Dissertation Proposal

Course: Cybersecurity and Web Development

By: Lucas Malik

Student ID: 22806287

Date: 27/10/2024

Contents

[Section 1: Introduction 3](#_Toc180950961)

[Section 2: Background Review 4](#_Toc180950962)

[Section 3: Aims and Objectives 5](#_Toc180950963)

[Section 4: Methodology 6](#_Toc180950964)

[Section 5: Implementation 7](#_Toc180950965)

[Section 6: Testing and Evaluation 8](#_Toc180950966)

[Section 7: Professional, social, economic, and legal issues 9](#_Toc180950967)

[Section 8: Resource Requirements 10](#_Toc180950968)

[Section 9: References, Information Sources that Provide a Context for the Project. 11](#_Toc180950969)

[Appendix 1: Project Activities Plan 12](#_Toc180950970)

# Section 1: Introduction

**Research Question:** How can Zero Trust principles using Identity and Access Management “IAM”, and Multi-Factor Authentication “MFA” in AWS reduce unauthorised access in cloud-based web applications, and what measurable reductions in security incidents can be expected?

The rapid adoption of cloud computing has introduced new security challenges, making web applications increasingly vulnerable to cyber threats. Traditional security methods have proven insufficient in modern environments, where devices, users, and applications often operate beyond the secure boundaries of internal networks.

Zero Trust has emerged as a security model which solves these challenges, operating on the principle of “never trust, always verify.” By requiring continuous identity verification and restricting access through strict controls, Zero Trust minimises unauthorised access risks. This project will examine how AWS’s native IAM and MFA tools can support Zero Trust principles, with the objective of assessing their impact on reducing security incidents in cloud-based web applications.

# Section 2: Background Review

**Cloud Security Vulnerabilities** - As organisations increasingly migrate applications and services to the cloud, web applications have become more exposed to cyber threats. Unlike traditional onsite systems, cloud environments operate on distributed infrastructures, often depending on remote access and shared resources. This architecture introduces unique security risks, as cloud applications are accessible from numerous networks and devices, resulting in potential evasion of traditional security measures. Attackers can exploit these vulnerabilities through various techniques such as credential theft, privilege escalation, and lateral movement, which pose a serious risk to cloud security.

**Limitations of Traditional Security Models** - Traditional security models often assume that everything within an organisation’s network can be trusted, with measures in place to keep external threats out. Unfortunately, this approach in cloud environments is insufficient. Cloud applications frequently interact with external networks making them prone to insider threats, compromised accounts and attacks that bypass perimeter defences. Without continuous verification, traditional security models leave opportunities that attackers can exploit, especially in cloud environments with complex and changing access requirements.

**Relevance of Zero Trust** - The Zero Trust model solves these security vulnerabilities assuming that no user or device should be trusted by default, regardless of their network location. Operating on the principle of “never trust, always verify,” Zero Trust enforces continuous identity verification and strict access control at every point of access. The requirements of Zero Trust align well with modern security needs, making sure every access request is authenticated and authorised. AWS supports Zero Trust with tools such as IAM and MFA, which offer detailed access control and layered identity verification, lowering the risk of unauthorised access.

# Section 3: Aims and Objectives

**Aim:** The design and implementation of a secure, cloud-based web application in AWS leveraging Zero Trust principles using IAM and MFA, reducing unauthorised access and enhancing security.

**Objectives:**

* Deploy essential AWS infrastructure, including an EC2 instance within a VPC, to securely host the web application, performing an initial vulnerability scan to identify and address any critical weaknesses.
* Implement monitoring and logging tools, including AWS CloudTrail for continuous tracking of activities and if feasible integrate GuardDuty for additional real-time threat detection capabilities.
* Configure and test IAM policies and MFA settings to ensure secure and reliable access control. Collect data to measure how well these settings protect the system.
* Conduct a post-implementation vulnerability scan to identify any remaining security weaknesses following Zero Trust implementation.
* Gather and review security data to compare how effective the Zero Trust approach is against traditional security methods, checking if it reduces risks more effectively.

