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

19CSE495 PROJECT PHASE-1

PROPOSAL SUBMISSION

Group Number:

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

Domain Area: Cybersecurity

Objective of the Project : To propose a security framework that uses both Zero Trust Architecture and Endpoint Detection and Response to overcome cyber security risks in healthcare. This project aims to create a multilayered defense that protects PHI and important systems from threats.

Problem Statement: The digitization of the healthcare industry has introduced significant cybersecurity issues with traditional security models being ineffective against modern threats like RATs and insider attacks. These threats expose PHI affecting both patient safety and privacy. Traditional models fail to protect against these attacks leading to the need for a more robust security framework.

Literature Review:

[Foundation] Three important reference papers (for research-oriented projects) or three existing systems (for application-oriented projects) that form the basis for your problem. Proving that your problem is relevant and technically challenging to address it.

[Discussion] What problem does each of them address, pros and cons of the solution

Selected papers/systems approved by project guide:

S#	Name	Roll Number	Paper Title/ System name	URL/Reference Link of the paper/system selected	IEEE/ACM Publication or source	Year	Scopus Journal with impact factor/ Transaction/ conference	How the selected paper/system is relevant for your project?
1	Varun Dipu Sankar	AM.EN.U4CSE 22359	Endpoint Detection and Response: Why Use Machine Learning?	https://ieeexplore.ieee.org/abstract/document/8939836	IEEE	2019	Conference (ICTC 2019)	The paper reviews Endpoint Detection and Response (EDR) techniques and notes a growing use of modern machine learning methods. These include Random Forest, SVM, and Deep Learning, which help detect advanced threats. This information is relevant to our project since we are implementing EDR within Zero Trust Architecture (ZTA) in healthcare. By using the machine learning insights from this framework, we can set up real-time monitoring with smart anomaly detection and quick incident response. This improves our ability to protect vital healthcare data from advanced attacks like insider threats and

								ransomware.
2	Sherin Shibu	AM.EN.U4CSE 22355	Zero trust cybersecurity: Critical success factors and a maturity assessment framework	https://www.sciencedirect.com/science/article/pii/S0167404823003223	Elsevier (Computers & Security Journal)	2023	Scopus Indexed Journal	This paper delves into why Zero Trust works in actual organizations through the collection of expert views via a Delphi study. Out of this, the authors create a maturity model centered on eight primary areas - identity, endpoints, applications, data, networks, infrastructure, visibility, and automation. For our project, it's helpful because it provides a systematic approach to considering how to apply Zero Trust incrementally. While the research examines Zero Trust in the general industry, we can apply the framework to healthcare. This assists us in strategizing how to protect sensitive assets such as patient data, medical devices, and hospital infrastructure more systematically.
3	Sivakumar Harini	AM.EN.U4CSE 22363	Zero-Trust Architecture for Smart City Healthcare Systems	https://ieeexplore.ieee.org/abstract/document/10959543	IEEE	2025	2nd International Conference on Advanced Innovations in Smart Cities (ICAISC)	This paper proposes a tailored Zero Trust Architecture (ZTA) for healthcare in smart cities. It introduces IAM,

								MFA, micro-segmentation, anomaly detection, and encryption to secure sensitive patient data and infrastructure. It directly supports our project by showing how ZTA can be applied in the healthcare sector.

Summarized survey of all the papers:

S#	Paper Title/ System name	Student Reader name	Main problem addressed in the paper/ Use-cases of the system	Methodology used in the paper/ System to solve the problem	Contributing Results achieved in the paper	What is the limitation of this paper/system in solving the problem that you address
1	Endpoint Detection and Response: Why Use Machine Learning?	Varun Dipu Sankar	The growing complexity of endpoint cyberattacks shows the shortcomings of traditional EDR techniques.	A systematic literature review (SLR) was conducted. The authors created research questions, identified keywords, and searched four major databases: IEEE, ScienceDirect, ACM, and Springer Link, for papers published between 1990 and 2019. After applying inclusion and exclusion criteria, they selected and analyzed 68 papers to identify trends	The review shows a strong trend towards machine learning based EDR solutions. Random Forest, SVM, Logistic Regression, and Deep Learning emerged as the most effective algorithms, providing high accuracy in malware/attack detection. The paper highlights that ML-based approaches improve scalability, reduce false positives, and enable faster incident response compared to traditional techniques.	While the paper provides a thorough review of machine learning applications for Endpoint Detection and Response (EDR), it has a general cybersecurity focus rather than addressing the healthcare sector. This an important gap because healthcare systems have specific constraints such as life critical systems, legacy devices, and higher privacy requirements for patient data (PHI) than other sectors of cybersecurity. The paper does not address what the performance of ML based EDR solutions would be in specific healthcare attack scenarios such as compromise of electronic health records (EHR) systems with ransomware or compromise of medical IoT devices.

