Faculty of Information Technology

ITRMA4-12 – Research Methodologies in IT

Research

Project

Student number and name	EDUV8219015 – John Crouse
Project title	The Role of Zero Trust Architecture in Securing Modern Enterprise Networks
Submission date	24/06/2025

Project submitted in partial fulfilment of the requirements for ITRMA4

Table of Contents

1. Abstract

Cyber-attacks against modern enterprise networks have rapidly changed after the outbreak of the COVID-19 outbreak. Enterprises needed different methods and strategies to secure their networks. This study will introduce the Zero Trust Architecture (ZTA) and investigate it along with machine learning (ML). The key threats that traditional models encounter will be assessed as well as the key principles and components of ZTA. Moreover, a literature review will be conducted to analyse how effective ZTA is at securing enterprise networks. ML will also be investigated to find out its potential in enhancing ZTA with automating access control, threat detection, and the mitigation of security risk. Furthermore, an optimised ML-driven ZTA framework will be proposed to solve the problem of flawed internal threat protection. This model will be more adaptive to evolving cyber-attacks, especially internal. It will use a qualitative research methodology. It will employ the phenomenological research design under the constructivist paradigm to understand expert experiences and perceptions. The target population of this study will consist of cybersecurity professionals and IT managers with relevant experience in ZTA and enterprise network security. Furthermore, purposive sampling will be used to choose participants. The sample size for this study will be relatively small for the purpose of data saturation. Semi-structured interviews with open-ended questions will be used to collect data, and thematic data analysis will be used to identify patterns and gather insights on collected data. Ultimately, the goal of this study is to propose an intelligent, scalable, and cost-effective ZTA framework that incorporates an ML algorithm to secure cloud-based enterprise networks.

2. List of Abbreviations

ACE	- Access Control Engine
AI	– Artificial Intelligence
APT	– Advanced Persistent Threat
CABS	– Cloud Access Security Brokers
EDR	– Endpoint Detection and Response
IaaS	– Infrastructure as a Service
IAM	– Identity and Access Management
IDS	– Intrusion Detection System
IPS	– Intrusion Prevention System
MFA	– Multi-Factor Authentication
ML	– Machine Learning
PaaS	– Platform as a Service
PEP	- Policy Enforcement Point
PLA	– Physical Layer Authentication
RBAC	– Role-Based Access Control
SaaS	– Software as a Service
SDN	– Software-Defined Networking
SIEM	– Security Information and Event Management
SSO	– Single Sign-On
VPN	– Virtual Private Network
ZTA	– Zero Trust Architecture
ZTNA	– Zero Trust Network Access

3. Introduction

3.1. Basic Overview of the Topic

After the rise of the COVID-19 pandemic, the accelerated shift to remote work environments and cloud computing has fundamentally changed the cybersecurity strategies that enterprises employed. Traditional network security models, such as perimeter-based and Defense in Depth models, have become less effective against more advanced cyber threats, due to their implicit trust and flawed perimeter-based defenses. The Zero Trust Architecture (ZTA) addresses this problem with promise by incorporating the least privileged access and continuous verification. However, ZTA also comes with its own flaws like high performance overhead, implementation costs. And integration complexity. Machine learning (ML) has emerged as a powerful potential enhancement to ZTA. ML has shown to offer various capabilities like automated threat detection, real-time anomaly monitoring, and intelligent access control, to cover the weaknesses of ZTA. This study explores the integration of ML with ZTA. Additionally, it proposes a more adaptive architecture that will be more effective at protecting enterprise cloud environments.

3.2. Background to the Study

Enterprises recently became more reliant on remote and cloud work, and traditional security architectures have become less effective at countering large-scale attacks as a result. ZTA has proven to be effective by implementing continuous verification and least privileged access. Machine learning algorithms have also shown potential in enhancing threat detection and automating access control decisions, potentially overcoming existing ZTA limitations.

3.3. The Problem Statement

Traditional network security models assume inherent trust based on network locations, leaving their enterprises at risk of large-scale breaches. Cybercriminals use advanced attacks to exploit traditional security models' trust-based weaknesses (Gudala *et al.*, 2021). Despite ZTA's effectiveness in reducing these risks, its adoption remains difficult due to high costs, complex integration with legacy systems, increased system overhead, and lack of industry standard (Phiayura & Teerakanok, 2023).

Machine learning has shown potential in enhancing cybersecurity by automating access control, improving anomaly detection, and reducing manual security management burdens (Mangayarkarasi *et al*., 2024). Existing research lacks standardised ML-based approaches for ZTA, raising concerns about its effectiveness at detecting and mitigating internal and external cyber-attacks. There is a need to refine ZTA with intelligent ML-driven mechanisms to optimise security without drastically increasing costs and complexity.

3.4. Research Questions/Hypothesis

How can ZTA, enhanced with machine learning, improve enterprise network and cloud environment security compared to traditional models? What are the challenges enterprises face when implementing ZTA into their networks? Moreover, how can machine learning algorithms cover the weaknesses of ZTA to improve its effectiveness in securing cloud work environments in enterprises?

Hypothesis: The integration of machine learning algorithms in ZTA will enhance network security by improving threat detection, and reducing unauthorised access, making ZTA more effective practical for enterprise network security and cloud work environments.

3.5. Research Aim & Objectives

This study explores ZTA integration in enterprise security and the use of machine learning to prevent unauthorised access and cyber-security in cloud computing.

Research Objectives:

- To investigate how ZTA can enhance network security.
- To identify key strategies for the successful implementation of ZTA.
- To explore how ML algorithms can address the limitations of ZTA to improve the overall security of cloud computing in enterprises.

4. LITERATURE REVIEW

4.1. Introduction

This section will focus on reviewing existing research done on different network security architectures. The challenges of existing security models will be explored and explained. The origin and role of the Zero Trust Architecture (ZTA) will be explored in depth, and it will be compared to existing traditional network security models. This literature review will also attempt to find strategies for effective implementation of ZTA, as well as identifying gaps in existing research done on network security models.

4.2. Define Key Concepts

- **Access Control Engine (ACE):** A network security component that continuously evaluates user trust levels for granting users access to the network's resources (Pampattiwar & Chavan, 2023).
- **Cloud Access Security Brokers (CABS):** A security solution that gives control and visibility over cloud-based applications and data. It also enforces security policies (Ahmad *et al*., 2022).
- **Endpoint Detection and Response (EDR):** A network security solution that continuously monitors network endpoints and responds to threats in those endpoints (Kaur & Tiwari, 2021).
- **Enterprise Network Security:** Measures and strategies that are designed and implemented in an enterprise's network to protect it from potential threats.
- **Infrastructure as a Service (IaaS):** A cloud computing model that provides resources like servers, storage, and networking, to virtualise computing over the internet (Malla & Christensen, 2020).
- **Identity and Access Management (IAM):** A framework of policies and technologies that ensure that only the correct users and devices gain access to the network.
- **Intrusion Detection System (IDS):** A network security component that monitors network traffic within a network to find potential threats and security breaches (Saranya *et al*., 2020).

- **Intrusion Prevention System (IPS):** A network security component that actively tries to prevent identified threats by blocking or rejecting malicious activities in real time (De Araujo-Filho *et al*., 2021).
- **Least Privilege Access:** This principle emphasises that only the least amount of access should be given to a user. Only the absolute necessary resources can be granted to a user to complete their work, and no more than that.
- **Multi-Factor Authentication (MFA):** This security process uses multiple verification layers like biometrics, passwords, and one-time pins (OTPs) to authenticate users (Suleski *et al*., 2023).
- **Machine Learning (ML):** A subfield of Artificial Intelligence (AI). It focuses on training machines to perform like humans using algorithms and large amounts of data.
- **Micro-Segmentation:** The principle that splits a network into multiple segments to limit lateral movement within the network. These network segments isolate attacks to be countered more efficiently.
- **Platform as a Service (PaaS):** A cloud computing model that provide hardware and software tools, allowing developers to build, deploy, and manage applications.
- **Policy Enforcement Point (PEP):** An enforcement point used in a network to enable, monitor and terminate connections between subjects and resources. PEP consists of two parts: the client and the resource (Creutz & Dartmann, 2023).
- **Role-Based Access Control (RBAC):** A security model that grants users and devices access to certain resources or applications of a network based on their role in an organisation (Singh & Kumar, 2024).
- **Software as a Service (SaaS):** A subscription based, cloud computing model that provides software applications over the internet, mitigating the need for local installation and maintenance (Seifert *et al*., 2023).
- **Software-Defined Networking (SDN):** A network architecture approach that enables centralised and programmable network management by separating the control plane from the data plane (Haji *et al*., 2021).
- **Security Information and Event Management (SIEM):** A system that collects, analyses, and logs data and responds to network security events.
- **Single Sign-On (SSO):** An authentication process that allows users to use the same set of login credentials to access multiple other applications (Alaca & Oorschot, 2020).

