**EVALUATING THE EFFECTIVENESS OF ZERO TRUST ARCHITECTURES IN HYBRID WORK ENVIRONMENTS**

Manikanta Puttoj

23249889

Programme Code – Research in Computing CA1

# National College of Ireland

# 1. Abstract

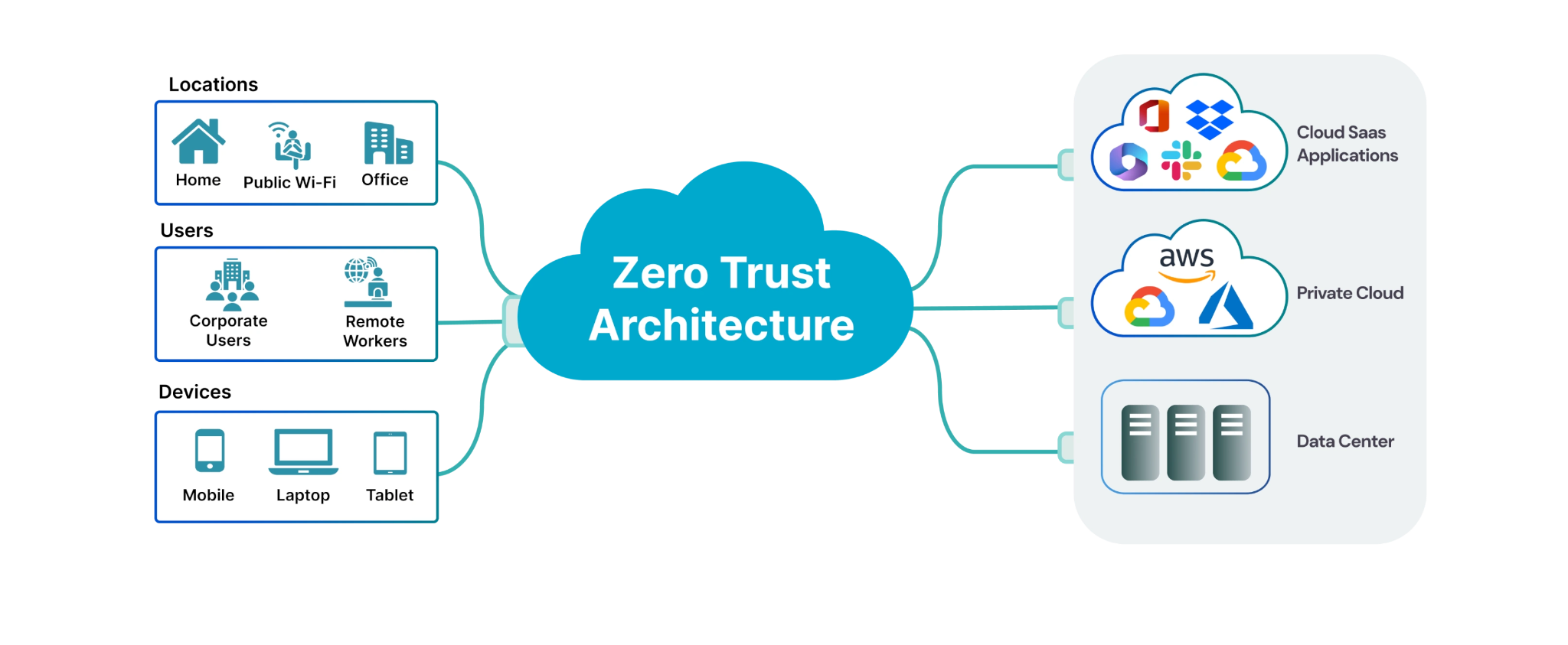
This research explores the effectiveness of Zero Trust Architecture (ZTA) in securing hybrid work environments. Where employees access corporate resources from both remote and on-site locations. Traditional perimeter-based security models have proven insufficient in addressing modern cybersecurity challenges. The challenges include lateral movement, insider threats, and device diversity. ZTA, guided by the principle of “never trust, always verify,” offers a dynamic, identity-centric approach to mitigate these risks. Despite its growing adoption, there is a notable lack of empirical evidence. It has been demonstrating ZTA’s impact in practical hybrid deployments, particularly regarding user experience and operational efficiency. This study proposes the development of a simulated hybrid test environment to implement. It also evaluates core ZTA components such as identity verification. This also implies device posture checks and continuous monitoring. Using Python for simulation and analysis, the research aims to provide quantifiable insights into security improvements and usability outcomes. This has also offered valuable guidance for future organizational ZTA implementations.

