SEMINAR REPORT ON
ZERO TRUST NETWORK ACCESS

Submitted by

Fathima Farhana K I
(20420037)

Under the guidance of

Mrs. Sariga Raj

In partial fulfilment of the requirements for the award of the Degree

of **BACHELOR IN TECHNOLOGY**
in
INFORMATION TECHNOLOGY

DIVISION OF INFORMATION TECHNOLOGY
SCHOOL OF ENGINEERING
COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY KOCHI – 682022

SCHOOL OF ENGINEERING
COCHIN UNIVERSITY OF SCIENCE AND TECHNOLOGY

CERTIFICATE

This is to certify that this Seminar report entitled **"Zero Trust Network Access"** submitted by **Fathima Farhana K I** in partial fulfilment of the requirements for the award of the degree of Bachelor of Technology in Information Technology of Cochin University of Science and Technology, Kochi during the academic year 2023-24, is a bonafide record of work carried out under our guidance and supervision.

Mrs. Sariga Raj
Project Guide

Dr. Daleesha M Vishwanathan
Head of the Department

ACKNOWLEDGMENT

The seminar on the topic “Zero trust Network Access” was taken as a part of the curriculum for the award of a B. Tech degree in Information Technology Engineering. At the outset, I thank almighty God for making our endeavour a success. We also express our gratitude to Ms Daleesha M Viswanathan, Head of Department for providing us with adequate facilities, ways, and means by which we were able to complete this Seminar. I express my sincere gratitude to our faculty Mrs. Sariga Raj, Information Technology Division for her constant support and valuable suggestions without which the successful completion of this Seminar would not have been possible.

I express my immense pleasure and thankfulness to all the teachers and staff of the Department of Information Technology, CUSAT for their cooperation and support. Last but not the least, I thank all others, especially my classmates and my family members who in one way or another helped me in the successful completion of this work.

DECLARATION

I, Fathima Farhana k I hereby declare that this is the record of authentic work done by me during the year 2023 – 24 under the guidance of Mrs. Sariga Raj, Professor at School of Engineering, CUSAT and that no part has formed the basis for the award of any degree, diploma, associateship, fellowship or any other similar title or recognition in any other University.

Fathima Farhana K I

(20420037)

ABSTRACT

Zero Trust (ZT) has become a very hot approach for building secure systems, promoted by industry and government as a new way to produce systems with a high degree of security. ZT is based on not trusting any request for accessing resources. Because of the possibility of increasing the security of enterprise systems there has been a large amount of publication on different aspects of this strategy. ZTNA mandates continuous verification of users, devices, and applications, regardless of their location or network connection.

This new era of the industry is characterized by the integration of artificial intelligence and the Internet of Things (IoT) to optimize production processes. To ensure sustainability and continuous industrial performance, Industry 5.0 integrates automated technology, robots, humans, and others. This modern paradigm relies on data and high-level security to achieve sustainability and error- free production operations. For improving the resilience of Industry 5.0 through adversary mitigation, this manuscript introduces a Zero-Trust Network-based Access.

CONTENTS

1. **INTRODUCTION** 7
2. **EVOLUTION OF ZERO TRUST** 8
3. **ZERO TRUST PRINCIPLES BY MICROSOFT** 9
4. **ZERO TRUST ARCHITECTURE**.. 10
5. **ZTA IMPLEMENTATION TECHNIQUE** 13
6. **APPLICATION OF ZTA**.. 14
7. **LIMITATION OF ZTA**.. 15
8. **CONCLUTION** 15
9. **REFERENCE**.. 16

1. INTRODUCTION

In an era where cyber threats loom large and traditional network security models fall short, the concept of Zero Trust has emerged as a beacon of security in an otherwise precarious digital landscape. Zero Trust Network Access (ZTNA) represents a paradigm shift in cybersecurity philosophy, advocating for a fundamental change from the traditional notion of implicitly trusting entities within a network to a more rigorous and proactive approach of continuously verifying and validating every access request.

