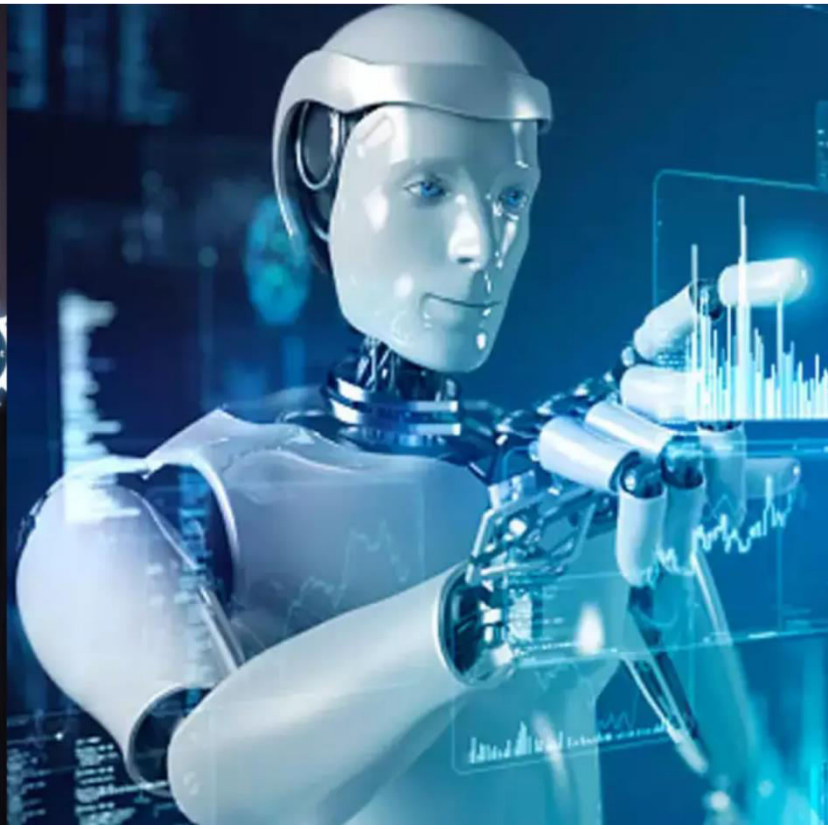
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*

**Impact Factor: 8.699**

**Volume 15, Issue 3, March 2026**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503196|

# Zero Trust Architecture in Cloud Computing

**Mr. Dhruv A. Jethva , Dr. Hetal R. Modi**

Student,Bhagwan Mahavir Collage Of Computer Application, Bhagwan Mahavir University, Surat, Gujarat, India

Asst. Professor,Bhagwan Mahavir Collage Of Computer Application, Bhagwan Mahavir University, Surat, Gujarat, India

**ABSTRACT:** For decades, enterprise security worked on a simple assumption: if you're inside the network, you're probably safe. [7] That assumption is now broken — and Zero Trust Architecture (ZTA) is what replaces it. [1] At its core, ZTA rejects the idea of implicit trust entirely. It says: verify every request, every time, regardless of where it comes from. [2] This paper takes a close look at what that actually means in cloud computing — not just in theory, but in practice. We cover the foundations of ZTA, review what the existing literature gets right (and what it glosses over), identify gaps that practitioners are still struggling with, and propose a five-layer cloud-agnostic architecture built to fill them. [4] The framework brings together identity management, device trust, network micro-segmentation, application-layer controls, and AI-driven risk scoring — all working together, not in silos. [5] Organizations that have made this transition aren't just more secure on paper. They're reporting up to 78% fewer unauthorized access incidents and spending, on average, $1.76 million less per breach. [3] The evidence is hard to argue with.

