



**Faculty of Engineering and Technology
Computer Science Department
Comp438 – Internet of Things Security
Final Project**

Zero Trust Architecture (ZTA)

Malak Mustafa – 1212986

Mona Atta – 1202262

Ibraheem Abu Hijleh – 1203065

Dr. Mohammad Alkhanafseh

Date: 17/6/2025

Table of Contents

Abstract.....	2
Introduction	4
Overview of the Zero Trust Authentication	4
Architecture and Functionality in IoT	5
Relevance in IoT	6
Security Challenges or Known Attacks in IoT & Importance of ZTA.....	6
Proposed or Existing Solutions and Recent Research Enhancements in Zero Trust Architecture for IoT	8
Security Threats, Limitations, and IoT-Relevant Challenges.....	9
Recent Research Solutions (2018–2024).....	9
i-ZTA – Intelligent Zero Trust Architecture using AI	9
Trust-aware Access Control using Federated Learning in ZTA-IoT.....	11
Containerized ZTA for Microservices.....	12
Attribute-Based Access Control with ZTA.....	13
Real-world Application and Future Scope	15
Future Scope	17
Comparative Analysis using Tables and Figures.....	18
Conclusion.....	22
References	22

Table of Figures

Figure 1 Overview Zero Trust Architecture 1	4
Figure 2 Overview Zero Trust Architecture 2	5
Figure 3 Core Zero Trust Logical Components	5
Figure 4 Overview ZTA Security Challenges	7
Figure 5 How Zero Trust Works.....	8
Figure 6 i-ZTA Structure	10
Figure 7 Architectural overview of federated learning for IoT networks.....	12
Figure 8 Zero Trust microservices communication enforced by Istio in Kubernetes	13
Figure 9 How ABAC can be incorporated into a ZTA	14
Figure 10 Trust Assessment Model.....	15
Figure 11 Smart City.....	16
Figure 12 Blockchain-enabled device authentication solution in a zero-trust IoT environment	17
Figure 13 Zero Trust Vs Traditional Network.....	20
Figure 14 Key Differences Between Traditional & Zero Trust Security Models	20
Figure 15 Benefits of IoT	21

Abstract

The conventional perimeter-based organization assurance model cannot adjust to the advancement of current innovation.

Zero belief could be an unused sort of organized security demonstration, which is based on the concept of never believing and continuously confirming.

Whether the get to subject is within the inside arrangement or the external arrangement, it has to be verified to access assets.

The zero-belief show has gotten broad consideration in investigate and hone since it can meet the modern security necessities. Be that as it may, the application of zero belief is still in its earliest stages, and endeavors, organizations, and people are not completely aware of the points of interest and drawbacks of zero belief, which significantly hinder the application of zero belief.

This paper presents the existing zero-belief engineering and analyzes the center innovations, including personality confirmation, reach control, and belief appraisal, which are basically dependent on the zero-belief engineering. The most relevant arrangements beneath each innovation are compared and analyzed to summarize the points of interest and impediments, as well as the current challenges and future investigate patterns.

Introduction

The distributed, heterogeneous, and dynamic nature of connected devices makes traditional perimeter-based security models inadequate in the age of growing Internet of Things (IoT) ecosystems. By embracing the idea of "never trust, always verify," Zero Trust Architecture (ZTA) has become a revolutionary method that reinterprets security. Through continuous authentication, micro-segmentation, and dynamic access control, ZTA improves security in the Internet of Things. This paper examines the fundamental ideas, difficulties, and practical uses of ZTA in IoT. The study also examines new developments in ZTA implementation and how important it is for protecting a variety of IoT environments, including industrial systems, smart cities, and healthcare.

Overview of the Zero Trust Authentication

The fundamental idea behind the Zero Trust Architecture (ZTA) security model is "never trust, always verify." ZTA, in contrast to conventional perimeter-based security, makes the assumption that adversaries may be found both inside and outside the network. ZTA offers a strong framework for protecting devices, data, and communications in the Internet of Things, where devices are frequently dispersed and resource-constrained.

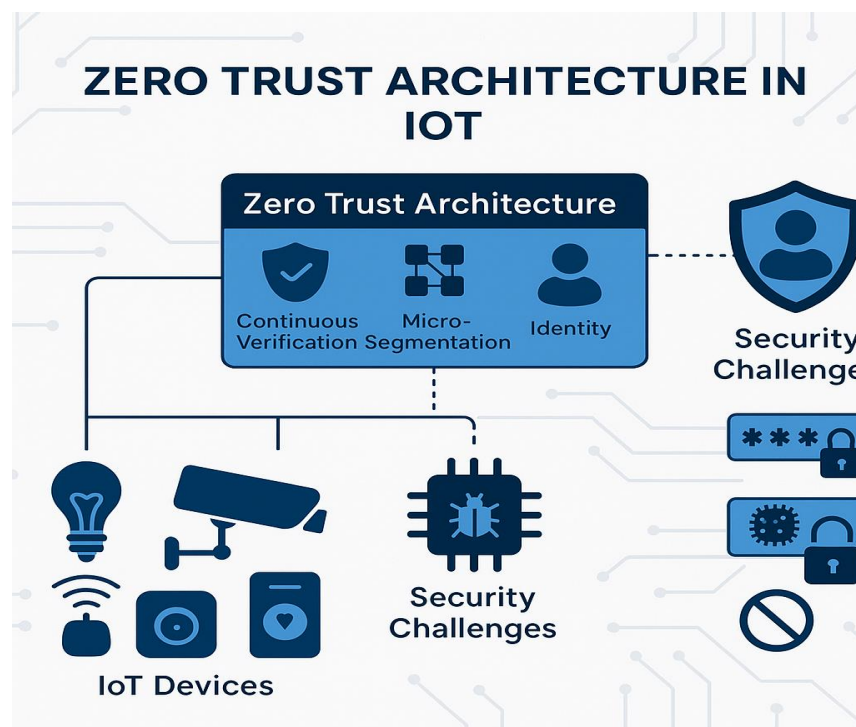


Figure 1 Overview Zero Trust Architecture 1

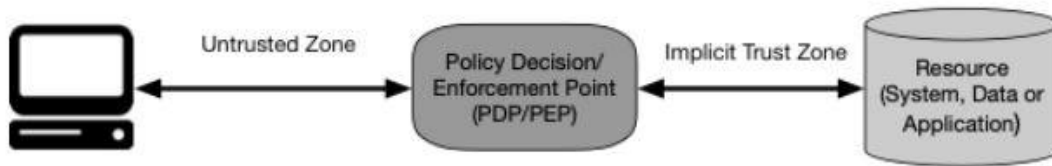


Figure 2 Overview Zero Trust Architecture 2

Architecture and Functionality in IoT

ZTA has been modified for the Internet of Things to handle the special features of linked devices, which are frequently varied, resource-constrained, and dispersed throughout different environments.

