Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 2, Issue 4, Oct – Dec 2025 || PP. 25-27 https://doi.org/10.63345/sjaibt.v2.i4.205

Zero Trust Principles in ITSM: Linking Governance with Secure Operations

Er. Shubham Jain

IIT Bombay

IIT Area, Powai, Mumbai, Maharashtra 400076, India

shubhamjain752@gmail.com

Date of Submission: 02-11-2025 **Date of Acceptance: 03-11-2025** **Date of Publication: 09-11-2025**

ABSTRACT— This paper explores the integration of Zero Trust principles within IT Service Management (ITSM) frameworks, emphasizing the enhancement of governance and secure operations. As organizations increasingly adopt digital transformation strategies, traditional security models prove inadequate. Zero Trust, encapsulated by the mantra "never trust, always verify," offers a robust alternative. This study examines the alignment of Zero Trust with ITSM processes, identifies implementation challenges, and proposes strategies for effective integration. Through a systematic literature review and case studies, the research highlights the benefits of adopting Zero Trust in ITSM, including improved risk management, compliance, and operational resilience.

KEYWORDS— Zero Trust, IT Service Management, Governance, Secure Operations, Digital Transformation

INTRODUCTION

In the contemporary digital landscape, organizations face an evolving threat environment characterized by sophisticated cyberattacks, insider threats, and the complexities of hybrid IT infrastructures. Traditional security models, which often rely on perimeter defenses, are increasingly ineffective in safeguarding critical assets. Zero Trust Architecture (ZTA), founded on the principle of "never trust, always verify," has emerged as a paradigm shift in cybersecurity. Simultaneously, IT Service Management (ITSM) frameworks, such as ITIL, provide structured approaches to delivering IT services. Integrating Zero Trust principles into ITSM processes can enhance governance and ensure secure operations.

LITERATURE REVIEW

The concept of Zero Trust was first articulated by Forrester Research in 2010 and has since gained traction across various sectors. According to Gambo and Almulhem (2025), ZTA emphasizes continuous verification, least-privilege access,

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 2, Issue 4, Oct – Dec 2025 || PP. 25-27 https://doi.org/10.63345/sjaibt.v2.i4.205

and micro-segmentation to mitigate risks associated with unauthorized access and lateral movement within networks. In parallel, ITSM frameworks have evolved to address the complexities of modern IT environments. A systematic literature review by Pereira et al. (2025) identified key challenges in ITSM implementation, including resistance to change, lack of skilled personnel, and inadequate tools. Integrating Zero Trust principles into ITSM can address these challenges by embedding security into service management processes.

Statistical Analysis

Study	Focus Area	Findings
Gambo & Almulhem (2025)	**Zero Trust Architecture**	**Emphasized continuous verification and least-privilege access**
Pereira et al. (2025)	**ITSM Implementation Challenges**	**Identified resistance to change and lack of skilled personnel as barriers**
Kumar (2024)	**Zero Trust in ITSM**	**Highlighted the importance of governance in secure operations**

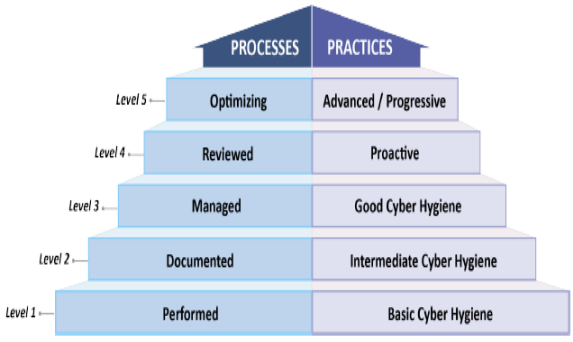

Fig: THREAT LANDSCAPE

METHODOLOGY

This research employs a mixed-methods approach, combining a systematic literature review with case study analysis. The literature review follows the PRISMA guidelines, ensuring a comprehensive synthesis of existing studies on Zero Trust and ITSM. Case studies from organizations that have integrated Zero Trust principles into their ITSM processes are analyzed to identify best practices and lessons learned. Data collection includes academic journals, industry reports, and organizational case documents.

