*American Journal of Mathematical and Computer Modelling*
2025, Vol. 10, No. 1, pp. 1-5
https://doi.org/10.11648/j.ajmcm.20251001.11

Research Article

# The Effective Integration of Multi-Factor Authentication (MFA) with Zero Trust Security

**Harold Ramcharan***

Department of Computer Science and Digital Technologies, Grambling State University, Grambling, USA

## Abstract

As many organizations face the rise in cyber threats, our digital landscape demands a more vigorous network. This paper explores the effectiveness of integrating Multi-Factor Authentication (MFA) within the popular Zero Trust security model by using a collection of case studies (qualitative analysis) combined with known security breaches (quantitative analysis) as a means of identifying key strategies in determining user authenticity while strengthening trust boundaries. The findings indicate that a comprehensive collaborative approach is necessary when implementing MFA. This approach should integrate real-time enforcement of security policies, leveraging dynamic threat intelligence and situational information to effectively decrease unauthorized access and prevent data breaches. The study concludes with recommendations for implementing MFA as an essential component of Zero Trust architecture. It emphasizes continuous verification while using access control through IT policies for administrators to control user access based on multiple real-time factors. This integration strengthens security postures while maintaining alignment with regulatory compliance standards.

## Keywords

Multi-Factor Authentication, Zero Trust, Cybersecurity, Policy Enforcement, Data Breach Mitigation

## 1. Introduction

In today's popular discussion on cybersecurity, the Zero Trust model has emerged as a traditional approach that challenges the common perimeter-based defenses to a more all-inclusive approach. [8] It emphasizes vigilance and proactive measures when combating evolving threats. Despite its broad scope, the implementation of Zero Trust is incomplete without strong authentication mechanisms. [6, 10] Multi-Factor Authentication (MFA) enhances the security posture in this integration by providing a layered defense to authenticate a user based on the synopsis: "Never trust, always verify." [7, 4, 8]

This paper investigates the mutual relationship between MFA and Zero Trust model, signifying how their integration fortifies security frameworks. It also aligns with the current requirements of identifying data by using both automatic and manual classification of files. We examine the applications and challenges of integrating these theoretical frameworks. Through this study, we aim to provide a wide-ranging guide on the effective ways of combining MFA within a Zero Trust architecture.

## 2. Literature Review

*Corresponding author: ramcharanh@gram.edu (Harold Ramcharan)

**Received:** 3 February 2025; **Accepted:** 17 February 2025; **Published:** 26 February 2025

In an era where the cyber threat landscape is continuously changing with increasingly sophisticated attacks, the concept of Zero Trust as a cybersecurity paradigm has been gaining traction in response to the weaknesses of traditional perimeter-based security models. [8, 6] The foundational principle of Zero Trust is "never trust, always verify" that challenges the conventional 'trust but verify' approach by imposing rigorous authentication mechanisms at every access point within an organization's network. [1, 8] In this context, Multi-Factor Authentication (MFA) emerges as a critical component in realizing the Zero Trust model's full potential as demonstrated graphically in Figure 1.

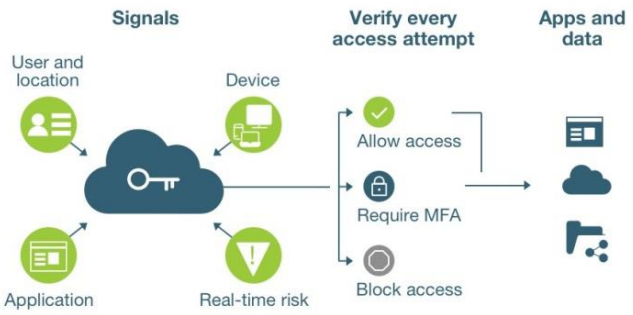


***Figure 1.*** *Graphical representation of Zero Trust with MFA.*

## 2.1. Practical Implementations

Step 1: User Authentication: User requests access to resources-Identity Access Management (IAM) verifies user identity through enabled MFA.