# Keywords: Zero Trust Architecture, Hybrid Work, Cybersecurity, User Experience, Identity Verification.

# 1. Introduction

## 1.1 Background and Research Problem

The trend of hybrid workplaces, where workers switch between remote and office-based working, has completely changed how organizations run and protect networks. This model has also come with a lot of challenges especially how to provide secure access to a distributed workforce, diversity of devices and network conditions. Perimeter-based security models that is based on the assumption that everything within a corporate network is trusted has become more and more ineffective. To address such shortcomings, the Zero Trust Architecture (ZTA) is an upcoming cybersecurity framework in response. In contrast to perimeter-based models, a guiding principle of ZTA is defined as never trust and always verify (Paul *et al.,* 2024). These foundational modules that include micro-segmentation, identity and access management, device posture checks, and real-time monitoring help minimize the attack surface and enhance threat containment. As organizations shift to the hybrid model, using ZTA offers an essential additional benefit of not only improving security but keeping access control in line with the emerging realities of operations (Paredes and Restrepo, 2025). This study examines how ZTA is to be used and how effective it is in hybrid settings, trying to keep a balance between security and user experience.



**Figure 1: Zero Trust Architecture (ZTA)**

(Source: Mateen, 2024)

## 1.2 Research Question

* How can Zero Trust Architectures be effectively implemented and evaluated to enhance security in hybrid work environments, while balancing user experience and operational efficiency?

## 1.3 Significance and Rationale

The Zero Trust Architecture (ZTA) is becoming increasingly relevant in the real world because organizations are facing complex security challenges in hybrid work environments (Ahmadi, 2024). Although cybersecurity standards like NIST recommend ZTA, there is a dearth of empirical, direct research on how well it performs in real-world deployments. The current literature concentrates on theoretical advantages but not on quantifiable results. The effect of ZTA on user experience and working processes is commonly not taken into consideration. The research on these facets is critical because effective deployment needs to raise high levels of security and restricted interruption of productivity and user contentment without compromising effectiveness in dealing with technical efficiency and adoption by the organization. This research will give quantifiable information to enable the stakeholders to rationalize between the technical advantages and the trade-off wherein the adoption of ZTA will be more evidence-based and with the user in mind.

## 1.4 Contributions and Benefits

The research project will furnish immense contributions to an emerging area of cybersecurity with a metrics-based analysis of Zero Trust Architecture (ZTA) in hybrid working atmospheres. It tries to categorize the gap between the theoretical framework and practical implementation issues. This project will provide the actionable success metrics in the form of security incidents and regular user interactions simulated by building a testbed model, which can then be utilized by the firm as criteria to measure the effectiveness of its ZTA (Taskin, 2025). These are measurable gains in resistance to breaches, robust authentication, and preventive impacts to lateral pushing. Moreover, the project focuses on user experience, which is one of the unattended aspects in ZTA deployment. This study will find such friction points by examining the results of usability testing and user feedback analysis, which may lead to decreased productivity or root dissatisfaction. The other major advantage is the ability to give attention to organization-readiness factors, including the suitability of existing infrastructure, digital literacy of the employees, and policy.

## 1.5 Document Structure



**Figure 2: Document Structure**

(Source: self-created)

# 2. Literature Review

## 2.1 Evolution of Enterprise Security Models

According to Zohaib et al. (2024) historically, enterprises focused heavily on perimeter models of security, sometimes termed a ‘castle-and-moat strategy’ of security. These models presupposed the existence of threats lying outside the network and the trustworthiness of internal systems as trustworthy. With cloud computing and remote work, such models are increasingly becoming obsolete, especially with the introduction of mobile devices. New threats are internal threats, compromised credentials, and lateral movement on the networks.