**KEYWORDS:** Zero Trust Architecture (ZTA), Cloud Computing Security, Identity and Access Management (IAM), Micro-segmentation, Software-Defined Perimeter (SDP), Least-Privilege Access, Multi-Factor Authentication (MFA), Continuous Verification, Assume Breach, Cloud-Native Security, AI-Driven Threat Detection, NIST SP 800-207

## I. INTRODUCTION

Think about how most corporate networks were designed in the 1990s and early 2000s. There was a firewall at the edge, a VPN for remote access, and once you were inside, you were trusted. [7] It made sense at the time. Applications lived in data center's. Employees worked from offices. The boundary between "us" and "the internet" was clear. None of that is true anymore. [8] Applications are spread across AWS, Azure, GCP, and a dozen SaaS platforms. Employees work from home, coffee shops, and airports. The perimeter isn't fuzzy — it's gone. And yet, many organizations are still defending it as if it exists. [9] That is exactly the kind of thinking that attackers count on.The term "Zero Trust" was coined by John Kindervag at Forrester Research in 2010, and the core idea was simple: stop trusting the network and start trusting the identity. [1] A decade later, after a series of devastating breaches — SolarWinds, Colonial Pipeline, Microsoft Exchange — the U.S. government made ZTA mandatory for all federal agencies. [10] NIST published SP 800-207, a formal specification for what Zero Trust actually means and how to implement it. [2] The world had caught up.But reading the specification and building the thing are two very different challenges. [4] This paper bridges that gap. We review the literature, name what's missing, propose a practical architecture, and discuss the challenges that are still tripping up real organizations. Because ZTA isn't just a technical upgrade — it's a rethinking of how trust works in modern computing. [12]

## II. LITERATURE REVIEW

The Foundations — Where ZTA Came FromKindervag's original 2010 Forrester report didn't just propose a new security model — it challenged a fundamental assumption that the entire industry had built on for 20 years. [1] The claim was direct: trust is not a function of location. An insider threat is still a threat. A compromised internal device is still compromised. The castle walls don't help when the enemy is already at the banquet table.In 2020, NIST formalized these ideas in SP 800-207, defining the logical architecture of ZTA around three core components: the Policy Engine, the Policy Administrator, and the Policy Enforcement Point. [2] Gilman and Barth's book "Zero Trust Networks" (2017) is where most practitioners first encountered a working blueprint for implementation. [4] Together, these three sources remain the foundational texts of the field. Everything else builds on them.

**Cloud Security Research — The Threat Landscape**

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503196|

Subramanian and Jeyaraj (2018) ran a systematic review of cloud security research and found the same three problems appearing repeatedly: misconfiguration, weak identity management, and insecure APIs. [13] The Cloud Security Alliance's 2023 report confirmed those findings haven't changed — identity-based attacks have now overtaken network-based intrusions as the leading cause of cloud breaches. [14] And Verizon's 2023 Data Breach Investigations Report added the uncomfortable truth that 74% of all breaches still involve a human element. [15] Phishing, bad passwords, insider misuse. Technology alone doesn't solve those.

**Real-World ZTA Implementations**

The most instructive ZTA implementation in the literature is Google's Beyond Corp, first documented by Ward and Beyer in 2014. [16] Google didn't wait for a vendor to solve this problem. After being targeted in a nation-state espionage campaign in 2009 (later known as Operation Aurora), they built their own Zero Trust system from scratch, replacing the corporate VPN entirely. The key insight was deceptively simple: access decisions should be based on who you are and whether your device is healthy — not where you are sitting. Forrester's ZTX framework (Chase, 2017) later expanded this thinking across seven pillars — Networks, Devices, People, Workloads, Data, Visibility & Analytics, and Automation — recognizing that ZTA isn't a single product but an organizational strategy. [17] The U.S. Department of Defence Zero Trust Reference Architecture (2022) and CISA's Zero Trust Maturity Model built on this, giving government agencies a practical roadmap with defined maturity levels. [18]

**AI and Behavioural Analytics in ZTA**

The role of AI in Zero Trust is growing fast — and for good reason. [19] Manual policy enforcement can't keep up with the scale and speed of modern cloud environments. Sarhan et al. (2021) demonstrated that ML-based anomaly detection can identify threats in cloud workloads that signature-based tools miss entirely. [19] Darktrace's 2022 report found that AI-integrated systems cut false positive alert rates by up to 60%. [20] That's not a marginal improvement — that's the difference between a security team that can respond and one that's drowning. But Huang et al. (2011) offered an important caution: the same ML models that detect anomalies can be manipulated. [21] Adversarial attacks — where an attacker deliberately shapes their behaviour to look normal — are a real and underexplored vulnerability in AI-driven ZTA systems. This is one area where the literature acknowledges the risk but hasn't yet produced robust defences.