- **Virtual Private Network (VPN):** A secure network that allows users to browse public networks securely and privately, by encrypting network traffic.
- **Zero Trust Architecture (ZTA):** A network security architecture that emphasises on the principle of “Never trust, always verify”. In other words, no one in the network can be trusted, and everyone in the network needs to be verified before being granted access (Fernandez & Brazkuk, 2024).

4.3. Challenges of Traditional Security Models

4.3.1. Perimeter-Based Security Threats & Vulnerabilities

The perimeter-based network security model has been the most common model used by enterprises worldwide, since it has been highly effective at mitigating most security risks. However, as the technologies and strategies for countering cyber threats have evolved, so have those of the attackers. More recently, technologies and strategies for breaching corporate networks have become increasingly sophisticated and have become more difficult to detect. The traditional perimeter-based model is left with five major vulnerabilities. They will be briefly discussed.

Implicit Trust of Internal Users: Most network security models have been designed to protect the network from attacks outside the business. However, these models were always built on trust inside the business. This would leave a business wide open to any attacks initiated from inside the organization, for example, an insider pretending to be an employee of the company or an employee committing the crime for their own personal gain (Kang *et al*., 2023). Once an attacker gains access to the internal network, they are left free to do whatever they want within the network.

Lack of Granular Access Control: The traditional model grants access to users based on their location. This can cause the wrong user to be given over-privileged access. Consequently, this could result in several major problems like data loss, and the accidental modification or deletion of data. This could cause distrust between users within the organization and difficulty in traceability for data breaches and data loss (Khan *et al*., 2022).

Cloud and Remote Work Risks: Due to cloud computing and remote work allowing resources to be accessible from many locations, perimeter-based network models are becoming increasingly ineffective and redundant, and more personal devices and home networks are becoming vulnerable to security breaches. The common security risks that come with cloud computing and remote work include phishing attacks, unsecure Wi-Fi use, unathorised access from weak passwords, password sharing, unencrypted file sharing, and account hijacking (Arunkumar, 2023).

Lateral Movement: Due to enterprise networks continuously expanding, cyber attackers can breach their networks more effectively by moving in the network laterally. They can implement advanced persistent threats (APTs) more effectively. These cyber-attacks are a lot more sophisticated and emphasise attacking the enterprise's network undetected. (Smiliotopoulos et al., 2024) states that APTs are most used for stealing sensitive information, committing espionage, and disrupting the most crucial systems and operations within the network.

Phishing and Credential Theft: The perimeter-based network security model leaves the enterprise's network vulnerable to phishing attacks and credential theft. Cyber attackers commonly use phishing. This is a method of cyber-attack where the attackers disguise emails they send to users of the network as emails from the legitimate enterprise, to harvest the credentials or to trap them into a malicious website (Varshney *et al*., 2024).

4.3.2. Insider Threats & Lack of Visibility

An insider threat is a cyber-attack committed by an individual that works within the target enterprise or organisation and gains unauthorised access. These attacks can be committed by current employees, former employees, contractors, vendors, and business partners or investors (Yuan & Wu, 2021). These attacks can be intentional or unintentional. Insiders can be categorised into three types:

- Malicious insiders misuse access to intentionally harm the enterprise through data and information theft, system sabotage, or leaking sensitive information.
- Negligent insiders harm the organization unintentionally, by falling for phishing traps, sharing credentials, or accidentally configuring the enterprise's network security incorrectly or improperly.

- Compromised insiders are users of the enterprise that have been hacked or have had their devices hijacked to access the network and harm the enterprise.

Due to traditional security models focusing their efforts on outside threats to the network, they often fail to properly monitor and control threats that come from inside the network (Yaseen, 2023). Four major visibility vulnerabilities can be found within parameter-based network security models:

- Networks can be faced with limited monitoring and tracking of internal activity and lateral movement within the network. This can make it marginally easier for insiders to gain access to sensitive information and resources within the network.
- Enterprise networks can have weak authentication and access control. This causes difficulty in tracing the insider’s movement and detecting unauthorised actions within the network.
- Enterprises can be left at risk of data exfiltration. In other words, sensitive information can be stolen from the network without triggering any alerts within its systems.
- Many parameter-based models lack the ability to detect Shadow IT. Shadow IT means that an unauthorised device or application has access to the network and its information and resources.

4.3.3. Inability to Protect Cloud & Remote Work Environments

Most parameter-based network security models are ineffective at protecting cloud and remote work environments because of their designed focus on outside threats (Arunkumar, 2023). There are several key reasons why these security models struggle to provide adequate protection. They include unsecured home networks, use of personal devices, lack of employee training, inconsistent use of VPNs, and weak password authentications.

4.4. Overview of Zero Trust Architecture

4.4.1. The Key Principles of Zero Trust Architecture

The ZTA combats the weaknesses of traditional parameter-based network security models by incorporating eight key principles. These key principles will be briefly discussed:

Never Trust, Always Verify: The most important and well defining principle of ZTA is the "Never Trust, Always Verify" principle. He *et al*. (2022) explains that this principle emphasises no one trust in the enterprise's network at all. No user, device or application can be trusted. Any access from inside or outside of the network can only be granted after maximum authentication and continuous verification.

Least Privilege Access: The "Least Privilege Access" principle is an essential principle incorporated in ZTA that emphasises on minimal access granted to an authorised and verified user. This simply means that the autorised user can only access the resources and information necessary to complete the necessary work, and no more than that (Teerakanok *et al*., 2021). This ensures that the intentions of the granted access are only in good will, and that lateral movement is restricted.

Micro-Segmentation: Micro-segmentation is a principle that focuses on dividing a network into smaller segments, by deploying a Policy enforcement point (PEP) closer to the data or resources and placing virtual firewalls (Syed *et al*., 2021). This is done with the purpose of preventing the spread and escalation of an already occurring cyber-attack, by isolating the attack in the current segment. This makes countering the cyber-attack a lot more effective and efficient and it restricts lateral movement within the network.

Multi-Factor Authentication (MFA): Multi-factor Authentication is the principle that enforces multiple layers of authentication and verification in network segments (Ahmadi, 2024). Most network security models have one layer of authentication, but this principle is essential in the ZTA to mitigate the risk of easy unauthorised access. This principle ensures that only the correct people can be granted access to the network's information and resources.

Continuous Monitoring and Analytics: ZTAs use continuous monitoring and analytics. With this principal security teams are assigned in the network to monitor user behaviour, device activity and network traffic. This helps the network to detect threats and counter them swiftly and effectively.

Device and Endpoint Security: ZTAs integrate the principle of device and endpoint security. This principle ensures that only "trusted" devices have access to the network's resources and information, though they would still have to be authorised and continuously verified the same as untrusted devices.

Encryption of Data: Encryption of data is a significant requirement of the ZTA. In the ZTA data needs to be encrypted in transit and at rest (Syed *et al*., 2021). This principle ensures that the sensitive data and resources in the network stay integral and confidential, and that they can't be altered by security breaches in any way shaped or formed.

Policy Enforcement Based on Context: ZTA enforces policy based on multiple contexts. These contexts can include the user's identity, the security of the device accessing the network, or the risk level of the user or device. Security policy enforcement for ZTA includes remote endpoints, cloud environments, and Internet of Things (IoT) devices (Nahar *et al*., 2024). They are applied and integrated throughout the entire network.

4.4.2. The Components of a Zero Trust Network

A Zero Trust Network can be composed of several components that work cohesively to ensure strict access control, authentication and continuous verification of users, and detection of security breaches. They include:

Identity and Access Management (IAM): IAM is the component that allows digital identities to be created, deleted, and managed for users and devices on the network. Its main purpose is to make identity and access management in a work environment more secure (Indu *et al*., 2018). Examples of IAM can include MFA, Single Sign-On (SSO), and role-based access control (RBAC).

