BUCKINGHAMSHIRE NEW UNIVERSITY
EST. 1891

School of Creative and Digital Industries

Module Title:	Project	**Module Code:**	COM7002
Assignment No/Title:	Final Report(CW2)	**Assessment Weighting:**	100%
Submission Date:	Wednesday 22 August 2025 by 14:00	**Feedback Date:**	+ 3 Weeks
Module Tutor:	Justin Luker	**Degree:**	Masters
Student ID:	**22322896**	**Student Name:**	**Abhishek Kudiri**
1st Supervisor:	**Nick Day**	**2nd Supervisor:**	**Benjamin Aziz**
Course:	MSc. Cyber Security		
Word Count:	**14746**		

Plagiarism Statement

I certify that this report is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation, whether they be books, articles, reports, lecture notes, and any other kind of document, electronic or personal communication. I also certify that this report has not previously been submitted for assessment in any other module or course of study, except where specific permission has been granted from all supervisors involved, and that I have not copied in part or whole or otherwise plagiarised the work of other students and/or persons.

Print Full Name:	Abhishek Kudiri	Date:	11-11-2024
Signature (electronic):	K Abhishek		

Pathway B:

Project Title:

Zero trust policy design for securing remote and hybrid workforces

Acknowledgments:

I express sincere gratitude to my supervisors, Nick Day and Benjamin Aziz, for their invaluable guidance. I thank the cybersecurity professionals from World Wide Technology and Barclays UK for their insightful contributions, and survey participants for their input. My appreciation extends to my peers for their support throughout this project.

Abstract:

The increasing incidence of these work models has introduced complex challenges for regular cybersecurity approaches, which often rely on perimeter-based security measures. This research explores the progress of a Zero-trust policy which mainly aims at strengthening security within remote and hybrid work environments. Zero Trust Architecture (ZTA), the core principle is “never trust, always verify,” and offers a modern approach focused on strict identity verification, continuous monitoring, and least privilege access. This research widely analyses Zero Trust principles and their application in securing dispersed workforces. It inspects critical components such as identity and access management (IAM), multi-factor authentication (MFA), endpoint security, and network segmentation. It discusses the specific policy adjustments required to mitigate risks in remote and hybrid settings. Additionally, the study addresses implementation challenges, privacy and compliance considerations, and the role of continuous monitoring and artificial intelligence in detecting emerging threats. This research also aims to provide a combination of literature review, case studies, and policy design with a useful and organised Zero Trust. The resulting policies are expected to support organisations in their cybersecurity postures and balance security with usability for a secure and productive remote workforce.

Keywords: Zero Trust Policy Design, Zero Trust Architecture (ZTA), Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Segmentation, endpoint security, Policy for Zero Trust

Table of Contents :

Introduction:

Remote and hybrid work have changed how organisational processes are conducted. While this flexibility brings its benefits it also opens up new cybersecurity risks. The traditional methods for protecting the network perimeter of an organisation no longer apply as employees work remotely by using mostly personal devices and cloud services. This shift made businesses more vulnerable to increased threats of cyberattacks, phishing, malware and credential compromise that will result in massive data breaches with colossal financial losses (Abwnawar et al., 2017; Fang & Guan, 2022). In response to the evolving challenges, Zero Trust Architecture (ZTA) is, therefore, today's go-to solution. Zero trust is founded upon the principle of trusting no one automatically, neither within nor external to the network, as against traditional security methods that trust those individuals and appliances in the network. This approach ensures constant verification of every device and user, using stringent identity authentication, multi-factor authentication (MFA) and need-to-know surveillance of access (The 'Zero Trust' Model in Cybersecurity: Towards understanding and deployment, n.d., 2022; Rose et al., 2020). By assuming that threats can originate both inside and outside the network zero trust seeks to minimize vulnerabilities by continuously validating trust and restricting access to sensitive data.

With the remote and hybrid work model, employees are usually spread across different locations using multiple devices to carry out their work. In such a scenario, this method of constant verification and restricted access comes in very handy. Zero Trust's focus on stringent identity verification, IAM, MFA, endpoint security and network segmentation makes it a promising solution for securing these work environments (Microsoft Security Blog, 2023). While Zero Trust has been in vogue, according to a Cisco report, though almost 86.5% of the organisations have initiated implementing some aspects of the model, just 2% of them have achieved total maturity across all the pillars of Zero Trust, which translates into much work left to be done (CSO Online, n.d.). Few of the challenges include managing diverse work contexts that may not fit neatly into traditional security models, constant monitoring, and how to integrate Zero Trust into current systems (Schneider Electric, 2022). The aim of this dissertation is to develop a comprehensive Zero Trust policy specifically tailored for remote and hybrid workforces and by doing so this study will investigate how Zero Trust can mitigate the particular cybersecurity threats connected to these work settings and offer workable solutions for putting its tenets into practice in order to secure remote work. This will include utilisation of such building blocks as IAM, MFA, endpoint protection, network segmentation and policy renewal with security as a part.

The dissertation will also discuss how emerging technologies, specifically Artificial Intelligence (AI), can be utilised to revolutionise threat detection and response mechanisms in a Zero Trust. Through AI's superior capabilities like machine learning and data clustering, organisations can attain the ability to identify advanced and upcoming threats more effectively and efficiently. AI can persistently watch

an incredible volume of network traffic, identify anomalies and react to prospective security breaches in real-time, building a dynamic defense. The paper will also cover the privacy, compliance and user experience considerations that arise from implementing a Zero Trust model on hybrid and remote workforce security. Although Zero Trust significantly enhances security through not trusting users from outside and inside the network, it is also challenging to preserve users' privacy and fulfill regulatory compliance standards. The research will discuss how organisations can maintain user experience and strong security controls in a way that Zero Trust architecture is not an obstacle to operational effectiveness. Their impact will be covered by case studies and best practice for the optimal, secure and compliant Zero Trust setting (Ishide et al., 2022; Safeguarding the Hybrid Workforce with a Zero Trust Approach, n.d., 2023; Rustam, Ranaweera and Jurcut, 2024).

The reason this research is so important is that traditional perimeter-based security just doesn't cut it anymore as organisations continue to adapt to remote and hybrid work, developing effective security like Zero Trust is crucial to protecting sensitive data and defending against growing cybersecurity threats. This dissertation aims to provide organisations with the tools they need to implement Zero Trust, helping them stay secure while maintaining productivity and complying with industry regulations (Fang & Guan, 2022). It goes without saying that corporations need to reconsider their approach to cybersecurity as more companies embrace remote and hybrid work. Regardless of where employees are working from, Zero Trust provides a framework that can assist guarantee that critical data and systems are kept safe by providing a detailed policy and practical recommendations, this dissertation will offer valuable insights into how businesses can enhance their cybersecurity posture while facing the challenges of today’s distributed work environments (Buck et al., 2021).

Background:

Modern organisations now function in a completely different environment due to the quick transition to remote and hybrid work patterns, which offer stretch but also pose serious cybersecurity problems. Conventional security which usually focuses on the defensive side, is becoming less and less effective at protecting the expanding number of distributed workforces.

Remote and hybrid models can subject organisations to increased internal and external threats. The dangers of cyberattacks via malware, phishing and theft of credentials are heightened, particularly if workers utilise personal devices or access cloud services outside secured company networks. Yet such risks are by no means the monopoly of hybrid or remote working—closely allied risk domains, like phishing and credential compromise, can just as easily take place on-premises if employees neglect to follow best security practice or bring insecure devices into the office. Especially applicable in knowledge work sectors, where the work is even more dependent on digital technology and cloud services, this renders flexible and dependable security controls even more essential. Conversely, those industries such as hospitality that continue to offer primarily face-to-face services have fewer

remote work security concerns, yet electronic transactions such as reservations and processing payments nonetheless require strong protection against cyber attacks.

Zero Trust Architecture (ZTA) has emerged as a modern solution for these challenges. By presuming that threats can exist both inside and outside the network, ZTA enforces strict identity verification, continuous monitoring, and the principle of least privilege access giving importance to critical security elements including IAM, Multi-factor authentication (MFA), and network segmentation, this study will also examine the development and application of a Zero Trust policy expected for both remote and hybrid work settings by addressing major implementation challenges, policy adjustments, and the role of emerging technologies like artificial intelligence in mitigating evolving threats.

Rationale:

This dissertation responds to a zero-trust policy model for securing remote and hybrid workplaces. While the deployment of conventional perimeter-based security products has been in use to secure organisations for ages, the transition to remote and hybrid work exposed their limitations. It is not that work from home is less secure than work onsite, but that traditional security approaches are insufficient to deal with the unique threats posed by geographically dispersed employees. Without proper controls to block internal and external threats, organisations are more vulnerable. A zero-trust approach offers a more dynamic and robust security structure, offering ongoing authentication of users and devices wherever they are.

The dissertation aims to explore and evaluate how Zero Trust principles such as Identity and Access Management (IAM), multi-factor authentication (MFA), endpoint security and network segmentation can be effectively applied to secure remote work settings, Also covers the crucial policy changes that can reduce risks unique to these settings and evaluates implementation issues, privacy concerns, and compliance issues, also this study investigates how artificial intelligence and ongoing monitoring can be used to spot new threats.

By explaining a thorough literature review, case studies, and policy design, this research aims to deliver a structured, practical zero-trust. It is anticipated that such a framework would help organisations improve their cybersecurity posture while maintaining usability, eventually allowing for safe and effective remote and hybrid workforces.

Ethical Considerations:

Employees must be made to feel that their privacy is not being disrespected and for this, transparency in the way the monitoring data is being collected and used is necessary. To achieve this balance, organisations may adopt a judicious monitoring approach, where data gathering is limited to what is necessary for security and business purposes. Communication is critical - employees should be told what information is being monitored, why they require it and how it is to be safeguarded.

Steer clear of excessively intrusive monitoring that will harm morale, work-life balance and trust. Establish clearly defined policy setting down the rules of monitoring in a bid to maintain staff privacy and satisfy security needs. Providing employees with regular forum to comment and suggest changes further aids this balance.

One more crucial action is to involve employees in policy design processes. Open forums and decision-making processes can foster understanding, diminish resistance and establish a sense of collective responsibility for cybersecurity. Employees can also be informed about the contribution of monitoring to a safe working environment through awareness programs and training sessions.

Moreover organisations must make sure that monitoring policies are enforced in a fair and uniform way for everyone in the workforce. Monitoring or access control must be non-discriminatory, and there must be efficient grievance redressal mechanisms. Privacy-guarding technologies (PETs) like data anonymisation and data encryption can restrict exposure of the personal data but allow proper surveillance.

Legal compliance, i.e., regulation according to GDPR, is most necessary in maintaining employee information. Regular audits, impartial monitoring and transparent reporting processes can be used in making data accumulation ethical and compliant. The designation of a special data protection officer (DPO) or an internal watchdog group can also promote accountability.

Lastly, striking a balance between security and protection of individual rights is a continuous process of review and amendment. Organisations should not view privacy protection as a hindrance to security but as a means of creating a stable and sound working environment. By fostering open communication, transparency, and impartial implementation of policies, organisations are able to create a system that secures their interests as well as those of their employees.