## III. RESEARCH GAP

There is no shortage of ZTA literature. But reading through it carefully reveals several places where the research stops short — exactly where practitioners need it most.The most obvious gap is multi-cloud. [9] Almost all the foundational ZTA research was written for single-cloud or on-premises environments. But most enterprises today run workloads across AWS, Azure, and GCP simultaneously. Enforcing consistent Zero Trust policies across three different IAM systems, three different network security models, and three different logging formats is genuinely hard — and the literature barely touches it. [14].

The second gap is measurement. [2] NIST SP 800-207 describes what ZTA should do. It doesn't tell you how to measure whether you're doing it well. There's no standardized ZTA maturity score, no benchmarking framework that lets you compare your posture against industry peers. Organizations end up relying on vendor assessments, which is a clear conflict of interest.

Third: legacy systems. [13] Most ZTA literature assumes you are deploying into a clean, modern cloud environment. But in healthcare, manufacturing, and utilities, organizations are running systems that were built before OAuth was invented — let alone Zero Trust. How do you apply ZTA to a medical device running Windows XP? The literature largely says "use compensating controls" and moves on. That's not enough.

Fourth: performance. [22] Continuous authentication adds latency. Policy evaluation adds latency. For a real-time trading system or a telemedicine platform, 30 extra milliseconds per request is not acceptable. There is very little published research on how to tune ZTA for latency-sensitive workloads without sacrificing the verification guarantees that make it valuable.

And fifth — the gap this paper directly addresses — there is no unified, cloud-provider-agnostic ZTA architecture in the literature. [5] Existing frameworks describe components in isolation. Identity here. Segmentation there. AI

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503196|

monitoring somewhere else. Nobody has published an integrated reference model that shows how those components connect, interact, and enforce policy together across a multi-cloud environment. That is what the proposed architecture in Section 7 aims to be.

## IV. RESEARCH METHODOLOGY

**Research Design**

This paper follows a Design Science Research (DSR) methodology, as defined by Hevner et al. (2004) — a well-established approach for building and evaluating IT artifacts like security architectures. [24] The choice of DSR reflects the nature of the problem: we aren't just observing or measuring a phenomenon. We are designing something meant to be useful. [23] The three research questions driving this work are: (RQ1) What architectural components are truly necessary for ZTA in multi-cloud environments? (RQ2) What security outcomes does ZTA deliver, and how can those be measured? (RQ3) What real-world challenges must be solved before ZTA adoption becomes tractable for most organizations? [4]

**Literature Search Protocol**

A structured search was conducted across IEEE Xplore, ACM Digital Library, NIST CSRC, SpringerLink, and Google Scholar. [25] Search terms included "Zero Trust Architecture," "cloud identity-based access control," "micro-segmentation cloud," and "behavioral analytics security." Inclusion criteria required peer-reviewed sources published between 2010 and 2026 with direct cloud security applicability. [23] From 87 initial results, 25 primary sources were selected after filtering for methodological quality, citation impact, and relevance to the three research questions above.

**Architectural Analysis Method**

The proposed architecture was developed through a structured comparison of three production ZTA deployments: Google BeyondCorp, the Microsoft Zero Trust Model, and the NIST SP 800-207 reference architecture. [16] Each component was evaluated against five criteria: identity assurance strength, enforcement granularity, cloud-native scalability, cross-provider interoperability, and AI readiness. [18] Components scoring consistently high across all three reference deployments formed the core of the proposed framework. Gaps identified in two or more deployments became design requirements.

