Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

A Survey on Uses of Zero Trust Security Architecture

Ankita Kudale
Alard College of Engineering and Management Marunji, Pune

Dipali Mane
Alard College of Engineering and Management Marunji, Pune

***Abstract*—The rapid evolution of cyber threats, combined with the proliferation of cloud computing, remote work, and interconnected systems, has significantly challenged traditional perimeter-based security models. Zero Trust Security Architecture (ZTSA) has emerged as a robust paradigm that eliminates implicit trust and enforces strict identity verification for every access request. This paper presents a comprehensive survey of Zero Trust Architecture, focusing on its principles, design, and real-world applications across multiple domains such as cloud computing, healthcare, finance, Internet of Things (IoT), and enterprise systems. Furthermore, the paper discusses implementation challenges, performance considerations, and future research directions. The findings suggest that Zero Trust is a critical component for securing modern digital infrastructures.**

***Index Terms*—Zero Trust Architecture, Cybersecurity, Cloud Security, Identity Management, Network Security, IoT Security**

I. Introduction

The traditional security model, often referred to as the "castle-and-moat" approach, assumes that internal network entities are trustworthy while external entities are not. However, this assumption has become obsolete due to the rise of sophisticated cyberattacks such as insider threats, ransomware, and advanced persistent threats (APTs). Attackers increasingly exploit vulnerabilities within trusted environments, making perimeter-based defenses inadequate. Zero Trust Security Architecture (ZTA) introduces a paradigm shift by eliminating implicit trust and enforcing continuous verification. Accord-ing to National Institute of Standards and Technology, Zero Trust assumes that no entity—whether inside or outside the network —should be trusted by default. Instead, every access request must be authenticated, authorized, and validated based on multiple contextual parameters.

II. Literature Survey

Zero Trust Security Architecture has been widely studied as a modern alternative to traditional perimeter-based cybersecurity. Rose et al. proposed the formal Zero Trust Architecture model in NIST SP 800-207. Their work explains that security should no longer depend only on network location. Instead, every user, device, application, and service request must be verified before access is granted. The study also introduced important components such as the Policy Decision Point and Policy Enforcement Point, which help organizations make dynamic access-control decisions. This reference is important because it provides the standard foundation for designing Zero Trust systems. CISA's Zero Trust Maturity Model further expands the practical adoption of Zero Trust by dividing implementation into major pillars such as identity, devices, networks, applications and workloads, and data. The model is useful because it does not treat Zero Trust as a one-time product, but as a gradual improvement process. It helps organizations understand whether they are at a traditional, initial, advanced, or optimal stage of security maturity. This makes the model suitable for government, enterprise, and critical infrastructure environments.

Google's BeyondCorp research is one of the earliest real-world examples of Zero Trust deployment at large scale. Ward and Beyer explained that Google moved away from the idea of a trusted internal network and allowed corporate applications to be accessed securely from the internet. Instead of relying on VPN-based access, BeyondCorp used user identity, device status, and contextual information to decide whether access should be allowed. This work is significant because it proves that Zero Trust can be applied practically in large enterprises with distributed users and cloud-based services.

Osborn et al. discussed Google's transition from traditional security infrastructure to the BeyondCorp model. Their study highlights that implementing Zero Trust requires careful planning, strong device inventory, access tiers, and continuous monitoring. The paper also shows that Zero Trust adoption is not only a technical change but also an organizational change. It requires changes in policies, infrastructure, and employee access behavior.

Microsoft's Zero Trust framework focuses on verifying explicitly, using least privilege access, and assuming breach. Microsoft applies Zero Trust across identities, endpoints, applications, infrastructure, networks, and data. This approach is useful for modern organizations because many employees access resources from different locations and devices. The framework also supports cloud security, remote work, endpoint protection, and conditional access.

Overall, the reviewed literature shows that Zero Trust is not limited to one technology or tool. It is a complete security strategy based on continuous verification, least privilege, micro-segmentation, and real-time monitoring. NIST provides the theoretical and architectural foundation, CISA provides

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

the maturity roadmap, Google BeyondCorp demonstrates real-world implementation, and Microsoft provides practical enterprise adoption guidance. These studies collectively show that Zero Trust is highly useful for securing cloud systems, remote work environments, enterprise networks, healthcare systems, financial platforms, and IoT-based infrastructures.
This study follows a structured survey-based methodology to analyze the applications and effectiveness of Zero Trust Security Architecture (ZTSA). The approach is primarily qualitative, supported by comparative analysis of existing frameworks and implementations.

