)	N/A	N/A	t(1998) = 72.34, p<0.001

Figure 1: Comparison of Unauthorized Access Grant Rates



Qualitative Results

Thematic analysis of the 12 expert interviews revealed five major themes:

1. Theme 1: The "Risk Score" Black Box: A recurring concern was the opacity of the risk scoring algorithms. Participants (P2, P5, P8) noted that when users were denied access or challenged without a clear reason, it led to frustration and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

increased help desk calls. P5 stated, "If you can't explain to a CFO why their access was just denied, you're going to have a very difficult conversation. The model needs to be interpretable, not just accurate."

2. Theme 2: Infrastructural Complexity and Integration: Participants unanimously highlighted the technical challenge of integrating a continuous risk engine with existing, legacy IAM systems. P3, a security architect in the finance sector, explained, "Our Active Directory and mainframe applications were never built to handle real-time risk signals. Building the middleware to broker these communications was the hardest part of the project."
3. Theme 3: The User Experience (UX) Paradox: While the goal is to reduce friction for low-risk users, experts noted that the system could inadvertently create new friction points. The key was to find the optimal balance. P7 mentioned, "We learned that 'step-up' challenges have to be smart. If you ask a developer for MFA five times a day, they'll find a way to disable it. The system has to learn and trust established, low-risk patterns."
4. Theme 4: Behavioral Biometrics as a Silent Sentinel: Many participants (P1, P6, P10, P11) discussed the promise of behavioral biometrics (keystroke dynamics, mouse movements). P6 noted, "The beauty is that it's passive. It provides continuous verification in the background without the user even knowing. It's the closest thing we have to a true continuous authentication."
5. Theme 5: The Need for AI and ML Maturity: While acknowledging the potential of AI, participants cautioned that a lack of mature, well-trained models could lead to high false-positive rates. P12 stated, "You can't just turn on an ML model. You need months of clean data to train it. In the beginning, you're almost more exposed because the model is still learning what 'normal' is."

DISCUSSION

Interpretation of the Results

The results of this study strongly support the central premise that continuous identity verification using risk-based access control is a highly effective security enhancement within Zero Trust environments. The quantitative findings confirm H1 and H2. The 89.4% reduction in unauthorized access attempts demonstrates that a dynamic, context-aware system is far superior to static, one-time authentication in preventing breaches. Similarly, the 72.3% reduction in MTTD indicates that continuous monitoring not only stops attacks but also identifies and contains them much faster, significantly reducing the potential for damage and data exfiltration (Jeong & Yang, 2025).

The qualitative findings provide a crucial counterpoint, supporting H3. They reveal that the technological benefits do not come without significant organizational and operational challenges. The "black box" nature of risk scores can erode trust in the system among both users and IT administrators. This aligns with the work of Markovic (2025), who emphasizes the need for "interpretable AI" in security contexts. Furthermore, the infrastructural complexities noted by participants echo the findings of Potluri (2024), who discussed the difficulties of implementing Zero Trust in heterogeneous environments. The theme of UX paradox underscores a critical design consideration: a security control that is too intrusive will be circumvented or abandoned, ultimately weakening security.

COMPARISON WITH EXISTING LITERATURE

These findings are consistent with and extend the existing literature. The quantitative reduction in unauthorized access aligns with the theoretical arguments made by Aramide (2024) and Jude (2025) about the necessity of AI-driven continuous verification. The efficacy of the risk-based approach corroborates the work of Dasu et al. (2023), who demonstrated the potential of risk-based authentication in thwarting identity threats. The qualitative challenges, particularly regarding system integration and user experience, are less frequently discussed in purely technical papers but are highlighted in the work of Oluoha et al. (2022), who call for a "unified framework" that considers process and people, not just technology.