Identity-Centric Security: Each application, user, and device needs to be able to prove their identity. Devices authenticate themselves using distinct credentials, such as secure tokens or certificates.

Micro-Segmentation: The network is separated into more manageable, discrete parts. To reduce attackers' ability to move laterally, devices are only permitted to communicate with the systems and services that are required.

Continuous Verification: Risk factors, behavior analytics, and real-time context are used to dynamically reevaluate access decisions (e.g., location, time of access, device health).

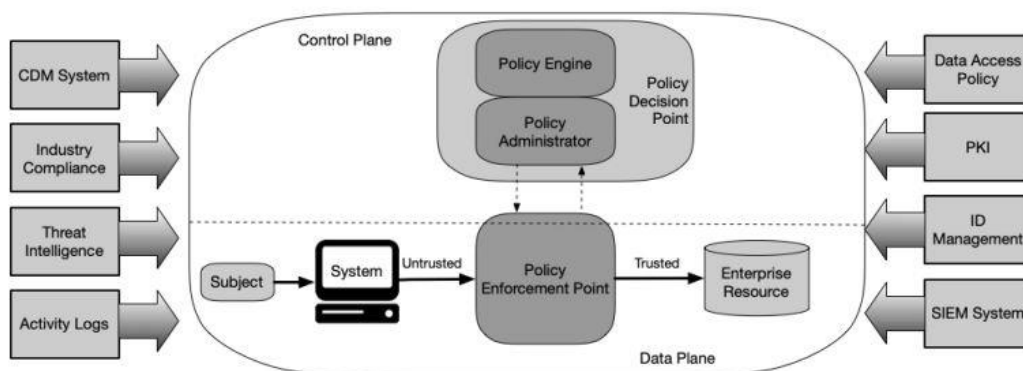


Figure 3 Core Zero Trust Logical Components

Relevance in IoT

Pertinence of Zero Believe Design (ZTA) in IoT

IoT environments are exceedingly energetic, with differing gadgets frequently working in uncertain situations. Numerous IoT arrangements endure from.

Security Challenges or Known Attacks in IoT & Importance of ZTA

1. **Major Security Challenges in IoT:** IoT environments confront noteworthy security issues due to their large-scale, heterogeneous, and frequently uncertain nature. Key challenges include:

- **Gadget Personality Spoofing & Unauthorized Get to:** Assailants imitate genuine gadgets due to frail or truant confirmation instruments.
- **Man-in-the-Middle (MITM) Assaults:** IoT gadgets regularly communicate over decoded conventions.

Aggressors can capture and control activity between gadgets and servers.

- **Unreliable Firmware & Physical Helplessness:** Numerous IoT gadgets run obsolete firmware and need secure upgrade components. Conveyed in open or uncontrolled regions, they are inclined to alteration and equipment assaults.
- **Deficiently Observing:** Most gadgets need logging, behavioral analytics, or real-time interruption discovery due to asset imperatives.

2. Why These Threats Are Critical in IoT

- 1) IoT devices are often **unattended, physically accessible, and remotely exploitable.**
- 2) Traditional network security (e.g., firewalls) is ineffective for **decentralized, dynamic environments.**
- 3) A breach in a single device can compromise an entire system, especially in critical sectors like:
 - a. Healthcare
 - b. Smart Grids
 - c. Industrial Automation

3. How Zero Trust Architecture (ZTA) Addresses These Challenges

ZTA transforms IoT security by applying "never trust, always verify" principles at every layer:

Powerless default qualifications (e.g., hardcoded passwords).

- 1] Need for secure firmware overhauls, taking off gadgets defenseless to known abuses.
- 2] Unreliable communication conventions, uncovering information to capture attempts, and control.
- 3] Negligible built-in security controls, making them simple targets for botnets (e.g., Mirai, Mozi).
- 4] Conventional perimeter-based security models fall flat in IoT since.
- 5] Gadgets are dispersed over different systems (e.g., savvy homes, mechanical IoT, healthcare).
- 6] Assaultants can bypass firewalls by compromising a single powerless gadget.