				and machine learning techniques used in Endpoint Detection and Response (EDR).		
2	Zero trust cybersecurity: Critical success factors and a maturity assessment framework	Sherin Shibu	Many organizations struggle with Zero Trust because they lack clear guidelines, practical strategies, and evaluation mechanisms. As a result, adoption becomes complex, fragmented, and difficult to measure over time.	The researchers engaged in a three-round Delphi study with 12 cybersecurity experts, building consensus through this iterative process. They developed consensus on the most important Critical Success Factors (CSFs) of Zero Trust adoption, and used the input to develop a multi-dimensional maturity assessment framework that organizations can utilize to assess and inform their Zero Trust implementation.	The study points to eight important areas that need attention for Zero Trust to work well: identity, endpoints, applications and workloads, data, networks, infrastructure, visibility and analytics, and automation. Looking at all these areas together gives a complete picture of how Zero Trust can be implemented in practice. The maturity framework is designed to help organizations check their current level of security, uncover weak spots, and plan a gradual path toward full Zero Trust adoption. This approach moves organizations away from one-off or patchy efforts and instead guides them toward a more structured and reliable security strategy.	Although the framework is very useful, it does have some limitations. The study was based on input from only 12 experts, which means the range of perspectives may not fully reflect the diversity of challenges organizations face when adopting Zero Trust. In addition, the maturity model was presented as a concept and has not yet been tested in real-world environments. This opens up an opportunity to adapt and validate the model in sensitive domains like healthcare, where the stakes are higher — protecting electronic health records, securing medical IoT devices, ensuring the availability of life-critical systems, and meeting strict regulations.
3	Zero-Trust Architecture for Smart	Sivakumar Harini	Smart city healthcare systems face serious risks from interconnected	The authors put forward a Zero Trust framework built specifically for healthcare systems in	The proposed model offers a scalable and layered defense strategy that can adapt as healthcare	The framework is conceptual and has not been tested in real-world healthcare environments. Practical issues such as latency, cost, and usability remain unaddressed,

	City Healthcare Systems		infrastructures and cyberattacks on patient data.	smart cities. The idea is to make sure that no user or device is trusted by default. Instead, every interaction is checked continuously using Identity and Access Management (IAM) along with Multi-Factor Authentication (MFA) and device verification. To stop attackers from moving around the network unnoticed, the framework uses micro-segmentation, which breaks the network into smaller, isolated sections. On top of that, it employs AI-powered anomaly detection to watch for unusual patterns or suspicious activity in real time. To further strengthen security, the system adds end-to-end encryption, secure communication protocols, and audit logging, all of which work together to protect sensitive patient data, ensure compliance with healthcare regulations, and create reliable records for investigations if a breach occurs.	infrastructures grow more complex. By enforcing continuous verification of users, devices, and data flows, it minimizes the chances of unauthorized access going undetected. The integration of AI-powered anomaly detection enables the system to spot insider threats and advanced persistent threats (APTs) in real time, giving healthcare providers a proactive way to respond before damage occurs. With its use of micro-segmentation, encryption, and secure logging, the framework not only protects sensitive patient health information but also ensures that hospitals can meet regulatory compliance requirements. Beyond security, the approach improves the overall resilience of healthcare systems, making them better prepared to withstand both external cyberattacks and internal risks in a smart city environment.	leaving a gap for validating and adapting ZTA in real healthcare settings.
4	Beyond the	Varun Dipu Sankar	The inadequacy of traditional	To overcome these challenges, the paper	The paper demonstrates that the	Despite its advantages, the paper acknowledges several limitations in