# Section 4: Methodology

This project makes use of a Zero Trust framework to enhance security within AWS cloud-hosted applications, focusing on IAM and MFA as prevention against unauthorised access. The methodology is structured into three keys phases: setup, monitoring, and evaluation, using AWS tools such as IAM and CloudTrail.

**Setup** – This phase involves designing a Zero Trust model on AWS infrastructure with minimal permissions and strict MFA. The setup includes deploying a Node.js application on an EC2 instance as a website structure for access control testing. Initial security checks will identify weaknesses, followed by practical testing of AWS configurations and deployments.

**Monitoring** - To assess zero trust effectiveness data collection will focus on:

* key metrics such as unauthorised access attempts.
* MFA usage frequency; and
* user activity logs.

**Evaluation** - Security performance will be assessed by comparing pre-implementation and post-implementation metrics to assess improvements in access control and unauthorized access reduction, with final checks on the effectiveness of Zero Trust configurations.

This practical approach aligns AWS tools and a Node.js application with Zero Trust principles, establishing a robust security environment for cloud applications.

# Section 5: Implementation

**AWS Infrastructure Setup** - A secure AWS Infrastructure setup will include Amazon Elastic Compute Cloud “EC2” for hosting the node.js application and Virtual Private Cloud “VPC” for network segmentation. SSL certificates will encrypt communications, protecting data-in-transit for strengthened security.

**Deploy Website Content** – Website files, including HTML, CSS, JavaScript, or another suitable language or framework, will be uploaded to the EC2 instance. A web server, such as Nginx or Apache, will be configured on the EC2 instance to securely serve the website content to users.

**IAM and MFA Configuration** - IAM roles will be configured with minimal and essential permissions only, avoiding unauthorised access. MFA will be applied to all sensitive resource access with one-time passwords to maintain robust authentication and support Zero Trust principles.

**Continuous Monitoring with CloudTrail -** CloudTrail will provide continuous monitoring by logging all access events, helping track and audit user activity. If additional time permits, GuardDuty will be enabled to detect real-time threats further enhancing the security posture by identifying unusual patterns or unauthorised access attempts.

**Baseline Metrics Collection –** Initial metrics will track system and access patterns, providing a starting point for later comparison. This data will help show how well IAM and MFA reduce security risks and enhance protection, with potential for additional tools to support data tracking as needed.

# Section 6: Testing and Evaluation

**Access Control Testing** - To verify the effectiveness of IAM and MFA configurations, access control testing will focus on a few high-risk scenarios by simulating unauthorised attempts to gain access to AWS resources. Each attempt will help determine whether the Zero Trust model blocks these effectively. Additionally, the response alerts generated by these unauthorised access attempts will be monitored to ensure they are triggered promptly and accurately, helping to ensure the capability of a rapid response in a real case scenario.

**Vulnerability Scanning** - To maintain the integrity of the AWS environment, a limited number of vulnerability scans will be conducted using AWS Inspector. Helping to identify configuration weaknesses, open ports, or unpatched software within the environment, ensuring that key vulnerabilities are detected and addressed to reinforce the security posture.

**Security Metrics and Analysis** - Metrics on security incidents, including unauthorised access attempts and the frequency of MFA usage, will be tracked, and compared to baseline data from this study as well as data from other relevant studies (if applicable). This analysis will demonstrate improvements, indicating if unauthorised access has decreased and whether the Zero Trust model offers measurable security benefits.

# Section 7: Professional, social, economic, and legal issues

**Professional Standards -** This project follows AWS’s Well-Architected Framework and CIS (Center for Internet Security) controls, ensuring best practices in configuring a secure cloud environment. These standards provide guidance on access management and network security, supporting a robust Zero Trust architecture.

**Social Implications -** Enhancing cloud security through Zero Trust increases public trust, mainly for organisations managing sensitive data. The approach ensures that users' privacy and data is protected with strict access controls and frequent verification, reducing the likelihood of unauthorised access. The Zero Trust model aligns with modern privacy expectations, reinforcing the responsibility that organisations must safeguard user data and enhance its reputation as a reliable and trustworthy guardian of information.

**Economic Implications -** While implementing Zero Trust requires initial investment in AWS services, the opportunity cost in the long run is that it reduces costs associated with data breaches and recovery efforts. Providing cost savings through building brand integrity, reputation, market share, reliable security and reduced risk exposure.