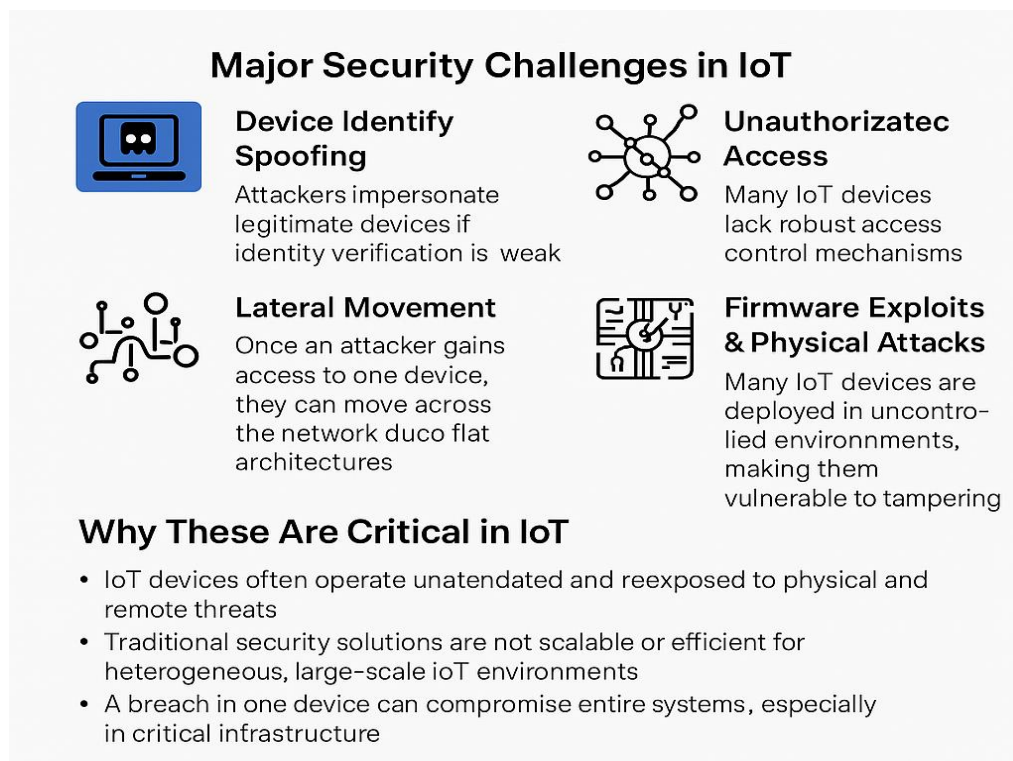
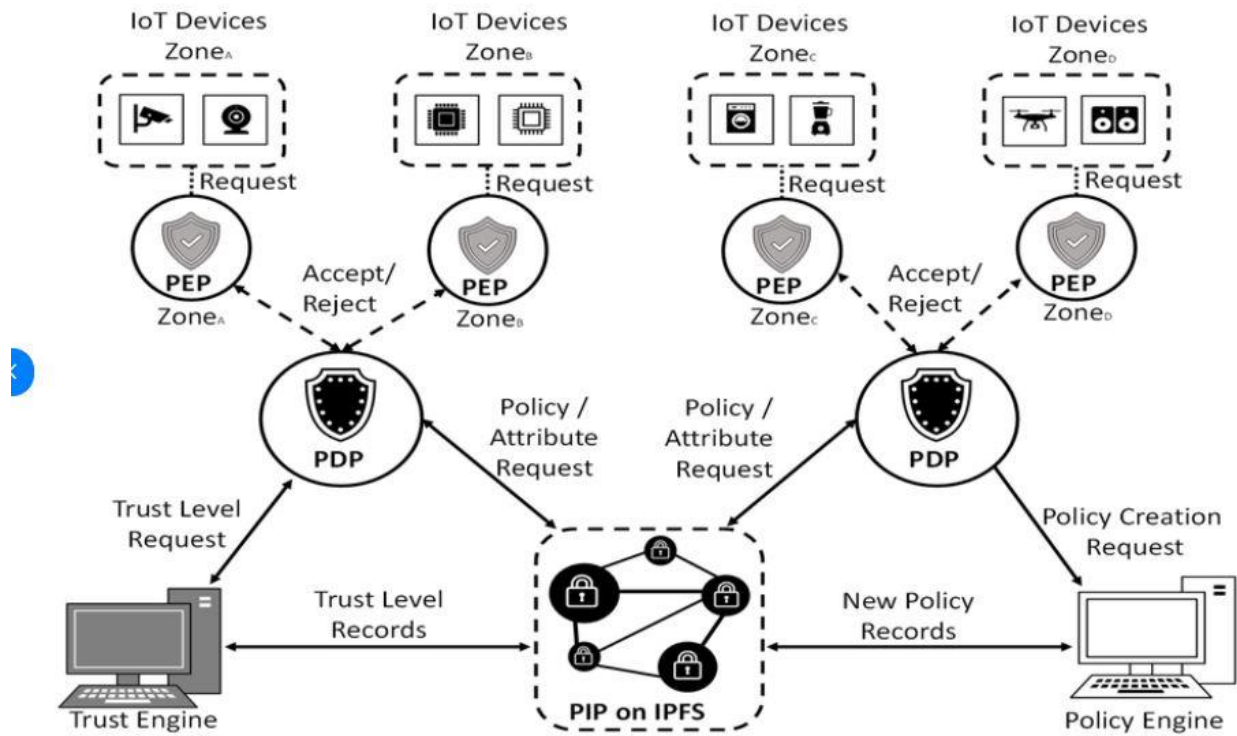


Figure 4 Overview ZTA Security Challenges



Zero-trust architecture for IoT devices.

Figure 5 How Zero Trust Works

Proposed or Existing Solutions and Recent Research Enhancements in Zero Trust Architecture for IoT

Zero Trust Architecture (ZTA) has emerged as a promising cybersecurity paradigm to address the inherent vulnerabilities of the Internet of Things (IoT), where devices are distributed, resource-constrained, and dynamically connected. Unlike traditional perimeter-based models, ZTA eliminates implicit trust and enforces continuous verification of users and devices, regardless of their network location. In the context of IoT, this shift is critical to mitigating modern cyber threats and establishing scalable, context-aware security.

This section presents an in-depth analysis of proposed and recent solutions from peer-reviewed literature between 2018 and 2024. Each solution is evaluated based on its security contributions, limitations, and suitability in addressing IoT-specific challenges.

Security Threats, Limitations, and IoT-Relevant Challenges

Zero Trust in IoT environments is designed to combat several pressing challenges:

- **Implicit Trust in Internal Networks:** Many IoT systems still rely on perimeter-based models, where internal devices are assumed trustworthy. This allows attackers to move laterally once inside.
- **Weak or Static Authentication:** Single-factor authentication is inadequate for IoT, where devices may be exposed and passwords reused.
- **Lack of Context-Awareness:** Traditional models ignore dynamic factors like location, device health, and behavior in access decisions.
- **Scalability and Device Heterogeneity:** Managing thousands of IoT devices with different capabilities makes centralized, static access control impractical.
- **Inadequate Trust Evaluation:** Static trust assignments do not reflect real-time behavior or evolving risk.

These limitations are critical in IoT because of the open, distributed nature of networks, the sheer volume of endpoints, and the potential physical consequences of breaches, such as in smart healthcare or industrial IoT.