Aim:

The dissertation's aim is to develop a structured Zero Trust policy to enhance cybersecurity for remote and hybrid workforces and in order to increase organisational security while maintaining usability and productivity, it looks at and applies Zero Trust concepts including identity verification, least privilege access and continuous monitoring.

Objectives:

- To design a Zero Trust policy tailored to secure remote and hybrid work environments, by exploring the key principles, such as IAM, MFA, endpoint security and network segmentation.
- To mitigate the risks associated with widely distributed workforces, along with analysing critical policy shifts required to protect against internal and external threats, focusing on unique challenges like device diversity, access points, and decentralised data flow.
- To assess the role of monitoring continuously and artificial intelligence (AI) in enhancing threat detection and response in real time.
- This dissertation aims at solving implementation, privacy, and regulatory challenges in zero trust, thus providing an enterprise with a structured and practical way of improving cybersecurity while allowing safe and productive remote work.

Risks:

The following risk table shows the risks associated with finishing this research study.

Table 1 Risk associated by finishing this research study

Description of Risk	Risk Resolution Action	Impact on Project Aim	Impact on Project Objectives	Impact on Project Plan
Insufficient Identity Management	Deploy robust IAM solutions like MFA and Single Sign-On (SSO).	Delays in achieving security goals.	Reduced effectiveness in access control mechanisms.	Adjust timelines to include IAM integration.
Legacy System Incompatibility	Implement hybrid solutions or modernize critical legacy systems.	Limits scalability of Zero Trust.	Incomplete coverage of security principles.	Allocate resources for system upgrades.
Resistance to Change	Conduct training and awareness campaigns for employees.	Slower adoption of Zero Trust policies.	Reduced compliance with policy measures.	Introduce phased implementation plans.
Alert Fatigue	Optimize threat detection systems to reduce false positives.	Missed critical security threats.	Reduced monitoring efficiency.	Schedule time for refining detection systems.
Cost Constraints	Prioritize cost-effective technologies and phased rollouts.	Delays in full Zero Trust implementation.	Limited deployment of comprehensive solutions.	Reevaluate budget allocation for priorities.

Complexity in Enforcement	Use automation tools to streamline policy enforcement.	Fragmented enforcement undermines security.	Reduced ability to maintain secure environments.	Plan for advanced automation tools.
Data Privacy Compliance	Regularly audit policies for alignment with regulations.	Risk of regulatory penalties.	Compromised trust and legal liabilities.	Incorporate compliance assessments into milestones.

Literature Survey:

Zero Trust Architecture (ZTA) is being adopted to safeguard enterprises from changing cyber threats due to the growing trend toward remote and hybrid work settings which has created new cybersecurity challenges, "Never trust, always verify" is the policy principle of ZTA, limiting access strictly on a need-to-know basis and continuously validating trust at every step. The effectiveness of the Zero Trust policy design in protecting remote and hybrid workforces is reviewed in this literature review.

Background and Principles of Zero Trust

The Zero Trust model is based on several guiding principles that are continuous verification, privilege access least, and an assumption that threat could be both inside and outside of the network. Repsol's Zero Trust architecture includes continuous authentication and segmentation in the interests of enhancing security and restricting unauthorized access especially within hybrid working environments (The 'Zero Trust' Model in Cybersecurity: Towards understanding and deployment, n.d., 2022).

Is zero trust architecture (ZTA) the ideal architecture to build secure systems? (Fernandez and Brazhuk, 2024)

While ZTA is a deserving answer to how security can be improved, whether it is the ideal form in which to build secure systems is debatable. There is too little technical data, and numerous questions about how well it would work remain unresolved, e.g., potential overhead, institutional practicability, and how effective it would be against threats in relation to other answers. While it contains valuable security concepts, more research and definition are needed to determine the suitability of ZTA for large-scale, highly secure deployments.

The Policy Decision Point (PDP) and Policy Enforcement Point (PEP) are important elements of the Zero Trust Architectures (ZTA) studied by NIST and communicate a commitment to ongoing verification, risk-based access control, and integration with policies that apply enterprise-wide. While the PDP analyzes access requests and makes risk-based access decisions - according to dynamic attributes of the user such as their identity, device posture, location and current threat intelligence - the PEP does not provide policy logic, only allowing or denying permission based on PDP decisions. The functional split further supports scalability, flexibility, and centralized policy creation and management. Because traditional PDPs are centralized, can be underutilized due to low availability, and lack of tamper resistance, Ho, Chen, and Lin (2023) proposed a Decentralized PDP model for Token Networks. Their model relies on distributed nodes for collaborative decision-making about access decision, allowing for trust without total reliance on a single entity and high availability. Though their work is focused on blockchain and Web 3.0 ecosystems, their model has applicability beyond tokens and to a distributed remote or hybrid work environment, whereby access requests could occur at respiratory endpoints and have an appropriate trust framework despite complete failure or malicious tampering of one or more nodes.

Recognizing the necessity for adaptability in complicated systems, Hong et al. (2023) created SYSFLOW, a programmable security architecture for edge, cloud, and IoT systems. SYSFLOW uses a central PDP to conduct fine-grained policy decisions in real time using system-level data. The corresponding PEP is an adaptable data plane, meaning the in-zone enforcement of the policies could occur with minimal performance loss. Ongoing monitoring with the data plane allows for quick mitigation of anomalous behavior, reinforcing aspects of the core ZTA. In more realistic large-scale parts of a campus, Brockelsby and Dutta (2021) noted that perimeter PEPs in the campus network do not allow access control perimeter for lateral movement in a zone. They suggest that performance optimized PEPs should have structure so they can telescope access in these zones while decreasing complexity internally. These new developments in paving the way toward adaptive, distributed, and intelligent use of the PDP/PEP development and design pathway for access control within the cybersecurity ecosystem.

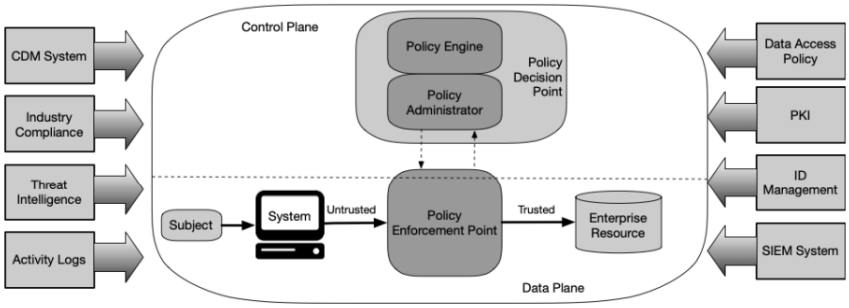

Figure 1 Core Zero Trust Logical Components

Identity and Access Management (IAM) is extremely crucial in Zero Trust implementation. High-Performance Computing (HPC), Artificial Intelligence (AI) and Machine Learning (ML) scientific workflows require a robust IAM solution due to infrastructural heterogeneity in distributed deployments. Alam et al. (2024) propose a federated IAM solution featuring multiple layers of security controls including single sign-on (SSO), multi-factor authentication (MFA), cloud-native protocols and time-restricted role-based access controls (RBAC). Such controls, being designed for Isambard-AI and UK-based HPC supercomputing Digital Research Infrastructures (DRIs), adhere to Zero Trust principles through strict access control requirements while maintaining compliance with the regulatory environment.

Security authentication is another pillar of Zero Trust that continuously authenticates user identities. Traditional single-factor authentication methods are no longer sufficient, and even MFA approaches require enhancements to mitigate emerging threats. Krishnan and Sreeja (2021) propose an adaptive authentication system that collects a composite set of attributes, including user behavior, application-specific data and device characteristics, to dynamically assess risk. This threat-based authentication aligns with Zero Trust in implementing strong controls with finely articulated security measures resolved in real time by way of threat assessment.

In the case of smart home IoT settings, Ameer, Benson, and Sandhu (2023) investigate weaknesses of existing RBAC and ABAC structures and introduce two integrated frameworks (HyBACRC and HyBACAC) as examples of advanced access to higher-order settings. These models combine the benefits of RBAC and ABAC by incorporating both user roles and contextual attributes for more granular access control. This aligns with the Zero Trust principles, ensuring dynamic, context-aware security. Alam et al. (2024) similarly apply RBAC in federated Identity and Access Management (IAM) solutions, enhancing security and compliance in distributed environments, further reinforcing Zero Trust's emphasis on strict access control.

Implementing Zero Trust for Remote and Hybrid Workforces

Data and system protection has become increasingly challenging with the emergence of remote and hybrid workforces, prompting organisations to adopt Zero Trust Architecture (ZTA) as a preemptive security solution. Based on the principle of "Never Trust, Always Verify," ZTA eliminates the built-in trust and applies ongoing verification to safeguard enterprise assets. Traditionally, companies applied Virtual Private Networks (VPNs) to offer secure distant access, yet VPNs have latency issues and potential weaknesses, which makes ZTA more effective (Adahman, Malik, and Anwar, 2022). Moudni and Ziyati (2023) highlight the manner in which Zero Trust enhances security in multi-cloud environments by enforcing strict identity validation before granting access to critical resources, which safeguards against threats associated with cloud-based cyber attacks. Its remedy is to tighten security and availability in multi-cloud storage with rigorous application of Zero Trust principles. Alawneh and Abbadi (2022) reply, however, that promising as it is, Zero Trust is non-standard and industry-specific implementation-driven with inconsistency in its application across enterprise security architectures. Where Moudni and Ziyati concentrate on Zero Trust's practical application in cloud security, Alawneh and Abbadi suggest the enforcement of Trusted Computing measures to establish more advanced zero-trust methods outside of cloud systems, namely for IoT, social networks and business systems. This divergence is proof of some underlying tension: whereas Zero Trust is an add-on to cloud security, widespread deployment across different infrastructures calls for more generic solutions and enterprise-friendly integration. So while ZTA is a potent alternative to traditional VPN-based models of security, its most auspicious potential hinges on equilibrium between practical implementation and standardised patterns to enable flexibility and scalability across different digital frontiers.

To address these issues, companies like Sanmina found that Zero Trust Exchange improved security through access granted only to approved users and it vastly improved operational efficiency and user experience. Now, with direct-to-cloud connectivity, it has gotten rid of latency issues, common with traditional VPNs and ensured that global teams will get better performance. That change also simplified all processes of hybrid and remote work, provided support for scalability and worked according to today's modern workforce's introduced requirements. The switch made it clearly apparent how adapting Zero Trust methodologies can efficiently counter security risks and performance challenges as well (Safeguarding the Hybrid Workforce with a Zero Trust Approach, n.d., 2023). Likewise, Microsoft highlights the importance of protecting devices, managing identities and

securing data as key parts of its Zero Trust strategy to handle risks in hybrid work setups (Microsoft Security Blog, 2023).