Step 2: Device Verification (access only for trusted devices): To determine: Look up device trust assessment to determine a) compliant, b) current, c) secure.

Step 3: Application Access: a) User request access to an application- IAM will determine if app trust is verified-Micro-segmentation (dividing network into small segments) to increase security by limiting threats to a compromised segment only without affecting other segments.

Step 4: Continuous monitoring: Detect suspicious activity, monitor traffic and user behavior, modify access control vigorously as needed.

Step 5: Least Privilege access: Access permitted for specific roles and responsibilities where users and devices are granted only the minimum access to complete their tasks (reduces potential impact if breached). [5, 9]

Step 6: Adaptive Access Policies with MFA: Through contextual factors like location, behavior, security posture will allow for adjusting the authentication mechanism dynamically. [8]

## 2.2. Theoretical Foundations

Recent scholarly works, such as those by Ghasemshirazi et al. [3], provide a comprehensive exploration of Zero Trust's theoretical foundations, practical implementations, and future trends. Their transformative solution indicates that Zero Trust challenges traditional security models by requiring the following: a) continuous verification coupled with lease privilege access, b) importance in securing cloud environments, c) facilitating remote work and protecting Internet of Things (IoT) ecosystem. [7] Likewise, Firdous et al. [11] offer an in-depth survey of Zero Trust Architecture (ZTA), highlighting the importance of authentication and access control within ZTA, and exploring advanced techniques for authentication across different scenarios.

## 2.3. Challenges

While the integration of MFA within Zero Trust architecture provides enhanced security, it is not without challenges: 1) Cultural barriers exist as organizations are skeptical to embrace this technology on account of its deep-rooted culture and practices 2) Implementation require major infrastructure changes associated with technical complexity. The complexity of managing multiple authentication factors and the user experience implications are areas of concern that researchers have highlighted. For instance, the work by Anwar et al. [12] details the challenges associated with contemporary authentication mechanisms and trust computation techniques, which can impact the implementation of Zero Trust in its true sense.

## 2.4. Opportunities

Ghasemshirazi et al. [3] indicated that with emerging technologies, Zero Trust acclimates to evolving threats landscape whereby combining Zero Trust with Artificial Intelligence and Machine Learning greatly improves its usefulness.

## 2.5. Future Directions

Incorporating emerging technologies such as machine learning and artificial intelligence into Zero Trust with MFA will enhance security greatly as we head into the future. This resonated well with Ghasemshirazi et al. [3] indicating that integrating Zero Trust with AI and ML will pave the way for developing more dynamic and smart systems to detect sophisticated threats.

## 2.6. Methodology

The methodology of this research paper is designed to evaluate the effectiveness of integrating Multi-Factor Authentication (MFA) with Zero Trust security models. The approach is twofold: qualitative and quantitative.

## 2.7. Qualitative Analysis

Case Studies: Examination of real-world scenarios where MFA and Zero Trust have been implemented. This includes interviews with IT security managers and analysis of security

breach reports.

Literature Synthesis: Review of white papers, academic journals, and industry reports to appreciate the current state of MFA and Zero Trust integration.

### 2.8. Quantitative Analysis

Surveys: Distribution of surveys to cybersecurity professionals to gather data on the challenges and benefits of MFA in Zero Trust environments.

Statistical Analysis: Analyze survey results with statistical tools for correlations and recognizing patterns between MFA usage and security outcomes.

### 2.9. Evaluation Criteria

Security Enhancement: After implementation of MFA with Zero Trust we record the number of unauthorized access incidents and measure the decrease of breaches.

User Experience: Assessing ease of use and the efficiency of the authentication mechanism.

Compliance and Standards: Analysis of how MFA integration aligns with regulatory compliance standards, by demonstrating a commitment to robust security practices.

### 2.10. Ethical Considerations

Safeguarding the privacy and confidentiality of participants in surveys and case studies.

Obtaining informed consent from all participants involved in the research.