Recent Research Solutions (2018–2024)

i-ZTA – Intelligent Zero Trust Architecture using AI

Authors: Ramezanpour & Jagannath (2022) [4]

How it works:

Uses reinforcement learning to assign dynamic trust scores to devices and users based on their behavior. It leverages Policy Decision Points (PDPs) to constantly evaluate whether access should be granted, learning from past behavior patterns to improve security responses.

Problem it solves:

Replaces static rule-based access models that assume internal devices are trustworthy. Essential for 5G/6G and tactical networks requiring fast, real-time trust decisions.

Pros:

- Learns and adapts to behavior over time, improving security decisions.
- Handles zero-day attacks more effectively.
- Enables self-healing security posture through autonomous response.

Cons:

- Requires high computational resources.
- Needs large volumes of training data.
- Difficult to deploy on lightweight IoT devices.

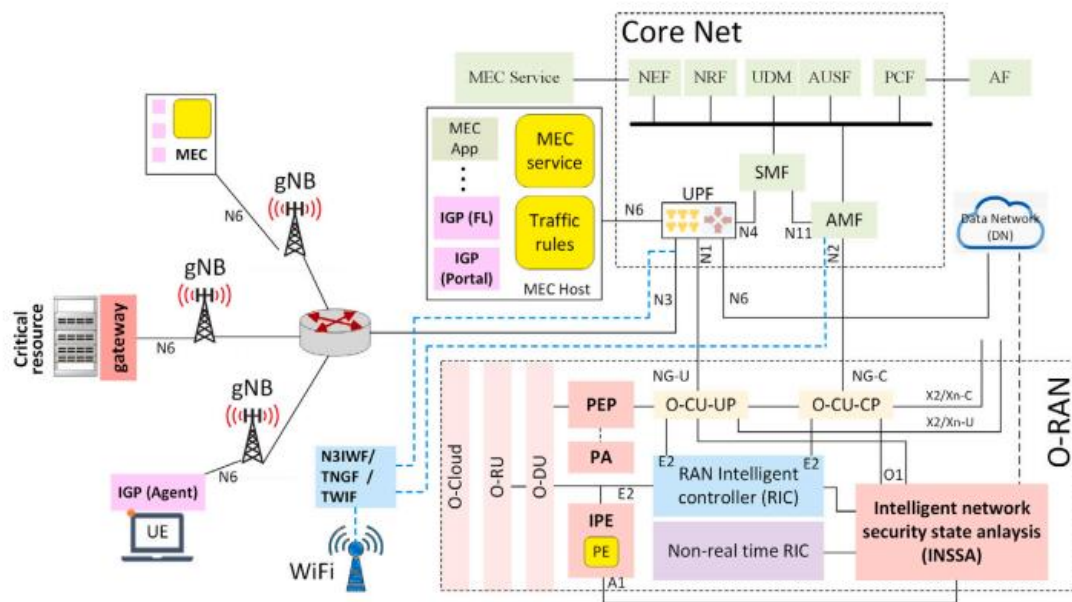


Figure 6 i-ZTA Structure

i-ZTA structure showing RL agent feeding trust scores into PDP, which then informs PEP for real-time enforcement (Ramezanpour & Jagannath, 2022) [4]

Trust-aware Access Control using Federated Learning in ZTA-IoT

Authors: Rjoub et al. (2024) [5]

How it works:

Implements Federated Learning (FL) to build trust models locally on IoT devices, sending only model updates to a central server. Avoids raw data transmission to preserve user privacy while collaboratively training a unified model.

Problem it solves:

Addresses centralized data collection and privacy concerns in distributed IoT networks.

Pros:

- Maintains data privacy by keeping it local.
- Suitable for large-scale, distributed IoT environments.
- Minimizes risks of data leakage during transmission.

Cons:

- Requires complex synchronization between nodes.
- Susceptible to model poisoning attacks.
- Needs secure update mechanisms for federated models.

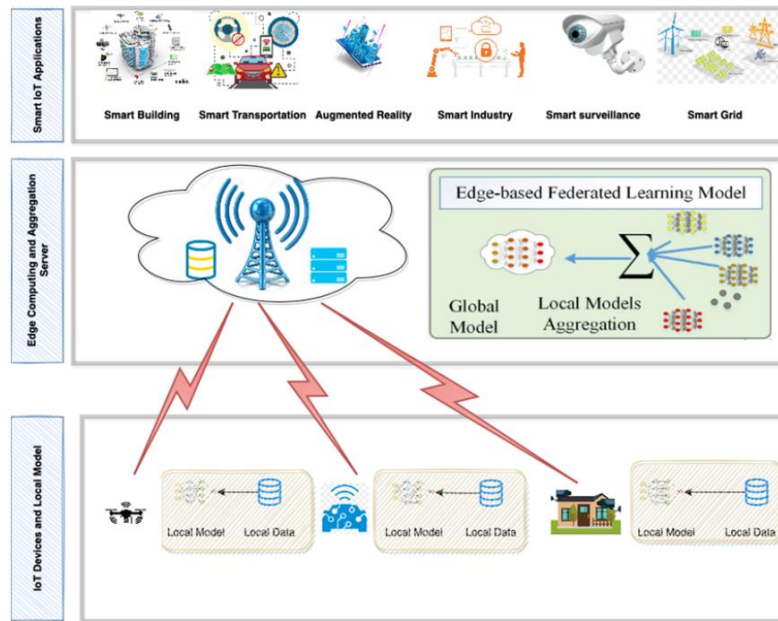


Figure 7 Architectural overview of federated learning for IoT networks

Containerized ZTA for Microservices

Authors: Weever et al. (2020)

How it works:

Uses Kubernetes for container orchestration and Istio Service Mesh to enforce mTLS and fine-grained service-to-service access policies. Focuses on securing internal 'east-west' traffic and microservices communication.

Problem it solves:

Solves lateral movement threats within containerized services by enforcing strict communication rules.

Pros:

- Easily scalable in cloud-edge IoT architectures.
- Provides granular traffic control within applications.
- Implements zero trust between internal services.

Cons:

- Does not incorporate user or behavior monitoring.
- Focuses only on services, not end devices.
- Requires high expertise in Kubernetes and Istio.