Full Zero Trust implementation is a work in progress and it takes time. Most organisations' systems are mixtures of the old and the new—think about scattered security logs across the office and the cloud systems. Ishide et al. (2022) explored how machine learning can play a vital role in enhancing security within hybrid environments. They proved that this technique could effectively spot unusual activity which has made it a strong tool in the challenges of modern cybersecurity. Machine learning stands out compared to traditional methods, which become swamped with logs spread across on-premises and cloud systems, since it can easily spot patterns and irregularities. This approach not only makes it easier to implement Zero Trust techniques but also puts companies in the driver's seat when it comes to potential risks. Smart technology can help firms build stronger defenses and adapt to the needs of today's remote and hybrid employees.

Benefits of Zero Trust in Securing Hybrid Work Environments

The Fourth Industrial Revolution has promoted digital change, forcing firms to adopt cloud platforms, artificial intelligence and data-sharing technology to be effective. Saleh et al. (2024) observe that the shift toward hybrid and remote working, fueled by COVID-19, introduced unparalleled cybersecurity concerns. With corporations relying on complex digital spaces, it becomes important to secure such spaces. Zero Trust Architecture (ZTA) is an active security model through ongoing validation and strict access to emails, storage, cloud services and endpoints (Microsoft, 2023). Unlike traditional security approaches, Zero Trust does not assume any device or user to be fully trusted, reducing the possibility of unauthorized access and data compromise. Harvard Business Review (2022) identifies that such a model offers the highest level of security while permitting frictionless and secure hybrid workflows. Zero Trust mitigates risk in hybrid IT environments, thus making it desirable to the need for robust cybersecurity (Saleh et al., 2024).Its granular access control and real-time authentication improve end-user experience and security. IIts real-time authentication and fine-grained access control improve both end-user experience and security. With companies undergoing digital reliance, the adoption of Zero Trust is a must to improve cyber defenses and to enable a secure, resilient hybrid workplace.

It is increasingly challenging to protect confidential data in sophisticated networks with work-from-home as the norm. Fang and Guan (2022), Zero Trust Networks (ZTN) address these challenges by merging contemporary Zero Trust ideologies with historical perimeter security. Organisations may remain secure while maintaining efficiency and collaboration thanks to this hybrid strategy. Zero Trust implementation might be time-consuming but many companies are figuring out how to implement it in their current systems, to demonstrate how Zero Trust adjusts to practical requirements, Fang and Guan have created a model specially made to safely link iOS devices to corporate resources and this strategy demonstrates that Zero Trust is about developing workable

solutions that enable organisations to safely adopt the future of flexible work, not merely cutting-edge technology.

As remote working and hybrid cloud environments grow, it is increasingly hard to safeguard sensitive information. According to Abwnawar et al. (2017), exchange of sensitive information among public and private data centers, mobile platforms and personal devices requires context-aware and adaptable access control. Data security is becoming increasingly sophisticated due to varied regulatory schemes, security measures and protection methods in different contexts. By combining Zero Trust concepts and solutions like SANTA (Secure Access for Networked Trustworthy Applications) that is a policy language designed to support access control for hybrid cloud deployments, firms can configure adaptive policies that can prosper in these heterogeneous clouds, delivering robust data protection.

As the Internet of Things (IoT) expands quickly, it presents additional security challenges. While it facilitates smooth communication between items and devices, it also raises issues with data privacy, denial-of-service (DOS) attack prevention and access control management. Purohit et al. (2017) argue that the implementation of Zero Trust principles in IoT networks has immense potential to increase security through enhanced authentication, data confidentiality and more secure access management. Because of its hybrid security approach, Zero Trust is an essential solution to protect both corporate data and networked devices underlying a tremendous percentage of today's technology.

Challenges in Adopting Zero Trust Policies

Implementing Zero Trust security models comes with many benefits but at a cost to companies with aging systems or those who perceive changing access needs. For instance, Zero Trust—thanks to the kind of advanced authentication capability no longer present in much OT hardware—is going to cause most companies to substantially invest in their upgrade (Schneider Electric, 2022). Insider attacks are also a major threat since they can cause the exfiltration of sensitive data in the network. Zero Trust, thus, is not an evolution but a necessity. It destroys the conventional security models with the help of the principle of least privilege by restricting the access tightly while ensuring each user and system is authenticated and authorized before granting access (S and Shankaramma, 2024). This approach is especially worth it for defending modern network infrastructures and even legacy systems, particularly for industries like finance, IoT, business operations and 5G networks.

Zero Trust (ZT) has also become a widely applied methodology to secure systems by assuming that no access request is to be trusted by default. The big challenge lies in the time taken for authenticating and verifying each access request, which might slow down workflows, especially in fast-paced environments like Industrial IoT (IIoT). AI can be helpful in the solution of this problem, opposed to traditional security approaches; Singh et al. (2023) found that integrating AI into Zero Trust systems will improve network access by up to 38%, enhancing efficiency without giving up on security. Yet, as Fernandez and Brazhuk (2024) point out the true potential of Zero Trust Architecture (ZTA) is still

being debated. While it promises enhanced security, there's a lack of clear, practical reports on its implementation and real-world effectiveness. They suggest that Zero Trust needs to be evaluated against existing security knowledge and that its claims need further scrutiny.

In brief, while there is great promise by AI in terms of enhancement for zero trust a lot more research needs to be conducted so that this real-world application is honed and how it can best balance the strong security features with high performance in the critical domain such as IIoT. Cloud-native applications introduce further complexity. Zero Trust secures these kinds of applications by encrypting traffic on the basis that every request gets authenticated and then only those make it through rigid checks. Organisation does not require changes to application code to execute Zero Trust due to the introduction of tools such as service meshes (Rodigari et al., 2021). However, deploying Zero Trust in multi-cloud environments comes with trade-offs. For example, a study that used Istio which is an open-source service mesh platform designed to manage and secure microservices applications discovered that, depending on the system configuration and the particular cloud environment, overall CPU and memory utilisation increased even though latency for processing HTTP requests was more consistent. This highlights the balancing act between strengthening security and managing resource efficiency.

Lastly, implementing Zero Trust requires a mindset change rather than only modernizing technology. For these changes to be long-lasting, leadership and security teams must actively participate and support them (The 'Zero Trust' Model in Cybersecurity: Towards understanding and deployment, n.d., 2022). In its dynamic state, the Zero Trust model will have to rely even more on integration with AI and optimisation of multi-cloud performance to deal with such challenges and create systems that are both more secure and more efficient for the future.

Yet another core challenge of deploying Zero Trust policies is their evolving architecture and strategic acumen for deployment. Lin et al. (2024) report this evolution, pointing out that a departure from perimeter-based to Zero Trust-based models results in high implementation complexities. Key components such as Policy Enforcement Points (PEPs) and Identity and Access Management (IAM) systems must support high real-time detection rates—something most modern infrastructures cannot currently accomplish. Additionally, their work introduces the early confluence of quantum technology and Zero Trust, which, promising more security with quantum keys, introduces an additional layer of complexity to organisations already dealing with traditional threats.

Ilyas, Mustafa Akal and Althebyan (2024) add to this by pointing out the biggest gap in Zero Trust adoption: a lack of clearly defined roadmap. They propose a maturity model to allow businesses to test their progress and identify areas for improvement. This shows the extent to which implementation of Zero Trust is no technical issue, but an organisational and a strategic one. Without clearly defined test tools, organisations risk having non-integrated deployments that undermine broad security.

In addition, as Mohammed et al. (2021) explain, trust is not just in users or devices—but data too. Their research shows how poor-quality data has the potential to undermine Zero Trust architecture, particularly where decisions are being taken on the basis of such shaky sets. In the absence of data governance, the most secure of Zero Trust policies have the potential to fail to establish trust in data-driven practices.

Continuous Monitoring and Artificial Intelligence (AI) in Threat Detection and Response

The convergence of AI and continuous monitoring is increasingly becoming essential for real-time threat detection and response, especially in transitory environments like remote and hybrid workforces. Continuous monitoring offers real-time analysis of system behavior to identify suspicious activity in advance. AI technologies, more precisely machine learning algorithms, have the ability to detect new, unidentified threats through pattern recognition and adaptability in learning, thus enhancing incident response (J Paramesh et al., 2024). The approach converts security postures from reactive to proactive, with predictive analytics and machine decision-making augmenting security measures. The use of AI aligns with Zero Trust Architecture (ZTA), in which dynamic contextual-based decisions are taken instead of statically credential-based on security decision-making (Gujar, 2024).

Increased integration of AI in traditional cybersecurity practices has brought encouraging results in institutions of higher learning. The rapid adoption of e-learning has exposed educational institutions to significant cybersecurity vulnerabilities. In turn, AI-based solutions are being used in combination with traditional practices to reverse these vulnerabilities. Review of Parambil et al. (2024) indicates the merging of AI as a part of cybersecurity tools within online higher learning, noting how AI methods remain highly effective against threats, while ensuring authentication as well as the protection of privacy. The discussion, however, includes concerns relating to data privacy, fairness as well as transparency, issues central when utilising AI in systems in which sensitive data is highly plentiful.

AI-driven continuous monitoring can also combine various sources of data, including activity logs and behavior analytics, to present a more comprehensive view of possible threats. AI does bring tremendous value, but integration must address ethical and technical issues like transparency and resilience. In remote and hybrid workforces where traditional perimeter defence is insufficient, AI-driven continuous monitoring becomes essential. It enables organisations to gain visibility across scattered endpoints, with the ability to provide quick incident response and improving cyber resiliency—key elements of a Zero Trust policy (Shanthi, Sasi and Gouthaman, 2023).

Successful application of AI in cybersecurity depends on delicate balancing of technical as well as ethical aspects. Privacy, strength and fairness must be tackled so that AI is used responsibly in application. Furthermore, the necessity of interdisciplinary interaction, constant monitoring of AI models by automatic mechanisms and humans and designing sound guidelines for managing AI are

all essential to ensuring a sustainable and ethical cybersecurity methodology (Parambil et al., 2024). With the implementation of controls, organisations have the capability of enhancing security, closing the windows of vulnerabilities and creating immunity against continually evolving cyber threats.

Future Directions and Research Gaps

The practical application of Zero Trust Architecture (ZTA) in small to medium-sized enterprises (SMEs) is a set of complex issues that go well beyond matters of technical design. Although Zero Trust is a potentially attractive alternative to traditional perimeter-based security models, particularly in relation to hybrid workforces, there are concerns related to cost, capability and on-going operational maintenance once ZTA has been established for SMEs. Issues of financial feasibility are prominent with regard to organisations with limited operating budgets and cybersecurity personnel to manage maintenance. Implementing one or more of the core concepts related to Zero Trust such as ongoing monitoring, identity management, as well as micro-segmentation requires not just an initial up-front cost, but ongoing technical support which makes it difficult for SMEs with limited financial resources (Rose et al, 2020).