At the same time, Zero Trust Architecture (ZTA) rejects the notion of inherent trust. It needs authorization of all users, devices, and transactions irrespective of location in the network. This change makes it possible to have finer control and fit more into the contemporary dynamics of work in an organization. The dynamicity and decentralization of environments favor the principles incorporated by ZTA of least privilege, continuous validation, and micro-segmentation.

## 2.2 Principles and Frameworks of Zero Trust

The title of the public action agreed upon by NIST Special Publication 800-207 does a good job of defining the essential basis of Zero Trust, formalizing seven principles, among which we find continuous authentication and policy enforcement along with real-time access decisions. Micro-segmentation, which is one such action, consists of dividing a network into distinct compartments.

According to Syed et al. (2022), Identity and Access Management (IAM) is the pinnacle of ZTA. Desirable authentication options that encompass biometrics, multi-factor authentication (MFA), and context-based identity authentication are needed. In the same way, device posture validation makes sure that violating devices that are insecure are denied access. The level of protection gets even stronger with endpoint detection and response (EDR) integration. All these components are forces that are tactfully coordinated to create a security model that is dynamic to the behavior of users, anomalies faced by the system, and the dynamic threat.

## 2.3 ZTA in Hybrid Work Environments

ZTA is a rational solution to secure assets on various access points as organizations shift towards a hybrid working model. According to Alotaibi *et al.* (2025), about three-quarters of the enterprises intended to invest more in ZTA in reaction to the complexities of hybrid work. Similarly, Prowell et al. (2021) predict that by the year 2026, two-thirds of businesses will eliminate the classic VPNs in favor of identity-based ZTA.

As noted by George (2024), the more important location-agnostic policies that are based on identity as well as context rather than IP or device location are required. Even in hybrid configurations, the problem with policy enforcement is that the employees work over insecure networks and on personal devices and in cloud-based applications.

The decoupling of the decision of access by ZTA is a possible direction forward but also highly dependent on a coordinated combination of tools and user training along with constant monitoring.

## 2.4 Challenges in Implementation

According to Rebouças Filho (2025), nonetheless, the implementation of ZTA has significant impediments regardless of its benefits. To begin with, legacy infrastructure and old applications usually cannot work well with new IAM or segmentation tools. Second, its initial configuration will be quite demanding with regard to architectural redesign, and it can be a heavy burden on the IT teams. There is another issue of usability. The reauthentication and the security dialogues can become very annoying to the users, which could reduce productivity and increase resistance. Moreover, the transitions may be impeded or halted by organizational slag and ambiguous leadership requirements. The lack of skilled staff is also one of the factors that hinder complete or perfect implementations. The significance of organizational preparedness, change management and phasing the deployment programs are highlighted by these challenges.

## 2.5 Security vs. Usability Trade-Off

According to Abbas and Ali (2024), the conflict between strong security and smooth user experience is another significant ZTA theme in the current research. Continuous monitoring systems are constantly intended to assess identity and device posture, and high-assurance systems can have latency and lower user satisfaction. On the other hand, usability-first design, meant to minimize authentication, also has the potential to lower security.

There are indications in recent literature that adaptive authentication, through which a check may be stricter based on the risk context, could provide a trade-off. Also, to limit the disturbance, the user-centered design principles can be employed, including the employment of behavioral biometrics and background validation.

## 2.6 Research Gap and Niche

Although the literature included with ZTA principles and theoretical benefits is robust, the studies measuring the effectiveness of ZTA in the hybrid work setting are absent. The existing body of research is based on simulation or unrealistic case studies that can be applied in only a few cases (Syed *et al*., 2022). Further, the cross-section between technical performance and user experience is touched upon by a few works. This project aims to fulfill that gap by evangelizing a measurable assessment of ZTA in an impure work testbed. It opens with cross-stitching security measures (e.g., resistance to breach simulation) with usability statistics (e.g., completion of a task, satisfaction scores).

This research will help to bring dedication to both the technical and real-world parts and add a holistic picture to the academic and practice-oriented understanding of the Zero Trust implementation.

