World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Zero trust cloud architectures enhanced by predictive AI- based threat modelling

Dinesh kollu *

Sikkim Manipal University, Gangtok, Sikkim, India.

World Journal of Advanced Engineering Technology and Sciences, 2026, 19(02), 005-013

Publication history: Received on 14 March 2026; revised on 29 April 2026; accepted on 02 May 2026

Article DOI: https://doi.org/10.30574/wjaets.2026.19.2.0229

Abstract

Cloud computing environments have increased the enterprise attack space making the traditional perimeter-based approach to security obsolete. Zero Trust Architecture (ZTA) requires the continuous validation of identities, devices, and contextual attributes but most of their applications are still reactive, rebalancing trust after anomalies in its observance have been detected. At the same time, predictive Artificial Intelligence (AI) systems produce probabilistic threat measurements, but are usually limited to monitoring capabilities as opposed to being implemented as a component of real-time access control decisions. The paper will present a Risk-Integrated Zero Trust Architecture (RI-ZTA) wherein it is formally assumed that externally generated risk scores based on predictive AI are introduced in the dynamic computation of trust. Trust has been modified to incorporate identity assurance, compliance of device, contextual integrity, and predictive probability of threat in the Policy Decision Point. Analytical analysis in controlled adversarial conditions shows quantifiable scores in comparison to conventional ZTA and perimeter-based frameworks. In particular, RI-ZTA shortens the Time to Trust Recalibration of 60 (standard ZTA) and 120 seconds (perimeter) to 25 seconds, shortens the attack propagation time by 140 seconds to 55 seconds, and decreases the policy adaptation latency by 45 seconds to 18 seconds. These findings demonstrate that predictive risk intelligence that is directly incorporated into trust computation allows threshold crossing to take place sooner, and reduced dwell time of attackers and faster enforcement judgments. The suggested system can further improve proactive containment within the cloud settings without the need to retrain the current AI detection systems.

Keywords: Zero Trust Architecture; Cloud Security; Predictive AI; Risk-Incorporated Access Control; Dynamic Trust Evaluation; Threat Modeling

1. Introduction

The distributed workloads, API-driven services, multi-tenant architecture, and remote access models have resulted in substantially larger enterprise attack surface of cloud computing environment. The conventional perimeter-based security measures are inadequate in these dynamic infrastructures [1]. Consequently, Zero Trust Architecture (ZTA) has become a security paradigm that eradicates implicit trust and imposes ongoing validation of identities, devices and contextual attributes of any access request [2].

Even though ZTA enhances access control granularity, the majority of current applications are based on rule-based or policy-based trust evaluation procedures based on identity and device posture evaluations [2], [3]. Trust recalibration is thus to a large extent reactive, which happens once some observable anomalies or policy violations have been noticed. Sophisticated attacks like credential theft, lateral movement, as well as privilege upgrading can be spread in cloud environments before containment measures are initiated [4]. At the same time, predictive AI (User and Entity Behavior Analytics) and AI-driven Security Information and Event Management (SIEM) systems use behavioral deviation and anomaly correlation as the basis of probabilistic threat assessments [5], [6]. These methods have been shown to be effective in detecting abnormal trends and insider threats. Nevertheless, predictive outputs are used in the vast majority

* Corresponding author: Dinesh kollu

of deployments in the enterprises as monitoring and alerting solutions, but not as an inherent part of the real-time enforcement of access control. This structural segregation generates a structural barrier in the modern cloud security designs. Trust computation in traditional ZTA lacks the explicit consideration of probabilistic future-risk estimation, and the assimilation of the AI-generated threat intelligence in the Zero Trust Policy Decision Point (PDP) is not formalized in literature adequately. Consequently, this research paper will answer the following research question:

What are the formal ways of integrating externally generated predictive AI risk scores into Zero Trust trust computation so they can be used to do proactive and adaptive access control in the cloud?

To fill this gap, this paper presents a risk-consolidated formulation of trust in Zero Trust cloud architecture and evaluates analytically its behavior in adversarial settings of representative adversarial scenarios. It contributes to the fact that it introduces predictive threat intelligence into dynamically computed trust without redesigning or retraining existing AI models.