The major reasons SMEs face barriers to Zero Trust adoption is a shortfall of financial constraints, a shortage of skilled people, and a limited understanding of audit-able and scalable ZTA frameworks (Mutabazi, Ndashimye & Ndibwile, 2023). A lot of existing literature makes assumptions regarding an organisation's beginning level of digital maturity or readiness of infrastructure (Buck et al 2021) which compounds the imbalance in research literature and available resources to the adoption of ZTA. In addition, Abdelmagid and Diaz (2025) explain that Zero Trust in the context of an SME is based on managing not only technical design, but also how to manage human and financial risks (before and after deployment) in order to be successful in implementing it. These gaps create a tangible need for economic feasibility studies, low cost suitable model for implementation and reasonable frameworks for migration to ZTA by SMEs or similar organisations.

The convergence of Operational Technology (OT) and Information Technology (IT) in hybrid environments will cause further complications in barriers to ZTA adoption beyond SMEs. Systems that rely on the Industrial Internet of Things (IIoT) must understand frameworks in real time, while maintaining performance, reliability, and secure access within both the physical and digital assets. Regardless, Crowther (2024) suggests an intersection of Zero Trust and shared responsibility model by exploring the development of a hybrid framework to address the operational complexity of IIoT environments. However, the assumptions of centralised control and prohibition of multi-stakeholder ipsilateral management at the deployed Next Generation Security Edge technology remain in stark contrast to OT environments, which remain indeterminate. This further supports the case for the need for more flexible, standardised models to support the operational requirements of critical infrastructure systems.

At the same time, Zero Trust principles are receiving greater attention at the application and software runtime level. Modern software development increasingly relies on third-party libraries that are trusted when executed as part of the runtime environment, which could create security vulnerabilities. Recently developed Software Supply Chain (SSC) attacks (e.g., Log4j) have noted big limitations with current permission models (Amusuo et al., 2025). Although ZTA principles such as continuous monitoring, least privilege, and explicit verification may help mitigate these risks, the authors of ZTA implementations presently have key concerns outside of the centre of the application and the enterprise environment (cost and complexity). This illustrates a significant gap in the research literature that needs to be addressed, including institutionalising ZTA models based on applications, architectures, and runtime environments with minimal overhead in code design.

Collectively, these findings confirm that although Zero Trust can be a powerful paradigm shift, the practical adoption of ZTA is also sporadic and stalled for a number of social, technical, and economic reasons. Further, there is a lack of common evaluation frameworks, particularly ones for evaluating ZTA across SMEs, hybrid infrastructures, IIoT systems, and software supply chains. Future research should focus on three areas: (1) the development of economically viable Zero Trust frameworks for constrained resource contexts; (2) domain-specific ZTA models that serve the needs of the digital transformation in OT-IT convergence and the IIoT contexts; and (3) Zero Trust integration into secure software development and runtime systems for continuous improvement.

While awareness of Zero Trust continues, we will only be able to obtain the benefits of Zero Trust through collaboration and the careful design of user-focused, context-sensitive implementation strategies that reflect the technological realities across sectors.

Methodology:

1. **Interview Data Collection**

This study employs an exploratory qualitative research approach to obtain detailed information on Zero Trust Policy implementation for securing remote and hybrid workforces. The aim is to obtain detailed opinions from cyber security professionals and complement these data with data from relevant blogs, research studies and industry reports.

Participants

1. **World Wide Technology (WWT)** research and development team as a **Senior Consulting Systems Engineer** with expertise in designing Zero Trust security infrastructures for banking organisations.
2. **Assistant Vice President** of Cybersecurity for **Barclays UK**, with experience in cybersecurity strategy, Zero Trust implementation, and threat reduction.

Interview Format

Open-ended questions were asked in the interviews to obtain answers of full length. The following topics were discussed:

- Security challenges with remote and hybrid workforces.
- To what extent Zero Trust philosophies help prevent such challenges.
- Key aspects of Zero Trust policies focusing on identity and access management (IAM), multi-factor authentication (MFA) and network segmentation.
- Challenges of implementation. How to resolve them.
- Use of artificial intelligence and machine learning for Zero Trust threat detection.
- Zero Trust architecture regulatory compliance role.

Process of Data Collection

- Carried out WhatsApp interviews, employing rapport with participants to facilitate free-flowing, unstructured discussion.
- Interviews were recorded from WhatsApp chat history for appropriate analysis.

Ethical Considerations

- Informed consent was provided to participants prior to interviews.
- Confidentiality and anonymity were maintained by using pseudonyms.
- Participants were informed about the right to withdraw at any time from study participation.
- Transcripts of the chats are stored securely and can be utilized only for academic purposes.

2. Content Analysis (Secondary Data Review)

To frame and support the findings realized using the interviews, this study will conduct a secondary data analysis. The review will be grounded upon peer-reviewed conference proceedings, authoritative cybersecurity guides such as NIST SP 800-207 and regulatory guides such as GDPR compliance. These articles shall be critically studied to determine the theoretical and practical implications of deploying Zero Trust. reater emphasis will be placed on documented cases of adoption examples by early adopter companies and case studies of Zero Trust success in the field sector by sector.

Benefit: This secondary data will aid in the confirmation and comparison of opinions held by interview respondents. It will bridge the gap between regulatory needs, academic research and real practice to give a comprehensive picture of Zero Trust effectiveness, deployment issues and solutions suited to industry.

3. Case Study Analysis

To compare the results of the interviews with real-world, practical deployments, the research will incorporate a case study analysis. This will be accomplished by analyzing detailed reports and documentation of organisations that have successfully implemented Zero Trust. Companies such as Microsoft, Sanmina and Repsol are some of the examples where Zero Trust has been applied successfully to hybrid working models. Through analysing these examples the research will contrast the organisations' plans, results and challenges with the result of the interviews.

Benefit: This analysis will enhance the practical relevance of the research and provide valuable insights into the real-world applicability of Zero Trust, helping to ground the research findings in actual organisational experiences.

Zero Trust Policy Design:

Zero Trust Security Policy for Remote and Hybrid Workforces

1. **Policy Statement**

   This policy outlines the responsibilities, standards, and controls put in place to achieve Zero Trust Architecture (ZTA) pertaining specifically to the security of remote and hybrid workforces. As per the verification-focused “Never trust, always verify” model, this policy enforces continuous authentication, access restrictions at every level for all users, devices and systems interfacing with the organisation’s digital resources, real-time threat assessment as well as monitoring.

2. **Purpose**

   Establish a security framework which:
   i) Reduces the chances of insider threats and outside attacks.
   ii) Protects access to vital systems regardless of user location.
   iii) Guarantees compliance with GDPR as well as other governing requirements.
   iv) Allows for expansion and performance efficiency at the same time not undermining security.

3. **Scope**

   This policy applies to:
   i) All employees, contractors, and third-party users accessing enterprise systems.
   ii) All devices (corporate and BYOD), applications, and services used in remote and hybrid work environments.
   iii) All digital assets, data repositories, and network infrastructure under the organisation’s

control.

4. Guiding Principles of Zero Trust

Table 2 Main Principles of Zero Trust

Principle	Description
Verify Explicitly	Authenticate and authorise based on all available data points (user identity, device, location, workload, etc.).
Use Least Privilege Access	Restrict access rights to the minimum necessary. Implement Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC).
Assume Breach	Design as if a breach has already occurred. Minimise blast radius and prevent lateral movement.
Continuous Monitoring	Implement AI-driven monitoring tools (e.g., UEBA, ML anomaly detection) for real-time threat response.

5. Key Controls and Policy Directives

5.1 Identity and Access Management (IAM)

- Making sure that all users who need to use sensitive systems use **MFA** and **Single Sign-On (SSO)**.
- Use cloud native protocols and time-based RBAC to set up federated IAM frameworks (Alam et al, 2024).
- Use **access controls** that are aware of the situation and change based on real-time risk assessments (Krishnan & Sreeja, 2021).
- Every **three months** all access rights should be checked.

5.2 Network Segmentation and Micro-Segmentation

- All business networks must be divided into smaller parts using **micro-segmentation** methods.
- Sensitive assets like HR systems and financial databases that need to be kept in separate areas with very specific firewall rules.
- When possible, use software-defined networking (SDN) to enhance dynamic segmentation.

- According to 62.5% of respondents from survey phased **segmentation models** are the best way to handle issues such complex remote access and legacy systems.

5.3 Device Security and Endpoint Management

- All devices must be enrolled in a **Mobile Device Management (MDM)** system with remote wipe capability.
- **Compliance checks** must be conducted before any device is granted access.
- Endpoint Detection and Response (EDR) tools must be deployed organisation-wide.

5.4 Continuous Monitoring & AI Integration

- Utilise tools powered by **AI/ML** to conduct **User Entity Behaviour Analytics** (UEBA) for both users and entities.
- Insider threats or accounts that have been compromised can be discovered through the use of anomaly detection algorithms.
- Centralised logging alongside **real-time alerts** should be enforced with security teams available around the clock.
- Regular audits of machine learning models are essential to validating **accuracy** and **compliance** concerning fairness, ethics and algorithmic discrimination.

5.5 Data Protection and Encryption

- Confirm that all data is encrypted during transit and at rest using at least TLS 1.3 standard encryption protocols.
- Identify sensitive data using established data classification frameworks.
- **Enforce Data Loss Prevention** (DLP) Policies on cloud platforms as well as endpoints.

5.6 Application Security

- All applications should be regarded according to the Zero Trust principles and cloud native apps and other services should be handled using service mesh tools like Istio (Rodigari et al., 2021).
- For both internal and external applications, regular penetration testing, vulnerability scans and code audits are required.
- In smart device environments, implement adaptive access policies such as **HyBRCAC** and **HyBACRC** (Ameer et al., 2023).

5.7 Policy Enforcement and Governance

- The **Policy Decision Point** (PDP) shall make all access decisions based on continuous context validation.
- The **Policy Enforcement Point** (PEP) must enforce all PDP decisions without exception.
- Establish a Zero Trust Governance Committee to oversee implementation and conduct annual reviews.
- All staff must complete Zero Trust Awareness Training upon joining and annually thereafter.

6. Roles and Responsibilities

Table 3 Roles and Responsibilities

Role	Responsibility
CISO	Overall responsibility for Zero Trust enforcement and regulatory compliance.
IT Security Team	Technical implementation of IAM, monitoring, and segmentation policies.
HR & Training	Deliver security awareness programs; track training compliance.
Employees & Contractors	Comply with access control measures and report anomalies or policy breaches.

7. Compliance and Monitoring

- **Internal audits will be used to confirm adherence to this policy.**
  - Inspections by regulatory bodies (e.g., GDPR).
  - Security evaluations with established KPIs.
- Termination, disciplinary action or suspension of access could follow non compliance.

8. Exceptions

The CISO must formally approve, justify and document any exceptions. Each and every exception must be accompanied by a risk assessment.

9. **Review Cycle**

This policy will be reviewed annually or sooner if:

- Significant security incidents occur.
- Regulatory or technological changes arise.
- Gaps are identified during audits.

Data Collection:

Qualitative data for the research were gathered through the instrumentality of semi-structured interviews of two experienced security professionals with extensive histories of Zero Trust policy application within their respective institutions. Participants were selected based on the number of years of field exposure as well as the degree of involvement in cybersecurity planning and operations. Interviews provided important information on challenges, solutions and best practices for deploying Zero Trust for remote and hybrid employees.