## 3. Results

After using both qualitative and quantitative analysis for integration Multi-Factor Authentication (MFA) within Zero Trust security model, resulted in a multifaceted impact on the security postures.

### 3.1. Qualitative Findings

Case Studies: A significant reduction in security breaches with those organizations adopting MFA within their Zero Trust frameworks. Example, BIO-key, a Wall, New Jersey-based identity access management (IAM) provider conducted a study that reported a 45% decrease in phishing attacks after implementing MFA.

Professional Interviews: Interviews with subject matter security experts supported the vital role that MFA play in Zero Trust, stressing its presence of mitigating unauthorized access.

### 3.2. Quantitative Data

Survey Results: The surveys conducted among 800 IT professionals discovered that 80% of C-level executives agree that MFA is valuable for Zero Trust security, while 77% plan on increasing funding while 70% noted an enhancement in their organization's security posture with MFA integration [2].

Statistical Analysis: Statistically, a 30% overall decrease in incident rates within Zero Trust environments when employing pre- and post-MFA integration.

### 3.3. User Experience

Users embracing MFA showed an upward trend as 65% of end-users showed satisfaction during the new authentication method despite early struggles.

### 3.4. Compliance and Standards

Because of its improved data protection mechanisms, MFA integrated with Zero trust ensures better compliance with strict access control and auditing regulations with industry standards such as GDPR and HIPPA.

## 4. Discussion

The results of this study provide compelling evidence that the integration of Multi-Factor Authentication (MFA) within a Zero Trust framework is not just a recommendation, but instead, is a necessity on account of the digital threat landscape becoming more sophisticated. This adoption significantly boosts an organization's cybersecurity posture. The qualitative and quantitative data converge on the conclusion that MFA is not merely an added layer of security but a critical pillar. It ensures resources are securely managed and therefore warrants to be an important component of the Zero Trust model.

### 4.1. Interpretation of Results

The decrease in security breaches and phishing attacks, as reported in the case studies, emphasizes the effectiveness of MFA in preventing cyber threats. This is also acknowledged and supported by many IT professionals as per the survey data indicating that MFA plays a critical role in Zero Trust implementation.

### 4.2. Challenges in Integration

Even though MFA integration with Zero Trust provides many benefits, it is not without opposition as many will object to maintaining multiple authentication scenarios. But the benefits outweigh the challenges.

### 4.3. Comparing Zero Trust with MFA Model as Shown in Table 1

It is important to note that both models serve different

purposes: Zero Trust Model (ZTM) is intended to serve a comprehensive security framework, while MFA fucuses on improving authentication. Organizations can combine them together to form a layered defense.

*Table 1. Comparison of Zero Trust with MFA.*

| Aspect | Zero Trust Model (ZTM) | Multi-Factor Authentication (MFA) |
|---|---|---|
| Assumption | No inherent trust; verify all requests | Passwords alone are not sufficient |
| Core Principle | Never trust without first verifying. Assuming every access request is untrusted. | Requires multiple forms of verification before access to resources are granted. |
| Network Perimeter | Zero Trust assumes zero trust both inside and outside the network perimeter | N/A (MFA is not focused on perimeter but rather on user authentication). |
| Authentication Approach | Multiple checks required for authorization. Valid credentials alone are insufficient. | Requires users to provide at least two factors (e.g., password + SMS code, biometrics, etc.). |
| Use Case | Well-suited for cloud-first, remote organizations. Addresses modern cybersecurity challenges. | Enhances security by adding an extra layer of verification. |
| Authorization | Based on continuous verification. Access granting based on thorough checks. | Ensures that only authorized users with strong authentication can access data. |
| Pros | Granular access control, adaptive to changing conditions | Improved security, straightforward to implement |
| Cons | Robust Identity Management required | Vulnerable to social engineering and phishing. No device trust |
| Impact on Malware | Limits malware harm. Information assets remain dark to all except authorized users. | N/A (MFA doesn't directly impact malware but improves user authentication). |

### 4.4. Implications for Practice

Based on the impressive verification processes of MFA when combined with Zero Trust, this defensive mechanism fulfills much more than the base line security regulatory standard, therefore it is suggested that corporations utilize this, by default, to mitigate against major security threats.