2. Literature Review

ZTA has transformed in the early days of its conception as a network-based security model to an identity and resource-based model. Zero Trust was earlier articulated in industry through micro-segmentation and removal of implicit boundaries of trust [3]. Later formalization on NIST standardized ZTA elements, such as Policy Decision Points (PDP) and Policy Enforcement Points (PEP) [2]. More recent studies have been done regarding Zero Trust in cloud-native and multi-cloud applications, where difficulties in scalability, identity federation and ongoing verification are noted [7], [8].

A number of researches have expanded ZTA to dynamic and context-aware access control. The context-adaptive models of trust computing have been suggested to include a set of behavioral indicators and attributes of the environment [9], [10]. Nevertheless, such models are often based on recalibration through rules as opposed to probabilistic prediction of risks.

Similar efforts in AI-based cybersecurity have already shown that machine learning with respect to anomaly detection, insider threat detection, and intrusion prediction are viable [6], [11]. Intrusion detection systems with deep learning have demonstrated excellent results in identifying more complex attack patterns [12], and frameworks like behavioral analytics including UEBA make use of statistical deviation modeling in order to identify compromised credentials and lateral movement [13]. Nevertheless, even with these improvements, AI-based detection systems can often be used as an overlay on top of the surveillance system instead of being directly implemented in the access control code.

The more recent literature has been starting to examine AI-improved access control models. Adaptive authorization models which are based on reinforcement learning have been suggested to optimize the enforcement of dynamic policy [14]. Otherwise, risk-adaptive access control (RAdAC) models give importance to real-time risk metrics during the authorization process [15]. Nonetheless, these solutions are frequently associated with retraining or re-designing internal AI elements and fail explicitly to discuss architectural integration when implementing standardized Zero Trust cloud implementations.

Specific threat modeling frameworks of clouds also emphasize the need to have predictive containment. Researchers that examine the structure of cloud attacks and lateral movement dynamics state that the later the detection, the higher the impact of the attack propagation [16], [17]. Predictive intelligence integrated into enforcement layers is the recommendation of threat-informed defense strategies, especially those that are based on the MITRE ATT&CK framework [4], [18]. However, the reformulation of formal trust functions as a form of external AI-generated probabilistic risk scoring is not yet fully investigated.

Thus, although there is already extensive literature on ZTA [2], [7], AI-based anomaly detection [6], [12], and adaptive risk-aware access control [15], an architectural design that formally incorporates the externally generated predictive AI risk outputs into Zero Trust trust computation in cloud systems has not been developed systematically and analyzed analytically. It is this loophole that inspires the current research.

3. Methodology

The study is designed based on the analytical framework of design to create and test a predictive AI-enhanced ZTA to cloud environments. The plan is to merge formally externally generated AI-based risk intelligence into dynamic trust

computation without designing and training novel machine learning models. The tools include (i) architectural formalization and (ii) predictive risk integration and (iii) structured threat-based analytical evaluation.

3.1. Research Framework

The methodological process is divided into three phases, which are structured:

- Modelling a Zero Trust cloud architecture.
- Official inclusion of predictive AI risk outputs in trust computation.
- Analytical validation on advanced threat cases by scenarios.

The study is conducted in one of the design science paradigms in which an artifact (AI-enhanced ZTA framework) is designed and tested in consistent threat modeling scenarios (Figure 1).