a. What is Zero Trust: Zero Trust is not merely a security protocol; it's a mindset. It challenges the conventional belief of trusting everything within the perimeter of a corporate network and instead adopts the principle of "never trust, always verify." In essence, Zero Trust assumes that breaches can and will occur, thereby necessitating a strategy where each access request is thoroughly authenticated, authorized, and encrypted before granting entry. This approach ensures that even if an attacker manages to infiltrate the network, their lateral movement and access to sensitive resources remain tightly restricted.

b. Why Zero Trust: The rationale behind adopting Zero Trust extends beyond mere security enhancements; it encompasses a spectrum of benefits that align with the evolving demands of modern enterprises.

    i. Productivity everywhere: Zero Trust empowers users to work securely from any location, at any time, and across any device. By removing the constraints of traditional perimeter-based security models, employees can seamlessly access resources without compromising security, thereby enhancing productivity and flexibility in today's dynamic work environment.

    ii. Cloud migration: As organizations increasingly embrace cloud technologies for their scalability and agility, the need for robust security measures becomes paramount. Zero Trust provides the framework for secure cloud migration by offering intelligent security solutions tailored to the complexities of modern cloud environments. This enables enterprises to leverage the benefits of digital transformation while safeguarding their data and assets from emerging cyber threats.

iii. Risk mitigation: Traditional security approaches often leave significant gaps that adversaries exploit to move laterally within a network, potentially causing widespread damage. Zero Trust mitigates these risks by implementing stringent access controls and continuous monitoring, effectively reducing the surface area for potential attacks. By adopting a Zero Trust model, organizations can proactively identify and address security vulnerabilities, thus minimizing the likelihood and impact of security breaches.

2. EVOLUTION OF ZERO TRUST

The concept of Zero Trust, initially popularized by security expert John Kindervag in 2010 during his tenure at Forrester Research, marked a significant departure from traditional network security paradigms. Kindervag's model advocated for the abandonment of implicit trust within networks and instead emphasized the necessity for continuous verification of all users and devices.

In 2019, the National Institute of Standards and Technology (NIST) further cemented the principles of Zero Trust by publishing guidelines and recommendations, providing a comprehensive framework for organizations to implement Zero Trust architectures effectively.

Building upon NIST's foundation, in 2023, the Cybersecurity and Infrastructure Security Agency (CISA) released version 2 of Zero

Trust guidance, incorporating insights from real-world implementations and emerging cybersecurity threats. This updated guidance aimed to refine and enhance Zero Trust strategies, ensuring organizations stay resilient against evolving cyber threats while embracing the benefits of a Zero Trust approach.

3. ZERO TRUST PRINCIPLES BY MICROSOFT

Microsoft, a leading advocate for Zero Trust principles, emphasizes three fundamental pillars that underpin their approach:

a. Verify Explicitly: The principle of "verify explicitly" entails the notion that access requests should never be granted based solely on assumed trust or network location. Instead, each access attempt must be explicitly verified through robust authentication and authorization mechanisms. This involves validating the identity of the user or device attempting to access resources and ensuring that they possess the necessary permissions to do so. By verifying access requests explicitly, organizations can mitigate the risk of unauthorized access and enforce granular access controls based on contextual factors such as user identity, device health, and behavioural analytics.

b. Use Least Privilege Access: The concept of "least privilege access" advocates for granting users and devices the minimum level of access required to perform their specific tasks or functions. Rather than providing unrestricted access to resources based on broad user roles or group memberships, organizations should adopt a principle of least privilege, wherein access permissions are tailored to the specific needs of individual users or devices. By limiting access to only what is essential for legitimate business purposes, organizations can minimize the potential impact of security breaches and reduce the attack surface available to adversaries.

c. Assume Breach: The principle of "assume breach" serves as a foundational mindset within the Zero Trust model, acknowledging the inevitability of security breaches and advocating for a proactive approach to security posture. Rather than operating under the assumption that the perimeter is impenetrable, organizations should adopt a mindset of continuous monitoring, detection, and response. By assuming that adversaries may have already compromised the network, organizations can implement robust threat detection and incident response capabilities to swiftly identify and mitigate security breaches. This proactive stance enables organizations to detect and contain security incidents more effectively, minimizing the potential impact on sensitive data and critical resources.

