Introduction and Background

A. History of Cybersecurity Threats in Distributed Environment:

With the maturity of information technology, the magnitude, frequency, and complexity of cyberattacks have grown exponentially against distributed digital resources and cloud-related settings.

Medium-sized organizations are currently also being attacked more than 100,000 times a day, affecting the services of both the traditional data center and the new IoT, edge, and cloud platforms.

Digital transformation and the emergence of telecommuting have forgotten the existence of defined boundaries, compelling companies to reevaluate the placement and implementation of security controls.

B. Limitations of traditional perimeter-based security models

The traditional trust-but-verify perimeter model presumes that once internal users and devices are authorized as being trustworthy, the current model is accurate and that neither internal users nor lateral movement can occur and that the blast radius increases with the breach.

Perimeter solutions have a hard time using secure dynamic access by remote workers, third parties, and cloud-based applications leaving gaps in threat prevention.

Solutions available also do not have continuous verification and adaptive access control mechanisms, which are critical to the contemporary threat environment.

C. The Zero Trust Paradigm Shift as a Security Paradigm:

Zero Trust model was created to ensure that implicit trust based on network location is replaced with never trust, always verify, i.e. that continuous authentication, controls based on context, and least-privilege access are ensured whenever an access request is made.

Zero Trust assumes the networks (both internal and external) are untrusted and divides the resources and introduces authentication, authorization and monitoring in all interactions between the user, device and the application.

This change in paradigm was motivated by the understanding that no single defense layer is adequate on its own and distributed and context-dependent controls are the paths to resilience.

D. Research objectives and scope:

The main aim is to give an overall perspective of the present position of the research of Zero Trust, with references made to the architecture concepts, access control, trust assessment algorithms, and identity verification.

It contrasts common Zero Trust strategies, their advantages and disadvantages, and the issues left unaddressed, particularly how to migrate real-life enterprise networks, which today are perimeter-based and security policies, to identity-based approaches to security.

It also seeks to determine feasible research and concrete research directions on the extension, automation, and optimization of Zero Trust solutions to changing distributed computing ecosystems.