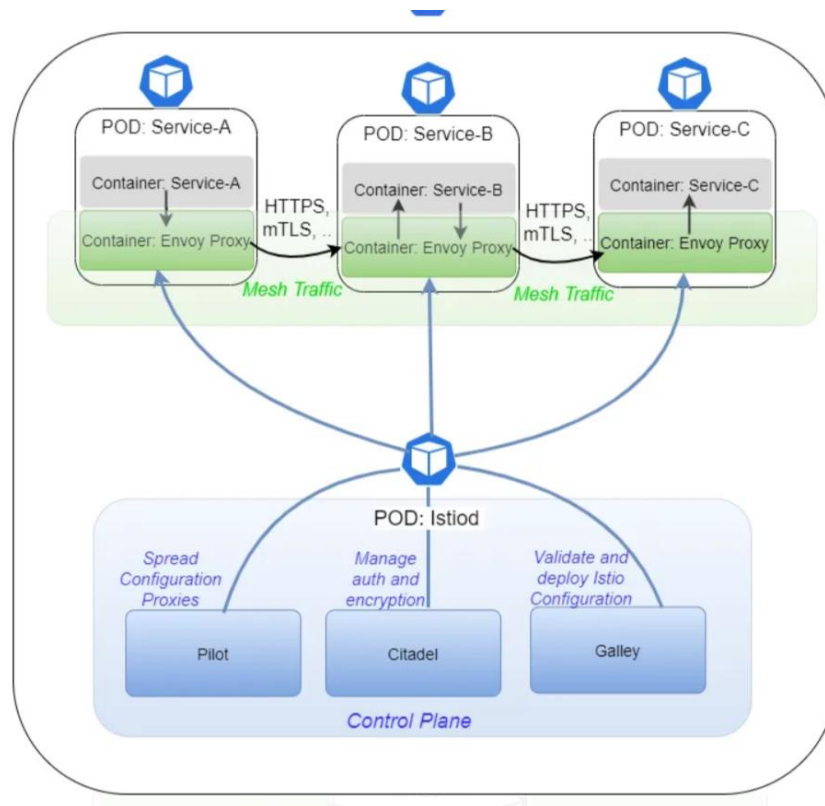


Figure 8 Zero Trust microservices communication enforced by Istio in Kubernetes

Attribute-Based Access Control with ZTA

Authors: Ghate et al. (2021) [10]

How it works:

Uses attributes such as device location, health, and time to drive access decisions. Employs automated extraction of attribute relations to formulate dynamic access policies that adjust to contextual changes.

Problem it solves:

Overcomes the rigidity of role-based access control (RBAC) by enabling flexible, context-driven access enforcement.

Pros:

- Highly flexible and context-aware.
- Adapts to changing environmental and user/device conditions.
- Ideal for mobile or industrial IoT environments.

Cons:

- Lacks widespread deployment and real-world testing.
- Requires strong attribute inference mechanisms.
- Less common in practice compared to RBAC.

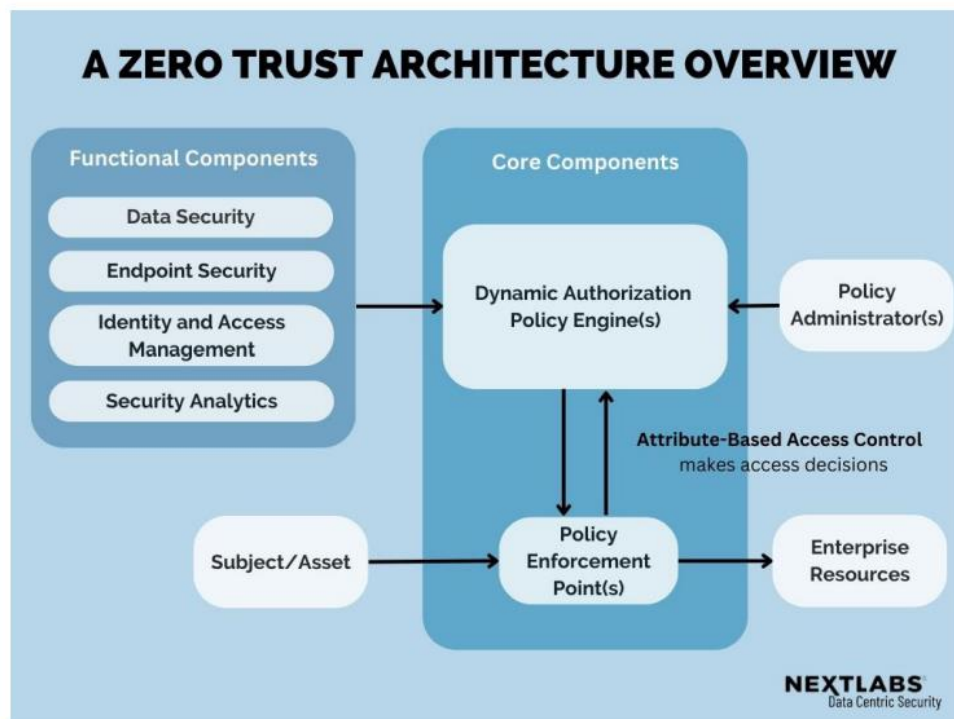


Figure 9 How ABAC can be incorporated into a ZTA

Real-world Application and Future Scope

Healthcare IoT:

- Medical devices and patient monitors are connected to networks requiring strict access control.
- By ensuring that users and devices are constantly authenticated, Zero Trust Architecture (ZTA) guards against device spoofing and illegal access.
- For instance, regular device health and user credential checks lower the possibility of hospital data breaches.
- The authors of the cited Chen et al. (2021) study suggest a four-dimensional ZTA framework based on "subject, object, environment, and behavior" that permits safe access control in healthcare settings.[7]