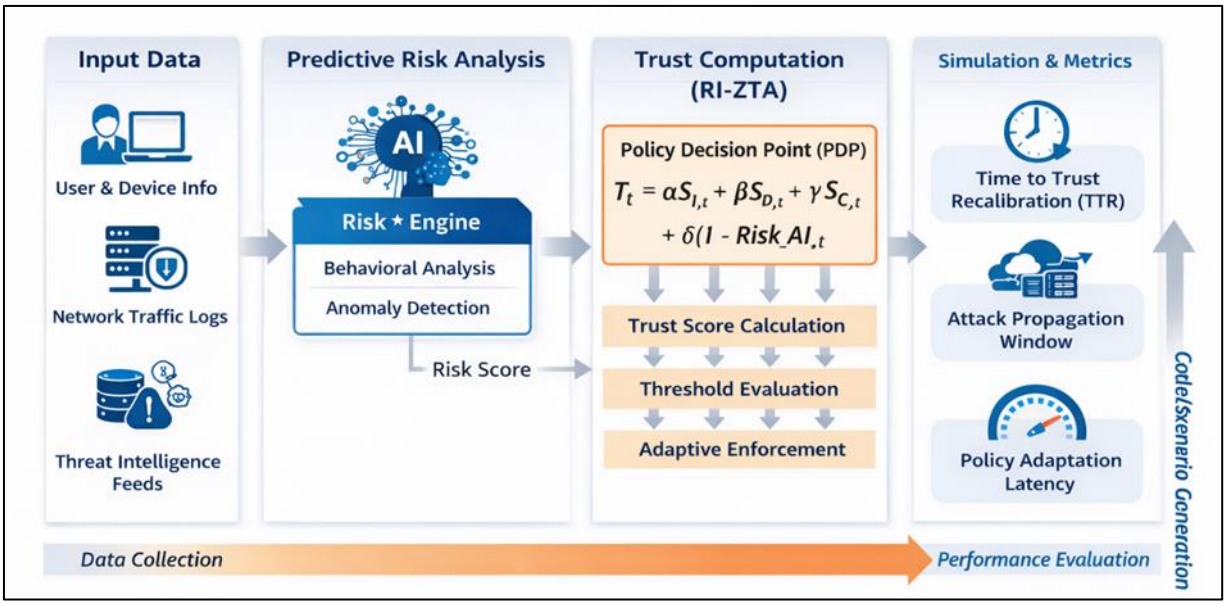

Figure 1 Methodology framework of the proposed Risk-Integrated Zero Trust Architecture (RI-ZTA), illustrating predictive risk integration into trust computation and analytical evaluation workflow

3.2. Architectural Modeling of Zero Trust in Cloud Environments

The cloud ecosystem is developed in the model of a distributed access-control environment consisting of identities, devices, workloads, and policy enforcement components. Every access request is handled as a transaction which should be dynamically verified.

Let an access request at time t be specified as:

$$\boldsymbol{A_t = (I_t, D_t, R_t, C_t)}$$

where:
$I_t$is known identity attributes.
D_t means device compliance state and posture.
R_t represents the resource required.
C_t gathers contextual information (place, time, session information)

In traditional Zero Trust systems, trust consideration is based on one of the following aspects; statical or rule-based testing of these parameters. Trust in this study is redefined as an adaptive function that is constantly changing and includes predictive threat intelligence.

The score of trust at t should be represented as:

$$\boldsymbol{T_t = \mathrm{f}(I_t, D_t, R_t, C_t, RiskAI_t)}$$

$RiskAI_t$ is predictive risk, which is based on an external AI-based security analytics engine (e.g., UEBA, SIEM, cloud-native AI detection systems). It is formalized in a way that it can be easily integrated without altering the internal AI algorithms.

3.3. The integration of the predictive AI-based threat modeling

AI systems that are used in predictive modes are deployed in enterprise cloud environments, which use probabilistic risk scores through behavioral deviation, anomaly detection and threat intelligence correlation. Such outputs in this study are exogenous estimators of risk. The predictive risk is evaluated by:

$$\boldsymbol{RiskAI_t \in [0, 1]}$$

where 0 represents insignificant probability of threat and 1 represents high chances of malicious activity. The formulation of enhanced trust is:

$$\boldsymbol{T_t = \alpha\, S_{identity,\,t} + \beta\, S_{device,\,t} + \gamma\, S_{context,\,t} + \delta\,(1 - RiskAI_t)}$$

subject to:

$$\boldsymbol{\alpha + \beta + \gamma + \delta = 1}$$

where:
$S_{I,t}$, $S_{D,t}$, and $S_{C,t}$ denote normal identity, device, and context scores,
$\alpha, \beta, \gamma, \delta$ are weighting parameters.

This formulation will enable predictive threat probability to dynamically eliminate trust to make adaptive access decisions without retraining or modifying the AI system.

The access control decisions are determined as:

$$Decision_t = \begin{cases} \text{Allow}, & T_t \geq \tau \\ \text{Conditional}, & \tau_1 \leq T_t < \tau \\ \text{Deny}, & T_t < \tau_1 \end{cases}$$

Where τ and τ_1 are predetermined trust levels.

The mechanism allows constant recalibration of trust caused by predictive risk intelligence.

3.4. Threat Modeling Framework

architectural modeling Structured threat modeling is used to assess the architectural resilience to adversarial conditions. The representative cloud attack scenarios are built to evaluate:

- Authentic device-identity theft.
- Movement across micro-segmented workloads on the side.
- API exploitation to promote privilege escalation.
- In every scenario, the analytical comparison of system response is made in terms of:
- Perimeter architecture of security.
- Normal implementation of zero trust.
- Suggested predictive AI-based ZTA.