Participant 1: Senior Consulting Systems Engineer at World Wide Technology (WWT) with a specialisation in Zero Trust implementations for global financial customers.

Participant 2: AVP, Cybersecurity, Zero Trust, CDN and BOT defense at Barclays UK.

Key Insights from Interviews

1. Security Threats of Remote and Hybrid Workforcess

- **Participant 1** said the challenge is that of balancing user experience and security, particularly with increased use of SaaS applications. Securing the applications and managing them without inconveniencing users is the core challenge.
- **Participant 2** identified that there is no well-defined perimeter of the network in remote locations. Since the employees are located at various locations and access the company, firms face the challenge of maintaining security without dealing with external networks.

2. The Zero Trust Role in Minimizing Challenges

- Zero Trust is essential to the security of remote employees, both presenters concurred. Companies minimize security risk by imposing rigid identity verification, authentication and ongoing verification.
- **Participant 1** opined that Zero Trust offers SaaS application-secured access with governance and compliance.
- **Participant 2** mentioned that the use of solutions like Zscaler, CrowdStrike and M365 Defender gives consistency in security despite roaming configurations.

3. Zero Trust's Major Elements

- **Identity and Access Management (IAM)** was considered the highest priority domain to be enabled with Zero Trust. The two participants emphasized the need for role-based access control (RBAC), multi-factor authentication (MFA) and continuous auditing.
- **Participant 2** demonstrated how user lifecycle management and authentication availability are particularly critical to a remote workforce.

4. Zero Trust Implementation Challenges

- **Participant 1** recognized the challenge of integrating various technologies and managing cross-functional collaboration.
- **Participant 2** posited that legacy systems pose significant challenges. Network segmentation and firewall stacking are the secrets to restricting the spread of future attacks.

5. Threat Monitoring within Zero Trust Environment

- The speakers both pushed for solution optimisation and platform integration so that efficient threat monitoring could be offered. They clarified that organisations tend to yield mixed results depending on the deployment method.

6. AI and Machine Learning's Role

- **Participant 2** mentioned the two-edged effect of AI on cybersecurity.
  AI provides the attackers with an edge by way of improved threat analysis and detection to make more sophisticated strategies.

7. Leadership Support and Adoption of Compliance

- **Participant 2** emphasized that Zero Trust policies must be data protection regulation compliant (e.g., GDPR, CCPA, HIPAA).
- The two participants believed in the notification and training campaign to receive the leadership's sanction for Zero Trust initiatives.

Survey

To facilitate research on Zero Trust Architecture (ZTA) for the protection of remote and hybrid workforces, data were collected through an online survey format, distributed via Google Forms. Staff in cybersecurity roles with substantial knowledge of their organization’s risk environment comprised the respondents with most group members holding senior positions in large IT and financial organizations and having experience of real-world implementation contexts. Drawing from expert surveys primarily in the areas of Identity and Access Management, Network Segmentation, Behavioural Analytics, Policy Enforcement, and generally in organizations that balance resource limits with remaining operationally and culturally resilient. Most of the participants indicated the use of

Multi-Factor Authentication (MFA) and Single Sign-On (SSO) systems were effective and expressed confidence in Role-Based Access Control (RBAC) policies which was expected. A few organizations have with UEBA (User and Entity Behaviour Analytics) or AI Analytics systems (which) were used to monitor for anomalous activities which shows some organizations are interested in moving toward more proactive security monitoring. The survey responses also showed that cultural readiness for Zero Trust varies and respondents demonstrated that leadership support was a key ingredient but some identified barriers to implementation such as, legacy technologies and reduction of awareness. Although many respondents had Zero Trust policies in place, several points out that their policies were poorly defined or still in development with limited accountability measures. These responses confirm the trends noted in the literature, that while there are more technical bases for Zero Trust than ever, adoption may still run into challenges, based on political, operational, and resource type barriers. The survey responses provide critical information around current gaps and opportunities in Zero Trust going forward. The excel provided below shows the individual responses.

Link: https://docs.google.com/spreadsheets/d/1WRe7PHB-UXrPlAE24Yrciq6yqKFBAOMhnAlLD_NSCec/edit?usp=sharing

Conclusion

The results of these interviews are worthwhile in providing an insight into the operational application of Zero Trust policies. While there remain challenges, organisations can enhance their cybersecurity position through proper IAM, network segmentation and ongoing monitoring. Future research may delve deeper into the utilisation of AI to strengthen Zero Trust solutions and resist emerging cyber threats.

Data Analysis:

6.1 Introduction

In this section, data gathered from primary (interviews) and secondary (literature review) sources are synthesized to study trends, issues and strategic priorities for the deployment of Zero Trust Architecture (ZTA) for hybrid and remote workforces.

6.2 Thematic Analysis of Interview Transcripts

Thematic analysis was used to determine overriding themes from cybersecurity expert interviews:

- Theme 1: Identity-Centric Security
  Identity was the most highlighted new boundary by the majority of interviewees, corroborating literature on the importance of IAM, RBAC and MFA in Zero Trust.
- Theme 2: Visibility and Continuous Monitoring
  Interviewers invariably highlighted that perimeter-based models fail to detect lateral

movement. This is corroborated by NIST SP 800-207 and literature citing the need for behaviour analytics and User and Entity Behavior Analytics (UEBA).

- Theme 3: Integration with Legacy Systems
  Practice testers noted that legacy IT infrastructures come up short of ZTA interoperability, in line with Gartner's alert about hybrid infrastructure limitations.
- Theme 4: AI & Automation's Role
  Different participants identified the growing necessity for AI as a tool for threat detection, supporting emerging academic insight on real-time analytics, especially within distributed networks.

6.3 Synthesizing Literature Review

- Scholarly literature (e.g., CISA, NIST, ENISA) advocates for micro-segmentation, encrypted data transmission and zero implicit trust.
- Studies show that ZTA raises detection levels but requires substantial initial investments and cross-department coordination.
- ZTA is increasingly being promoted in compliance solutions (e.g., GDPR).

Table 4 Comparison of Literature Review Insights and Interview Findings on Key Zero Trust Policy Dimensions

Dimension	Literature Review	Interview Insights
Identity Management	Central to ZTA; requires strong IAM/MFA	Real-world implementation varies; SSO and IAM integration challenges
Network Segmentation	Strongly supported; limits lateral movement	Difficult to implement without automation or SDN
User Behaviour Monitoring	Essential for anomaly detection	Not yet widely adopted; often budget-constrained
Cultural Readiness	Rarely addressed in academic work	Identified as a major barrier to ZTA adoption
Policy & Governance	Critical; must be adaptable and transparent	Often lacking clear enforcement strategies

6.4 Implications for Policy Design

The analysis reveals the need for:

- Adaptive access controls tailored to job roles.
- Behavioural analytics and automated threat detection.
- Training programmes to overcome human and cultural barriers.
- A phased implementation plan that accounts for legacy systems.

6.5 Conclusion

The alignment between theory and practice validates the Zero Trust principles outlined in the policy. However, successful adoption depends heavily on organisational readiness, stakeholder buy-in, and technical integration capabilities.

Discussion:

Case Studies

Implementing Zero Trust for Securing Remote and Hybrid Workforces

Syed Mubin Husain, a Senior Consulting Systems Engineer at Worldwide Technology (WWT), and Rohit Chaudhary, an Assistant Vice President at Barclays UK, are two experienced professionals whose insights play a crucial role in this case study. Their viewpoint clarified the difficulties that businesses encounter when putting zero-trust policies into place to protect remote and hybrid work environments, as well as the workable solutions they have discovered to deal with these problems.

The Challenges of Securing Remote and Hybrid Workforces

Due to remote and hybrid work arrangements, Cybersecurity has become more complicated. One of the main challenges, as Husain points out, is finding a balance between strong security and a smooth user experience. His clients, especially in the financial sector, face difficulties securing SaaS applications, which are becoming increasingly critical to their operations. Chaudhary shares similar concerns, stressing the lack of control over the networks and locations that employees use. To mitigate these risks, he underscores the importance of Data Loss Prevention (DLP) tools and security solutions like Microsoft 365 Defender, Zscaler, and CrowdStrike, which help safeguard company data outside of traditional network perimeters.

How Zero Trust Addresses These Challenges

The foundation of Zero Trust is the tenet "Never trust, always verify." Husain claims that to safeguard application traffic and stop data breaches, it focuses on identity, authorisation, authentication, and auditing. Zero Trust guarantees adherence and authenticates people before allowing them to access

resources from a distance. Chaudhary highlights the need for multi-factor authentication (MFA), which adds a crucial layer of protection against account takeovers.

Core Components of Zero Trust

The two main pillars of Zero Trust are Network segmentation and Identity and Access Management (IAM). Husain expresses how role-based access, which makes sure users only access the resources they require, can be implemented by enterprises using IAM. For geographically dispersed workforces, Chaudhary stresses the importance of effective IAM systems that avoid performance delays while managing user lifecycles and enforcing strong MFA protocols.

Network segmentation is another key element. By isolating parts of the network, segmentation limits the spread of threats like malware. Chaudhary suggests using layered firewalls, role-based access, and regular audits so outdated systems can be safeguarded.

Challenges in Implementing Zero Trust

Zero Trust implementation is a multi-step procedure that calls for meticulous preparation and cooperation. Husain highlights the challenges of integrating various technologies and aligning cross-functional teams, especially when applications are spread across multiple cloud environments. Chaudhary further notes that companies need to manage data protection laws like the CCPA, GDPR, and PCI DSS and choose systems that meet these requirements.

The Role of Emerging Technologies

The cybersecurity landscape is changing due to emerging technology. Chaudhary points out that by examining enormous volumes of data, developments in data analytics are enhancing danger detection. However, these same technologies can also be leveraged by attackers to develop more sophisticated attack methods. As cyber threats evolve, businesses must leverage these technologies to stay ahead of potential threats.

Scalability and the Future of Zero Trust

Zero Trust is scalable and advantageous for businesses of all sizes, according to both experts. Husain mentions that while smaller businesses may find it easier to implement, larger companies need a more strategic, gradual approach to deployment. Chaudhary states Zero Trust will evolve from a "nice-to-have" to a vital component of business security as cyber threats continue to increase.

Conclusion and Recommendations

This case study highlights how important Zero Trust is in the constantly changing cybersecurity environment of today and by considering the following, Organisations can strengthen their security behaviour:

1. **Prioritise Identity and Access Management (IAM):** Strong identity management techniques such as multi-factor authentication (MFA) and role-based access, are put into place to guarantee that only the appropriate individuals have access to the appropriate resources.
2. **Adopt Network Segmentation:** Regular auditing and the security of older legacy systems can help reduce risks and the impact of any breaches.
3. **Stay Compliant:** Customers and stakeholders are more confident when zero confidence techniques are implemented in accordance with industry standards and data protection laws.
4. **Leverage AI and Machine Learning:** Organisations may keep ahead of hackers by utilizing cutting-edge technologies for proactive risk management and real-time threat detection.
5. **Foster Organisational Buy-In:** Ensuring that leadership and employees share the Zero Trust ideals is essential for successful adoption and long-term sustainability.