4. ZERO TRUST ARCHITECTURE

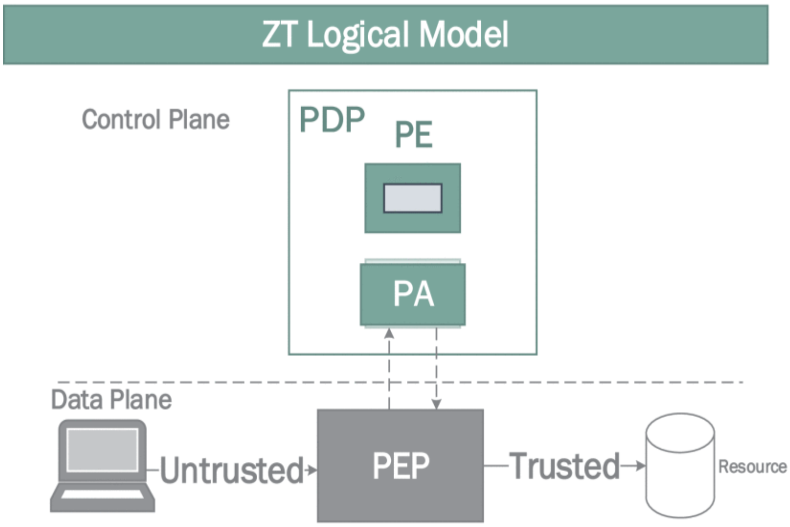
a. Traditional Model VS Zero Trust Model

Traditional Model	Zero Trust Model
• Focuses on perimeter defence, trusting everyone inside the network	• Embraces the principle of "Never trust, always verify," requiring continuous authorization
• Relies on a single perimeter firewall for defense	• Utilizes micro segmentation to isolate resources and limit the lateral movement of attackers
• Often requires purchasing and maintaining expensive hardware appliances to secure the network perimeter.	• potentially reduce costs by eliminating the need for virtual private networks (VPNs)

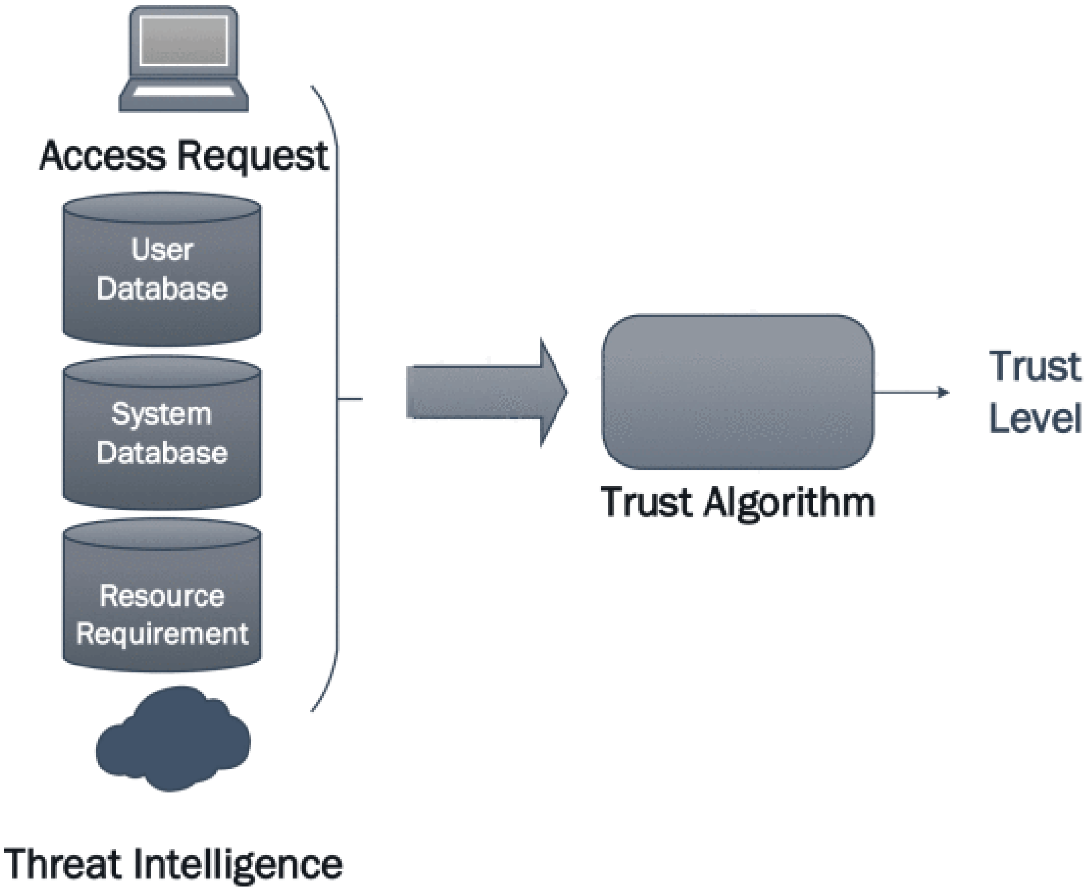
b. Components of Zero Trust Architecture