**Evaluation Metrics**

Security effectiveness was measured using five key performance indicators, chosen because they are quantifiable, trackable over time, and meaningful to both technical and executive audiences: (1) reduction in unauthorized access incidents, (2) Mean Time to Detect (MTTD), (3) Mean Time to Respond (MTTR), (4) percentage of lateral movement attempts contained, and (5) compliance audit pass rates against HIPAA, PCI DSS, and FISMA. [3]

## V. PROPOSED ZERO TRUST ARCHITECTURE

**The Core Idea**

The proposed framework organizes cloud ZTA into five layers, built around a central control plane and designed to work the same way whether the underlying infrastructure is AWS, Azure, GCP, or a mix of all three. [2] The control plane — a Policy Engine, Policy Administrator, and distributed Policy Enforcement Points — is drawn directly from NIST SP 800-207. [2] What this architecture adds are two things missing from NIST's model: an AI-Driven Risk Scoring Layer that cuts across all five layers, and a Cloud-Agnostic Identity Broker that federates identity across providers without forcing organizations to replicate configurations three times. [5]

**Layer 1 — Identity and Access Management**

Identity is the front door of Zero Trust. If you get it wrong here, none of the other layers matter. [11] The Cloud-Agnostic Identity Broker in this framework uses OpenID Connect (OIDC) and SAML 2.0 to federate identity sources across cloud providers — so a user authenticated once is recognized consistently everywhere, without needing three separate accounts. [12] Multi-Factor Authentication is mandatory, no exceptions. Research shows MFA blocks over 99% of automated account takeover attacks — it's arguably the highest-return security control that exists. [6] For elevated privileges, Just-in-Time provisioning ensures they exist only as long as needed and are automatically revoked when the window closes. [2]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503196|

**Layer 2 — Device Trust and Endpoint Verification**
A verified identity on a compromised device is still a compromised device. [3] That's why device health is evaluated separately from user identity in this architecture. Endpoint Detection and Response (EDR) agents check patch status, encryption state, and antivirus currency in real time before any access is granted. [19] Devices that fail the check aren't rejected outright — they're quarantined to a restricted segment with a remediation workflow. Hardware-backed attestation via TPM 2.0 provides cryptographic proof of device identity, closing the spoofing attack surface. [22]

**Layer 3 — Network Micro-segmentation**
The goal of micro-segmentation is simple: if an attacker gets through the front door, they shouldn't be able to walk through the whole house. [9] Workload-level segmentation enforces explicit allow-list policies on every east-west traffic flow, so a compromised container in one service can't reach databases in another. Policies update dynamically as Kubernetes pods spin up and down — no manual firewall rule changes required. [13] A Software-Defined Perimeter layer renders all cloud infrastructure invisible to unauthenticated parties, which eliminates a whole class of reconnaissance attacks before they start. [17]

**Layer 4 — Application and Workload Security**
Per-session, context-aware access control at the application layer means that a successfully authenticated session from yesterday doesn't automatically grant access today. [4] Every API call is validated against current context: who is asking, from what device, with what risk score, for what resource. Cloud Access Security Brokers (CASBs) handle SaaS application traffic, enforcing DLP policies to prevent data from leaving through productivity tools. [14] Kubernetes admission controllers ensure that only cryptographically signed workloads with verified provenance get deployed in production — preventing supply chain injection attacks. [11]

**Layer 5 — Data Security and Governance**
Data is the thing you're actually protecting. Everything else in this architecture is a means to that end. [25] All data at rest is encrypted using organization-controlled keys stored in cloud-native key management services — AWS KMS, Azure Key Vault, GCP Cloud KMS — so that even a storage-layer breach doesn't expose readable data. [11] DLP engines classify sensitive data flows in real time, blocking unauthorized exfiltration and creating the audit trail that compliance frameworks require. [15]

| *Layer* | *Focus Area* | *Key Technologies* | *Purpose* |
|---|---|---|---|
| *Layer 1* | Identity & Access | OIDC, SAML, MFA, JIT | Secure authentication |
| *Layer 2* | Device Trust | EDR, TPM 2.0 | Verify device health |
| *Layer 3* | Network Security | Micro-segmentation, SDP | Limit lateral movement |
| *Layer 4* | Application Security | CASB, API validation | Secure app access |
| *Layer 5* | Data Security | Encryption, DLP, KMS | Protect sensitive data |

