Cloud-Based Enterprise Information Systems Are Secure Using Zero Trust Architectures.

Mrs. Priyanka Sharma
Assistant Professor, Department of Management, Guru Kashi University, Talwandi Sabo, Bathinda
Email Id: priyankasharma2062026@gmail.com

Accepted: 20-09-2026 Published: 12-10-2026 Page No. 9-13 DOI: 10.5281/zenodo.24330068

Abstract— Enterprise information systems are now deployed and hosted in a flexible cloud or app-based environment rather than in a fixed, perimeter-protected data centre. In an environment like this, no device or user in the network is ever automatically trusted. In addition, a compromised credential threatens the entire action set of an adversary. In accordance with the principle of "never trust, always verify", this paper proposes zero trust architecture with layered approaches for cloud-based enterprise information system. How does the underlying technical architecture function? The study used a design-science research method. The design requirements were established by literature. We then propose a five-layer structure containing identity, device, network, application and data. The next step is to outline the decision and the flow of enforcement with monitoring.

For evaluating design effectiveness six criteria were suggested. Testing is carried on using classical perimeter model. The criteria include limiting the area for attack, avoiding lateral spread, fine-grained access control and others. According to the analysis, the model displays superior containment and visibility. Nonetheless, its complexity at the outset is high. Use staff training programme during first test run administratively required. Extensive SEO-based content writing. A reusable reference design, evaluation framework and prioritization of the control risk model will be available to organizations.

Keywords — Zero trust, cloud security, information systems, access control, micro-segmentation, continuous monitoring, design science.

I. INTRODUCTION

The IT of today is performing day-to-day office functions like writing email, creating documents, etc. The notion that remote workers are inside and outside the business almost meaningless because of the SaaS applications and cloud services of the business. Cloud computing is a model that allows access to a shared network resource. According to NIST, it is a model that requires. Businesses consider a service a great choice due to its flexibility and cost efficiency, scalability [2].

This creates a problem regarding the security. A conventional firewall is established to deny access and functions as a barrier between a trusted internal network and an untrusted external network. So if an attacker manages to take one identity or device, they have access to many other devices. The attacker can shift across the network. According to the zero trust model, both external and internal networks are not trusted. This makes the workings of this model more stringent and practical. Requests ought to be checked explicitly according to the identity of the requester, the state of the device as well as the context of the request.

An increasing number of organizations and government agencies are adopting the zero trust security models. Countless organizations are unable to generate a useful configuration.

RQ1.What are the requirements on the design of a zero-trust architecture to secure cloud-hosted information systems?

RQ2. In what way can we present or categorize these requirements into multilayer types for implementation purposes?

RQ3. How does the proposed architecture compare to a classic perimeter model in operational and security terms?

The resultant design requirements derived include a five-layer reference architecture with policy decision flow, analytical evaluation framework consisting of six criteria, simple risk model for prioritization of controls and a phased adoption roadmap.

II. HISTORY & IMPORTANT ASSIGNMENTS.

A. The design of security models for businesses:

The phrase "zero trust" was coined by Kindervag who thought we ought to treat all traffic on a network as untrusted, log it, inspect it. As detailed by Google's BeyondCorp, an industry implementation, access decisions depend on user and device, not network location. This means that workers can safely carry out their work without a VPN [5]. Ultimately, these concepts were combined and included in a reference model defined at NIST [3]. Simply put, Zero Trust is a fanciful term that denotes implementation of certain principles by an organization, which helps protect its users, assets, and resources. We will also introduce the policy enforcement point and the policy decision point. According to Gilman and Barth, the practitioner's perspective can build comparable frameworks.

B. Survey of materials used:

Syed et al. reviewed literature on zero trust after which they divided it into architecture, technologies and challenges. Note 7 states that actual assessments on application and effectiveness have very few research papers.

C. Politics of data and accessibility:

Abnormal behaviour detection is the basis for continuous verification. Authors of the reported study something about using a detection and intrusion detection system of anomaly in the network using processes of machine learning techniques. As Sommer and Paxson explain, it is hard to detect attacks against computer networks. In this respect, they state that misclassification is expensive, detection of true novel attacks is hard, normal traffic is slow-changing.

According to research papers, ABAC can perform authorization based on user, resource and environment attributes in a more fine-grain manner [10].

Earlier studies mainly explain basic principles and set out existing technologies, while not many cite a reference model binding together identity, device, network, application and data controls in one flow which allows for easy comparison of that design against a perimeter model.

III. RESEARCH PROCESS.

• Hevner and his co-authors [11] offer the precise concept of the design-science approach to information systems research in terms of the design, justification or evaluation of a purposeful artefact against stated criteria. It goes through four stages.

• The perimeter model of cloud ecosystems has a number of flaws.

• The scrutiny can refer to the studies [3], [5] and [7].

• The design requirements have been presented in section IV-A, the issues have been identified.

• The layers and policy flow arrangement is described having been specified under the artifact design.

