

PRESENTATION TOPIC:

Designing a Zero Trust Architecture (ZTA) framework for Small and Medium Enterprises (SMEs)

Submitted by:

- ▶ Name: Md Riad Hossain
- ▶ Student ID: 2434324
- ▶ Subject: Research Methods and Professional Development (ACFA7004_LON)

Submitted to:

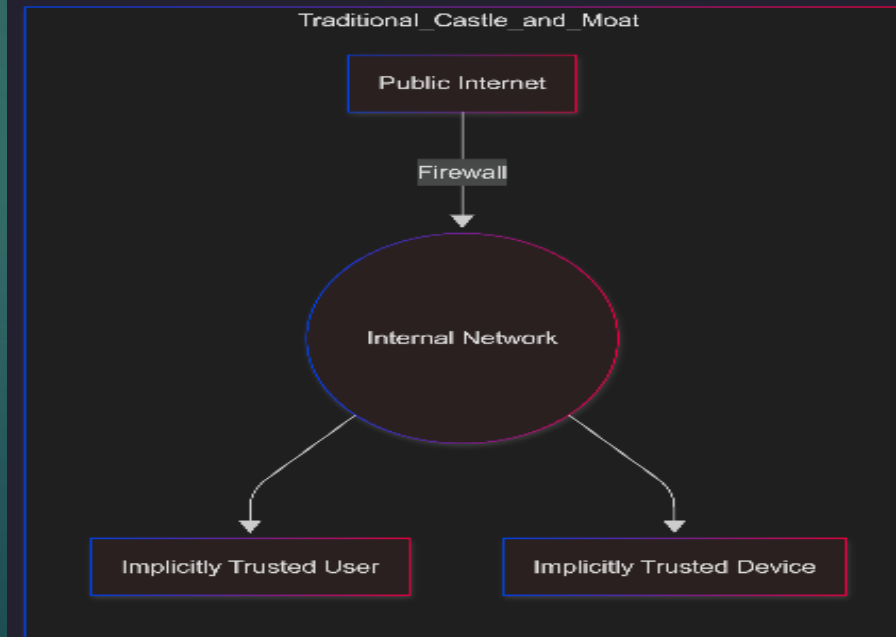
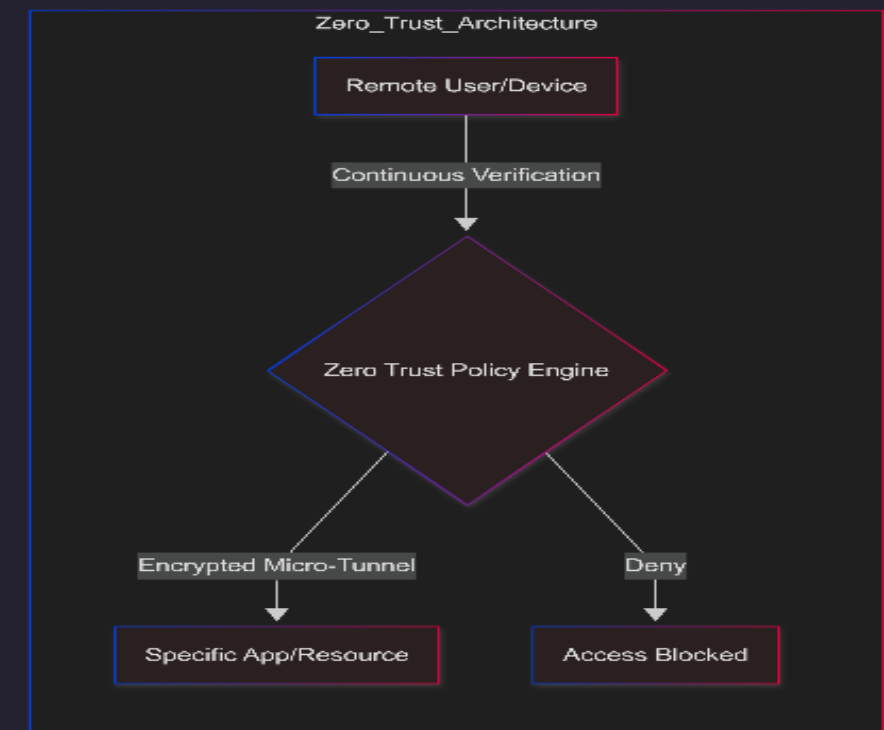
- ▶ Name: Dr. Suresh Shanmugasunadaram
- ▶ Lecturer: Research Methods and Professional Development (London campus)
- ▶ Module code: ACFA7004