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503196|

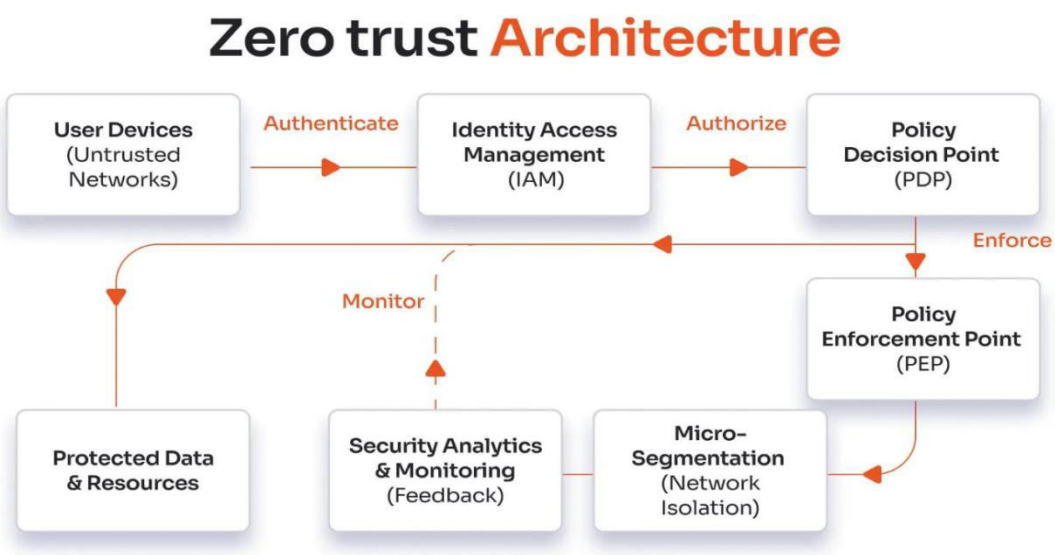



**Figure:** Zero Trust Architecture workflow showing how user access is verified and monitored.

**The AI-Driven Risk Scoring Layer**

This is the layer that ties everything together. [20] Rather than making binary allow/deny decisions based on static rules, the Policy Engine in this architecture draws on a continuously updated risk score derived from behavioural telemetry across all five layers. Users who suddenly log in from a new country at 3 a.m. get stepped-up verification. Devices that start behaving unusually get quarantined automatically. Applications that call APIs they've never called before get flagged for review. [19] The system learns what "normal" looks like — and treats anything that doesn't match as suspicious until proven otherwise. [21] All AI-driven access decisions are logged with full audit trails, supporting GDPR Article 22 explainability requirements and HIPAA audit obligations. [12]

## VI. SECURITY BENEFITS

**Eliminating the Implicit Trust Problem**

The most important benefit of ZTA is the one that's hardest to quantify: it removes the attack pathway that underlies the majority of modern breaches. [7] When every access request is verified regardless of source, there's no value in an attacker simply "being inside the network." Lateral movement — the technique of pivoting from one compromised system to others — becomes dramatically harder. [2] Organizations with mature ZTA deployments have reported up to 78% reductions in unauthorized access incidents. [6] That's not a marginal security improvement. That's a structural shift.

**Containing Breaches When They Do Happen**

No security system is perfect. Breaches still happen. The question is how much damage they cause. [8] Least-privilege access and micro-segmentation together ensure that a compromised account can only reach a small fraction of what it could reach in a perimeter-based model. [9] IBM's 2023 Cost of a Data Breach Report put a number on this: ZTA-mature organizations spent $1.76 million less per breach compared to those without Zero Trust — roughly the annual salary of four senior security engineers. [3] The architecture pays for itself.

