



**Evaluating Zero Trust Vulnerabilities in Identity  
and Access Management:  
Strengthening Security Posture in Dynamic  
Environments.**

**Kuruparan Sivalingam  
MS22904850**

A THESIS  
SUBMITTED TO  
SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY  
IN PARTIAL FULFILMENT OF THE REQUIREMENTS  
FOR THE DEGREE OF  
MASTER OF SCIENCE IN INFORMATION TECHNOLOGY (CYBERSECURITY)

SLIIT  
December 2024

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

---

Dr. Harinda Fernando

Approved for MSc. Research Project:

---

MSc. Programme Co-ordinator, SLIIT.

Approved for MSc:

---

Head of Graduate Studies, FoC, SLIIT

# DECLARATION

Declaration I declare that this is my own research thesis, and this thesis does not incorporate without acknowledgement any material previously published submitted for a degree or Diploma in Sri Lanka Institute of Information Technology or any other university or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Sign: - 

Date: - 18<sup>th</sup> of October 2024

# ABSTRACT

S. Kuruparan

MSc in Information Technology (Cyber Security)

**Supervisor:** - Dr. Harinda Fernando

In the era of widespread digital transformation, cybersecurity frameworks play a crucial role in protecting essential assets. The Zero Trust model has become prominent, advocating a “always verify, never trust” approach to secure network access and control. This study examines vulnerabilities within Zero Trust-based Identity and Access Management (IAM) systems, focusing on the challenges that arise in dynamic digital environments where technological advancements and shifting user behaviors impact security.

Using a mixed-methods approach, the research combines quantitative survey data from cybersecurity professionals with qualitative insights from case studies and expert interviews. Findings indicate that while Zero Trust models strengthen organizational security posture, they introduce operational complexities. High resource demands, integration difficulties, and the need for continuous monitoring pose challenges for organizations, potentially hindering efficient operations. These hurdles underscore the difficulty of balancing Zero Trust’s security benefits with streamlined processes. Additionally, the study reveals that Zero Trust IAM vulnerabilities become especially evident in fast-paced digital settings, where rapidly changing technology and varied user interactions demand an adaptive security approach.

To address these vulnerabilities, the study proposes a structured Zero Trust implementation framework, comprising seven key stages: preparation and assessment, identity verification and access control, network and device security, continuous monitoring via User Behavior Analytics (UBA), data security protocols, incident response, and compliance integration. Each stage targets specific challenges, aiming to enhance security without compromising operational efficiency. For example, identity verification and access control help ensure strict authentication, while network segmentation and endpoint security protect critical assets. Regular monitoring with UBA aids in detecting insider threats, and data security protocols like encryption and Data Loss Prevention (DLP) safeguard sensitive information.

This research contributes to cybersecurity in several ways. Academically, it advances understanding of the vulnerabilities within Zero Trust IAM systems, particularly in dynamic environments where these weaknesses are accentuated. Methodologically, it presents a replicable framework that integrates quantitative and qualitative approaches, providing a comprehensive lens for future cybersecurity research. Practically, the study offers actionable recommendations for organizations across industries, enabling them to bolster their security postures against emerging threats. These insights are invaluable for policymakers and industry leaders seeking to establish resilient cybersecurity standards and guidelines in a rapidly evolving digital landscape.

Ultimately, this research provides a detailed look at Zero Trust IAM vulnerabilities and emphasizes the need for adaptive security strategies to navigate the challenges of a

complex digital environment. By addressing key operational hurdles and proposing targeted solutions, this study makes a significant contribution to advancing cybersecurity practices. Its findings underscore the importance of flexible security measures that enable organizations to protect digital assets effectively, supporting organizational resilience within an interconnected and increasingly volatile digital space.

**Keywords:** *Zero Trust, Identity and Access Management (IAM), Cybersecurity frameworks, Data security protocols, Incident response, Data Loss Prevention (DLP) Vulnerability assessment, Cyber threat resilience, Organizational security, Digital asset protection.*

# ACKNOWLEDGEMENT

Even though the research development is an individually assigned academic achievement, I was well supported by my surrounding professionals and loved ones whom I like to be acknowledged with a grateful heart.

First, I like to thank my supervisor **Dr. Harinda Fernando**. His guidance was highly supportive to achieve my academic expectations.

In addition, I would like to take this opportunity to extend my appreciation to **Dr. Prasanna Sumathipala**, who holds the position of Head of Graduate Studies at the Faculty of Computing and Computer Systems Engineering at the Sri Lanka Institute of Information Technology.

Further, I like to thank all my academic lecturers of my master's program who supported and educated me by effectively addressing my knowledge gaps and further developed me to have much-maligned competencies. I like to thank the non-academic staff of the Sri Lanka Institute of Information Technology for their support in addressing all the administrative activities relating to the course.

Lastly, I like to deliver my thank to my loving family members. Your love, support, and kind encouragement always uplift my personal life, professional life, and academic life.