User and Device Authentication: ZTA reduces the risk of a network being attacked by splitting authentication into two parts: user authentication and device authentication. ZTA also uses strong authorisation mechanisms to verify the users' identities before granting them access to the network's resources and information (Cao *et al*., 2024). Examples can include biometrics, certificate authentication systems, physical layer authentication (PLA), or even password-less authentication systems.

Least Privilege Access Control: This component of ZTA ensures that authorised users only get access to enough information and resources to complete the necessary tasks (Kodakandla, 2024). This component follows the Least privilege access principle.

Micro-Segmentation: ZTA uses micro-segmentation to prevent lateral movement of cyber-attacks once the network's security has been breached. This is done by splitting the network into different parts or segments, isolating the attack in one part of the network to be countered more effectively (A Al-Ofeishat and Alshorman, 2023).

Network and Endpoint Security: This is a component in ZTA that protects endpoints and traffic in networks from cyber-attacks and exploits (Kamruzzaman *et al*., 2022). Endpoint security use measures and systems such as endpoint detection (EDR), intrusion detection/prevention systems (IDS/IPS), and firewall rules.

Data Security and Encryption: ZTA uses data encryption, securing data in transit and at rest. This protects data from being accessed by unauthorised users while the data is stored and while it is in the network traffic. This ensures data integrity, confidentiality, and availability (Mahawar, p.31).

Continuous Monitoring and Threat Detection: ZTA uses user behaviour-based anomaly detection to analyse user behaviour and respond to out of the ordinary patterns in behaviour (Yuan *et al*., 2018). These systems are used together with security analytics to respond to any potential network threats.

Security Policy Engine: ZTA uses a centralised system that enforces security policies in the network dynamically. This system adapts its access controls to certain contexts, such as user behaviour, device location, and device security.

Zero Trust Network Access (ZTNA): ZTA uses the Zero Trust Network Access that replaces traditional virtual private networks (VPNs), by continuously authenticating and verifying the user or device in the network (Sandhu *et al*., 2024). ZTNA grants secure access to users based on their identity, location, and device security. ZTNA also allows users to access only the necessary resources to do their work.

Cloud Security Integration: Cloud security extends the principles of ZTA to cloud computing. This ensures that consistent security policies are enforced for various service models such as hybrid cloud environments, multi-cloud environments, Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) (Gudimetla and Kotha, 2018).

4.4.3. Differences Between ZTA and Traditional Models

Based on various articles found, several key differences between the ZTAs and traditional models have been found. These differences include:

Security Approach: Traditional models have a perimeter-based security approach that focuses on protecting the network from outside threats (Stafford, 2020). Inside threats aren't considered due to implicit trust among their internal users.

Trust Assumptions: Traditional models trust internal users implicitly and for a long time, while ZTAs implements the "Never trust, always verify" principle. ZTAs trust no-one, not even internal users. In ZTAs every access request needs to be authenticated and then continuously verified (He *et al*., 2022).

Network Access: Traditional models allow users to have access to various resources and information within the network. ZTAs implement the "Least privilege access" principle. This restricts access of users within the network to only the necessary resources and information (Sharma, 2022).

Authentication: Traditional models typically use one-time authentication at login. Contrary to traditional models, ZTAs use continuous authentication and verification based on the "Never trust, always verify" principle (Nahar *et al*., 2024).

Lateral Movement: In traditional models, cyber-attackers can move freely in the network once they have gained access to the network. On the other hand, in ZTAs, micro-segmentation restricts unauthorised users from accessing the rest of the network by splitting the network into multiple segments that need authentication and continuous verification to access. This makes lateral movement in ZTA networks significantly more difficult and mitigates the single point-of-failure problem in the network (Mämmelä et al., 2016).

Protection Scope: Traditional models typically protect only on-premises users and devices within the network, making them more susceptible to endpoint breaches. On the other hand, ZTAs protect both on-premises and cloud and remote parts of the network by incorporating end-point protection.

Remote Work Security: Most enterprise networks that use traditional security models require virtual private networks (VPNs), firewalls, and web gateways to secure personal devices and home Wi-Fi routers working in the network. These technologies can still be compromised and exploited (Assunção, 2019). ZTAs do not rely on VPNs to protect remote users and devices. Instead, instead use Zero Trust Network Access (ZTNA) to secure remote access to the enterprise network.

Threat Detection: Traditional models use reactive security measures. I other words they detect the threats after the attack in the network happened. ZTAs use proactive security measures. They continuously monitor user behaviour and react to unusual or suspicious activities within the network (Nahar *et al*., 2024).

Device and Endpoint Security: Traditional models have a limited focus on device security and focus more on the on-premises network. On the other hand, security and verification on users and devices based on certain contexts, before granting them access to the network.

Cloud Security: Traditional models are not designed to protect cloud or even hybrid environments, because of their parameter-based approach to network security. ZTAs' protection goes beyond the network itself and protects cloud and hybrid environments.

4.5. Implementation Strategies for ZTA

4.5.1. Identity and Access Management

Identity and Access Management (IAM) is a key component of ZTA. IAM ensures that only the correct users and devices are authorised and authenticated to access the network and its resources. Traditional models allow access to users and devices based on their locations, increasing the chances of a successful breach of the network's security. IAM in ZTAs mitigate this common problem by authenticating users and devices upon every access request and continuously verifying them as they move and work in the network (Indu *et al*., 2018). This is done regardless of whether the users are members of the enterprise or not. Key IAM strategies in ZTA would include:

- **Multi-Factor Authentication (MFA):** Multi-Factor Authentication is an IAM strategy that implements multiple verification factors such as a password with a biometric or a one-time pin (OTP) (Suleski *et al*., 2023). This strategy is highly effective at preventing unauthorised access.
- **Least Privilege Access:** With the least privileged access strategy, authorised users only gain access to the limited resources and information to be able to do the necessary work. This protects the rest of the network's sensitive information and resources from being accessed by users, whether they are outside attackers or disgruntled employees (Brickley & Thakur, 2021).
- **Role-Based Access Control (RBAC):** With role-based access control, access policies are given to users of the network based on their roles in the enterprise. These roles are established in hierarchies, and they represent the qualifications, responsibilities, and tasks of the user within the enterprise (Singh, 2024). This prevents users with lower roles in the enterprise hierarchy accessing information and resources that would only be permitted to higher roles in the enterprise.
- **Continuous Authentication:** Traditional models typically rely on a single login to gain access to the network. This leaves the network at risk of being breached by a cyber-attacker and allows the attacker to move laterally within the network. IAM in ZTAs mitigates this risk by continuously verifying the identity of the users and devices that have access to the network. This helps to detect anomalies and remove access from suspicious users and devices (Teerakanok *et al*., 2021).

- **Single Sign-On (SSO):** Single Sign-On is an integral strategy of IAM (Sharma, 2022). This strategy balances enhanced security and user convenience by allowing users to be authenticated once and gain secure access to multiple parts of the network.
- **Device Identity Verification:** Device Identity Verification is an IAM strategy implemented in a network that ensures that only the authorised and trusted devices can access the network. This reduces the risk of network endpoints being compromised or exploited.

4.5.2. Micro-Segmentation

Micro-segmentation is another key component of ZTA. Micro-segmentation is a ZTA strategy that divides the network into multiple segments, allowing the network to isolate a cyber-attack in one segment and prevent lateral movement within the network (A Al-Ofeishat, 2023). This mitigates the common problem traditional models face: single point of failure. Micro-segmentation has several benefits that make it an essential and viable strategy for the implementation of ZTAs.

Firstly, micro-segmentation minimises the attack surface on a network by limiting access to only the essential information and resources. Secondly, it prevents lateral movement of the cyber-attacker, even if they only compromised a single endpoint of the network. Thirdly, it enhances compliance by isolating sensitive and valuable data and enforcing strict access policies. Fourthly, it continuously enforces and evaluates dynamic policies of users and devices, based on user identity, device safety, and device location. Lastly, it isolates and segments workloads based on their sensitivity and risk level, to protect critical applications and services.

Micro-segmentation is implemented using software-defined networking (SDN), firewalls, and identity-based policies (Zanasi *et al*., 2024). Least privilege access can also be enforced to increase security in the network and its resistance to cyber-attacks.