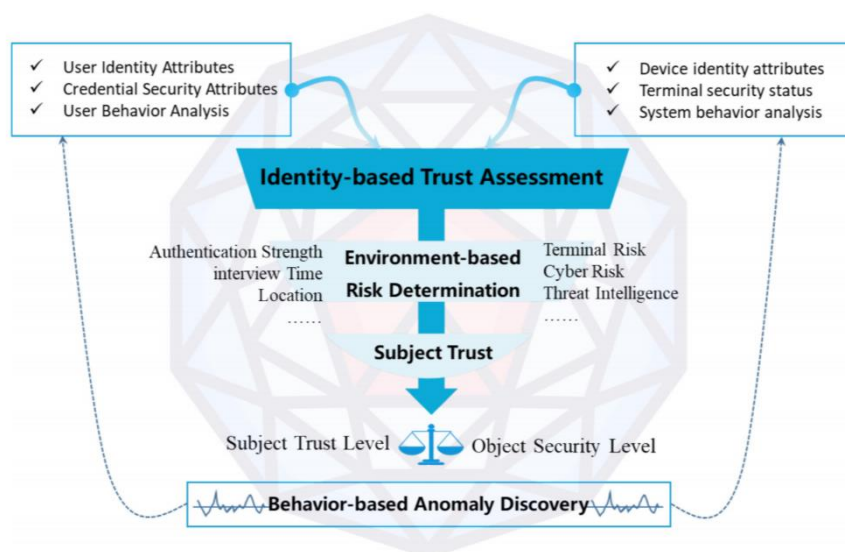


Figure 10 Trust Assessment Model

Smart City:

- Widespread IoT devices include environmental sensors, traffic lights, and security cameras.
- If a device is compromised, ZTA's micro-segmentation restricts lateral movement, containing attacks.
- Large numbers of dispersed devices can be managed privately thanks to federated learning-based trust evaluation.

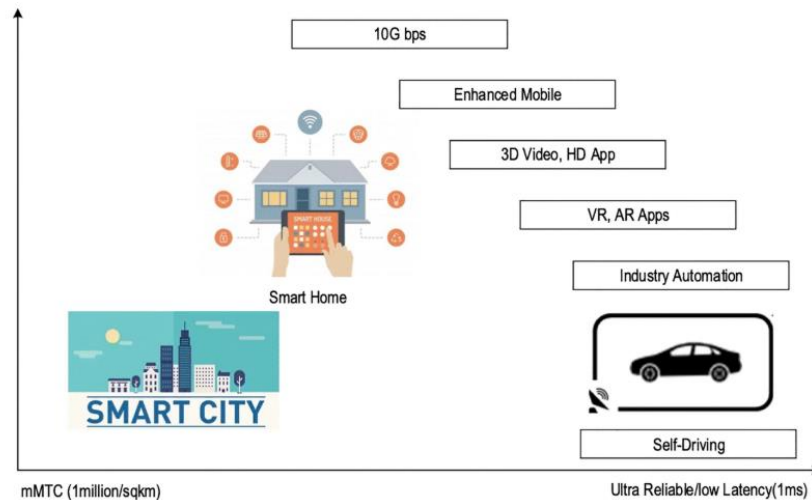


Figure 11 Smart City

Industrial IoT:

- Critical infrastructure is controlled by factory sensors and controllers.
- By using containerized environments to secure east-west traffic between microservices and devices, ZTA guards against lateral movement and insider threats.
- Policies are dynamically adjusted to changing operational contexts by attribute-based access control (ABAC).
- BasIoT supports Zero Trust by verifying each device's identity before access is granted and managing access policies via smart contracts, making it suitable for large-scale industrial environments. [8]

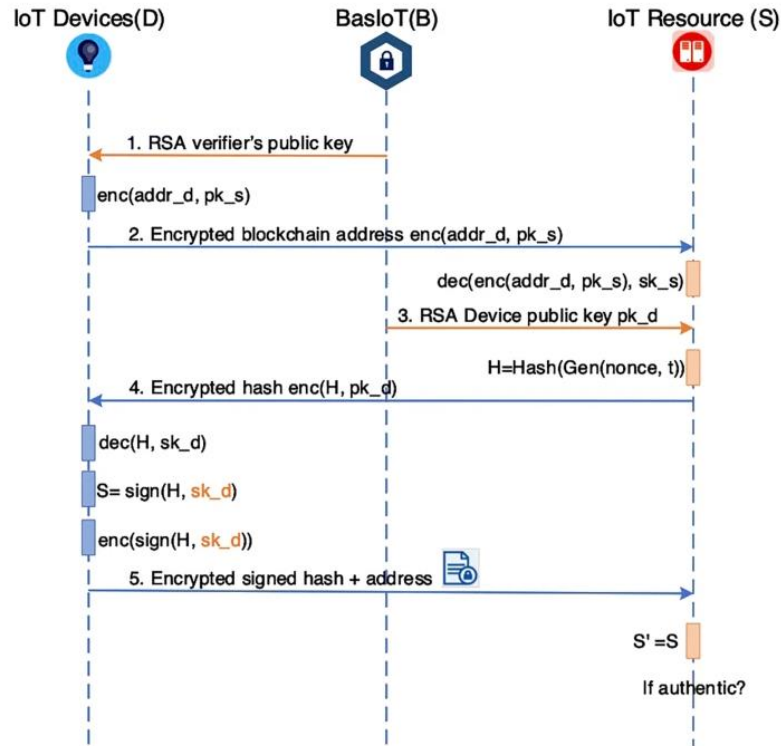




Figure 12 Blockchain-enabled device authentication solution in a zero-trust IoT environment

Future Scope

- Scalability:** As the number of IoT devices continues to rise exponentially, future ZTA solutions must be designed to support large-scale device ecosystems. Traditional centralized authentication methods are becoming insufficient. To address this, decentralized identity systems—such as blockchain-based ID management and Decentralized Identifiers (DIDs)—are expected to play a vital role. These systems allow devices to authenticate securely without relying on a single point of failure, which improves system resilience and scalability in distributed environments like smart hospitals or cities.
- AI-powered Trust Engines:** Emerging Zero Trust models are integrating artificial intelligence to continuously assess and adapt trust levels in real time. By analyzing behavioral patterns, network traffic, access history, and contextual signals, AI models can detect anomalies such as unauthorized data access or device misuse. This enables proactive policy adjustments based on evolving risks, offering a dynamic and intelligent layer of protection against both known and unknown threats.