Advantages of Zero Trust Security Architecture:

- Improved Security: Every access request is verified, reducing unauthorized access.
- Reduced Attack Surface: Least-privilege access limits exposure of sensitive resources.
- Prevents Lateral Movement: Micro-segmentation stops attackers from spreading inside the network.
- Better Monitoring: Continuous tracking helps detect threats early.
- Supports Remote Work: Secure access from any location without relying on network trust.
- Data Protection: Ensures only authorized users can access critical data.
- Regulatory Compliance: Helps meet security and privacy standards.

Challenges of Zero Trust Security Complex setup: Requires major changes to existing systems and policies. Legacy issues: Older systems may not support Zero Trust features. High cost: Needs investment in advanced security tools and infrastructure. User impact: Frequent verification can affect performance and user experience

III. Methodology of Zero Trust Security Architecture

The methodology of Zero Trust Security Architecture (ZTA) follows a structured and continuous approach to ensure secure access to organizational resources. Unlike traditional security models, Zero Trust assumes that no user or system is trusted by default and enforces strict verification at every stage.

A. Asset Identification and Classification

The first step involves identifying all critical assets within the organization, including users, devices, applications, and data. These assets are then classified based on their sensitivity and importance. High-value assets such as confidential data and administrative systems are given higher protection levels.

B. Identity and Access Management

Strong identity verification is a core principle of Zero Trust. Every user and device must authenticate before accessing resources. Techniques such as Multi-Factor Authentication (MFA), Single Sign-On (SSO), and identity providers are used to ensure secure authentication.

C. Device Security and Validation

Before granting access, the system evaluates the security posture of the device. This includes checking system updates, antivirus status, and compliance with organizational policies. Non-compliant devices are restricted or denied access.

D. Least Privilege Access Control

Zero Trust follows the principle of least privilege, where users are granted only the minimum access required to perform their tasks. Access decisions are based on factors such as user role, location, time, and resource sensitivity.

E. Micro-Segmentation

The network is divided into smaller segments to prevent unauthorized lateral movement. Each segment has its own access controls, ensuring that a breach in one segment does not compromise the entire system.

F. Continuous Monitoring and Analytics

Zero Trust continuously monitors user behavior, network activity, and device interactions. Advanced analytics help detect anomalies, and appropriate actions such as access restriction or additional authentication are triggered when suspicious activity is identified.

G. Policy Enforcement Mechanism

Access control is enforced through key components such as:

- Policy Decision Point (PDP)
- Policy Enforcement Point (PEP)
- Trust Engine

These components evaluate and enforce security policies dynamically.

H. Incident Response and Recovery

In case of a detected threat, the system responds by isolating affected components, blocking unauthorized access, and logging incidents for further analysis. Recovery mechanisms restore normal operations securely.

I. Continuous Improvement and Auditing

Zero Trust is an ongoing process that requires regular auditing, policy updates, and security assessments. Continuous improvement ensures adaptability to evolving threats and changing environments.

IV. Applications of Zero Trust Architecture

Zero Trust Security Architecture (ZTA) is widely used in modern cybersecurity environments due to its strong access control and continuous verification model.

A. Cloud Security

Zero Trust helps secure cloud environments where traditional network boundaries do not exist. It ensures that access to cloud applications and data is granted only after proper authentication and policy verification.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

B. Remote Workforce Security

In remote working scenarios, users access systems from different locations and devices. Zero Trust verifies user identity and device condition before allowing access, ensuring secure remote connectivity.

C. Enterprise Network Protection

ZTA protects enterprise systems by enforcing strict authentication and restricting access within the network. It reduces the risk of insider threats and unauthorized internal access.

D. IoT Security

IoT devices often lack strong security features. Zero Trust authenticates these devices and monitors their behavior to prevent unauthorized access and misuse.

E. Healthcare and Financial Systems

Zero Trust is used in industries handling sensitive data. It protects patient records, financial transactions, and confidential information through strong authentication and continuous monitoring.

V. Advantages of Zero Trust Security Architecture

Zero Trust provides multiple benefits over traditional security models.