4.5.3. Continuous Monitoring & Threat Detection

Traditional network security models typically rely on static and periodic defences to protect the network. However, unlike traditional models, ZTAs use a proactive approach to protecting the network. This is done by implementing the strategy of continuous monitoring and threat detection. This is an essential component that ensures security by maintaining it in real-time and continuously monitoring user behaviour, network traffic, and network vulnerabilities (Ike *et al.*, 2021). This aspect of ZTA integration also has several key components.

Real-time security analytics is a component of threat detection that uses AI-driven analytics and machine learning to detect anomalies, potential threats, and suspicious activities within a network (Sharma, 2022). These activities can include suspicious login locations, unauthorised login and data access attempts, or even abnormal data transfers.

Behaviour-based detection is a tool used in ZTA to detect unusual or suspicious activities within the network. At first it establishes normal activity patterns of users and devices, then it searches and identifies deviations of these patterns and flags them as potential attackers in the network (Ahmadi, 2024). Action is taken according to these behaviour flags.

Endpoint detection and response (EDR) is a component in threat detection that continuously monitors endpoints of a network. It detects threats like malware, ransomware and unauthorised modifications and automatically responds to them before they spread through the rest of the network (Karantzas and Patsakis, 2021).

Zero Trust Network Access is a component of ZTA that continuously evaluates, and changes access permissions of users based on their risk levels and security. ZTNA adapts access controls by using risk-based authentication and policy enforcement.

Security Information and Event Management (SIEM) is the component of threat detection that uses real-time alerting technology and forensic analysis to provide a wide view of the network areas and mitigate threats in the network (González-Granadillo *et al.*, 2021).

Continuous monitoring and threat detection combines all these components to continuously monitor the network, detect and respond to threats early, and strengthen the resistance of the network to any inside and outside cyber-attacks. These measures perfectly align with the main principles of ZTAs, ensuring that the network's security stays strong and adaptable for a long time.

4.6. Machine Learning in ZTA

Machine learning is a key part of the successful implementation of ZTA. Machine learning significantly improves identity authentication, identity authorisation, and anomaly detection to mitigate unauthorised access and other cyber threats. Machine learning is used in ZTA to detect abnormal patterns and anomalous behaviour in user activities that would usually have bypassed traditional security models. Through continuous learning and adapting to new attack patterns, ML-driven ZTA significantly enhances security in cloud environments.

A hybrid ML-driven algorithm combines supervised and unsupervised learning techniques to improve identity authentication and threat detection, and follows three key processes:

- **Identity Authentication and Authorisation:** Machine learning greatly improves identity authentication by analysing network traffic, user behaviour, access requests, and device history and then flagging any abnormalities that could suggest being threats to the network (Chinamanagonda, 2022). These are strengths that are not usually found in traditional models.
- **Anomaly Detection and Behaviour Analytics:** These are essential components in ML-based ZTA algorithms. With behaviour analytics baseline activity patterns are established so that deviations in these baseline patterns can be determined and detected. This improves ML-driven algorithms' ability at detecting anomalies in user behaviour and responding to more sophisticated and subtle cyber-attacks (Veeramachaneni, 2025).

- **Real-time Threat Mitigation and Automated Response:** Real-time threat mitigation technologies like IDS and CASBs are used in ML-driven algorithms to improve their threat detection (Chinamanagonda, 2022). After potential threats get detected, automated responses get triggered to retaliate against these threats and evaluate them. This also reduces the number of false positives in the network.

It has been strongly suggested that ML-driven ZTA has several benefits for enterprise networks that would include automated access control, reduced insider threats, enhanced cloud security, and reduced false positives.

4.7. Case Studies on ZTA Adoption

4.7.1. Google's BeyondCorp

BeyondCorp adopted ZTA at Google and enforced strict identity and device verification. They implemented MFA to ensure that only verified and managed devices could access BeyondCorp's resources. Moreover, they implemented an access control engine (ACE) to continuously evaluate the trust of users of their network (Nguyen *et al*., 2023). An internet-facing proxy was implemented at BeyondCorp to ensure every access request was authenticated and authorised, and if an unfamiliar device was detected, they would be quarantined for evaluation.

4.7.2. Cisco

Cisco is a network technology company that Implemented ZTA in their network. They implemented adaptive access control, machine learning, and identity verification, and as a result were able to detect and retaliate to potential threats in real-time (Haddon and Bennett, 2021). They ultimately became more resistant to cyber-attacks from inside and outside their network and more efficient and controlling threats in their systems.

4.7.3. Lessons Learned from Real-World Implementations

These case studies of ZTA adoption have shown several important lessons to learn. Firstly, BeyondCorp's implementation of MFA and managed device policies have demonstrated that strict identity and device verification is crucial to preventing and eliminating unauthorised access. Secondly, Cisco's use of machine learning to efficiently detect and respond to threats in real-time has been a prime example of the significance of continuous monitoring and adaptive access control for security maintenance. Thirdly, BeyondCorp's strategically migrated low-risk workflows have demonstrated how gradual migration, and phased implementation helps to minimise risks during data transitions. Lasty, it has been clearly shown that ZTA is highly effective at strengthening an enterprise network's resistance to internal and external threats using proactive security approaches and technologies.

4.8. Identified Gaps in Existing Research

There are several gaps in existing research on Zero Trust Architecture and ML-based ZTA algorithms. Currently there is a lack of standardised machine learning models, limited real-world implementation studies of ZTA and ML-based algorithms in ZTA, and several challenges in anomaly detection accuracy. ZTA faces a lot of performance and scalability related issues, especially when they need to be implemented in large enterprise networks. ML-based algorithms are also difficult to integrate in legacy systems. Moreover, privacy concerns regarding continuous monitoring of users still need to be further explored and addressed. Overall machine learning techniques for the refining of ZTA are currently underdeveloped and strategies need to be developed to integrate machine learning in ZTA with efficiency and accuracy.

4.9. Summary

Zero Trust Architecture (ZTA) enhances enterprise network security by enforcing strict access controls and continuous verification. However, challenges like high costs and complex integration hinder the adoption of ZTA. This study highlights the strengths and limitations of ZTA as well as emphasising the potential of machine learning (ML) in improving network security when integrated into ZTA. Machine learning improves threat detection, adaptive authentication, and automation. ML-driven ZTA algorithms can analyse user behaviour, detect real-time anomalies, and protect endpoints more proactively through refined access control. Future research should focus on optimising ML-driven ZTA models to improve usability while reducing false positives. This can ensure that enterprises can effectively counter ever developing cyber threats.

5. Research Methodology

5.1. Introduction

This section will discuss the research methodology that will be used for this research, including the paradigm, population, sampling method, data collection and analysis methods, quality of data, and associated logistics and limitations like timeframe and budget. The research methodology with all these following research aspects will be chosen, described and justified. Choosing the appropriate research methodology will assist in finding solutions for the proposal to the challenges of the Zero Trust Architecture.

5.2. Summary Table

Aspects	**The Research project**
Research Methodology	Qualitative
Reasoning	Inductive
Research Design	Phenomenology
Paradigm	Constructivism
Population	Security professionals in enterprises
Sampling Method	Non-probability (purposive)
Sample Size	5 – 10 participants
Data collection method	Semi-structured interviews
Question type	Open-ended questions
Data analysis	Thematical analysis
Quality of data	Trustworthiness and credibility
Use	Applied research
Limitations	Time and participant availability
Time frame	10 months
Budget	R500 – R1500
Ethical considerations	Informed consent, anonymity, voluntary

5.3. Research Methodology - Qualitative

There are two main types of research methodologies: quantitative and qualitative methodology. The qualitative research methodology focuses on descriptive and non-numerical data like words, experiences, and perceptions. In the qualitative methodology the "why" and "how" questions are asked to understand phenomena (Kamal, 2019). Methods of qualitative data collection can include open-ended questions in semi-structured interviews and observations (Tenny *et al*., 2017). This methodology uses inductive reasoning and the constructivist paradigm. Phenomenology, ethnography, and grounded theory are common research designs used in qualitative research, and it allows the researcher to explore and understand real-world events, experiences, and opinions (Muzari *et al*., 2022). Sampling is usually done non-randomly in qualitative research with the purpose of gathering insights from knowledgeable and experienced participants, especially during purposive and quota sampling (Mweshi & Sakyi, 2020). Lastly, qualitative research uses thematic analysis to identify patterns collected while keeping context of the data analysis in mind (Tisdell *et al*., 2025).