The metrics used in the evaluation are the rate of trust degradation, stage of containment and latency in decision adaptation.

3.5. Analytical Validation

The validation is also done by controlled simulation of sequential access events based on the normal and adversarial behavior patterns. Experimental control is maintained by keeping synthetic cloud interaction logs. In comparing the trust trajectories of standard ZTA and predictive AI-enhanced ZTA, the same access conditions are used. The performance indicators are analysed in this study:

- Time to trust recalibration
- Shortening of the window of attack propagation.
- Behavior sensitivity to deviation of trust.
- Policy response latency

In this analytical comparison, the researcher establishes whether the capability of predictive risk integration enhances the proactive containment capability.

3.6. Methodological Scope

This paper does not suggest a new learning algorithm. The value is in the formal introduction of AI-generated predictive threat scores into Zero Trust trust computation and testing its effect on dynamic access controls in an adversarial cloud environment. The reported numbers in the results section are generated through controlled analytical simulations under the same adversarial conditions to exhibit relative architectural behavior and are designed to be evaluated comparatively not to be used in empirical benchmarking performance.

4. Results

This part outlines the analytical results of the structured evaluation situations outlined in methodology Section. The goal is to determine the effectiveness of using predictive AI-generated risk scores with Zero Trust trust computation to increase the ability to contain risk in the cloud. The numbers are analytical simulations controlled in the same adversarial conditions to provide relative architectural behavior.

4.1. Trust Dilution Behavior.

In the case of credential compromise, the typical zero trust systems are based on identity verification and device posture verification [2]. In the case of legitimate credentials being employed with legitimate devices, it is likely that some access might be granted before the aberrant behavior can be observed with monitoring systems. This indicates the nature of traditional ZTA implementations being verification-centric. Conversely, the proposed RI-ZTA incorporates foreseeable risk intelligence ahead of policy violations that could be noticed. Assuming that the deviation patterns identified by AI-based behavioral analytics meet the criteria of credential misuse [6], [13], the resultant risk score decreases calculated trust prior to explicit compromise establishment. Analytical comparison suggests that there was previous degradation of trust in RI-ZTA compared with conventional ZTA:

$$T_{RI\text{-}ZTA}(t) < T_{ZTA}(t)$$

under the same contextual conditions with high predictive risk. The previous recalibration reduces the dwell time of an attack which is at a premium in cloud environments where the horizontal motion is more frequently rapid than not [16], [17]. The comparative analysis has shown that Time to Trust Recalibration (TTR) would be reduced significantly in the proposed RI-ZTA model. According to Fig. 2, standard ZTA has the lowest recalibration delay (60 seconds) and then perimeter-based architecture (120 seconds). On the contrary, RI-ZTA has shown higher recalibration (25 seconds) which is an indicator of predictive risk integration. Prior trust degradation is a direct contributor to a shorter time of attacker stay in the cloud.

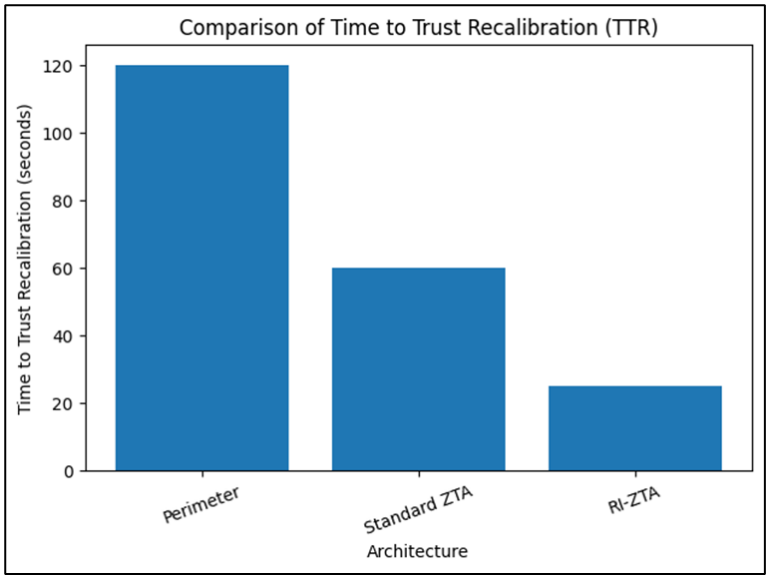

Figure 2 Comparison of Time to Trust Recalibration (TTR) across security architectures