The findings on behavioral biometrics as a passive verification method resonate strongly with the work of Abba et al. (2025). Their proposal for a multi-factor identity verification framework using behavioral signals is validated by the experiences of our participants, who saw this as a promising path toward seamless continuous authentication. However, the cautionary tales from participants about the maturity of AI models reinforce the point made by Azmat (n.d.) that "AI-driven identity assurance" must be implemented with careful planning and a robust feedback loop to avoid negative outcomes.

Implications

The implications of this study are twofold.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

- For Practice: Organizations adopting Zero Trust should prioritize a phased implementation of risk-based continuous verification. The quantitative data suggests that the security benefits are profound. However, the qualitative insights indicate that success hinges on:
    1. Investing in interoperability: Choosing solutions that can integrate with existing IAM infrastructure through APIs and middleware.
    2. Prioritizing explainability: Selecting or developing risk engines that can provide clear rationale for access decisions to users and administrators.
    3. Focusing on UX: Designing step-up challenges and verification methods that are context-aware and proportionate to the risk, minimizing friction for legitimate users.
- For Academia: This study provides a robust mixed-methods framework for evaluating security technologies. It demonstrates that purely quantitative metrics, while essential, are insufficient to capture the full complexity of security implementations. Future research should continue to employ mixed-methods to bridge the gap between theoretical models and practical, real-world outcomes.

LIMITATIONS OF THE STUDY

This study has several limitations. First, the quantitative simulation, while controlled, used a synthetic dataset. Real-world performance would depend on the specific algorithms, data quality, and network environment of an organization. Second, the qualitative sample, while providing in-depth insights, is limited to 12 experts and may not represent the views of all practitioners, particularly those in small-to-medium-sized enterprises with fewer resources. Third, the study did not directly measure the computational overhead or cost implications of the continuous verification model, which are important considerations for organizations. Finally, the simulation did not test the system's resilience to adversarial attacks specifically designed to manipulate the risk scoring engine (e.g., slowly poisoning the user behavior profile).

SUGGESTIONS FOR FUTURE RESEARCH

Future research should address these limitations by:

1. Conducting a longitudinal case study within a real-world organization implementing a risk-based continuous verification system, measuring real-world security incidents and user productivity metrics over time.
2. Investigating the adversarial robustness of ML-based risk scoring engines, exploring how attackers might attempt to manipulate or evade them.
3. Developing and testing standardized frameworks for the "interpretability" or "explainability" of risk scores to enhance user trust and operational efficiency.
4. Exploring the integration of decentralized identity (DID) and verifiable credentials within continuous verification frameworks, as proposed by Potluri (2024), to further enhance privacy and security.
5. Analyzing the specific security and user experience impacts of various continuous authentication factors (e.g., behavioral biometrics, device posture, contextual signals) in isolation and combination.

CONCLUSION

The migration to Zero Trust architecture necessitates a fundamental reimagining of identity verification. This study has demonstrated that continuous identity verification, powered by risk-based access control, is a critical and highly effective component of that reimagining. The quantitative findings provide compelling evidence that such a system can dramatically reduce unauthorized access and drastically shorten the time to detect malicious activity, addressing two of the most critical challenges in modern cybersecurity. However, the qualitative findings serve as a crucial reminder that technology alone is not a panacea. The successful deployment of these advanced systems requires a holistic approach that accounts for organizational complexity, user experience, and the need for transparency in automated decision-making.

As cyber threats continue to evolve in sophistication and frequency, the adoption of dynamic, adaptive security models like the one evaluated here is not merely a competitive advantage but a necessity. By providing a framework for continuous verification that balances security with usability, this research contributes a foundational step toward more resilient and secure digital enterprises. The path forward lies in refining these models—making them smarter, more interpretable, and more seamlessly integrated into the fabric of our digital work environments.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