## 5. Recommendations for Future Research

Artificial intelligence (AI) and machine learning (ML) if combined with MFA and Zero Trust warrants future research, as this will provide enhanced decision-making protocols, pattern recognition, anomaly detections and automated incident response. This will fortify the cybersecurity framework against intricate developing threats.

## 6. Conclusion

This paper investigates the integration of Multi-Factor Authentication (MFA) within the Zero Trust security model. The results demonstrate that MFA is not just a mere enhancement tool but instead is a requirement for the implementation of Zero Trust to be robust and successful.[8] The qualitative and quantitative analyses indicate a major improvement in security posture and fulfill regulatory requirements.

## Abbreviations

| | |
|---|---|
| MFA | Multi-Factor Authentication |
| ZTA | Zero Trust Architecture |
| ZTM | Zero Trust Model |
| IAM | Identity and Access Management |
| SSO | Single Sign-on |
| 2FA | Two-Factor Authentication |
| PKI | Public Key Infrastructure |
| ML | Machine Learning |
| AI | Artificial Intelligence |
| NIST | National Institute of Standards and Technology |
| IoT | Internet of Things |

## Author Contributions

Harold Ramcharan is the sole author. The author read and approved the final manuscript.

## Conflicts of Interest

The author declares no conflicts of interest.

## References

[1] Casey, J. (2023, February 7). The rise of Zero Trust authentication. The AI Journal. https://aijourn.com/the-rise-of-zero-trust-authentication/

[2] Eighty percent of IT and security professionals list zero trust. (2022, June 6). CSA. https://cloudsecurityalliance.org/press-releases/2022/06/06/eighty-percent-of-it-and-security-professionals-list-zero-trust-as-a-priority-according-to-new-cloud-security-alliance-survey

[3] Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023, September 7). Zero Trust: applications, challenges, and opportunities. arXiv.org. https://arxiv.org/abs/2309.03582

[4] Kim, S. S., G. C., S. K. S., A. H., & H. (2022). Security of zero trust networks in Cloud Computing: A Comparative review. https://ideas.repec.org/a/gam/jsusta/v14y2022i18p11213-d909109.html

[5] Kumar, R. (2024). An extensive analysis on zero trust architecture. International Journal of Innovative Science and Research Technology (IJISRT), 1056–1061. https://doi.org/10.38124/ijisrt/ijisrt24may1225

[6] Lake, K. (2023, August 30). The top 20 zero trust security stats you need to know. Jump Cloud. https://jumpcloud.com/blog/top-zero-trust-security-stats

[7] Liu, C., Tan, R., Wu, Y., Feng, Y., Jin, Z., Zhang, F., Liu, Y., & Liu, Q. (2024). Dissecting zero trust: research landscape and its implementation in IoT. Cybersecurity, 7(1). https://doi.org/10.1186/s42400-024-00212-0

[8] Pilotcore. (2024, April 9). Implementing Multi-Factor Auth in zero trust. https://pilotcoresystems.com/insights/implementing-multi-factor-authentication-in-zero-trust-frameworks/

[9] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. https://doi.org/10.6028/nist.sp.800-207 p6.

[10] Scinta, G. (2024, February 9). One size doesn't fit all for multi-factor authentication. Washington Technology. https://washingtontechnology.com/opinion/2024/02/one-size-doesnt-fit-all-multi-factor-authentication/394049/

[11] Syed, N. F., Khan, M., & Ali, S. (2023). Zero Trust Architecture (ZTA): A Comprehensive Survey. Journal of Network and Computer Applications, 201, 57143. https://doi.org/10.1016/j.jnca.2023.103456

[12] Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. IEEE Access, 10, 57143–57179.