On the other hand, the quantitative research methodology is used to collect and analyse numerical data to identify, test hypotheses, and analyse the relationships between different variables. Quantitative research uses deductive reasoning to objectively and systematically quantify and measure phenomena. This methodology uses structured research design, usually in the form of experiments, surveys, and questionnaires, to collect data (Watson, 2015). Sampling is done randomly to emphasise generalisation. Types of random probability sampling include simple random sampling, systematic sampling, stratified sampling, and cluster probability sampling. Lastly, quantitative research uses statistical data analysis (Ahmad *et al*., 2019).

Overall, the qualitative research methodology will be the most appropriate methodology in the case of this study due to its flexibility and depth. Using this research approach will help to find the experiences and challenges of ZTA implementation in enterprise networks. Moreover, this will gather more meaningful and authentic data, leading to deeper insights into how enterprises adopt ZTA and how professionals deal with the problems that come with ZTA.

5.4. Reasoning - Inductive

The qualitative research methodology uses inductive reasoning. Inductive reasoning is a bottom-up approach that uses specific observations and patterns in data to develop broader and generalised theories and conclusions (Sauce & Matzel, 2022). Inductive reasoning allows insights to naturally emerge from the real-life experiences of participants. This enables the researcher to identify common themes, explore a variety of perspectives, and expand on existing knowledge without the restrictions of pre-defined hypotheses (Barroga *et al*., 2023).

The quantitative research methodology, on the other hand, uses deductive reasoning. Deductive reasoning is a top-down logical approach that starts with general theories and hypotheses and tests them with structured data collection methods to come to more specific conclusions. This method of reasoning relies on measurable variables and predefined assumptions to confirm or debunk existing theories with concrete empirical evidence. Overall, deductive reasoning ensures consistency, objectivity, and replicability (Sauce & Matzel, 2022).

This study will use inductive reasoning. Given its exploratory nature and reliance on authentic descriptive data, inductive reasoning will the most appropriate to implement in this study. It will help the researcher have a more nuanced understanding of the challenges of ZTA implementation and respect the complexity of real-life experiences of individuals.

5.5. Research Design - Phenomenology

Phenomenology is one of several types of qualitative research designs. This research design focuses on investigating and understanding how individuals experience certain phenomena in real life (Alhazmi & Kaufmann, 2022). This design allows the researcher to gather deep and valuable insights from participants, and to interpret and give meaning to the participants' experiences. One of the biggest advantages that come from phenomenology is its focus on depth and authenticity. It is simply a positivist research approach that presents findings based on grounded human experience.

On the other hand, quantitative research uses surveys and experiments as research designs, to collect and analyse numerical data. Surveys involve distributing structured questionnaires with close-ended questions to a large group of participants. Surveys aim to measure variables and identify trends and, in a population (Ghanad, 2023). Experiments involve manipulating one or more independent variables under controlled conditions and observing the effects they have on other dependent variables (Mohajan, 2020). Overall quantitative research designs researchers to find and identify cause-and-effect relationships and test hypotheses with objectivity and high precision.

This study will use the phenomenological research design. This qualitative research design will help provide trustworthiness and credibility to this study. It will align this study's goal of understanding real life experiences. It will ensure that the findings of this study will accurately align with the reality of participants' experiences. Ultimately, this research design will contribute greatly to both theory and practice in the field of security and network engineering.

5.6. Paradigm - Constructivism

Constructivism is a qualitative research paradigm that focuses on the social construction of reality and understanding how individuals make sense of their personal experiences to learn (MacLeod *et al*., 2022). It explains that knowledge is mainly gained through human interaction and interpretation. Constructivism is especially well suited with the qualitative research methodology, because its main goal is to explore the experiences, values, perceptions, and beliefs. Moreover, it focuses more on complexity, depth, and different perspectives, rather than measurable variables and narrow meanings in ideas (Bogna *et al*., 2020).

Positivism, on the other hand, is a quantitative research paradigm that focuses on objectivity, measurement, and observable phenomena. Positivism is grounded in the belief that there can only be one objective external reality, and that it can be studied through statistical analysis and empirical observation. The positivist paradigm encourages the researcher to test existing hypotheses, identify patterns in collected data, and generalise findings in populations. This paradigm prioritises reliability, replicability, and the discovery of universal laws of truths (Park *et al*., 2020).

This study will be grounded in the constructivist paradigm. Implementing this paradigm will support this study in its goal to understand and respond to phenomena that network security professionals experience in different ways and their perspectives on these experiences. Great insights and information would be gathered without needing to convert them into quantifiable data. This will also enhance the relevance, credibility, and authenticity of the information gathered during the study.

5.7. Population – Network Security Professionals

In the field of research, the population refers to a group of individuals or entities that share the same characteristics and participate in the findings of the study (Hossan et al., 2023). Properly defining the population in a study will help the researcher gain more relevant and applicable results from the intended group.

The population for this study will include network security professionals in Gauteng, South Africa. This group will be chosen based on their relevance to network security, the ZTA model, and machine learning algorithms. These network security professionals will be assumed to have a significant amount of first-hand experience with network security and working with machine learning algorithms.

5.8. Sampling Method – Non-Probability (Purposive)

Non-probability sampling is a qualitative method of sampling where the researcher selects specific participants to collect data for their research. In purposive sampling, participants that are the most relevant for the study topic are chosen. Here the researcher intentionally chooses participants based on specific characteristics and criteria that will align with the goals of the study (Andrade, 2021). Its goal is to gain information and deep understanding from the participant group that have a greater amount of knowledge and experience on the topic being studied.

Probability sampling, on the other hand, is a quantitative method of sampling the lets the researcher select participants using random methods. Common types include simple random, systematic, stratified, and cluster sampling. This type of sampling ensures that every member of a population has an equal chance of being chosen (Rahman *et al*., 2022).

This study will use a non-probability sampling method, more specifically purposive sampling. Unlike random sampling, this method will include individuals who have more real-life experience and informed opinions. These participants will provide more nuanced and valuable insights on the ZTA model and the incorporation of machine learning algorithms in the model. The study will thus have improved trustworthiness.

5.9. Sample Size – 5 to 10 Participants

In qualitative research, the sample size is not determined by statistical power as it is in quantitative research. It is rather determined by data saturation. This simply means that eventually there will be a point at which no new insights or perspectives will be gained from further data sampling (Sarfo *et al*., 2021). Purposive samples need to be “short and sweet”. The sampling process needs to focus less on quantity and more on the quality of the data. The data being collected needs to be authentic, valuable and adequate to answer research questions effectively.

Sampling five to ten participants will be the most appropriate for this qualitative research approach. Firstly, this sample size will align well with the phenomenology design to better understand the experiences, challenges, and perspectives of professionals working in network security, specifically in the context of implementing the ZTA model. Secondly, it will ensure manageability, depth, thorough thematic analysis, and accurate interpretation of findings in the study. Lastly, it will offer transferable insights for enterprises implementing the ZTA model.

5.10. Data Collection Method – Semi-Structured Interviews

Semi-structured interviews are effective for qualitative data collection. During these interviews, pre-determined open-ended questions are asked to participants. The questions asked in these interviews are not necessarily pre-set. The interviews can have guidelines to what questions can be asked and to then be followed up by “on-the-fly” questions for the purpose of elaboration and deeper understanding (Karatsareas, 2022). They provide flexibility and seek to deeply understand the experiences, perspectives, and insights of different participants.

Structured interviews, on the other hand, are more effective for quantitative data collection. Structured interviews allow researchers to ask prepared sets of close-ended questions in a specific sequence (Naz *et al*., 2022). Structured interviews are more consistent than semi-structured interviews, since they ask each participant in a population the same questions. This makes data easier to collect, quantify and compare.

In this study, semi-structured interviews will be conducted. It will explore the challenges and strategies involved in implementing the ZTA model in modern enterprise networks. Due to ZTA being a relatively new and developing concept, gathering knowledge and opinions from network security professionals will be essential for the study's authenticity and credibility. These interviews will also allow a researcher to ask sequential questions and elaborations to gain more nuanced insights of how the ZTA model, and the incorporation of machine learning algorithms are perceived.