# 3. Research Method and Specification

## 3.1 Proposed Solution

The effectiveness of Zero Trust Architectures (ZTA) in hybrid work environments, a simulated testbed environment will be developed. This environment will emulate a small to medium-sized organization operating under a hybrid work model, consisting of both remote and in-office users accessing corporate resources through various devices and networks (Paredes and Restrepo, 2025). The testbed will simulate real-world hybrid conditions to ensure the study remains practically applicable. The Zero Trust framework will be deployed using conceptual components, which include Identity verification through login protocols and role-based access control (RBAC), Device posture validation by simulating compliant and non-compliant endpoints, Micro-segmentation through access control policies across applications, and Centralized logging and monitoring to trace user behavior and detect anomalies. The performance of this security framework will then be measured through defined security metrics and usability indicators to assess its operational feasibility and impact.

## 3.2 Research Activities or Project Plan

The project will be carried out in sequential phases over 10 weeks, following a structured plan. Each activity is essential in addressing the research question through qualitative analysis and primary research because Tools like Python support statistical analysis, which is a core component of quantitative research.

|  |  |
| --- | --- |
| **Activity** | **Description** |
| Baseline Vulnerability Assessment | Identify security gaps in the hybrid environment. |
| ZTA Controls Deployment | Deploy identity, segmentation, posture checks, and logging. |
| Data Collection | Gather data on breaches, authentication, and device behavior. |
| Usability Testing | Simulate tasks; record completion rates and times. |
| Data Analysis | Analyze metrics using Python. |
| Feedback Evaluation | Assess usability feedback thematically. |
| Comparison and Evaluation | Compare outcomes against baseline data. |
| Reporting Challenges | Document issues and adoption readiness. |
| Final Review | Compile and finalize project findings. |

**Gantt Chart with Weekly Tasks and Milestones**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Activity** | **Week 1** | **Week 2** | **Week 3** | **Week 4** | **Week 5** | **Week 6** | **Week 7** | **Week 8** | **Week 9** | **Week 10** |
| Project setup and literature alignment |  |  |  |  |  |  |  |  |  |  |
| Environment simulation and vulnerability scan |  |  |  |  |  |  |  |  |  |  |
| ZTA deployment- identity verification |  |  |  |  |  |  |  |  |  |  |
| ZTA deployment- device posture & logging |  |  |  |  |  |  |  |  |  |  |
| Breach simulation & data collection |  |  |  |  |  |  |  |  |  |  |
| Usability testing with simulated users |  |  |  |  |  |  |  |  |  |  |
| Data analysis- Python |  |  |  |  |  |  |  |  |  |  |
| Qualitative feedback analysis via NVivo |  |  |  |  |  |  |  |  |  |  |
| Evaluation & comparison with baseline |  |  |  |  |  |  |  |  |  |  |
| Documentation and final reporting |  |  |  |  |  |  |  |  |  |  |

The Gantt chart visualizes a project with a neat schedule. There have been initial activities that have been accomplished such as the setup and simulation of the environment, which signify desirable progress. Nevertheless, the sloppiness in ZTA setup and breakage simulation hints at risk points. Future work is scheduled, and such critical stages as analysis and reporting are still to be done within the planned schedule. It is advisable to monitor actively. Blue is Completed, yellow is Planned, and Red is the task that is Delayed.

## 3.3 Tools and Test Data

Python will be used as the core simulation and analysis tool in the research. Hybrid work scenarios will be simulated in Python with multiple user roles, access patterns, and authentication events (Souza *et al.,* 2023). It will also facilitate the parsing and analysis of the log-based systems like the success rate of log-ins, hacking attempts and policy execution. With libraries like pandas, matplotlib, and scipy, Python enables efficient data processing, statistical comparison, and visual representation of results. Its flexibility allows for automation of tasks, reproducibility of experiments, and ethical testing using synthetic data. It has made it ideal for this cybersecurity-focused study.

## 3.4 Evaluation Plan

The evaluation of the Zero Trust model will focus on both security effectiveness and user experience. Security metrics will include a reduction in attack surface through pre- and post-deployment vulnerability scans. It includes authentication success/failure rates and outcomes of simulated breach attempts. Usability will be assessed via task completion rates, system latency during resource access. This has subjective user satisfaction using the System Usability Scale (SUS) (Vlachogianni and Tselios, 2022). These combined metrics will offer a balanced assessment of ZTA’s performance in a hybrid work environment.