## TABLE OF CONTENTS

DECLARATION	ii
ABSTRACT	iii
ACKNOWLEDGEMENT	v
TABLE OF CONTENTS	6
List of Figures	9
List of Tables	10
Chapter 01. Introduction	11
<b>1.1 Background</b>	11
<b>1.2 Research Problem or Question</b>	13
<b>1.3 Aims and Objectives</b>	16
Chapter 02. Literature Review	20
<b>2.1 Review of Existing Literature</b>	20
2.1.1 Introduction to Zero Trust Architecture	20
2.1.2 Identity and Access Management Fundamentals	22
2.1.3 Vulnerabilities in Identity and Access Management	24
2.1.4 Zero Trust and IAM Integration	27
2.1.5 Strengthening Security Posture with Zero Trust	32
2.1.6 Case Studies and Practical Implementations	35
2.1.7 Challenges and Considerations	37
<b>2.2. Gap Identification</b>	39
2.2.1. Comprehensive Evaluation of Zero Trust Implementations	39
2.2.2 Integration of Advanced Identity Verification Methods	39
2.2.3 Impact of Zero Trust on Operational Efficiency	40
2.2.4 Incident Response and Recovery within Zero Trust Frameworks	40
<b>2.3. Conceptual Framework</b>	40
2.3.1 Independent variables	41
2.3.2 Dependent variables	42
Chapter 03. Research Objectives, Hypotheses and Research Questions	44
<b>3.1 Research Objectives</b>	44
<b>3.2 Hypotheses</b>	47
3.2.1 Hypotheses	47
3.3 Research Questions	48
<b>3.4 Evaluation framework</b>	50

3.4.1 H1 & H2 (Identity Verification and Access Control)	50
3.3.2 H3 & H4 (User Behaviour Analytics and Advanced Verification)	50
3.3.3 H5 & H6 (Incident Response, Data Security, and Compliance)	50
3.3.4 H7 & H8 (Hybrid/Multi-Cloud and Compliance Integration)	51
<b>3.4 Expected outcomes</b>	51
3.4.1 Enhanced Security Posture Through Advanced Identity Verification Methods	51
3.4.2 Improved Operational Efficiency with Identity and Access Management Systems	51
3.4.3 Effective Detection and Mitigation of Insider Threats Using User Behaviour Analytics (UBA)	52
3.4.4 Accelerated Authentication and Access Management Through Advanced Verification.	52
3.4.5 Enhanced Incident Response and Recovery Times	52
3.4.6 Strengthened Security in Hybrid and Multi-Cloud Environments	53
3.4.7 Stronger Compliance and Governance Through Zero Trust	53
Chapter 04. Research Design and Methodology	54
<b>4.1. Research Design</b>	54
4.1.1 Phased Approach	55
<b>4.2. Sampling Strategy</b>	56
4.2.1 Target Population	56
4.2.2 Sampling Strategy	56
4.2.3 Sample Selection	56
4.2.4 Sample Size	57
4.2.5 Qualitative Phase	57
4.2.6 Data Integration	57
<b>4.3. Data Collection Methods</b>	57
4.3.1 Qualitative Data Collection	58
4.3.2 Quantitative Data Collection	59
<b>4.4. Data Analysis Techniques</b>	59
4.4.1 Qualitative Analysis	59
4.4.2 Quantitative Analysis	60
Chapter 05. Significance and Expected Contributions	61
<b>5.1 Significance of the Study</b>	61
5.1.1 Theoretical Significance	61
5.1.2 Practical Implications	62
5.1.3 Policy and Framework Development	62



5.1.4 Enhanced Security Posture	63
<b>5.2 Expected Contributions</b>	63
5.2.1 To Academic Knowledge	63
5.2.2 Advancement of Methodologies	63
5.2.3 Practical Tools and Strategies	64
5.2.4 Policy Recommendations	64
Chapter 06. Ethical Considerations	65
<b>6.1 Informed Consent</b>	65
<b>6.2 Confidentiality</b>	66
<b>6.3 Risk Mitigation</b>	66
<b>6.4 Ethical Review Approval</b>	67
Chapter 07. Timeline	69
<b>7.1 Month 1-2: Literature Review and Research Design</b>	69
<b>7.2 Month 3-4: Ethical Approval and Participant Recruitment</b>	69
<b>7.3 Month 5-6: Data Collection</b>	70
<b>7.4 Month 7-8: Data Analysis</b>	70
<b>7.5 Month 9-10: Findings Synthesis and Drafting of Report</b>	70
<b>7.6 Month 11-12: Finalization and Dissemination</b>	71
Chapter 08. Resources	72
<b>8.1 Equipment and Software</b>	72
8.1.1 Computing Hardware	72
8.1.2 Software Licenses	72
8.1.3 Secure Data Storage	72
8.1.4 Survey and Interview Tools	72
<b>8.2 Access to Databases and Academic Journals</b>	73
<b>8.3 External Collaborations and Partnerships</b>	73
8.3.1 Industry Partnerships	73
8.3.2 Academic Collaborations	73
8.3.3 Cybersecurity Forums and Communities	73
Chapter 09. Results and Analysis	74
<b>Hypothesis</b>	90
Regression Analysis	90
Interpretation	90
References	106

## **List of Figures**

- Figure 1: Logical components of ZTA architecture.
- Figure 2: Zero Trust Architecture
- Figure 3: A Zero-Trust IAM Framework for CC/CbC
- Figure 4: Referenced zero trust IAM integrated framework.
- Figure 5: Policy management based dynamic identity and access management
- Figure 6: Policy development methods
- Figure 7: Focused areas in zero trust architecture
- Figure 8: Parties involved in the authentication process.
- Figure 9: Conceptual Framework Diagram
- Figure 10: Identity Verification
- Figure 11: Access Control Mechanisms
- Figure 12: Network Security Measures
- Figure 13: Device Security
- Figure 14: User behaviour Analytics
- Figure 15: Data Security Protocols
- Figure 16: Incident Response and Recovery
- Figure 17: Compliance and Governance
- Figure 18: Overall impact of Zero Trust Implementation