5.11. Question Type – Open-Ended

Open-ended questions are questions usually asked in qualitative research. They do not restrict participants from predefined answers. Instead, they allow participants to provide their own creative and original answers based on their own real-life experiences and perspectives (Elliott, 2022). These questions are the typical "how", "what", and "why" questions.

Close-ended questions, on the other hand, are usually asked for in quantitative research. These questions usually provide participants with predefined answer choices. Close-ended questions can include "yes-or-no" questions, multiple choice questions, or scale rating questions. These questions simplify the quantification, statistical analysis, and comparison of data collected from participants in a large sample. These questions are ideal for surveys, structured interviews, and questionnaires (Jain, 2021).

Open-ended questions will be asked in the semi-structured interviews. Asking participants open-ended questions in semi-structured interviews will help the researcher to explore challenges and implementation strategies of the ZTA model in depth. Participants will also be allowed to express their thoughts freely and the researcher will be able to uncover unanticipated issues.

5.12. Data analysis – Thematic

Thematic analysis is a method of qualitative data analysis that is ideal for identifying, analysing, and interpreting common themes within qualitative data. It focuses on the knowledge, experiences, values and opinions of different individuals. Most importantly, thematic analysis is independent of specific theoretical frameworks, allowing the researcher to implement any research paradigm into their study (Miller & Brewer, 2020). This study will use thematic analysis. It follows a six-phase framework.

Firstly, it familiarises the data. In this phase the researcher reads and re-reads the interviews to better understand the data collected. Secondly, it generates initial codes. In the case of this study, the relevant portions of the text will be coded based on recurring ideas, statements, and observations related to ZTA challenges and implementation strategies. Thirdly, it searches for themes. Similar codes will be grouped together, and preliminary themes will be formed from them. Fourthly, it reviews the themes. The researcher will be able to review and refine the themes, ensuring they accurately represent the datasets and answer research questions. Fifthly, they define and name the themes. In this phase every theme will be defined and named according to their contribution the understanding of the topic of ZTA and machine learning. Lastly, it produces the report (Dawadi, 2020). All the themes will be integrated into the final research report. Direct quotes from network professionals will support this research report to provide important insights.

5.13. Quality of Data – Credibility & Trustworthiness

When the quality of the collected data is considered, it should focus on two key ideas. Credibility refers to the confidence of the findings being truthful. It is the qualitative equivalent of internal validity. To achieve credibility, the study should apply triangulation, reflexivity, prolonged engagement, and peer debriefing (Ahmed, 2024). Trustworthiness refers to the transferability, dependability, and confirmability of the collected data (Haq *et al*., 2023). Following the guidelines of credibility and trustworthiness will ensure reliability for the study. Moreover, it will help gather more valuable insights into ZTA.

5.14. Use – Applied Research

Applied research is a form of qualitative research that is conducted to solve practical and realistic problems through the systematical application of theoretical knowledge of specific situations. Contrary to basic research focusing on the expansion of general and theoretical knowledge, applied research focuses on gathering actionable insights and recommendations that can improve practices and systems in the field of study (Akcigit *et al*., 2021). The main goal of applied research is to find solutions to specific problems and form strategies that can be applied to real-world situations.

Basic research, on the other hand, is also known as pure or fundamental research. It is a form of qualitative research that focuses on expanding general knowledge. It also focuses on understanding phenomena and/or underlying principles without immediate practical application. Basic research lets the researcher explore theories, concepts and ideas to gain deeper knowledge that can support applied research of future discoveries (Shi *et al*., 2022).

This study will conduct applied research. Applied research will be the most appropriate type of research to conduct for this study. This study will not only focus on understanding the theory behind ZTA and the implementation of machine learning but also strive to gain deeper insights into them by exploring the real-life, challenges and strategies from network security professionals. Using applied research will help to address contemporary problems within the cyber security space, provide practical guidance to organisations and professionals, and translate existing theory to real-world strategies.

5.15.Time frame

Tasks	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Topic Design	🟥									
Literature Review		🟥								
Research Design			🟧							
Proposal				🟨						
Group Selection & Topic Finalisation				🟩						
Ethical Clearance				🟩						
Research Ethical Committee					🟦					
Data Collection & Analysis						🟦				
Report					🟦	🟦	🟦	🟦	🟦	🟦
Presentation				🟪					🟪	🟪

5.16.Budget

This study will be conducted on a relatively small scale. Expenses will be kept to a minimum by leveraging existing resources and conducting semi-structured interviews that will be cost-effective. The budget in total will add up to a minimum of R 500 and a maximum of R 1 500.

Cost items	**Amount (R)**
Data bundles	R 300
Printing and photocopying	R 200
Transport	R 400
Others	R 100
Total	R 1000

5.17. Conclusion

In conclusion, this study proposes a structured plan to explore the challenges and implementation strategies of ZTA in securing enterprise networks. It will employ a qualitative approach, supported by inductive reasoning, a phenomenological research design, and the constructivist paradigm. Purposive, non-probability sampling with open-ended questions in semi-structured interviews will be used to collect data from five to ten network security professionals. The collected data will be thematically analysed to identify patterns and insights. The study will be conducted with strict adherence to key ethical considerations, like confidentiality, anonymity, informed consent, and voluntary participation. Research will be conducted over a ten-month period with a feasible budget. Furthermore, research will be conducted to contributed to applied research by providing practical insights to guide the successful implementation of ZTA in real-world contexts.

6. Ethical Considerations

Ethical considerations will be the most important part of this research project. They ensure that participants are treated with respect, fairness and dignity. Three major ethical considerations will be taken during this study. Before conducting interviews with participants, informed consent will need to be obtained from. This means that they will need to be fully informed on the nature, goals, and scope of the study, and their rights will need to clearly be explained, especially their right to withdraw at any point during interviews (Husband, 2020). Participants will have to sign consent forms to confirm that their participations will be voluntary.

Anonymity and confidentiality will need to be taken into consideration. Personal identifiers should not be recorded and responses from all participants will have to be coded and stored securely. The information gathered from these interviews will need to be used solely for academic purposes (Laryeafio & Ogbewe, 2023).

To ensure that participants will not feel coercion or pressure, they will be informed that their responses will be recorded only for educational purposes. Participants will also need to know that their responses will be completely anonymous.

7. List of References

A Al-Ofeishat, H. and Alshorman, R., 2023. Build a secure network using segmentation and micro-segmentation techniques. *International Journal of Computing and Digital Systems*, *16*(1), pp.1499-1508.

Ahmad, S., Mehfuz, S., Mebarek-Oudina, F. and Beg, J., 2022. RSM analysis based cloud access security broker: a systematic literature review. *Cluster computing*, *25*(5), pp.3733-3763.

Ahmad, S., Wasim, S., Irfan, S., Gogoi, S., Srivastava, A. and Farheen, Z., 2019. Qualitative v/s. quantitative research-a summarized review. *population*, *1*(2), pp.2828-2832.

Ahmadi, S., 2024. Zero trust architecture in cloud networks: Application, challenges and future opportunities. *Journal of Engineering Research and Reports*, *26*(2), pp.215-228.

Ahmed, S.K., 2024. The pillars of trustworthiness in qualitative research. *Journal of Medicine, Surgery, and Public Health*, *2*, p.100051.

Akcigit, U., Hanley, D. and Serrano-Velarde, N., 2021. Back to basics: Basic research spillovers, innovation policy, and growth. *The Review of Economic Studies*, *88*(1), pp.1-43.

Alaca, F. and Oorschot, P.C.V., 2020. Comparative analysis and framework evaluating web single sign-on systems. *ACM Computing Surveys (CSUR)*, *53*(5), pp.1-34.

Alhazmi, A.A. and Kaufmann, A., 2022. Phenomenological qualitative methods applied to the analysis of cross-cultural experience in novel educational social contexts. *Frontiers in psychology*, *13*, p.785134.

Andrade, C., 2021. The inconvenient truth about convenience and purposive samples. *Indian journal of psychological medicine*, *43*(1), pp.86-88.

Arunkumar, J.R., 2023. Study Analysis of Cloud Security Chanllenges and Issues in Cloud Computing Technologies. *Journal of Science, Computing and Engineering Research*, *6*(8), pp.6-10.