Introduction

- ▶ This presentation focuses on designing a Zero Trust Architecture specifically for small and medium enterprises (SMEs). Cybersecurity has become a critical concern due to increasing digital transformation, where organizations rely on cloud computing, remote work, and mobile access. SMEs are particularly vulnerable because they often lack sufficient resources and expertise to defend against modern threats. As traditional security models struggle to keep up with these changes, there is a growing need for more flexible and adaptive approaches. This research aims to address that gap by proposing a practical and cost-effective Zero Trust solution.

Traditional Security vs Zero Trust

- ▶ This slide illustrates the structural differences between traditional “castle-and-moat” security and Zero Trust Architecture. In the traditional model, security is built around a hardened perimeter where the firewall protects the internal network, and anything inside is assumed to be safe. This creates a major flaw known as implicit trust, where users gain broad access after initial authentication. If attackers compromise credentials, they can move freely within the network. In contrast, Zero Trust shifts security away from the perimeter and focuses on individual resources. Every request is continuously verified using identity, device health, and contextual information. Users are granted access only to specific applications through encrypted micro-tunnels, significantly reducing the attack surface and preventing unauthorized movement.



Modern Threats

- ▶ Cyber threats today are more advanced and frequent than ever before. Attackers commonly use phishing techniques to steal user credentials, while ransomware attacks can disrupt entire systems by encrypting critical data. Unlike traditional attacks that targeted infrastructure, modern threats often exploit weak authentication mechanisms. Once access is gained, attackers can escalate privileges and spread laterally across systems. This evolving threat landscape highlights the urgent need for stronger identity-based security models such as Zero Trust.

Zero Trust Concept & SME Challenges

- ▶ Zero Trust is based on the principle “never trust, always verify,” meaning that no user or device is trusted by default. Every access request must be authenticated and continuously validated, regardless of whether it originates from inside or outside the network. This approach significantly reduces the risk of unauthorized access. However, SMEs face significant challenges in adopting Zero Trust due to limited budgets, lack of skilled personnel, and reliance on outdated systems. These constraints make it difficult for smaller organizations to implement complex security frameworks.

Research Problem & Aim

- ▶ Although Zero Trust provides strong security, it is primarily designed for large enterprises with advanced infrastructure and expertise. SMEs struggle to adopt these frameworks due to high costs, complexity, and the risk of misconfiguration. This creates a gap between theoretical models and practical implementation. The aim of this research is to design a scalable and cost-effective Zero Trust framework tailored for SMEs, focusing on simplicity, usability, and real-world applicability without compromising security.

Objectives, Components & Methodology

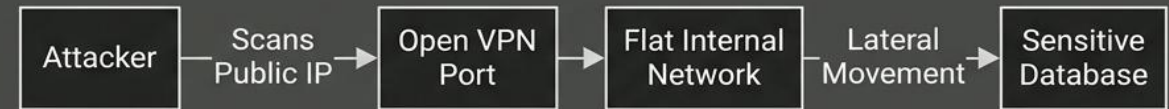
- ▶ This research aims to analyze existing Zero Trust frameworks, identify SME-specific challenges, and design a simplified model that can be effectively implemented. Key components of Zero Trust include Identity and Access Management, Multi-Factor Authentication, device security, network segmentation, and continuous monitoring. These components work together to enforce strict access control and detect suspicious activity. To develop and validate the framework, this study follows a Design Science methodology, combining qualitative and quantitative approaches, including literature review.