Within the Zero Trust Architecture, several critical components collaborate to enforce the principles of continuous verification and least privilege access. At its core are the Policy Decision Point (PDP) and Policy Enforcement Point (PEP), which together orchestrate access control decisions. The PDP evaluates access requests against established policies and contextual data, determining whether access should be granted or denied. This decision is then enforced by the PEP, which intercepts access attempts and enforces the decisions made by the PDP in real-time. These components form the dynamic backbone of access control, ensuring that access decisions are not only made based on explicit policies but also on the current context, such as user identity, device health, location, and time of access.

Complementing the PDP and PEP is the Policy Administration (PA) component, which oversees the management and configuration of access control policies. Administrators define and maintain policies that dictate who can access what resources under specific conditions, ensuring alignment with organizational security requirements and compliance regulations. Working in tandem with PA is the Policy Engine (PE), responsible for evaluating access requests against established policies and generating access control decisions. The PE serves as the decision-making mechanism within the architecture, dynamically adapting access privileges based on contextual changes and policy updates.



Central to the Zero Trust Architecture is the Trust Algorithm, which assesses the trustworthiness of users, devices, and other entities seeking access to network resources. By considering factors such as user behaviour, device integrity, authentication strength, and contextual information, the Trust Algorithm dynamically adjusts access control decisions. This continuous evaluation ensures that access privileges remain aligned with the evolving security posture of the organization, mitigating the risk of unauthorized access. Together, these components form a comprehensive framework for access control within the Zero Trust Architecture.



Trust Algorithm (TA) can be implemented in various ways to effectively evaluate the trustworthiness of entities seeking access to network resources. One approach involves distinguishing between criteria-based and score-based TA. In criteria-based TA, multiple conditions are assessed before granting access, ensuring that specific criteria are met. Conversely, in score-based TA, a confidence level is calculated based on various factors and compared to a predetermined threshold. Another distinction lies between singular-based and contextual-based TA. Singular-based TA makes decisions without considering past behaviour, while contextual-based TA leverages historical data to assess whether current actions align with typical behaviour patterns. Contextual-based TA, by analysing past behaviour, offers a more nuanced understanding of user actions, making it the optimal choice for robust trust evaluation in dynamic environments.

5. ZTA IMPLEMENTATION TECHNIQUE

In the implementation of Zero Trust Architecture (ZTA), several critical steps are essential to ensure comprehensive security measures:

a. Identify and Classify Assets: This initial step involves identifying and categorizing all assets within the network, including data, applications, and devices. By classifying assets based on their sensitivity and importance to the organization, security teams can prioritize protection efforts and allocate resources effectively.

b. Least-Privilege Access: Implementing the principle of least privilege ensures that users and devices only have access to the resources necessary to perform their designated tasks. By limiting access rights to the bare minimum required for functionality, organizations can minimize the risk of unauthorized access and potential data breaches.