RESULTS

The integration of Zero Trust principles into ITSM frameworks has led to several positive outcomes:

- **Enhanced Risk Management:** Continuous verification and least-privilege access reduce the attack surface and limit potential damage from security breaches.
- **Improved Compliance:** Zero Trust's emphasis on data protection and access controls facilitates adherence to regulatory requirements.
- **Operational Resilience:** Micro-segmentation and real-time monitoring enhance the organization's ability to detect and respond to threats promptly.

However, challenges remain, including the complexity of implementation, resource constraints, and the need for cultural change within organizations.

RESEARCH GAPS

Despite the growing interest in integrating Zero Trust with ITSM, several research gaps persist:

- **Quantitative Impact Analysis:** Limited studies assess the measurable impact of Zero Trust integration on ITSM performance metrics.

- **Scalability Challenges:** Research on scaling Zero Trust principles in large, complex IT environments is scarce.
- **Cultural and Organizational Factors:** There is a need for studies exploring the human factors influencing the adoption of Zero Trust in ITSM.

CONCLUSION

Integrating Zero Trust principles into ITSM frameworks offers a strategic approach to enhancing governance and securing operations in modern IT environments. While the benefits are evident, organizations must address implementation challenges and consider cultural factors to ensure successful adoption. Future research should focus on empirical studies to quantify the impact of Zero Trust on ITSM performance and explore strategies for overcoming identified barriers.

REFERENCES

- *Gambo, M. L., & Almulhem, A. (2025). Zero Trust Architecture: A Systematic Literature Review. arXiv. Retrieved from https://arxiv.org/abs/2503.11659*
- *Pereira, R. F., et al. (2025). An IT Service Management Literature Review: Challenges, Benefits, Opportunities, and Implementation Practices. Information. Retrieved from https://www.researchgate.net/publication/349857851*
- *Kumar, R. (2024). Zero Trust: Safeguarding ITSM Against Emerging Threats. ITSM Docs. Retrieved from https://www.itsm-docs.com/blogs/itil-concepts/zero-trust-security*
- *Sripathi, D. R., & Murali, N. (2025). A Systematic Literature Review of Zero Trust Architecture and Software-Defined Perimeters. SSRN. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5358310*
- *Miles, L. (2024). Mastering Zero Trust Security in IT Operations. Cloud Security Alliance. Retrieved from https://cloudsecurityalliance.org/blog/2024/06/14/mastering-zero-trust-security-in-it-operations*
- *Koeppen, D. (2025). Zero-trust is redefining cyber security in 2025. Computer Weekly. Retrieved from https://www.computerweekly.com/opinion/Zero-trust-is-redefining-cyber-security-in-2025*
- *Microsoft. (2025). How the Microsoft Secure Future Initiative brings Zero Trust to life. Microsoft Security Blog. Retrieved from https://www.microsoft.com/en-us/security/blog/2025/05/15/how-the-microsoft-secure-future-initiative-brings-zero-trust-to-life*
- *Zscaler. (2025). What Is Zero Trust? | Benefits & Core Principles. Zscaler. Retrieved from https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust*
- *Ishu Anand Jaiswal, & Dr. Shakeb Khan. (2025). Leveraging Cloud-Based Projects (AWS) for Microservices Architecture. Universal Research Reports, 12(1), 195–202. https://doi.org/10.36676/urr.v12.i1.1472*
- *Sudhakar Tiwari. (2023). Biometric Authentication in the Face of Spoofing Threats. IRT, 9(5), 402–420.*
- *Yadav, N., Prasad, R. V., Kyadasu, R., Goel, O., Jain, A., & Vashishtha, S. (2024). Role of SAP Order Management in Managing Backorders in High-Tech Industries. SJMARS, 3(6), 21–41.*
- *SecurityScorecard. (2025). What Is Zero Trust Security and Why Does It Matter in 2025?. SecurityScorecard. Retrieved from https://securityscorecard.com/blog/what-is-zero-trust-security-and-why-does-it-matter-in-2025*
- *Tailscale. (2025). The State of Zero Trust report 2025. Tailscale. Retrieved from https://tailscale.com/resources/report/zero-trust-report-2025*