**Legal Implications -** The Zero Trust approach aids legal issues such as compliance with regulations like GDPR by enforcing strict access controls and detailed logging activities. Lowering the legal risks by showing evidence of documented security practices that meet privacy and compliance requirements.

# Section 8: Resource Requirements

**Software Requirements:**

AWS Command Line Interface (CLI): For efficient and scriptable management of AWS resources, allowing streamlined setup and configuration.

**AWS Services**

|  |  |
| --- | --- |
| AWS Systems Manager | Manages, automates, and applies patches to EC2 instances, supporting Zero Trust with role-based access controls. |
| EC2 Instances | Needed for hosting and testing the web application in a secure cloud environment. |
| VPC (Virtual Private Cloud) | Provides network segmentation and isolation, a major part of implementing Zero Trust architecture. |
| IAM (Identity and Access Management) | Critical for configuring roles, permissions, and enforcing MFA to ensure strict access controls. |
| CloudTrail | Enables logging of access events and tracks user activities, essential for auditing and continuous monitoring. |
| AWS Inspector | For performing vulnerability assessments and identifying potential configuration issues, unpatched software, or open ports. |
| AWS Key Management Service (KMS) | Provides encryption key management for secure data storage and transport in line with Zero Trust principles. |
| AWS Config | Monitors configuration changes to ensure resources stay compliant, providing critical support for continuous security monitoring. |
| GuardDuty (if time permits) | Adds an additional layer of security with real-time threat detection and alerting for unusual activity. |
| CloudWatch (if time permits) | Monitors system performance (CPU, memory, disk) and application logs, enabling proactive alerts for unusual patterns or issues. |
| AWS QuickSight **(unsure)** | To analyse and visualize metrics collected from CloudTrail, IAM, and MFA, helping evaluate the Zero Trust model's effectiveness. |
| **Amazon S3 (unsure)** | Offers secure storage with IAM and KMS integration, ideal for storing logs or static application resources. |

# Section 9: References, Information Sources that Provide a Context for the Project.

Roslan, N.I., Mazman, N.T., & Johari, N.F.A. (2024). *Zero Trust Architecture: A Paradigm Shift in Network Security* - This paper provides a detailed review of Zero Trust Principles, focusing on Identity and Access Management (IAM), Multi-Factor Authentication (MFA), and related security controls. Available at [Zero Trust Architecture: A Paradigm Shift in Network Security](https://www.techrxiv.org/doi/full/10.36227/techrxiv.172165641.12548858/v1)

Amazon Web Services (AWS) Security Blog. (2020). *Zero Trust architectures: An AWS Perspective*. - Although not an academic source, the AWS blog offers a detailed overview of Zero Trust principles, tools, and practical steps for implementing Zero Trust in cloud environments, showcasing AWS’s capabilities for secure and reliable setups.

Amazon Web Services (AWS). (n.d.). *AWS Well-Architected Framework*. Amazon Web Services, Inc. - This framework outlines best practices for secure, reliable, and efficient cloud architectures, supporting the use of IAM, MFA, and Zero Trust principles in AWS.

Amazon Web Services (AWS). (n.d.). *AWS Documentation.* - A comprehensive resource offering technical guides on IAM, security practices, and AWS configurations to support Zero Trust implementation. Available at <https://docs.aws.amazon.com/>

Wang, W., Sadjadi, S. M., Rishe, N., & Mahara, A. (2024, May). *Applying Transparent Shaping for Zero Trust Architecture Implementation in AWS: A Case Study.* Available at [2405.01412](https://arxiv.org/pdf/2405.01412)

OpenAI. (2024). *ChatGPT (October 2024 version)*. OpenAI. [ChatGPT](https://chatgpt.com/) - ChatGPT was used to assist with research, idea structuring, and refinement for clarity in sections such as objectives and methodology, with all final content and analysis being original work.

# Appendix 1: Project Activities Plan

Gantt Chart (Draft)

Please Note: Additional time is provided at the end in case of any unforeseen circumstances or improvement.

A graph on a screen

Description automatically generated