• The evaluation compares the architecture to the perimeter model on six pre-defined criteria. All of the criteria are rated low, medium, high level on the basis of justification from 100 words (Section V).

• The assessment that is being held has a quality character and also has an analytical character. The ratings are based on the cited literature; whose reasons are more certain than deduction labour. Section VII provides an overview of the effect of this decision.

IV. SUGGESTED STRUCTURE

A. Design Specifications.

The literature was used to derive six requirements.

• R1: Always verify access requests with identity, device health and context.

• R2: the minimum privilege should be provided which is to be limited scope wise and time wise.

• R3: is a center that makes the assumption of breach in order to segment an environment and restrict lateral movement.

• R4: records and logs every access decision made.

• R5: Make sure that the real data is safe, not just the means of transport.

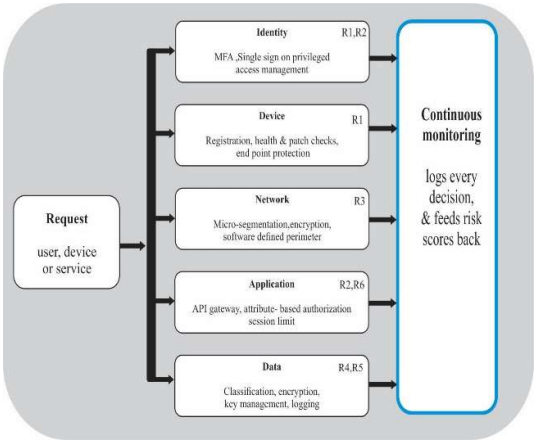
• R6: Stay usable in order that the security controls do not cause users to circumvent them.

B. Five-Layer Reference Architecture

Layer	Main Controls	Requirement Addressed
Identity	Utilize multiple forms of authentication and single access to login in high privilege access	R1, R2
Device	Device Configuration and Patch Registration for Enhanced Protection	R1.
Network	The software-defined perimeters involve network micro-segmentation and encrypted traffic.	R3.
Application	The functions of the application API Gateway can use attribute-based authorization, session limits, etc.	R2, R6
Data	The data should be categorized and stored in an encrypted manner at rest and in transit by using appropriate keys which should be responsive to logs	R4, R5

Table I illustrates the levels of a proposed zero-trust architecture.

Five layers each verify access and report to one monitoring plane.



(Figure 1). A five-layer zero-trust reference architecture with a monitoring plane.

C. The Process of Designing and Enacting Policy. As stated in the NIST model, every access request is intercepted by a policy enforcement point (PEP). It also interrogates a policy decision point (PDP) for a verdict.

A user or service will request access to use the resource to initiate the flow.

• The PEP transfers the identity, device, and context attributes to the PDP for requesting permissions.

• The PDP assesses these criteria with regard to the relevant policy a. The Incident command Centres Risk Score and the latest ABAC rules.

• The PDP may choose to allow, refuse or direct the use of step-up authentication involving an additional authentication component.

• If granted access, the PEP will connect to the resource that has the most minimal privilege level.

• The conduct and verdict are recorded and therefore used on an ongoing basis this can deactivate the session in case of any abnormal behaviour.

Every request is checked by the PDP before the PEP opens a session.

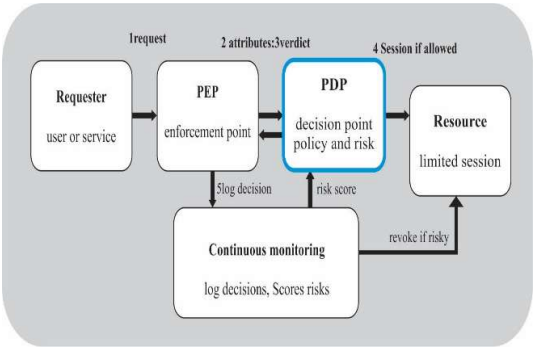


***Figure. 2**. Policy decisions and implementations flow between the PEP, PDP, and monitoring.*

D. To Prioritize the protection of the various assets: It is possible to estimate the relevant residual risks, this being achieved by multiplying the probabilities of being compromised by the related impact and then deducted the figures that already account for effective control. The equation $R_i = L_i \times I_i \times (1 - e_i)$ may be used to approximate the asset risk R. L_i refers to the likelihood of compromise in the expression. In contrast, the

I_i indicates the impact, and e_i (which takes value 0-1) gives the overall efficiency of the measures taken. The initial step is to provide assets with a high Li × Ii and a small. The necessity for periodic reviews and updates of the values of L_i, I_i and e_i, based on relevant risk assessment undertaken by the organization, would be essential.

V. ANALYTICAL EVALUATION.

In table II, there are six criteria to compare the approach against a perimeter model.

Criterion	Perimeter Model	Proposed Zero Trust Model	Rationale
Attack-surface reduction	Medium	High	Resources are hidden until access is verified
Lateral-movement containment	Low	High	Micro-segmentation and per-request checks limit spread
Access-control granularity	Low	High	Attribute-based, resource-level decisions
Visibility and auditability	Medium	High	Every decision is logged and analyzed
Usability	High	Medium	Extra verification may add friction; step-up only on risk
Implementation complexity	Low	High	More components, policy design, and integration effort

Table 2 provides a qualitative evaluation (Low / Medium / High) of the security models.