By adopting a well-rounded, collaborative approach, organisations can safeguard sensitive information, manage risks more effectively, and position themselves for success in an increasingly digital world.

Conclusions:

This research effort resulted in a well-developed Zero Trust security policy to strengthen cybersecurity for remote and hybrid workers, taking into account the additional complexity of securing remote environments. While reviewing relevant literature, and conducting semi-structured interviews with professionals in the field of cybersecurity, engaging with an online survey of industry professionals, as well as examining case studies of organizations adopting ZTA supported the delivery of a Zero Trust Policy based on IAM, MFA, endpoint security, network segmentation, and taking into account the role of continuous monitoring and artificial intelligence (AI) to advance organizational resilience.

The research goal - to create and validate a Zero Trust security policy for the securing of remote and hybrid workforces - was achieved by working with identity-centric access control principles while maintaining least privilege principles and AI-enabled continuous monitoring organized into a structured policy adaptable to the needs of an organization. All of the original research objectives were achieved: the research findings on ZTA identified requirements and barriers in distributed environments, developed a policy with both technical and governance control aspects, validated the policy through real organizational implementations, and positioned the development of a phased approach to avoid the challenges specifically related to cost, user resistance, and regulatory compliance issues in advance of the implementation of the policy.

The findings indicated that ZTA is a required mechanism to mitigate risk with remote or hybrid work where perimeter-based security models alone are insufficient. The IT and finance professionals were able to provide contextual relevance and meaning to all-access requests based on identity-centric security and the least privilege access as ways to protect information and be sure all access requests are verified. The proposed policy combined some of these concepts to provide a systematic method to address risk vulnerabilities. The case studies of organizations utilising ZTA to increase security showcases the need for considering and balancing security with productivity and efficiency.

A significant contribution of the research is the focus on continuous monitoring and the utilisation of AI-enabled User and Entity Behaviour Analytics (UEBA). The research and use of AI would enable near-real-time detection of threat, enabling adaptive mitigation in light of the fluid nature of cyber threat characteristics with the remote and/or distributed workforce. In the research, barriers to implementation of ZTA were identified including legacy system integration, scalability as it relates to SMEs, and the regulatory requirements of compliance with legislation such as the General Data Protection Regulation (GDPR). The proposed policy included a way to reduce barriers to integration through structured policy decision-making, enforcement strategies (i.e. updating controls), and governance arrangements ensuring regulatory compliance and operational scalability.

The stakeholder feedback indicated some implementation barriers, specifically user resistance and costs. The research addressed these proposed barriers in the encounters designed around the users

who would be participating in the Zero Trust implementation, and phases of implementation, so the investment would be consistent with organizational priorities and available resources. Lastly, the research explored potentially interesting directions for the next spaces to investigate, especially regarding how future challenges will impact ZTA in new environments like the Internet of Things (IoT) and the software supply chain.

In conclusion, this research achieved its intended aim and goals by producing an applied and adaptable Zero Trust security policy to improve cybersecurity for remote and hybrid workers. The findings point to clear pathways to help organizations mitigate the concerns associated with modern workplaces, primarily through identity verification, ongoing monitoring, AI-enhanced analytics, while maintaining compliance and usability. Future investigations might explore particular examples of large-scale implementation in resource-limited contexts as well as the trajectory of shifting regulations that can build resilience in Zero Trust implementations from continually evolving threats from cybercriminals.

Recommendations for Further Work :

To maintain the effectiveness and relevance of this Zero Trust Security Policy in addressing emerging cybersecurity threats, recommended additional work would be appropriate in numerous strategic and technical aspects. These recommendations aim to improve the depth, flexibility and future state readiness of Zero Trust deployed for remote and hybrid workforces.

1. AI-Driven Policy Decision and Enforcement

Future work should explore AI and ML integration in the Policy Decision Point (PDP) and Policy Enforcement Point (PEP) functions. Static access rules have an essential baseline protection element, but cannot change in detecting and responding to advanced threat detection. AI-enhanced PDPs can analyse behaviour patterns and risk signals in real time, allowing for more precise and dynamic access decisions. Similarly, intelligent PEPs could respond autonomously to anomalous behaviours by restricting or revoking access without human intervention.

2. Expansion of Context-Aware Risk-Based Access

Further exploration into adaptive models such as Hybrid Behaviour Attribute-based Access Control (HyBACAC and HyBACRC), which incorporate behavioural attributes, environmental stimuli, and real-time risk assessment need to be undertaken. These models are particularly useful for BYOD and hybrid workers on untrusted networks. Regular updates and tests of such a model increase accuracy and reduce false positive incidents enhance user experience while still maintaining a level of security.

3. Automation and Policy Lifecycle Management

In order to scale Zero Trust policies, organizations must be empowered to automate access policy lifecycle management. Lifecyle management involves the creation, validation, simulation, deployment, and eventual retirement of access policies. Access policies can be managed in an automated fashion by means of Infrastructure-as-Code (IaC) and DevSecOps practices. By doing so, multiple organizations could employ tools like Open Policy Agent (OPA) and Rego, in order to manage granular policy logic against cloud-native platforms, ensuring policies can be consistently applied while removing opportunities for humans to misconfiguring service(s), while enhancing agility.

4. Integration with Emerging Technologies

With the emergence of technologies like quantum computing, edge computing, and 6G technology, it is imperative to examine how Zero Trust concepts may apply to such technologies. Next steps should include testing Zero Trust policies against quantum resistant encryption policies, and furthermore extend tests into how micro-segmentation and secure identity models apply to edge computing in highly distributed environments. Such forward-papering ensures the security models will remain relevant and applicable within future infrastructures.

5. Threat Intelligence Sharing and Federated Learning

In order to bolster collective defence capabilities, the institution should consider the establishment of secure, privacy-preserving mechanisms for sharing threat intelligence with trusted partners. Federated learning and secure multi-party computation are examples that may be used to share behavioural patterns and indicators of compromise without disclosing sensitive data. This may produce rich contextual information for the PDP while still adhering to data protection legislation.

6. User Awareness and Behavioural Training

Security awareness training must be more than static annual compliance training. Future opportunities to engage staff in awareness training should involve gamification, phishing simulations, or behavioural change models. Using behavioural analytics to tailor content for users based on their own behaviours will reinforce safe behaviours and reduce the potential for insider threats and social engineering.

7. Zero Trust Maturity Assessment Framework

Lastly, The institution may want to explore the adoption of a Zero Trust Maturity Model, following NIST or CISA architecture, to continuously evaluate and benchmark the status of implementation across departments. This may inform investment decisions, highlight short-falls and ensure that maturity in the deployment of Zero Trust strategies keeps pace with technology growth and maturity of the institution.

Glossary :

TERM	DEFINITION
ZERO TRUST ARCHITECTURE (ZTA)	A cybersecurity framework based on the principle "Never trust, always verify," which assumes no implicit trust in any user, device, or system and enforces continuous verification and strict access control at every step.
POLICY DECISION POINT (PDP)	The centralized or decentralized component responsible for evaluating access requests by applying dynamic security policies based on user identity, device posture, location, threat intelligence, and other contextual attributes.
POLICY ENFORCEMENT POINT (PEP)	The component that enforces access control decisions made by the PDP, managing the connection between users/devices and resources without making policy decisions itself.
IDENTITY AND ACCESS MANAGEMENT (IAM)	A system framework for managing digital identities and controlling access permissions to enterprise resources, often involving authentication and authorization processes.
ROLE-BASED ACCESS CONTROL (RBAC)	An access control model where permissions are assigned to users based on their organizational roles, restricting access to only what is necessary for those roles.
ATTRIBUTE-BASED ACCESS CONTROL (ABAC)	An access control model where access decisions are based on attributes such as user location, device state, time, and other environmental factors, allowing more granular and dynamic control.
HYBRID BEHAVIOUR ATTRIBUTE-BASED CONTROL (HYBACAC / HYBACRC)	Advanced access control frameworks combining role-based and attribute-based controls with behavioural analytics for fine-grained, context-aware authorization.
MULTI-FACTOR AUTHENTICATION (MFA)	A security mechanism requiring users to provide two or more independent authentication factors (e.g., password, biometric, token) to verify identity.
SINGLE SIGN-ON (SSO)	An authentication process allowing users to access multiple applications with a single set of login credentials, improving convenience while maintaining security.

MOBILE DEVICE MANAGEMENT (MDM)	Technology solutions that manage, monitor, and secure mobile devices, ensuring compliance with corporate security policies, including remote wipe capabilities.
ENDPOINT DETECTION AND RESPONSE (EDR)	Tools designed to continuously monitor and respond to threats targeting endpoint devices such as laptops, smartphones, and IoT devices.
USER AND ENTITY BEHAVIOUR ANALYTICS (UEBA)	Analytical techniques that use AI and machine learning to detect anomalous behaviour patterns of users and devices that may indicate insider threats or compromised accounts.
DATA LOSS PREVENTION (DLP)	Policies and tools implemented to prevent unauthorized transmission or leakage of sensitive data both within and outside the organizational network.
SERVICE MESH	An infrastructure layer that manages secure communication between microservices in cloud-native environments, often supporting Zero Trust principles.
ISTIO	An open-source service mesh platform that provides traffic management, security, and observability for microservices, enabling policy enforcement without changing application code.
TRANSPORT LAYER SECURITY (TLS)	A cryptographic protocol that secures data in transit between devices and networks; TLS 1.3 is the latest and most secure version widely adopted.
INDUSTRIAL INTERNET OF THINGS (IIOT)	Networked industrial devices and sensors often deployed in critical infrastructure; present unique challenges for Zero Trust due to real-time and operational constraints.
ZERO TRUST EXCHANGE	A security platform that facilitates direct-to-cloud connectivity while enforcing Zero Trust principles to improve security and performance for distributed users.
QUANTUM SECURITY	Emerging security techniques using quantum computing principles (e.g., quantum keys) intended to enhance cryptographic strength, with implications for future Zero Trust implementations.

References:

Abdelmagid, A.M. and Diaz, R. (2025). Zero Trust Architecture as a Risk Countermeasure in Small–Medium Enterprises and Advanced Technology Systems. *Risk Analysis*. doi:https://doi.org/10.1111/risa.70026.

Abwnawar, N. *et al.* (2017) 'Towards data privacy in heterogeneous cloud environments: An extension to the SANTA policy language', in *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)*. *2017 Second International Conference on Fog and Mobile Edge Computing (FMEC)*, Valencia, Spain: IEEE, pp. 14–19. Available at: https://doi.org/10.1109/FMEC.2017.7946401.

Adahman, Z., Malik, A.W. and Anwar, Z. (2022). An analysis of zero-trust architecture and its cost-effectiveness for organisational security. *Computers & Security*, 122. doi:https://doi.org/10.1016/j.cose.2022.102911.