c. Strong Identity and Access Management: Robust identity and access management (IAM) practices are crucial for enforcing access controls and verifying the identity of users and devices. Implementing multi-factor authentication (MFA), strong password policies, and user provisioning/de-provisioning processes helps strengthen authentication mechanisms and prevent unauthorized access.

d. Continuous Monitoring: Continuous monitoring of network traffic, user activities, and system behaviour is vital for detecting security threats in real-time. By leveraging advanced security analytics and threat intelligence, organizations can identify suspicious behaviour that may indicate a potential security breach.

e. Network Segmentation: Network segmentation involves dividing the network into smaller, isolated segments to contain and mitigate the impact of security incidents. By segmenting the network based on asset classification and access requirements, organizations can limit the lateral movement of attackers and minimize the scope of potential breaches.

f. Data Encryption: Encrypting data both in transit and at rest helps safeguard sensitive information from unauthorized access or interception. By implementing encryption protocols such as Transport Layer Security (TLS) for network communications and encryption algorithms for data storage, organizations can ensure the confidentiality and integrity of their data assets.

6. APPLICATION OF ZTA

Under the application of Zero Trust Architecture (ZTA), two prominent examples demonstrate its effectiveness in diverse contexts:

a. Beyond Corp: Google's implementation of the zero trust model, Beyond Corp, revolutionizes traditional security practices by enabling secure work from virtually any location without relying on a traditional VPN. Beyond Corp employs user- and device-based authentication and authorization to provide secure access to Google's core infrastructure and corporate resources. By eliminating the dependency on perimeter-based security measures, BeyondCorp enhances security posture and flexibility for employees, enabling them to work securely from anywhere, at any time.

b. ZTA in Industry 5.0: Industry 5.0, characterized by the integration of robots and smart machines into manufacturing processes, emphasizes efficiency and automation. ZTA, particularly Zero Trust Network Access (ZTNA), plays a crucial role in enhancing the efficiency and security of organizations operating in Industry 5.0. By implementing ZTNA, organizations can ensure secure access to critical resources and control systems, mitigating the risk of unauthorized access or cyber threats. This enables Industry 5.0 companies to optimize production processes, reduce labour-intensive tasks, and enhance overall operational efficiency while maintaining robust security measures.

7. LIMITATIONS OF ZTA

The limitations of Zero Trust Architecture (ZTA) include complexity, usability, and cost. Implementing ZTA requires expertise and resources due to the deployment of advanced security technologies and complex access control policies, which can be challenging for smaller organizations. Additionally, the rigorous authentication and authorization processes of ZTA may lead to user frustration and reduced productivity. Moreover, the initial investment and ongoing operational costs associated with ZTA implementation can be substantial, potentially straining organizational budgets. Balancing robust security with usability and cost considerations is essential for successful ZTA adoption.

8. CONCLUTION

In conclusion, Zero Trust Architecture (ZTA) represents a paradigm shift in cybersecurity, challenging traditional trust assumptions and promoting dynamic security measures. By emphasizing continuous verification, least privilege access, and micro-segmentation, ZTA offers a proactive approach to safeguarding digital assets in today's evolving threat landscape. Its alignment with modern work trends positions ZTA as a guiding philosophy for the future of cybersecurity, promising enhanced resilience and adaptability in the face of emerging threats.

9. REFERENCES

- NIST Special Publication 800-207 - Zero Trust Architecture, August 2020
- A Zero-Trust Network-Based Access Control Scheme for Sustainable and Resilient Industry 5.0, KHALED ALI ABUHASEL, October 2023
- https://ieeexplore.ieee.org/abstract/document/9773102
- https://www.microsoft.com/en-in/security/business/zero-trust
- https://www.ais.com/from-trust-issues-to-total-security-embracing-zero-trust/
- Zero Trust Implementation in the Emerging Technologies Era: Survey Abraham Itzhak Weinberga, Kelly Cohenb, January 2024
- Proceedings of the Digital Privacy and Security Conference 2019
- https://medium.com/google-cloud/zero-trust-access-with-beyondcorp-d6ed11889e3c