There appear to be alternate equilibria. The proposed model bests perimeter model in the four standards of security as it tests every request and does not assume the trust of the request based on its location in the overall network. Nonetheless, it isn't as user-friendly and is rather complicated to implement. Verification and policy management would require dedicated onboard devices and expertise. The ensuing section explains how cost savings could be achieved through the use of risk-based step-up authentication. On account of the fact that detection takes place through the analytics [9], we can see continuous monitoring as an additional control rather than an alternative to strong identity management and segmentation.

VI. PLAN FOR EXECUTION.

The organization can choose to slow down the process so that the risk is lower and learning takes place. As demonstrated in Fig. 3, the roadmap consists of four phases which flows through audits and governance.

• Begin with a careful evaluation of the users, devices, programs and data on the environment and messages between them. Make use of the risk model in section IV-D to risk rank the assets.

• The identity is the second phase The obligated implementation of MFA and SSO, as well as a privileged account review.

• Establish frequent evaluations and revisions due to alterations that happen in business practices. When a firm's goals and objectives change; policies of the firm shall also be changed. It is therefore advisable to review the policies monthly. A bet policy is one which is always being improved and never finished.

• The design phase must be monitored in the fourth step of the 5-step approach to incident response planning. Logs are centralized, typically in a security information and event management (SIEM) system. The outcomes of tested incidents are regularly examined for verification.

Adoption in four phases, with governance running througout

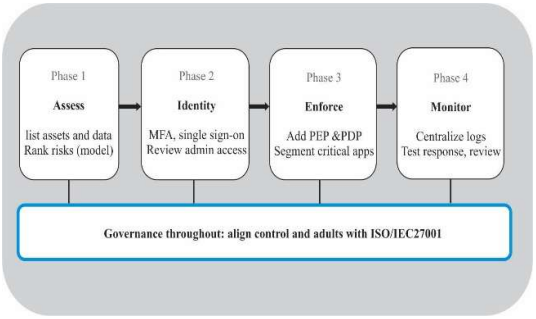


Figure. 3. A roadmap built of four phases, with continuous governance.

An Information Security Management System (ISMS) such as ISO/IEC 27001 allows the

controlled documentation and repeatable responsibility and audit through all four sizes.

VII. LIMITATIONS

The review which is the basis for this study suggests that the measure of the table II is not measured, but reasoned. The outcomes will differ as per deployments and several organizations size, fund etc will differ the outcomes. A risk model is a straightforward assessment of the likelihood and impact whose quality depends on the assessment of inputs. Future research should focus on creating a testbed or case-study organization to facilitate metric assessments. The result measures which will cause a better understanding of deploying a zero trust architecture. Also, the objectives are to measure delay in authentication, attempts of lateral movement being blocked and time taken to detect incidents by a bunch of organizations. Additionally, businesses can evaluate user experience and productivity, as well as the relevance of zero trust to multi-cloud, IoT, and OT (operational technology) scenarios through the rollout.

VIII. CONCLUSION

A zero trust reference architecture for the cloud-based enterprise information systems is made using five layers. For every access request, there is a policy decision flow and enforcement flow. According to our analyses, containment, granularity and visibility model is superior to a perimeter model. The added complexity of the benefits is causing users to experience friction. A systematic priority roadmap employs a basic risk assessment model to ensure that efforts are aimed at major risk activity. The functional and non-functional requirements are not adequately validated.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Spec. Publ. 800-145, Sep. 2011.

[2] M. Armbrust et al., "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[3] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Spec. Publ. 800-207, Aug. 2020.

[4] J. Kindervag, "Build security into your network's DNA: The zero trust network architecture," Forrester Research, Cambridge, MA, USA, Nov. 2010.

[5] R. Ward and B. Beyer, "BeyondCorp: A new approach to enterprise security,"; login, vol. 39, no. 6, pp. 6–11, Dec. 2014.

[6] E. Gilman and D. Barth, Zero Trust Networks: Building Secure Systems in Untrusted Networks. Sebastopol, CA, USA: O'Reilly Media, 2017.

[7] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (ZTA): A comprehensive survey," IEEE Access, vol. 10, pp. 57143–57179, 2022.

[8] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Commun. Surveys Tuts., vol. 18, no. 2, pp. 1153–1176, 2nd Quart., 2016.

[9] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in Proc. IEEE Symp. Security Privacy, Oakland, CA, USA, 2010, pp. 305–316.

[10] V. C. Hu et al., "Guide to attribute based access control (ABAC) definition and considerations," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Spec. Publ. 800-162, Jan. 2014.

[11] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," MIS Quart., vol. 28, no. 1, pp. 75–105, Mar. 2004.

[12] Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements, ISO/IEC 27001:2022, 2022.