- 
Integration with Edge Computing: Future Zero Trust systems will increasingly shift toward edge-based implementations. Edge computing allows trust assessment and access control decisions to occur closer to the data source or device, reducing latency and improving responsiveness, especially important for mission-critical IoT use cases like remote surgeries or autonomous emergency response. This architecture also helps distribute the computational load, which is essential for large-scale deployments.
- 
Lightweight Protocols and Cryptography: IoT devices often have limited processing power and energy capacity, making conventional encryption methods inefficient. Future ZTA systems must adopt lightweight cryptographic algorithms such as PRESENT or ECC to ensure secure authentication and data protection without overloading constrained devices. These optimized protocols will be crucial for enabling scalable and efficient Zero Trust implementations in real-world IoT environments.

Comparative Analysis using Tables and Figures

Table 1 Traditional IoT Security vs Zero Trust Approach

Traditional IoT Security	Zero Trust Approach
Trust devices inside the perimeter	Verifies all devices continuously
Flat networks enable lateral movement	Micro-segmentation isolates devices
Weak or no identity/authentication	Strong identity and MFA
Insecure communication protocols	Encrypted, verified communications
Lacks monitoring and response	AI-driven anomaly detection and automation

Table 2 Comparative Analysis of Zero Trust Authentication Solutions in IoT

Solution	Key Strength	Limitation	Target IoT Context	Trust Evaluation Method	Privacy Preservation	Real-Time Adaptability	Deployment Complexity
i-ZTA (2021)	AI-based real-time trust scoring	High computational cost	Smart cities, 5G IoT	Reinforcement Learning (AI)	Low	High	High
FL-ZTA (2024)	Federated trust, privacy-preserving	Coordination and model security	Smart cities, transportation IoT	Federated Learning	High	Medium	Medium
Container ZTA (2022)	Secures east-west microservices	Lacks user/device behavior analysis	Edge computing, microservices	Service Mesh Policies	Medium	Low	Medium–High
ABAC-ZTA (2021)	Fine-grained attribute-based control	Not widely deployed	Mobile, dynamic IoT environments	Attribute-Based Access Policies	Medium	High	High

Table 3 Real-World Applications of ZTA in IoT

Application Domain	IoT Characteristics	Security Challenges	ZTA Implementation Features
Healthcare IoT	Patient monitors, medical devices, EHR systems	Device spoofing, unauthorized access, and data breaches	Continuous user/device authentication, behavior-based access control (Chen et al., 2021)
Smart City	Traffic systems, environmental sensors, surveillance cameras	Lateral movement attacks, privacy risks, and data leakage	Micro-segmentation, federated trust models, and dynamic access control
Industrial IoT	Factory controllers, sensors, and automation systems	Insider threats, lateral attacks, insecure protocols	Containerized microservices, ABAC, blockchain-based identity verification (BasIoT)