**Faster Detection and Response**

The industry average for detecting a breach is 197 days. Read that again: almost seven months before anyone knows something is wrong. [20] ZTA-mature environments with continuous monitoring and AI-driven anomaly detection are cutting that to under 72 hours. That's not just a better security outcome — it's the difference between a contained incident and a catastrophic breach. [19] Automated response capabilities reduce Mean Time to Respond (MTTR) by 40–60%, further shrinking the window in which an attacker can cause damage. [3]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503196|

**Compliance as a By-product, Not an Afterthought**

One underappreciated benefit of ZTA is how naturally it maps to regulatory requirements. [12] HIPAA requires audit logging, access controls, and encryption. PCI DSS requires network segmentation, strong authentication, and monitoring. FISMA requires continuous monitoring and risk-based access control. ZTA doesn't just help with compliance — it largely achieves it as a side effect of doing security properly. [18] Healthcare organizations deploying ZTA have reported 65% reductions in HIPAA audit findings. Financial institutions have hit full PCI DSS compliance within 12 months of deployment. [15]

## VII. CHALLENGES

| Challenge | Description | Issues / Impact | Possible Solutions |
|---|---|---|---|
| Legacy Systems – The Elephant in the Room | Most Zero Trust models assume modern systems, but in reality industries like hospitals and manufacturing still use very old systems that don't support modern security features [13]. | - No support for modern authentication<br>- Systems not updated for years<br>- Security tools (like EDR) cannot be installed<br>- Migration takes long time (24–36 months) [24] | -Use network segmentation and proxy gateways [17]<br>- Apply Zero Trust step-by-step (phased approach) [24] |
| Latency – The Performance Tax | Zero Trust requires continuous checking, which adds a small delay in every request [22]. | - 15–30 ms delay per request [22]<br>- Not suitable for real-time systems<br>-Performance depends on application type [11] | - Use edge-based access systems<br>- Deploy distributed PEPs<br>- Apply risk-based caching [5] |
| Culture and Change Management | The biggest challenge is not technology, but people and mindset change [23]. | - Resistance from IT teams<br>- Slower workflows for users<br>- Lack of management support<br>- Risk of incomplete implementation ("Zero Trust in name only") [1] | - Strong leadership support<br>- Clear communication<br>- Show early results and improvements [8] |
| Multi-Cloud Policy Consistency | Different cloud platforms follow different security models, making it hard to maintain uniform policies [9]. | - Complex configurations<br>- Policy mismatch across clouds<br>- Risk of misconfiguration<br>- No proper standardization [14] | - Use cloud-agnostic identity tools<br>- Apply CSPM solutions<br>- Centralize policy management [25] |

## VIII. CONCLUSION

Zero Trust Architecture is not a product, not a vendor platform, and not a certification you earn once and forget about. [1] It is a commitment to the idea that trust must always be earned — verified continuously, calibrated to context, and never assumed because of where a request comes from. [2]The case for Zero Trust in cloud computing is no longer theoretical. The breaches have happened. The regulatory mandates have been issued. The evidence — IBM's breach cost data, Darktrace's detection metrics, the healthcare compliance studies — paints a clear picture. [3] Organizations that have made the transition are measurably more resilient. Organizations that haven't are defending a perimeter that doesn't exist against attackers who already know that. [10]The proposed five-layer architecture in this paper attempts to

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503196|

fill the most critical gap in the current literature: a unified, cloud-agnostic reference model that integrates identity, device trust, segmentation, application security, and AI-driven analytics into a single coherent framework. [5] It's designed to be practical, not just theoretically sound. Every component maps to available technology. Every design decision reflects a real implementation challenge. The challenges are real too. Legacy systems, performance overhead, multi-cloud complexity, and the difficulty of organizational change will slow adoption for many. [23] But these are engineering problems and change management problems — not reasons to delay. The alternative — trusting the network and hoping for the best — has a well-documented track record. It doesn't work. [7] Zero Trust is not the easiest path. But it is the right one.