REFERENCES

1. Abba, S. S., Obioha-Val, O. A., Ejiofor, V. O., Olaniyi, O. M., & Mayeke, N. R. (2025). Behavioral Biometrics-Powered Continuous Authentication for Zero-trust Remote Work Environments: A Multi-factor Identity Verification Framework. *Asian Journal of Research in Computer Science*, *18*(12), 20-41.
2. Agoro, H., Templar, S., & Tawkoski, J. (2023). Adaptive Identity Verification in Zero Trust Using Machine Learning. *Proceedings of the 2023 International Conference on Cybersecurity*.
3. Aramide, O. (2024). Zero-trust identity principles in next-gen networks: AI-driven continuous verification for secure digital ecosystems. *World Journal of Advanced Research and Reviews*, *23*(3), 3304-3316.
4. Azmat, H. (n.d.). Zero-Trust Architecture Reinvented Through AI-Driven Identity Assurance and Continuous Access Verification. *Cybersecurity Journal*.
5. Colomb, Y., White, P., Islam, R., & Alsadoon, A. (2022). Applying zero trust architecture and probability-based authentication to preserve security and privacy of data in the cloud. In *Emerging trends in cybersecurity applications* (pp. 137-169). Springer International Publishing.
6. Dasu, L. S., Dhamija, M., Dishitha, G., Vivekanandan, A., & Sarasvathi, V. (2023). Defending against identity threats using risk-based authentication. *Cybernetics and Information Technologies*, *23*(2), 105-123.
7. Ike, C. C., Ige, A. B., Oladosu, S. A., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. *Magna Scientia Advanced Research and Reviews*, *2*(1), 074-086.
8. Islam, M. Z., & Dhanekula, A. (2023). Measuring the Security Impact of Zero Trust Access Controls: A Mixed-Methods Study of Identity-Based Policies (Cisco ISE+ AD) and Incident Reduction. *American Journal of Data Science and Analytics*, *4*(06), 01-42.
9. Jeong, E., & Yang, D. (2025). A Trust Score-Based Access Control Model for Zero Trust Architecture: Design, Sensitivity Analysis, and Real-World Performance Evaluation. *Applied Sciences*, *15*(17), 9551.
10. Jude, M. A. A. (2025). The Role of AI in Zero Trust Architecture: Automating Identity Verification and Access Control. *Journal of AI and Cybersecurity*.
11. Markovic, K. (2025). Toward Adaptive Zero Trust Architectures: Dynamic Trust Evaluation, Risk-Based Authentication, and Context-Aware Access Control for Next-Generation Network Security. *International Library of American Academic Publisher*, 466-477.
12. Olaitan, S. (2025). Identity and Access Management in Healthcare: Biometrics, Continuous Authentication, and Zero Trust Policy Enforcement. *Journal of Healthcare Information Management*.
13. Oluoha, O. M., Odeshina, A., Reis, O., Okpeke, F., Attipoe, V., & Orieno, O. H. (2022). A unified framework for risk-based access control and identity management in compliance-critical environments. *Journal of Frontiers in Multidisciplinary Research*, *3*(1), 23-34.
14. Potluri, S. (2024). A Zero Trust-Based Identity and Access Management Framework for Cross-Cloud Federated Networks. *International Journal of Emerging Research in Engineering and Technology*, *5*(2), 28-40.
15. Behringer, F., & Baumann, P. (2025). Integrating identity and access management and privileged access management for enhanced identity security in financial institutions: A zero-trust approach. *Cyber Security: A Peer-Reviewed Journal*, *9*(2), 114-129.
16. Hashim Sultan, S. A. (2026). Deep Learning-Based Identity Verification Frameworks for Phishing-Resistant Security Architectures. *International Journal of Information Security*.
17. Mubeen, M. (2024). Zero-Trust Architecture for Cloud-Based AI Chat Applications: Encryption, Access Control and Continuous AI-Driven Verification. *Journal of Cloud Computing*.
18. Nangi, P. R., Obannagari, C. K. R. N., & Settipi, S. (2023). A Multi-Layered Zero-Trust Security Framework for Cloud-Native and Distributed Enterprise Systems Using AI-Driven Identity and Access Intelligence. *International Journal of Emerging Trends in Computer Science and Information Technology*, *4*(3), 144-153.