Zero Trust Security vs Traditional IT Networks

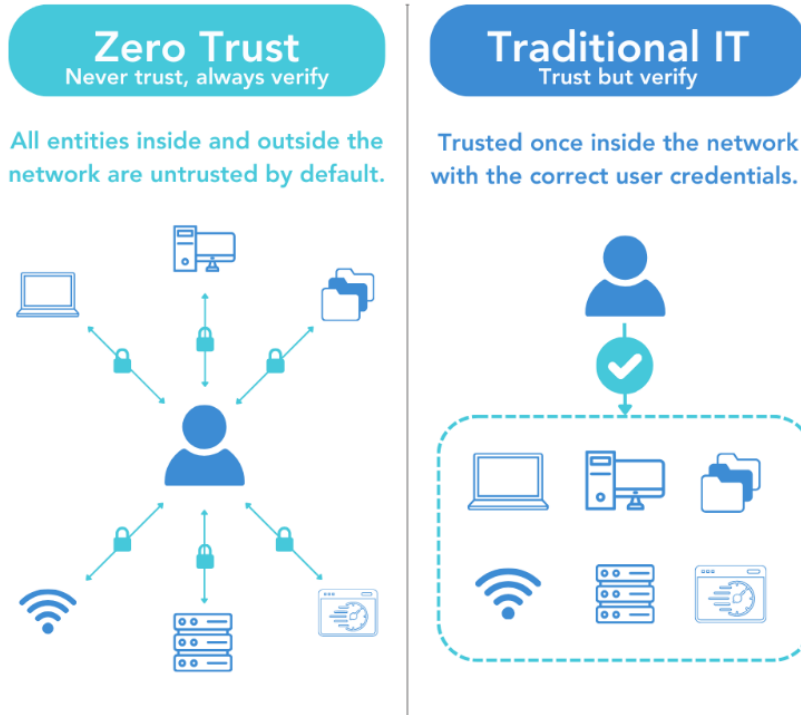


Figure 13 Zero Trust Vs Traditional Network

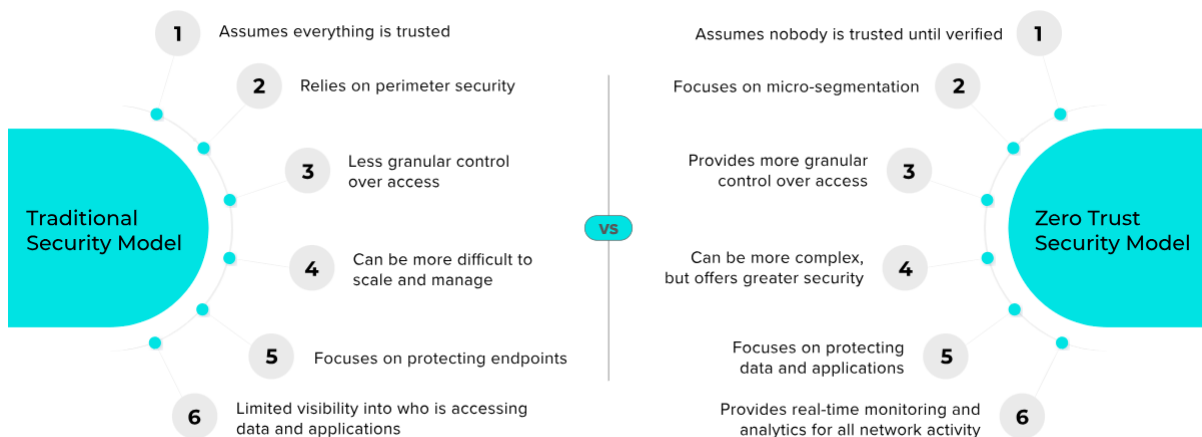


Figure 14 Key Differences Between Traditional & Zero Trust Security Models

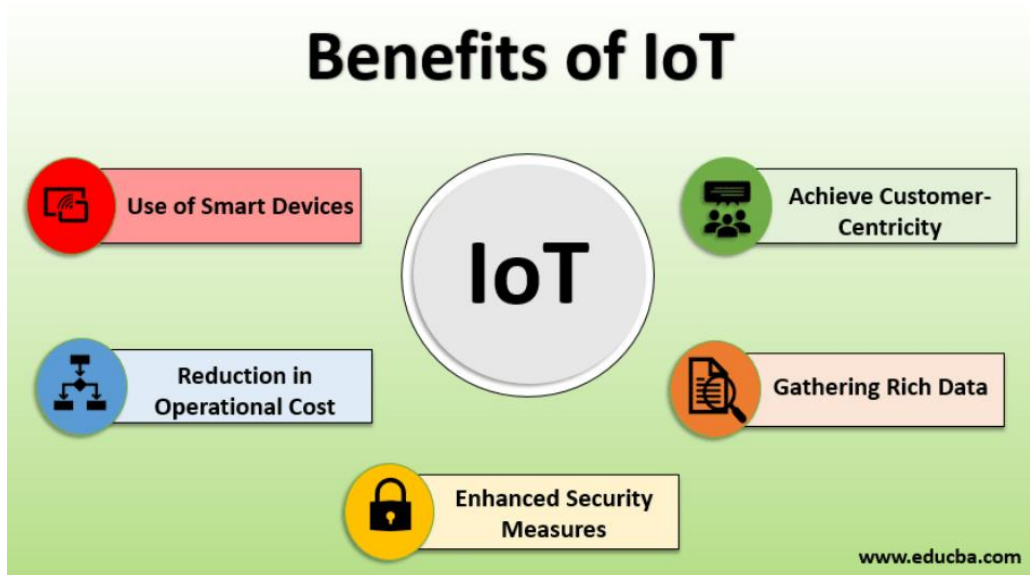


Figure 15 Benefits of IoT



Figure 16: Benefits of ZTA

Conclusion

By doing away with implicit trust and requiring constant verification at every layer, Zero Trust Architecture (ZTA) offers a paradigm shift in IoT environment security. ZTA shows its ability to address important security risks like device spoofing, lateral movement, and privacy violations through practical applications in smart cities, healthcare, and industrial systems. ZTA is positioned as a foundational model for the future of IoT cybersecurity due to continuous innovations like federated learning, lightweight cryptography, and AI-driven trust engines, despite its scalability and deployment complexity issues. ZTA will be essential to creating secure, adaptable, and resilient digital ecosystems as IoT systems develop further.

References

- [1] L. BOBELIN, "ZERO TRUST IN THE CONTEXT OF IOT: INDUSTRIAL LITERATURE REVIEW, TRENDS, AND CHALLENGES.," C&ESAR, PP. 37–52, 2023.
- [2] B. PAUL AND M. RAO, "ZERO-TRUST MODEL FOR SMART MANUFACTURING INDUSTRY," APPLIED SCIENCES, VOL. 13, NO. 1, P. 221, 2022.
- [3] S. ROSE, O. BORCHERT, S. MITCHELL, AND S. CONNELLY, "NIST SPECIAL PUBLICATION 800-207 ZERO TRUST ARCHITECTURE," NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY US DEPARTMENT OF COMMERCE, PP. 800–207, 2020.
- [4] K. RAMEZANPOUR AND J. JAGANNATH, "INTELLIGENT ZERO TRUST ARCHITECTURE FOR 5G/6G NETWORKS: PRINCIPLES, CHALLENGES, AND THE ROLE OF MACHINE LEARNING IN THE CONTEXT OF O-RAN," COMPUTER NETWORKS, VOL. 217, P. 109 358, 2022.
- [5] G. RJOUN, O. A. WAHAB, J. BENTAHAR, AND A. BATAINEH, "TRUST-DRIVEN REINFORCEMENT SELECTION STRATEGY FOR FEDERATED LEARNING ON IOT DEVICES," COMPUTING, VOL. 106, NO. 4, PP. 1273–1295, 2024.
- [6] B. ZYOUND AND S. L. LUTFI, "THE ROLE OF INFORMATION SECURITY CULTURE IN ZERO TRUST ADOPTION: INSIGHTS FROM UAE ORGANIZATIONS," IEEE ACCESS, 2024.
- [7] B. CHEN, S. QIAO, J. ZHAO, ET AL., "A SECURITY AWARENESS AND PROTECTION SYSTEM FOR 5G SMART HEALTHCARE BASED ON ZERO-TRUST ARCHITECTURE," IEEE INTERNET OF THINGS JOURNAL, VOL. 8, NO. 13, PP. 10 248–10 263, 2020.
- [8] S. LI, M. IQBAL, AND N. SAXENA, "FUTURE INDUSTRY INTERNET OF THINGS WITH ZERO-TRUST SECURITY," INFORMATION SYSTEMS FRONTIERS, VOL. 26, NO. 5, PP. 1653–1666, 2024.
- [9] L. LUPASCU, "ZERO TRUST ARCHITECTURE ON KUBERNETES WITH ISTIO SERVICE MESH," MEDIUM, OCT. 24, 2022.

[10] N. GHATE, S. MITANI, T. SINGH, AND H. UEDA, "ADVANCED ZERO TRUST ARCHITECTURE FOR AUTOMATING FINE-GRAINED ACCESS CONTROL WITH GENERALIZED ATTRIBUTE RELATION EXTRACTION," IN IEICE PROCEEDING SERIES, VOL. 68, ISSUE C1-5, DEC. 2021, DOI:10.34385/PROC.68.C1-5.

[11] NEXTLABS, "IMPLEMENTING A ZTA NIST NCCoE OVERVIEW," WHITE PAPER, 2024.