## 3.5 Ethical Considerations

This study will adhere to strict ethical standards to ensure the protection of all stakeholders and maintain research integrity (Roje *et al.,* 2023). No real personal or sensitive data will be collected or processed at any stage. All testing will be conducted using simulated user accounts and virtual environments to avoid privacy risks. Monitoring activities will be confined to evaluating system performance and simulated interactions only. The research will fully comply with GDPR, with NCI’s ethical guidelines and informed consent requirements wherever applicable.

# References

Abbas, S.M. and Ali, M., 2024. User-Centric Analysis Of Zero Trust security: Evaluating Impact And Adoption.

Ahmadi, S., 2024. Zero trust architecture in cloud networks: Application, challenges and future opportunities. Ahmadi, S.(2024). Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. Journal of Engineering Research and Reports, 26(2), pp.215-228.

Alotaibi, A., Aldawghan, H. and Aljughaiman, A., 2025. A review of the authentication techniques for internet of things devices in smart cities: opportunities, challenges, and future directions. Sensors, 25(6), p.1649.

George, A.S., 2024. Assessing the strategic merits of sd-lan adoption across complex enterprises. Partners Universal International Research Journal, 3(3), pp.61-84.

Mateen (2024). Zero Trust Architecture: Protect Your Business Inside Out. [online] Miniorange.com. Available at: <https://www.miniorange.com/blog/what-is-zero-trust-architecture/>.

Paredes, E.C. and Restrepo, L.F., 2025. An In-Depth Analysis of Zero Trust Architectures in Hybrid Work Environments: Security, Scalability, and Policy Implications. Quarterly Journal of Emerging Scientific Trends and Technologies, 15(5), pp.15-27.

Paredes, E.C. and Restrepo, L.F., 2025. An In-Depth Analysis of Zero Trust Architectures in Hybrid Work Environments: Security, Scalability, and Policy Implications. Quarterly Journal of Emerging Scientific Trends and Technologies, 15(5), pp.15-27.

Paul, E.M., Mmaduekwe, U., Kessie, J.D. and Dolapo, M., 2024. Zero trust architecture and AI: A synergistic approach to next-generation cybersecurity frameworks. International Journal of Science and Research Archive, 13(2), pp.4159-4169.

Prowell, S., Manz, D., Culhane, C., Ghafoor, S., Kalke, M., Keahey, K., Matarazzo, C., Oehmen, C., Peisert, S. and Pinar, A., 2021. Position Papers for the ASCR Workshop on Cybersecurity and Privacy for Scientific Computing Ecosystems. US Department of Energy (USDOE), Washington DC (United States). Office of Science.

Rebouças Filho, W.L., 2025. The Role of Zero Trust Architecture in Modern Cybersecurity: Integration with IAM and Emerging Technologies. Brazilian Journal of Development, 11(1), pp.e76836-e76836.

Roje, R., Tomić, V., Buljan, I. and Marušić, A., 2023. Development and implementation of research integrity guidance documents: Explorative interviews with research integrity experts. Accountability in Research, 30(6), pp.293-330.

Souza, P.S., Ferreto, T. and Calheiros, R.N., 2023. EdgeSimPy: Python-based modeling and simulation of edge computing resource management policies. Future Generation Computer Systems, 148, pp.446-459.

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

Taskin, E., 2025. The Transitioning from Individual Implementation of Zero Trust Architecture to AI-driven Tools: Reducing Manual Workloads and Increasing Efficiency through AI in ZTA.

Vlachogianni, P. and Tselios, N., 2022. Perceived usability evaluation of educational technology using the System Usability Scale (SUS): A systematic review. Journal of Research on Technology in Education, 54(3), pp.392-409.

Zohaib, S.M., Sajjad, S.M., Iqbal, Z., Yousaf, M., Haseeb, M. and Muhammad, Z., 2024. Zero trust vpn (zt-vpn): A systematic literature review and cybersecurity framework for hybrid and remote work. Information, 15(11), p.734.