IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, March 2026
Impact Factor: 8.2

Zero Trust Architecture: A Modern Security Framework for Digital Enterprises

Aditya Badhekar[1], Sonali Kadhane[2], Akanksha Gite[3]
Computer Science Department[1-3]
Dr. D. Y. Patil Arts, Commerce, Science College, Pimpri Pune

Abstract: *In the modern digital environment, organizations are increasingly dependent on cloud computing, mobile applications, remote employees, and interconnected systems. While these advancements improve efficiency and productivity, they also expose organizations to sophisticated cyber threats such as ransomware, phishing attacks, insider misuse, and data breaches. Traditional perimeter-based security models are no longer sufficient because they assume that users inside the network can be trusted. This assumption has proven to be dangerous in today's distributed IT environments.*

Zero Trust Architecture (ZTA) is a modern cybersecurity framework that eliminates implicit trust and enforces continuous verification of users, devices, and applications before granting access to resources. This paper presents a detailed explanation of Zero Trust Architecture, including its background, principles, core components, working process, implementation strategy, benefits, challenges, and future scope. The paper also highlights how Zero Trust enhances organizational security by minimizing unauthorized access and limiting the impact of cyberattacks. The study concludes that Zero Trust is not just a technical solution but a strategic transformation in cybersecurity management.

Keywords: *Zero Trust Architecture, cybersecurity framework, identity verification, least privilege, micro-segmentation, enterprise security*

DOI: 10.48175/IJARSCT-31482