	Firewall: Implementing Zero Trust with Network Microsegmentation		perimeter-based defenses (castle-and-moat) in addressing modern cyber threats such as insider threats, APTs, cloud, IoT, and mobility. Once breached, attackers can move laterally with little resistance, making critical data and infrastructure vulnerable.	adopts Zero Trust Architecture (ZTA) in combination with network microsegmentation. ZTA is built on the principle of "never trust, always verify," enforcing least privilege access and continuous authentication of users and devices. The proposed framework integrates identity and access management, network security controls, encryption, monitoring, and analytics. Microsegmentation divides networks into smaller isolated segments, each governed by granular access policies to reduce lateral movement. The methodology is further demonstrated through case studies, including a financial institution and a healthcare organization, where microsegmentation was implemented to enhance compliance, secure sensitive data, and strengthen overall cybersecurity posture.	integration of Zero Trust and microsegmentation significantly improves security outcomes. Organizations that adopted this approach were able to minimize lateral movement, reduce their attack surfaces, and achieve faster detection and response times to threats. Enhanced visibility into network traffic allowed for more effective anomaly detection and forensic analysis. The study also shows that microsegmentation enables organizations to meet stringent compliance requirements such as HIPAA and GDPR by protecting sensitive workloads like electronic health records and financial data. Real-world deployments in both financial and healthcare institutions highlighted tangible improvements, including regulatory compliance, better network performance, improved monitoring, and stronger resilience against sophisticated attacks.	implementing Zero Trust and microsegmentation. Defining effective segmentation policies requires detailed mapping of assets, applications, and data flows, which is a complex and resource-intensive process. The introduction of segmentation boundaries may also lead to performance overhead or latency if not carefully optimized. Scalability is another concern, as continuous monitoring and enforcement across large and hybrid network environments demand significant investment in automation and orchestration. Additionally, the study identifies gaps in long-term research, particularly regarding operational costs, user experience, and performance impacts. While the paper provides strong evidence of ZTA's effectiveness, it does not fully explore emerging challenges such as quantum-era security risks or the difficulties smaller organizations may face in adopting advanced SDN- and automation-driven solutions.
5	A critical analysis	Toufeeq SK	The paper addresses the	The methodology employed in this	The paper's results demonstrate that Zero	The paper identifies several limitations in the current state of

	of Zero Trust Architecture		critical evaluation of the claims and practical realities of Zero Trust Architecture as a security strategy for enterprise systems. The authors analyze whether ZTA, which is frequently promoted as a new and highly secure approach, actually delivers on its promises when scrutinized with the rigorous methods of security theory and security patterns.	paper centers on the use of security patterns as analytical tools to systematically evaluate and design Zero Trust Architectures (ZTA); by mapping ZTA concepts, mechanisms, and claims onto established security patterns and principles drawn from classical security theory, the authors decompose industrial ZTA proposals into their constituent abstractions, sketch a preliminary reference architecture using these patterns, and assess ZTA's ability to address threats and fulfill its security promises, thereby providing a structured, theory-driven critique supported by extensive pattern-based analysis rather than by empirical case studies or quantitative data.	Trust Architecture is primarily an aggregation of established security concepts articulated through security patterns, with its touted novelty lying more in systematic practice than in unique mechanisms; the authors clarify the core abstractions and typical architectural models used in industry, show that current ZTA implementations often lack deep technical guidance and fail to address all security threats comprehensively, expose major unresolved issues such as policy complexity and performance overhead, and ultimately propose a more precise reference architecture rooted in classical security theory, concluding that ZTA's strength is in its disciplined implementation and its role in fostering greater security awareness, rather than in revolutionary innovation	Zero Trust Architecture (ZTA) as follows: there is a lack of detailed technical guidance and comprehensive real-world implementation reports, which makes the practical adoption of ZTA challenging; the overhead and complexity introduced by ZTA, especially with dynamic trust evaluation and fine-grained access policies, are not well understood or measured, potentially leading to significant performance and management burdens; the reliance on microsegmentation leads to an explosion in the number of policies and administrative complexity, making security management more difficult; some threats, especially those arising from application-level interactions or insider attacks, are not fully addressed by ZTA's control-at-access-points approach; furthermore, governance aspects such as role engineering and compliance are insufficiently integrated within current ZTA models; finally, there is a pressing need for systematic threat enumeration, better security reference architectures, and integration of secure system development methodologies to make ZTA more practical and effective.
6	Research on Medical Security	Harini Sivakumar	The main problem addressed in this paper is the increasing network	The methodology used in this paper involves designing a medical security	The results achieved in this paper include the design and simulation of a zero-	The paper identifies several limitations of the proposed zero-trust medical security system: first, the authentication process, while