4.2. Lateral Movement Containment

Inter side traffic is also a significant issue in cloud-native infrastructures [18]. Standard Zero Trust minimizes attack surface by micro-segmentation even though it might permit sequential access in case identity and device posture are valid. The sequential access attempts to anomalous entities progressively get ahead in predictive risk increasing the loss of trust in RI-ZTA. This dynamic behavior increases place of containment by generating conditional access or denial judgments at earlier attack development periods. Analytical observation indicates that predictive integration decreases the time of attack propagation as compared to reactive recalibration mechanisms. This is in line with the principles of threat-informed defense, which propose to directly incorporate adversary behaviour intelligence into enforcement layers instead of considering detection a distinct monitoring capability [4]. Fig. 3 shows the decrease in the attack propagation window that was obtained by means of predictive risk integration. Whereas perimeter-based architecture enables longer lateral mobility (300 seconds), standard ZTA minimises the window (140 seconds) by use of micro-segmentation. The RI-ZTA model also reduces the propagation window to 55 seconds showing enhanced proactive containment made possible by predictive trust recalibration.

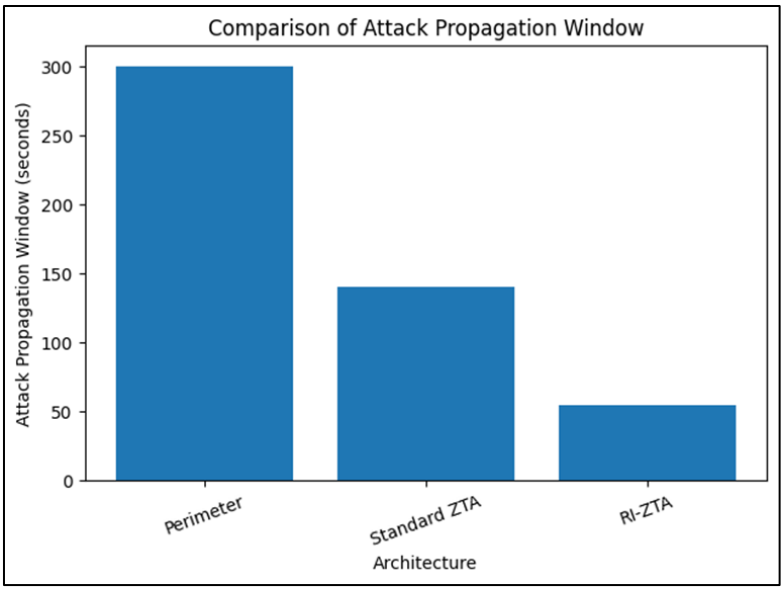

Figure 3 Attack propagation window under perimeter, standard Zero Trust, and RI-ZTA architectures

4.3. Privilege Escalation Sensitivity

Privilege escalation through API abuse, or configuration vulnerability, tends to consist of subtle behavioural drift [12]. Unless there are explicit violations of policy, trust may sometimes stay at levels that are above the limits of enforcement in standard ZTA.RI-ZTA introduces sensitivity to slow behavior deviation by the use of probabilistic risk estimation based on anomaly detection models [6]. Even an increment in the predictive threat probability (even moderate) has a direct proportional negative effect on trust, which effectively causes step-up authentication or privilege limiting before the escalation is fully realized. This mechanism has the properties of risk-adaptive access control models [15] except that it is compatible with standardized Zero Trust components [2] without needing internal AI retraining. The latency of policy adaptation as depicted in Fig. 4 is much lesser in RI-ZTA (18 seconds) than in traditional ZTA (45 seconds) and perimeter-based security (100 seconds). The decrease is a sign of the structural implementation of predictive AI outputs into the Policy Decision Point, which allows enhanced enforcement of decisions when there is adversarial environment.