Alam, S.R. *et al.* (2024) 'Federated Single Sign-On and Zero Trust Co-design for AI and HPC Digital Research Infrastructures', in *SC24-W: Workshops of the International Conference for High Performance Computing, Networking, Storage and Analysis*. *SC24-W: Workshops of the International Conference for High Performance Computing, Networking, Storage and Analysis*, Atlanta, GA, USA: IEEE, pp. 1756–1764. Available at: https://doi.org/10.1109/SCW63240.2024.00220.

Alawneh, M. and Abbadi, I.M. (2022) 'Integrating Trusted Computing Mechanisms with Trust Models to Achieve Zero Trust Principles', in *2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*. *2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, Milan, Italy: IEEE, pp. 1–6. Available at: https://doi.org/10.1109/IOTSMS58070.2022.10062269.

Ameer, S., Benson, J. and Sandhu, R. (2023) 'Hybrid Approaches (ABAC and RBAC) Toward Secure Access Control in Smart Home IoT', *IEEE Transactions on Dependable and Secure Computing*, 20(5), pp. 4032–4051. Available at: https://doi.org/10.1109/TDSC.2022.3216297.

Amusuo, P.C. *et al.* (2025) 'ZTD_{JAVA}: Mitigating Software Supply Chain Vulnerabilities via Zero-Trust Dependencies', in *2025 IEEE/ACM 47th International Conference on Software Engineering (ICSE)*. *2025 IEEE/ACM 47th International Conference on Software Engineering (ICSE)*, Ottawa, ON, Canada: IEEE, pp. 1294–1306. Available at: https://doi.org/10.1109/icse55347.2025.00148.

Brockelsby, W. and Dutta, R. (2021) 'Traffic Analysis in Support of Hybrid SDN Campus Architectures for Enhanced Cybersecurity', in *2021 24th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*. *2021 24th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN)*, Paris, France: IEEE, pp. 41–48. Available at: https://doi.org/10.1109/ICIN51074.2021.9385530.

Buck, C., Olenberger, C., Schweizer, A., Völter, F. and Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, 110, p.102436. Available at: https://doi.org/10.1016/j.cose.2021.102436.

CSO Online. (n.d.). *9 in 10 organisations have embraced zero-trust security globally*. [online] Available at: https://www.csoonline.com/article/1249027/9-in-10-organisations-have-embraced-zero-trust-security-globally.html.

Crowther, K.G. (2024) 'Blending Shared Responsibility and Zero Trust to Secure the Industrial Internet of Things', *IEEE Security & Privacy*, 22(5), pp. 96–102. Available at: https://doi.org/10.1109/msec.2024.3432208.

Fang, W. and Guan, X. (2022) 'Research on iOS Remote Security Access Technology Based on Zero Trust', in *2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC)*. *2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC)*, Chongqing, China: IEEE, pp. 238–241. Available at: https://doi.org/10.1109/ITOEC53115.2022.9734455.

Fernandez, E.B. and Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces*, [online] 89, p.103832. doi:https://doi.org/10.1016/j.csi.2024.103832.

Gujar, S.S. (2024) 'Real-Time Threat Detection and Response Using AI for Securing Critical Infrastructure', in *2024 Global Conference on Communications and Information Technologies (GCCIT)*. *2024 Global Conference on Communications and Information Technologies (GCCIT)*, BANGALORE, India: IEEE, pp. 1–7. Available at: https://doi.org/10.1109/GCCIT63234.2024.10862978.

Ho, P.-H., Chen, H.-Y. and Lin, T.-N. (2023) 'Zero Trust Architecture of Token Network', in *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*. *2023 IEEE International Conference on Metaverse Computing, Networking and Applications (MetaCom)*, Kyoto, Japan: IEEE, pp. 674–675. Available at: https://doi.org/10.1109/MetaCom57706.2023.00120.

Hong, S. *et al.* (2023) 'SysFlow: Toward a Programmable Zero Trust Framework for System Security', *IEEE Transactions on Information Forensics and Security*, 18, pp. 2794–2809. Available at: https://doi.org/10.1109/TIFS.2023.3264152.

Ishide, K. *et al.* (2022) 'ML Detection Method for Malicious Operation in Hybrid Zero Trust Architecture', in *2022 IEEE International Conference on Computing (ICOCO)*. *2022 IEEE International Conference on Computing (ICOCO)*, Kota Kinabalu, Malaysia: IEEE, pp. 264–269. Available at: https://doi.org/10.1109/ICOCO56118.2022.10031702.

Ilyas, M., Akal, M. and Althebyan, Q. (2024) 'Maturity Model for Corporate Sector Based on Zero Trust Adoption', in 2024 International Conference on Engineering and Emerging Technologies (ICEET). 2024 International Conference on Engineering and Emerging Technologies (ICEET), Dubai, United Arab Emirates: IEEE, pp. 1–7. Available at: https://doi.org/10.1109/ICEET65156.2024.10913750.

Kumar, G.S., Kandavel, N. and Madhavan, K. (2020) 'To Discovery The Cloud Services Authentication An Expert Based System Using Multi-Factor Authentication', in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*. *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India: IEEE, pp. 1014–1016. Available at: https://doi.org/10.1109/ICACCS48705.2020.9074195.

Krishnan, V. and Sreeja, C.S. (2021) 'Zero Trust-Based Adaptive Authentication using Composite Attribute Set', in *2021 IEEE 3rd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS)*. *2021 IEEE 3rd PhD Colloquium on Ethically Driven Innovation and Technology for Society (PhD EDITS)*, Bangalore, India: IEEE, pp. 1–2. Available at: https://doi.org/10.1109/PhDEDITS53295.2021.9649474.

Lin, J. *et al.* (2024) 'Quantum-Enhanced Zero Trust Security: Evolution, Implementation, and Application', in *2024 International Conference on Quantum Communications, Networking, and Computing (QCNC)*. *2024 International Conference on Quantum Communications, Networking, and Computing (QCNC)*, Kanazawa, Japan: IEEE, pp. 211–215. Available at: https://doi.org/10.1109/QCNC62729.2024.00040.

Ma, M., Yu, Z. and Liu, B. (2023) 'Automatic Generation of Network Micro-Segmentation Policies for Cloud Environments', in *2023 4th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)*. *2023 4th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT)*, Nanjing, China: IEEE, pp. 1–5. Available at: https://doi.org/10.1109/AINIT59027.2023.10212857.

Mishra, S. and Chitkara, M. (2023) 'Service Level Trust Key Encryption based Cloud Security using Starvation End-Point Encryption', in *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)*. *2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)*, Raichur, India: IEEE, pp. 01–05. Available at: https://doi.org/10.1109/ICICACS57338.2023.10099816.

Mohammed, M. *et al.* (2021) 'A Zero Trust Model Based Framework For Data Quality Assessment', in *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*. *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA: IEEE, pp. 305–307. Available at: https://doi.org/10.1109/CSCI54926.2021.00123.

Moudni, M.E. and Ziyati, E. (2023) 'A Multi-Cloud and Zero-Trust based Approach for Secure and Redundant Data Storage', in *2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM)*. *2023 10th International Conference on Wireless Networks and Mobile Communications (WINCOM)*, Istanbul, Turkiye: IEEE, pp. 1–6. Available at: https://doi.org/10.1109/WINCOM59760.2023.10323009.

Mutabazi, P., Ndashimye, E. and Ndibwile, J.D. (2023) 'Investigating the Challenges Companies in Rwanda Face when Implementing Zero-Trust Network', in *2023 10th International Conference on*

Future Internet of Things and Cloud (FiCloud). *2023 10th International Conference on Future Internet of Things and Cloud (FiCloud)*, Marrakesh, Morocco: IEEE, pp. 382–392. Available at: https://doi.org/10.1109/ficloud58648.2023.00062.

Parambil, M.M.A. *et al.* (2024) 'Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects', *Computers and Education: Artificial Intelligence*, 7, p. 100327. Available at: https://doi.org/10.1016/j.caeai.2024.100327.

Paramesh, J. *et al.* (2024) 'Developing an Adaptive Security Framework for Real-Time Threat Detection and Response in Cloud-Network Systems', in *2024 International Conference on Cybernation and Computation (CYBERCOM)*. *2024 International Conference on Cybernation and Computation (CYBERCOM)*, Dehradun, India: IEEE, pp. 644–648. Available at: https://doi.org/10.1109/CYBERCOM63683.2024.10803141.

Petrovska, J., Memeti, A. and Imeri, F. (2019) 'SOA Approach - Identity and Access Management for the Risk Management Platform', in *2019 8th Mediterranean Conference on Embedded Computing (MECO)*. *2019 8th Mediterranean Conference on Embedded Computing (MECO)*, Budva, Montenegro: IEEE, pp. 1–4. Available at: https://doi.org/10.1109/MECO.2019.8760095.

Purohit, K.C. *et al.* (2017) 'Hybrid approach for securing IoT communication using authentication and data confidentiality', in *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*. *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*, Dehradun, India: IEEE, pp. 1–6. Available at: https://doi.org/10.1109/ICACCAF.2017.8344678.

Rose, S. *et al.* (2020) *Zero Trust Architecture*. National Institute of Standards and Technology. Available at: https://doi.org/10.6028/NIST.SP.800-207.

Rodigari, S. *et al.* (2021) 'Performance Analysis of Zero-Trust multi-cloud', in *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)*. *2021 IEEE 14th International Conference on Cloud Computing (CLOUD)*, Chicago, IL, USA: IEEE, pp. 730–732. Available at: https://doi.org/10.1109/CLOUD53861.2021.00097.

Rustam, F., Ranaweera, P. and Jurcut, A.D. (2024) 'AI on the Defensive and Offensive: Securing Multi-Environment Networks from AI Agents', in *ICC 2024 - IEEE International Conference on Communications*. *ICC 2024 - IEEE International Conference on Communications*, Denver, CO, USA: IEEE, pp. 4287–4292. Available at: https://doi.org/10.1109/ICC51166.2024.10622943.

Safeguarding the Hybrid Workforce with a Zero Trust Approach. (n.d.). Available at: https://www.zscaler.com/resources/industry-reports/hybrid-workforce-protection-zero-trust.pdf [Accessed 4 Jan. 2025].

Saleh, M. *et al.* (2024) 'An Analysis of Cybersecurity Mandates in the Context of Digital Reliance within Hybrid IT Models', in *2024 IEEE Annual Congress on Artificial Intelligence of Things (AIoT)*. *2024 IEEE Annual Congress on Artificial Intelligence of Things (AIoT)*, Melbourne, Australia: IEEE, pp. 169–172. Available at: https://doi.org/10.1109/AIoT63253.2024.00041.

Shanthi, R.R., Sasi, N.K. and Gouthaman, P. (2023) 'A New Era of Cybersecurity: The Influence of Artificial Intelligence', in *2023 International Conference on Networking and Communications (ICNWC)*. *2023 International Conference on Networking and Communications (ICNWC)*, Chennai, India: IEEE, pp. 1–4. Available at: https://doi.org/10.1109/ICNWC57852.2023.10127453.