	System Based on Zero Trust		security threats and vulnerabilities in intelligent medical systems, particularly concerning data leakage and remote attacks that can directly threaten patients' lives. The paper focuses on ensuring the security of medical information systems by integrating Zero Trust security principles, which require dynamic and continuous authentication and authorization of all access subjects, with medical systems. It aims to reduce network security risks in the medical field by proposing a Zero Trust-based medical security system that incorporates dynamic access control based on user behavior risk evaluation and trust assessment to improve the protection of medical equipment and sensitive medical data. This approach addresses the challenges	system based on the Zero Trust (ZT) security model, integrated with a dynamic access control framework that incorporates the Role-Based Access Control (RBAC) model along with a novel trust evaluation mechanism. This is achieved through the creation of an access control model called ABEAC (Access Based on Entity Assessment under Conditions of zero trust), which dynamically calculates user behavior risk values and trust levels using factors such as the value of medical data, vulnerability, and observed threat behaviors. The system architecture includes components such as a policy engine, policy administrator, continuous diagnosis and mitigation (CDM) system, identity management, and policy enforcement points, working together to authenticate and authorize access based on real-time risk and trust assessments. The methodology also	trust medical security system that effectively enhances the security of medical equipment and sensitive medical data through dynamic access control. The proposed system incorporates an access control model called ABEAC (Access Based on Entity Assessment under Conditions of zero trust), which dynamically evaluates user behavior risk and trust levels based on the RBAC model and other security parameters such as the value of medical data, vulnerability, and threat behavior. Through simulation experiments comparing ABEAC with an existing TMBRE model, the authors demonstrate that ABEAC more accurately reflects the relationship between behavior risk and trust, showing sharper risk increases and corresponding trust decreases in response to threatening behaviors. This dynamic adjustment improves security responsiveness, reduces the likelihood of illegal operations	accurate, is relatively cumbersome and results in low work efficiency, which could hinder practical deployment; second, although the system dynamically calculates user behavior risk and trust for access control, the model’s stability and applicability in real-world, complex medical environments still require improvement; third, as medical devices increasingly integrate with the Internet, a more comprehensive medical equipment model structure is needed to better address diverse network security challenges; lastly, the study recognizes the need to further optimize and shorten the identity authentication time while maintaining security, aiming to improve overall system performance and user experience in future work.

			posed by the complexity and sensitivity of medical information systems in an interconnected environment, such as IoT and cloud computing, where traditional security models are inadequate	involves simulating the model to validate its effectiveness, comparing the proposed ABEAC model with an existing model (TMBRE) regarding its ability to dynamically adjust trust and risk in response to user behavior, thereby enhancing security for medical devices and sensitive healthcare data.	by legitimate users, and better protects medical system resources.	
7	Enhancing Cybersecurity in the Philippines Healthcare Sector: A Zero Trust Survey	Sherin Shibu	The main problem addressed in the paper is the heightened vulnerability of the Philippine healthcare sector to cyberattacks, fueled by its rapid digitization and increasing use of electronic health records and interconnected medical devices. Traditional perimeter-based security models have proven inadequate for protecting sensitive patient data in this environment, as demonstrated by incidents such as the ransomware attack on	To address this issue, the authors employed a survey-based literature review methodology. They collated and examined existing research, case studies, and vendor solutions related to the Zero Trust security framework, giving special attention to both global developments and their relevance to the Philippine context. The methodology included analysis of academic literature, incident reports, recommendations from established cybersecurity frameworks, and vendor comparisons to synthesize a landscape of current	The paper's principal results highlight that Zero Trust frameworks offer clear advantages for healthcare including proactive prevention of cyber threats, continuous verification of users and devices, dynamic access controls, and cost-efficiency gains. Case studies and literature review suggest that Zero Trust can reduce breaches and deliver greater data protection compared to legacy methods. The discussion outlines vendor options and emerging architectures that could support healthcare institutions, and	The paper also highlights important limitations. Chief among them is the lack of Philippine-specific studies, pilot projects, or real-world Zero Trust implementations within the local healthcare sector. Much of the evidence for Zero Trust's effectiveness comes from international literature, making it necessary to extrapolate findings rather than rely on local data. Other limitations include implementation barriers due to resource constraints, technical complexity, and knowledge gaps in Philippine healthcare organizations. The authors call for additional, locally tailored research and demonstration projects to establish Zero Trust's efficacy in the unique regulatory and operational context of the Philippines.