Assunção, P., 2019, January. A zero-trust approach to network security. In *Proceedings of the digital privacy and security conference* (Vol. 2019). Porto Protugal.

Barroga, E., Matanguihan, G.J., Furuta, A., Arima, M., Tsuchiya, S., Kawahara, C., Takamiya, Y. and Izumi, M., 2023. Conducting and writing quantitative and qualitative research. *Journal of Korean medical science*, *38*(37).

Bogna, F., Raineri, A. and Dell, G., 2020. Critical realism and constructivism: merging research paradigms for a deeper qualitative study. *Qualitative Research in Organizations and Management: An International Journal*, *15*(4), pp.461-484.

Brickley, J.C. and Thakur, K., 2021. Policy of least privilege and segregation of duties, their deployment, application, & effectiveness. *Int J Cyber Secur Digit Forens*, *10*(4), pp.112-119.

Cao, Y., Pokhrel, S.R., Zhu, Y., Doss, R. and Li, G., 2024. Automation and orchestration of zero trust architecture: Potential solutions and challenges. *Machine Intelligence Research*, *21*(2), pp.294-317.

Chinamanagonda, S., 2022. Zero Trust Security Models in Cloud Infrastructure-Adoption of zero-trust principles for enhanced security. *Academia Nexus Journal*, *1*(2).

Colomb, Y., White, P., Islam, R. and Alsadoon, A., 2022. Applying zero trust architecture and probability-based authentication to preserve security and privacy of data in the cloud. In *Emerging trends in cybersecurity applications* (pp. 137-169). Cham: Springer International Publishing.

Creutz, L. and Dartmann, G., 2023, November. Decentralized Policy Enforcement in Zero Trust Architectures. In *2023 IEEE Future Networks World Forum (FNWF)* (pp. 1-6). IEEE.

Dawadi, S., 2020. Thematic analysis approach: A step by step guide for ELT research practitioners. *Journal of NELTA*, *25*(1-2), pp.62-71.

De Araujo-Filho, P.F., Pinheiro, A.J., Kaddoum, G., Campelo, D.R. and Soares, F.L., 2021. An efficient intrusion prevention system for CAN: Hindering cyber-attacks with a low-cost platform. *IEEE Access*, *9*, pp.166855-166869.

Elliott, J., 2022. The craft of using NVivo12 to analyze open-ended questions: an approach to mixed methods analysis. *The Qualitative Report*.

Fernandez, E.B. and Brazhuk, A., 2024. A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces*, *89*, p.103832.

Ghanad, A., 2023. An overview of quantitative research methods. *International journal of multidisciplinary research and analysis*, *6*(08), pp.3794-3803.

González-Granadillo, G., González-Zarzosa, S. and Diaz, R., 2021. Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), p.4759.

Gudala, L., Shaik, M. and Venkataramanan, S., 2021. Leveraging machine learning for enhanced threat detection and response in zero trust security frameworks: An Exploration of Real-Time Anomaly Identification and Adaptive Mitigation Strategies. *Journal of Artificial Intelligence Research*, *1*(2), pp.19-45.

Gudimetla, S.R. and Kotha, N.R., 2018. Cloud security: Bridging the gap between cloud engineering and cybersecurity. *Webology (ISSN: 1735-188X)*, *15*(2).

Haddon, D. and Bennett, P., 2021. The emergence of post covid-19 zero trust security architectures. *Information Security Technologies for Controlling Pandemics*, pp.335-355.

Haji, S.H., Zeebaree, S.R., Saeed, R.H., Ameen, S.Y., Shukur, H.M., Omar, N., Sadeeq, M.A., Ageed, Z.S., Ibrahim, I.M. and Yasin, H.M., 2021. Comparison of software defined networking with traditional networking. *Asian Journal of Research in Computer Science*, *9*(2), pp.1-18.

Haq, Z.U., Rasheed, R., Rashid, A. and Akhter, S., 2023. Criteria for assessing and ensuring the trustworthiness in qualitative research. *International Journal of Business Reflections*, *4*(2).

He, Y., Huang, D., Chen, L., Ni, Y. and Ma, X., 2022. A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, *2022*(1), p.6476274.

Hossan, D., Dato'Mansor, Z. and Jaharuddin, N.S., 2023. Research population and sampling in quantitative study. *International Journal of Business and Technopreneurship (IJBT)*, *13*(3), pp.209-222.

Husband, G., 2020. Ethical data collection and recognizing the impact of semi-structured interviews on research respondents. *Education Sciences*, *10*(8), p.206.

Ike, C.C., Ige, A.B., Oladosu, S.A., Adepoju, P.A., Amoo, O.O. and Afolabi, A.I., 2021. Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. *Magna Scientia Advanced Research and Reviews*, *2*(1), pp.074-086.

Indu, I., Anand, P.R. and Bhaskar, V., 2018. Identity and access management in cloud environment: Mechanisms and challenges. *Engineering science and technology, an international journal*, *21*(4), pp.574-588.

Jain, N., 2021. Survey versus interviews: Comparing data collection tools for exploratory research. *The Qualitative Report*, *26*(2), pp.541-554.

Kamal, S.S.L.B.A., 2019. Research paradigm and the philosophical foundations of a qualitative study. *PEOPLE: International Journal of Social Sciences*, *4*(3), pp.1386-1394.

Kamruzzaman, A., Ismat, S., Brickley, J.C., Liu, A. and Thakur, K., 2022, December. A comprehensive review of endpoint security: Threats and defenses. In *2022 International Conference on Cyber Warfare and Security (ICCWS)* (pp. 1-7). IEEE.

Kang, H., Liu, G., Wang, Q., Meng, L. and Liu, J., 2023. Theory and application of zero trust security: A brief survey. *Entropy*, *25*(12), p.1595.

Karatsareas, P., 2022. Semi-structured interviews. *Research methods in language attitudes*, pp.99-113.

Khan, M.J., 2023. Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews*, *19*(3), pp.105-116.

Khan, N., J. Houghton, R. and Sharples, S., 2022. Understanding factors that influence unintentional insider threat: a framework to counteract unintentional risks. *Cognition, Technology & Work*, *24*(3), pp.393-421.

Kodakandla, N., 2024. Securing Cloud-Native Infrastructure with Zero Trust Architecture. *Journal of Current Science and Research Review*, *2*(02), pp.18-28.

Karantzas, G. and Patsakis, C., 2021. An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. *Journal of Cybersecurity and Privacy*, *1*(3), pp.387-421.

Kaur, H. and Tiwari, R., 2021, November. Endpoint detection and response using machine learning. In *Journal of Physics: Conference Series* (Vol. 2062, No. 1, p. 012013). IOP Publishing.

Laryeafio, M.N. and Ogbewe, O.C., 2023. Ethical consideration dilemma: systematic review of ethics in qualitative data collection through interviews. *Journal of Ethics in Entrepreneurship and Technology*, *3*(2), pp.94-110.

MacLeod, A., Burm, S. and Mann, K., 2022. Constructivism: learning theories and approaches to research. *Researching medical education*, pp.25-40.

Mahawar, M.D., Safe Passage: Securing Information in Transit and at Rest. *Shielding the Data Kingdom: Mastering the Art of Computer Security*, p.31.

Malla, S. and Christensen, K., 2020. HPC in the cloud: Performance comparison of function as a service (FaaS) vs infrastructure as a service (IaaS). *Internet Technology Letters*, *3*(1), p.e137.

Mämmelä, O., Hiltunen, J., Suomalainen, J., Ahola, K., Mannersalo, P. and Vehkaperä, J., 2016, June. Towards micro-segmentation in 5G network security. In *European Conference on Networks and Communications (EuCNC 2016) Workshop on Network Management, Quality of Service and Security for 5G Networks*.

Mangayarkarasi, V.A., Vinayakan, K. and Kumar, A.D., 2024. Secure Cloud Data Storage with a Zero Trust Security Foundational Deep Learning Algorithm. *International Journal of Advanced Trends in Engineering and Technology*, *9*(2), pp.87-93.

Miller, S.P.M. and Brewer, J., 2020. Thematic analysis. *Retrieved January*, *18*, p.2021.

Mohajan, H.K., 2020. Quantitative research: A successful investigation in natural and social sciences. *Journal of economic development, environment and people*, *9*(4), pp.50-79.