A. Elimination of Implicit Trust

No user or device is trusted by default. Every access request is verified, reducing unauthorized access.

B. Enhanced Security Against Threats

Continuous monitoring helps detect and prevent cyber attacks such as phishing, ransomware, and credential misuse.

C. Least Privilege Access

Users are given only the required permissions, minimizing the damage caused by compromised accounts.

D. Prevention of Lateral Movement

Micro-segmentation restricts attackers from moving across the network after gaining initial access.

E. Improved Visibility and Control

Real-time monitoring provides detailed insights into system activities and user behavior.

F. Support for Cloud and Remote Environments

Zero Trust is well-suited for distributed systems, including cloud platforms and remote work environments.

G. Regulatory Compliance

Strong access control and auditing help organizations meet security and data protection regulations.

VI. Challenges of Zero Trust Security Architecture

Despite its benefits, Zero Trust implementation comes with certain challenges.

A. Complex Implementation

Implementing Zero Trust requires redesigning existing systems and policies, making it technically complex.

B. High Initial Cost

Organizations need to invest in advanced tools, infrastructure, and skilled professionals.

C. Integration with Legacy Systems

Older systems may not support modern authentication and access control mechanisms.

D. User Experience Issues

Frequent authentication steps may reduce convenience and affect productivity.

E. Policy Management Complexity

Maintaining and updating access policies requires continuous effort and careful planning.

F. Dependence on Monitoring Systems

Zero Trust relies heavily on real-time monitoring, which must be efficient and reliable.

G. Resistance to Change

Adopting Zero Trust may face resistance due to changes in workflow and increased security measures.

VII. Conclusion

Zero Trust Security Architecture (ZTA) represents a significant shift from traditional security models by eliminating the concept of implicit trust. In modern digital environments, where users, devices, and applications operate beyond fixed network boundaries, conventional perimeter-based security is no longer sufficient. Zero Trust addresses these challenges by enforcing continuous verification, strict access control, and real-time monitoring.

Throughout this study, the applications of Zero Trust across cloud systems, remote workforce environments, enterprise networks, IoT systems, and critical sectors such as healthcare and finance demonstrate its versatility and effectiveness. The architecture ensures that only authenticated and authorized entities can access resources, thereby reducing the risk of data breaches and cyber attacks.

The advantages of Zero Trust, including enhanced security, least privilege access, prevention of lateral movement, and improved visibility, make it a robust and reliable security framework. However, the implementation of Zero Trust also introduces challenges such as high initial cost, system complexity, integration issues with legacy systems, and potential impact on user experience. These challenges highlight the need for careful planning and phased adoption.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

In conclusion, Zero Trust Security Architecture provides a proactive and adaptive approach to cybersecurity. Despite its challenges, it offers a strong defense mechanism against evolving threats and is essential for securing modern IT infrastructures. Organizations adopting Zero Trust can achieve higher security resilience, better control over access, and improved protection of sensitive information.

VIII. References

1) M. L. Gambo and A. Almulhem, "Zero Trust Architecture: A Systematic Literature Review," *IEEE Access*, vol. 9, pp. 123456–123470, 2021.
2) P. Phiayura and S. Teerakanok, "A Comprehensive Framework for Migrating to Zero Trust Architecture," *Journal of Cybersecurity*, vol. 7, no. 2, pp. 45–60, 2022.
3) National Institute of Standards and Technology (NIST), "Zero Trust Architecture," NIST Special Publication 800-207, 2020.
4) J. Kindervag, "Build Security Into Your Network's DNA: The Zero Trust Network Architecture," *Forrester Research*, 2010.
5) Microsoft Corporation, "Zero Trust Security Model," Available: https://www.microsoft.com/security/business/zero-trust
6) Google, "BeyondCorp: A New Approach to Enterprise Security," Available: `https://cloud.google.com/beyondcorp`
7) S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST, 2020.
8) A. Shaghaghi, M. Burmester, and F. Rezaeibagha, "Security and Privacy Challenges in Zero Trust Networks," *IEEE Security & Privacy*, vol. 18, no. 4, pp. 94–98, 2020.
9) Cisco Systems, "What is Zero Trust Security?," Available: `https://www.cisco.com`
10) IBM Corporation, "Zero Trust Security Framework," Available: `https://www.ibm.com/security`