MVZT Framework Design & Attack Comparison

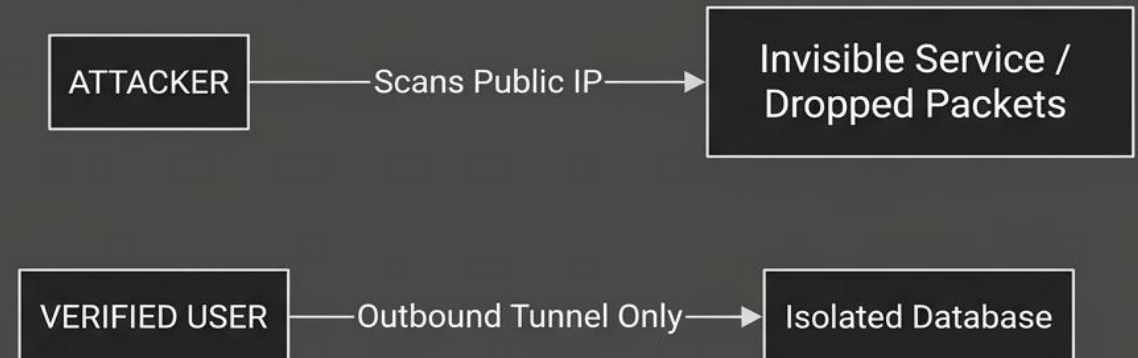
- ▶ This slide demonstrates how the proposed Minimum Viable Zero Trust framework addresses real-world attack scenarios compared to traditional VPN-based access. In a traditional setup, VPNs expose open ports that attackers can discover through public IP scanning. Once inside, the flat network structure allows lateral movement, enabling attackers to reach sensitive systems. In contrast, the MVZT approach removes exposed entry points by using outbound-only connections, making internal services invisible to unauthorized users. Malicious traffic is dropped before it can interact with the system, while verified users are granted secure, encrypted tunnels to specific resources. This ensures strict access control and prevents attackers from exploring the network.

NETWORK ATTACK COMPARISON: VPN vs. MVZT

BEFORE: TRADITIONAL VPN ARCHITECTURE



AFTER: MVZT (MINIMUM VIABLE ZERO TRUST) IMPLEMENTATION



Expected Outcomes & Implications

- ▶ The proposed framework is expected to significantly improve security by reducing the attack surface and limiting unauthorized access. It is designed to be cost-effective and easy to deploy, making it suitable for SMEs with limited resources. The framework also supports compliance with standards such as ISO 27001 and contributes to both academic research and practical cybersecurity solutions. By bridging the gap between theory and real-world application, it provides a scalable and adaptable model for different organizational environments.

Limitations

- ▶ Despite its benefits, the research has certain limitations. The framework is tested in a simulated environment, which may not fully represent real-world conditions. Factors such as user behavior are not completely incorporated, and time and resource constraints limit the scope of testing. While these limitations may affect generalizability, the findings still provide valuable insights into implementing Zero Trust in SME environments.

Conclusion

- ▶ In conclusion, traditional security models are no longer sufficient to address modern cybersecurity challenges. Zero Trust offers a more effective approach by eliminating implicit trust and enforcing continuous verification. However, its complexity makes it difficult for SMEs to adopt. This research addresses that issue by proposing a Minimum Viable Zero Trust framework that is both practical and affordable. The study demonstrates that strong security can be achieved without high cost, making Zero Trust more accessible to smaller organizations.

Future Work

- ▶ Future work will focus on implementing the framework in real-world SME environments to further validate its effectiveness. Integration with legacy systems can be explored, along with the addition of advanced security features and further cost optimization. Thank you for your attention, and I welcome any questions.

Thank you

