Department of Computer Science
Amrita School of Computing, Amritapuri Campus
B Tech CSE (2022 Admission)

19CSE495 PROJECT PHASE-1

PROJECT TITLE SUBMISSION

Group No: **D12**

Team Members

Roll No	Student Name
AM.EN.U4CSE22355	Sherin Shibu
AM.EN.U4CSE22356	Toufeeq SK
AM.EN.U4CSE22359	Varun Dipu Sankar
AM.EN.U4CSE22363	Harini Sivakumar

Project Guide:
Dr. Swapna M.P

Project Title: Secure Health: A Zero Trust Approach

Context of your work:

The work is based on the field of cybersecurity focusing on Zero Trust Architecture. It dives into the sub-area of healthcare security which is facing new vulnerabilities due to the rapid adoption of digital services. The project's topic is the mitigation of security attacks such as Remote Access Trojans (RATs) by integrating Zero Trust principles and Endpoint Detection and Response (EDR).

Abstract of project:

Rapid digitization has created significant cybersecurity risks due to which Traditional network security models are no longer effective against modern threats like Remote Access Trojans (RATs) and insider attacks. These attacks can expose Protected Health Information (PHI) and compromise security which impacts both the patient's privacy and safety. To address these challenges, this work proposes an integrated security framework that uses a combination of Zero Trust Architecture (ZTA) and Endpoint Detection and Response (EDR).Our architecture operates on the Zero Trust principle that states "never trust, always verify," assuming that every network entity is potentially malicious. We outline how to deploy this framework in a healthcare setting. Microsegmentation divides the network into isolated, secure compartments which isolates malware like RATS and helps contain breaches to a single segment. EDR platforms are implemented in each segment to provide continuous monitoring and behavior analytics. This enables real-time detection and automated responses to malicious activity. The combination of ZTA and EDR creates a multi-layered defense that safeguards critical systems and PHI protecting them against threats from legacy medical devices and dispersed IT infrastructure. A comparative evaluation of this unified strategy with conventional security measures shows a clear improvement in security strength. Although a Zero Trust model may introduce some operational overhead, the enhanced ability to contain breaches and protect sensitive information outweighs this trade off. This work offers a foundational blueprint for securing future healthcare environments, presenting a robust solution to a persistent cybersecurity challenge.