Singh, A. *et al.* (2023) 'Q-Learning Based Network Access Policy Management for Zero Trust Security in IIoT', in *2023 International Conference on Electrical, Electronics, Communication and Computers (ELEXCOM)*. *2023 International Conference on Electrical, Electronics, Communication and Computers (ELEXCOM)*, Roorkee, India: IEEE, pp. 1–5. Available at: https://doi.org/10.1109/ELEXCOM58812.2023.10370294.

S, N.G. and Shankaramma (2024) 'Framework Analysis and Zero Trust Security Issues in Contemporary Network Systems', in *2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)*. *2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)*, Bengaluru, India: IEEE, pp. 1–6. Available at: https://doi.org/10.1109/CSITSS64042.2024.10816783.

The 'Zero Trust' Model in Cybersecurity: Towards understanding and deployment. (n.d.). Available at: https://www3.weforum.org/docs/WEF_The_Zero_Trust_Model_in_Cybersecurity_2022.pdf.

Weinert, A. (2023). *Secure hybrid and remote workplaces with a Zero Trust approach*. [online] Microsoft Security Blog. Available at: https://www.microsoft.com/en-us/security/blog/2023/04/06/secure-hybrid-and-remote-workplaces-with-a-zero-trust-approach/.

Wu, Y.G., Yan, W.H. and Wang, J.Z. (2021) 'Real identity based access control technology under zero trust architecture', in *2021 International Conference on Wireless Communications and Smart Grid (ICWCSG)*. *2021 International Conference on Wireless Communications and Smart Grid (ICWCSG)*, Hangzhou, China: IEEE, pp. 18–22. Available at: https://doi.org/10.1109/ICWCSG53609.2021.00011.

Fernandez, E.B. and Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces*, [online] 89, p.103832. Available at: https://doi.org/10.1016/j.csi.2024.103832.

Appendix A: Project Plan (Unlimited Words):

Phase	Task	Start Date	End Date	Status
1. Project Initiation	Define scope and objectives	25-Nov-2024	30-Nov-2024	Completed
	Develop timeline and resources	27-Nov-2024	02-Dec-2024	Completed
	Obtain ethical approval	01-Dec-2024	05-Dec-2024	Completed
	Submit and approve research proposal Submit and approve research proposal	10-Jan-2025	11-Mar-2025	Completed
2. Literature Review	Conduct literature survey	06-Dec-2024	15-Jan-2025	Completed
	Identify research gaps	16-Jan-2025	25-Jan-2025	Completed
3. Data Collection	Conduct interviews (WhatsApp)	21-Nov-2024	21-Nov-2024	Completed
	Analyze case studies	10-Dec-2024	25-Dec-2024	Completed
	Administer survey (Google Forms)	15-Apr-2025	29-Apr-2025	Completed
4. Data Analysis & Policy	Analyze interview and survey data	30-Apr-2025	31-May-2025	Completed

	Design Zero Trust policy framework	15-May-2025	30-Jun-2025	Completed
	Validate policy design	01-Jul-2025	15-Jul-2025	Completed
5. Writing & Comp	Write dissertation chapters	01-Jun-2025	31-Jul-2025	Completed
	Compile appendices and materials	15-Jul-2025	10-Aug-2025	Completed
	Proofread and format dissertation	11-Aug-2025	15-Aug-2025	Completed
6. Submission	Final review and revisions	14-Aug-2025	16-Aug-2025	Completed
	Submit dissertation	18-Aug-2025	18-Aug-2025	Completed

Appendix B: Ethics Checklist (Unlimited Words):

A checklist should be completed for every research project. This is used to identify whether a full application for ethics approval needs to be submitted to the University Ethics Panel or one of its sub-committees. Further guidance can be found on the Ethics Blackboard shell.

1 Applicant details	
Name of Lead Researcher (applicant):	Abhishek Kudiri

2 Project details
Project title: Zero trust policy design for Securing Remote and hybrid workforces
Please provide a brief description of the project:

3 Research checklist Please answer each question by checking the appropriate box:			
Research that may need to be reviewed by an NHS Research Ethics Committee or another external Ethics Committee		YES	NO
1	Will the study involve recruitment of patients or staff through the NHS or Social Care, or the use of NHS data or premises and/or equipment?		✓
2	Does the study involve participants age 16 or over who are unable to give informed consent (e.g. people with learning disabilities: see Mental Capacity Act 2005)? NHS		✓
3	Will tissue samples (including blood) be obtained from participants?		✓
If you have answered 'Yes' to questions 1, 2 or 3 please refer to http://www.hra.nhs.uk/ for guidance. If external ethical approval is not needed, University ethical approval will still be required.			
Research participants		YES	NO
4	Does the study involve students within the University?		✓
5	Does the study involve employees of the University?		✓
6	Does the research involve potentially vulnerable groups: children, those with cognitive impairment, or those in unequal relationships? (eg your own students)		✓
7	Does the research involve members of the public or people worked with in a professional capacity?	✓	
8	Will the study require the co-operation of a 'gatekeeper' for initial access to the groups or individuals to be recruited and/or to give permission for initial contact? (e.g. children, students, members of self-help group, residents of nursing home, employees).		✓
Research methods		YES	NO

9	Will it be necessary for participants to take part in the study without their knowledge and consent at the time? (e.g. covert observation of people in non-public places)		✓
10	Will financial inducements (other than reasonable expenses and compensation for time) be offered to participants?		✓
11	Will the study involve discussion of sensitive topics or illegal activity (e.g. sexual activity, drug use)?		✓
12	Are drugs, placebos or other substances (e.g. food substances, vitamins) to be administered to the study participants or will the study involve invasive, intrusive or potentially harmful procedures of any kind?		✓
13	Is physical pain or more than mild discomfort likely to result from the study?		✓
14	Could the study induce psychological stress or anxiety or cause harm or negative consequences beyond the risks encountered in normal life?		✓
15	Will the study involve prolonged or repetitive testing?		✓
16	Is there a possibility that the safety of the researcher may be in question?		✓
17	Will any of the research take place outside the UK (excluding on-line surveys)?		✓
Data and confidentiality			
18	Will the research involve administrative or secure data that requires permission from the appropriate authorities before use?		✓
19	Will the research involve visual/vocal methods where respondents may be identified?		✓
20	Will research involve the sharing of data or confidential information beyond the initial consent given?	✓	
21	Will the research involve security-sensitive data? (eg commissioned by the military or under an EU security call; involve the acquisition of security clearances; concerns terrorist or extremist groups).		✓

If any item is checked "YES" you will need to seek advice from your supervisor / course leader regarding the appropriate sub-committee for ethical approval.

4. Declarations

I have read and will abide by the University's *Ethics Policy*.

I have read and will abide by the University's *Code Research Practice*.

I am aware of, and will abide by the ethical guidelines published by the relevant subject and/or professional associations most appropriate to my topic.

The responses given above are an accurate and true reflection of the nature of my research project.

Applicant:

Name: Abhishek Kudiri

Signed: 
Date: 14-12-2024

Project supervisor / Line manager

I confirm that the above details are accurate, the proposed methods are appropriate, ethical concerns have been considered and that time and resources are available for the research to take place.

Name (please print):
Signed:
Date:

Note: Electronic approval by above signatories is acceptable

Appendix C: Participant Consent Form (Unlimited Words):

BUCKINGHAMSHIRE NEW UNIVERSITY
EST. 1891

Notes

1. Black text forms the standard content of a consent form
2. **Consent by Rohit Chaudhary and Syed Mubeen**
3. Text notes in the grey boxes provide guidance only and are to be removed in the final consent form
4. Blue text indicates optional statements to add

Informed Consent for Zero trust policy design for securing remote and hybrid workforces

Please tick the appropriate boxes

1. Taking part in the study

I have read and understood the study information dated **[**20/11/2024**]**, or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction. ☐

I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason. I can withdraw my data up until [10/09/2025] which is the final date before data is analysed. ☐

I understand that taking part in the study involves sharing professional insights and experiences related to cybersecurity practices, particularly the implementation and challenges of Zero Trust policies in remote and hybrid workforces. This includes discussing industry challenges, emerging technologies, compliance with data protection regulations, and strategies for organisational buy-in. The information shared will be used solely for academic research purposes within the scope of a master's dissertation on Zero Trust Policy Design. ☐

Describe in a few words how information is captured, using the same terms as you used in the information sheet, for example: an audio-recorded interview, a video-recorded focus group, a survey questionnaire completed, an experiment, etc.].

For interviews, focus groups and observations, specify how the information is recorded (audio, video, written notes).

For questionnaires, specify whether participant or researcher completes the form.

☐

If there is a potential risk of participating in the study, then provide an additional statement:

I understand that taking part in the study has minimal risk as the information shared is professional and not personally sensitive. However, there is a potential risk of inadvertent disclosure of confidential company strategies or data, which will be mitigated by ensuring that no identifiable or proprietary information is included in the research outcomes.

2. Use of the information in the study

I understand that information I provide will be used for academic purposes, specifically to support the research on Zero Trust policy design for securing remote and hybrid workforces, and may be included in the dissertation and related publications.. ☐

List the planned outputs, e.g. reports, publications, website, video channel etc., using the same terms as you used in the study information sheet.

I understand that personal information collected about me that can identify me, such as my name or where I live, will not be shared beyond the study team. ☐

Under some circumstances, access to this information should be restricted to the researcher only.

I consent to the processing of my personal information for the purposes of this research study. I understand that such information will be treated as strictly confidential and handled in accordance with current UK Data Protection legislation. ☐

I agree that my information can be quoted in research outputs. ☐

I agree that my real name can be used for quotes. ☐

I agree to joint copyright the written information I provide, such as interview responses or additional written data, for use in the research study of **Abhishek Kudiri**. ☐

3. Future use and reuse of the information by others

I give permission for the interview responses and related data that I provide to be used for future research and learning purposes. ☐

Specify in which form the data will be stored, e.g. de-identified (anonymised) transcripts, audio recording, survey database, etc.. If needed, repeat the statement for each form of data you plan to store.

Specify whether stored data will be de-identified (anonymised), and how. Make sure to describe this in detail in the information sheet.

4. Signatures

Rohith Chaudary	Rohit	17-12-2024
Name of participant	Signature	Date

Syed Mubin Husain	Syed Mubin Husain	16-12-2024
Name of participant	Signature	Date

For participants unable to sign their name, mark the box instead of signing ☐

I have witnessed the accurate reading of the consent form with the potential participant and the individual has had the opportunity to ask questions. I confirm that the individual has given consent freely.

_____	_____	_____
Name of witness [IN CAPITALS]	Signature	Date

I have accurately read out the information sheet to the potential participant and, to the best of my ability, ensured that the participant understands to what they are freely consenting.

Abhishek Kudiri	Abhishek	14-12-2024
Name of researcher	Signature	Date

5. Study contact details for further information

Abhishek Kudiri, +44 7823765814, kudiriabhishek1998@gmail.com

One copy to be kept by the participant, one to be kept by the researcher

Other Appendixes (D, E, F etc. as required) (Unlimited Words):