			PhilHealth. This has created an urgent need for more modern, robust security approaches in healthcare	challenges and opportunities in healthcare cybersecurity for the Philippines.	emphasizes that even partial adoption of Zero Trust principles can yield meaningful security improvements for critical healthcare data.	
8	Trust No One? A Framework for Assisting Healthcare Organisations in Transitioning to a Zero-Trust Network Architecture	Toufeeq S K	The paper tackles the critical issue that healthcare organisations remain highly vulnerable to internal cyberattacks due to the prevalence of outdated legacy systems and the continuing reliance on traditional perimeter-based security models that focus only on protecting the network from external threats. Despite the development of the Zero Trust model, which aims to remove implicit trust within the network and continuously verify all activity, healthcare providers are often unable to adopt such solutions due to the challenges posed by incompatible or technologically	To address these challenges, the researchers conducted a mixed-method study, beginning with a comprehensive literature review to identify technological and organizational barriers blocking adoption of Zero Trust in healthcare. They then developed a practical framework tailored to healthcare environments, focusing on segmented implementation for legacy and modern systems. The methodology included extensive qualitative experimentation using Cisco Modelling Labs (CML), where hypothetical healthcare network topologies were built and different microsegmentation and access control strategies were tested. Quantitative analysis followed, including t-tests on packet	Key results from the study show that integrating Zero Trust principles such as microsegmentation, use of clustered firewalls, proxy servers for secure internet access, strict access control lists, and continuous monitoring can significantly increase security within healthcare networks and limit the impact of internal breaches. The proposed framework divides implementation into progressive stages, from basic security measures (multi-factor authentication, encrypted storage) and traffic monitoring, to device-level segmentation, access restrictions, and defense-in-depth strategies like DNS sinkholing and behavioural analytics. Simulation results proved that firewall clustering provides	However, the paper notes several limitations. Notably, real-world implementation may be hindered by the financial burden of deploying multiple firewalls and maintaining redundancy required by the Zero Trust approach. Some recommendations (e.g., behavioural analytics, VMware-based microsegmentation) could not be fully tested in simulation due to software and cost limitations. The test environment did not use actual outdated operating systems, which might lead to differences in real deployments. The authors acknowledge that simulation-based results may not fully capture the complexity of live patient-care networks, and call for future empirical studies and customisation for each healthcare organisation's needs. They stress that while the framework provides a secure path, adoption requires careful balancing of security with usability, resource availability, and uninterrupted patient care.

			limited medical devices and infrastructure. This situation is exacerbated by the surge in attacks like ransomware incidents and increased complexity during the COVID-19 pandemic.	latency to compare proxy and firewall-based segmentation approaches, ensuring recommendations would not negatively impact patient care in real environments.	security and acceptable latency, and that judicious segmentation of vulnerable devices can prevent attacks from spreading. The framework is presented as practical and translatable for small to medium-sized healthcare organisations, even those burdened by legacy systems.	

Project Proposal:

Our solution is creating a security framework consisting of ZTA and EDR. It relies on the principle of "Never trust, always verify" which assumes that every entity in the network is potentially malicious. Microsegmentation helps divide the network into compartments which will help contain attacks like RATs. EDR helps provide continuous monitoring, enabling real time detection of malicious activities. This provides a blueprint for securing healthcare networks by providing a solution to modern day attacks.