Muzari, T., Shava, G.N. and Shonhiwa, S., 2022. Qualitative research paradigm, a key research design for educational researchers, processes and procedures: A theoretical overview. *Indiana Journal of Humanities and Social Sciences*, *3*(1), pp.14-20.

Mweshi, G.K. and Sakyi, K., 2020. Application of sampling methods for the research design. *Archives of Business Review–Vol*, *8*(11), pp.180-193.

Nahar, N., Andersson, K., Schelén, O. and Saguna, S., 2024. A Survey on Zero Trust Architecture: Applications and Challenges of 6G Networks. *IEEE Access*.

Naz, N., Gulab, F. and Aslam, M., 2022. Development of qualitative semi-structured interview guide for case study research.

Nguyen, H.H., Lim, Y., Seo, M., Jung, Y., Kim, M. and Park, W., 2023, October. Strengthening information security through zero trust architecture: a case study in South Korea. In *International Conference on Intelligent Systems and Data Science* (pp. 63-77). Singapore: Springer Nature Singapore.

Pampattiwar, K.N. and Chavan, P.V., 2023. CBSOACH: design of an efficient consortium blockchain-based selective ownership and access control model with vulnerability resistance using hybrid decision engine. *International Journal of Computational Science and Engineering*, *26*(2), pp.129-142.

Park, Y.S., Konge, L. and Artino Jr, A.R., 2020. The positivism paradigm of research. *Academic medicine*, *95*(5), pp.690-694.

Phiayura, P. and Teerakanok, S., 2023. A comprehensive framework for migrating to zero trust architecture. *Ieee Access*, *11*, pp.19487-19511.

Rahman, M.M., Tabash, M.I., Salamzadeh, A., Abduli, S. and Rahaman, M.S., 2022. Sampling techniques (probability) for quantitative social science researchers: a conceptual guidelines with examples. *Seeu Review*, *17*(1), pp.42-51.

Sandhu, K., Bojja, S.G.R., Venkataramanan, S., Vangoor, V.K.R. and Thota, S., 2024. AI-Powered Anomaly Detection in Zero Trust Environments: A Comprehensive Review of Methods and Evaluation.

Saranya, T., Sridevi, S., Deisy, C., Chung, T.D. and Khan, M.A., 2020. Performance analysis of machine learning algorithms in intrusion detection system: A review. *Procedia Computer Science*, *171*, pp.1251-1260.

Sarfo, J.O., Debrah, T., Gbordzoe, N.I., Afful, W.T. and Obeng, P., 2021. Qualitative research designs, sample size and saturation: is enough always enough. *Journal of Advocacy, Research and Education*, *8*(3), pp.60-65.

Sauce, B. and Matzel, L.D., 2022. Inductive reasoning. In *Encyclopedia of animal cognition and behavior* (pp. 3414-3421). Cham: Springer International Publishing.

Seifert, M., Kuehnel, S. and Sackmann, S., 2023. Hybrid clouds arising from software as a service adoption: challenges, solutions, and future research directions. *ACM Computing Surveys*, *55*(11), pp.1-35.

Sharma, H., 2022. Zero Trust in the Cloud: Implementing Zero Trust Architecture for Enhanced Cloud Security. *ESP Journal of Engineering & Technology Advancements (ESP-JETA)*, *2*(2), pp.78-91.

Shi, Y., Wang, D. and Zhang, Z., 2022. Categorical evaluation of scientific research efficiency in Chinese universities: basic and applied research. *Sustainability*, *14*(8), p.4402.

Singh, K., 2024. Role-Based Access Control (RBAC) in Snowflake for Enhanced Data Security.

Singh, K. and Kumar, A., 2024. Role-based access control (RBAC) in Snowflake for enhanced data security. *International Journal of Research in Management, Economics and Emerging Technologies*, *12*(12), p.450.

Smiliotopoulos, C., Kambourakis, G. and Kolias, C., 2024. Detecting lateral movement: A systematic survey. *Heliyon*, *10*(4).

Stafford, V., 2020. Zero trust architecture. *NIST special publication*, *800*(207), pp.800-207.

Suleski, T., Ahmed, M., Yang, W. and Wang, E., 2023. A review of multi-factor authentication in the Internet of Healthcare Things. *Digital Health*, *9*, p.20552076231177144.

Syed, N.F., Shah, S.W., Shaghaghi, A., Anwar, A., Baig, Z. and Doss, R., 2022. Zero trust architecture (zta): A comprehensive survey. *IEEE access*, *10*, pp.57143-57179.

Teerakanok, S., Uehara, T. and Inomata, A., 2021. Migrating to zero trust architecture: Reviews and challenges. *Security and Communication Networks*, *2021*(1), p.9947347.

Tenny, S., Brannan, J.M. and Brannan, G.D., 2017. Qualitative study.

Tisdell, E.J., Merriam, S.B. and Stuckey-Peyrot, H.L., 2025. *Qualitative research: A guide to design and implementation*. John Wiley & Sons.

Varshney, G., Kumawat, R., Varadharajan, V., Tupakula, U. and Gupta, C., 2024. Anti-phishing: A comprehensive perspective. *Expert Systems with Applications*, *238*, p.122199.

Veeramachaneni, V., 2025. Integrating Zero Trust Principles into IAM for Enhanced Cloud Security. *Recent Trends in Cloud Computing and Web Engineering*, *7*(1), pp.78-92.

Watson, R., 2015. Quantitative research. *Nursing standard*, *29*(31).

Yaseen, A., 2023. AI-driven threat detection and response: A paradigm shift in cybersecurity. *International Journal of Information and Cybersecurity*, *7*(12), pp.25-43.

Yuan, F., Cao, Y., Shang, Y., Liu, Y., Tan, J. and Fang, B., 2018. Insider threat detection with deep neural network. In *Computational Science–ICCS 2018: 18th International Conference, Wuxi, China, June 11–13, 2018, Proceedings, Part I 18* (pp. 43-54). Springer International Publishing.

Yuan, S. and Wu, X., 2021. Deep learning for insider threat detection: Review, challenges and opportunities. *Computers & Security*, *104*, p.102221.

Zanasi, C., Russo, S. and Colajanni, M., 2024. Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks*, *156*, p.103414.

8. Appendices

Appendix A: Draft Interview Questions

The following open-ended questions will be used in semi-structured interviews will be used to gain insights from network security professionals. Insights will be gained on the implementation of Zero Trust Architecture (ZTA) in enterprise networks and the challenges and strategies related to it.

Section 1: Participant Background

1) What is your current role and experience in network security?
2) How familiar are you with the concept of Zero Trust Architecture?
3) Have you ever been involved with the implementation of ZTA in your organisation?

Section 2: Current Security Practices

4) What type of security model is currently implemented in your organization?
5) How effective do you think your current security model is in preventing current cyber threats?

Section 3: Zero Trust Implementation

6) What motivated your organization to consider or implement ZTA?
7) What components or technologies were the most critical when your organization implemented ZTA? For example, identity verification, micro-segmentation, Least Privilege access?
8) What challenges did you encounter during the planning and implementation phases of ZTA?
9) How did you address issues of legacy systems or infrastructure when you shifted to ZTA?

Section 6: Machine Learning in ZTA

10)How familiar are you with the use of ML in cybersecurity?

11)Have you explored or implemented ML techniques as part of your ZTA strategy?

12)What areas in ML have implemented, for example, identity authentication or anomaly detection?

13)What benefits has your organisation gained from implementing ML in your network security infrastructure?

14)What challenges has your organisation faced when you implemented ML in your network security infrastructure?

15)In your opinion, what are the key limitations and risks that come with using ML for continuous monitoring and threat detection?

16)How do you ensure the accuracy, fairness, and transparency of ML models used in your security systems?

Section 4: Outcomes & Reflections

17)What benefits did your organisation gain from implementing ZTA?

18)What limitations or drawbacks did you encounter when you implemented ZTA?

19)What best practices would you recommend to other organisations that want to implement ZTA?

20)Would you recommend the integration of ML in ZTA to other organisations?

Section 5: Ethical & Operational Considerations

21)How do you ensure data protection and user privacy with the implementation of ZTA?

22)Did ZTA have any significant impact on user experience or employee workflow in your organization?

23)Are there any ethical concerns or resistance that your organisation had to manage?