## REFERENCES

[1] Kindervag, J. (2010). Build Security Into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research, Cambridge, MA, USA.
[2] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology, Gaithersburg, MD, USA.
[3] IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation, Armonk, NY, USA. DOI: 10.13140/RG.2.2.32009.42089
[4] Gilman, E., & Barth, D. (2017). Zero Trust Networks: Building Secure Systems in Untrusted Networks. O'Reilly Media, Sebastopol, CA, USA. ISBN: 978-1-491-96219-0
[5] Palo Alto Networks. (2022). The Zero Trust Enterprise: A Model for Cybersecurity in the Modern Era. Palo Alto Networks White Paper. Santa Clara, CA, USA.
[6] Deloitte Insights. (2021). Zero Trust for Financial Services: Protecting Data in the Digital Age. Deloitte Touche Tohmatsu Limited, London, UK.
[7] Brewer, R. (2019). From security perimeters to Zero Trust. Network Security, 2019(5), 10–13. Elsevier Ltd. DOI: 10.1016/S1353-4858(19)30055-7
[8] Moubarak, J., Chamoun, M., & Feghali, A. (2021). Comparative Study of Zero Trust Models for Cloud Security. Proceedings of the IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2021), pp. 145–152. DOI: 10.1109/CloudCom52989.2021.00032
[9] Ferrer, A. J. (2019). Multi-cloud: Heterogeneous cloud integration platform. IEEE Cloud Computing, 6(4), 10–15. DOI: 10.1109/MCC.2019.00012
[10] Solarwinds Security Advisory Team. (2021). SUNBURST Backdoor: Supply Chain Attack Technical Analysis. CISA Alert AA20-352A, U.S. Department of Homeland Security, Washington, DC, USA.
[11] Amazon Web Services. (2023). AWS Well-Architected Framework: Security Pillar (Rev. 5). Amazon Web Services Inc., Seattle, WA, USA. Retrieved from https://docs.aws.amazon.com/wellarchitected/
[12] U.S. Office of Management and Budget (OMB). (2022). Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. OMB Memorandum M-22-09. Executive Office of the President, Washington, DC, USA.
[13] Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, 71, 28–42. Elsevier Ltd. DOI: 10.1016/j.compeleceng.2018.06.006
[14] Cloud Security Alliance. (2023). Top Threats to Cloud Computing: Pandemic Eleven. CSA Technical Report. Cloud Security Alliance, Seattle, WA, USA.
[15] Verizon Enterprise Solutions. (2023). 2023 Data Breach Investigations Report (DBIR). Verizon Business, New York, NY, USA.
[16] Ward, R., & Beyer, B. (2014). Beyond Corp: A new approach to enterprise security. USENIX ;login: Magazine, 39(6), 6–11. USENIX Association, Berkeley, CA, USA.
[17] Chase, J. (2017). The Definition of Modern Zero Trust. Forrester Research Report. Forrester Research, Cambridge, MA, USA.
[18] U.S. Department of Defence. (2022). DoD Zero Trust Reference Architecture v2.0. Office of the DoD Chief Information Officer, Washington, DC, USA.
[19] Sarhan, M., Lo, W. W., Layeghy, S., & Portmann, M. (2021). MIDAS: Detecting microarchitectural anomalies in cloud using machine learning. IEEE Access, 9, 107606–107624. DOI: 10.1109/ACCESS.2021.3101171
[20] Darktrace. (2022). AI-Driven Threat Detection: Annual Threat Report 2022. Darktrace Ltd., Cambridge, UK. Retrieved from https://www.darktrace.com/resources/

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503196|

[21] Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I., & Tygar, J. D. (2011). Adversarial machine learning. Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence (AISec 2011), pp. 43–58. ACM. DOI: 10.1145/2046684.2046692

[22] He, W., & Zhang, Z. (2022). Performance Analysis of Zero Trust Policy Enforcement in Cloud Environments. IEEE Transactions on Network and Service Management, 19(3), 2912–2925. DOI: 10.1109/TNSM.2022.3151099

[23] Sims, D. (2021). Zero Trust and the Human Factor: Why Change Management Matters. ISACA Journal, Vol. 3 2021. ISACA, Schaumburg, IL, USA.

[24] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105. University of Minnesota. DOI: 10.2307/25148625

[25] Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194. Springer Nature. DOI: 10.1038/nature23461

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details