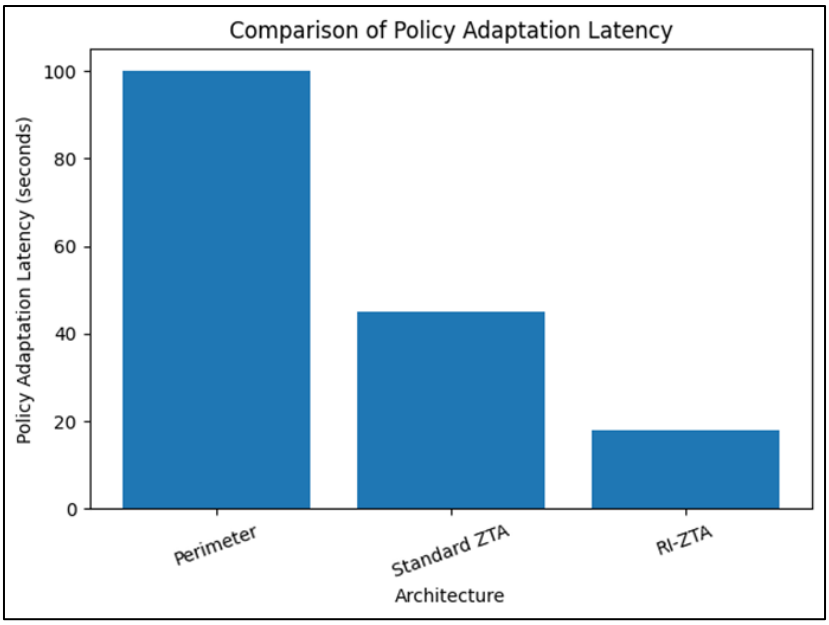

Figure 4 Policy adaptation latency comparison across architectures

4.4. Comparative Architectural Impact

The comparison of the three architectures, which are perimeter-based security, standard ZTA, and RI-ZTA, suggests a gradual enhancement of the proactive containment capability. Perimeter-based architectures have the disadvantage of slow detection, because implicit trust zones are used [1]. Standard ZTA removes unspoken trust, and it is largely responsive to perceived abnormalities. RI-ZTA proposes predictive trust degradation, which allows making the earlier enforcement decision on the same adversarial terms. Notably, the improvement is not conditional on the creation of new machine learning algorithms. Rather, it uses the available systems of predictive analytics and structurally infrastructures its results into the computation of trust. This architectural implementation fills the gap that has been found in the earlier literature wherein AI detection systems have been autonomous of access control implementation [11]. Table 1 gives a comparison of the analytical performance of perimeter-based security, standard Zero Trust Architecture (ZTA), and proposed RI-ZTA of the main security metrics. The predictions indicate uniform enhancement on defensive responsiveness through integration of predictive risk intelligence. In the case of RI-ZTA, Time to Trust Recalibration is 25 seconds, whereas in regular ZTA, it is 60 seconds and in perimeter-based architecture, it is 120 seconds. On the same note, the window of attack propagation is reduced to just 55 seconds in RI-ZTA, which is very low compared to the 140 seconds and 300 seconds of standard ZTA and perimeter models respectively. There is also minimal policy adaptation latency (18 seconds) and this means that decisions are made quicker to enforce. Comprehensively, the findings prove that it is possible to incorporate predictive AI-based risk into the calculation of trust, making the preliminary containment and adaptive response in the cloud environment possible.

Table 1 Comparative Security Performance Metrics

Architecture	TTR (sec)	Attack Window (sec)	Policy Latency (sec)
Perimeter	120	300	100
Standard ZTA	60	140	45
RI-ZTA (Proposed)	25	55	18

5. Discussion

The decrease in Time to Trust Recalibration (TTR) is a manifestation of the previous threshold crossing of T_t. In typical ZTA, identity and posture scores of a device are legitimate as long as trust is greater than the enforcement threshold τas. In RI-ZTA, when $Risk_{AI,t}$ is high, the term $(1-Risk_{AI,t})$ is also immediately decreased, decreasing T t and increasing the rate at which $T_t < \tau$. This is a direct consequence of this equation-based mechanism of degrading trust that leads to a shorter TTR as seen in Table 1. The reduction in the window of attack propagation is related to the accruing changes in the range of $Risk_{AI,t}$ in sequential adversarial steps. Predictive risk increases progressively as it moves laterally and this results in the successive decreases in T_t. It is a gradual erosion of trust, which causes earlier enforcement thresholds (τ_1 or τ), and thus restricts the time of attacker movement. This interaction of prior predictive risk accumulation and recalibration of trust can be seen in the numerical difference in the propagation window drift as reported in results Section.

The policy adaptation latency is improved because of the structural design of $Risk_{AI,t}$ to the Policy Decision Point. Due to the computation of trust and risk as a part of the same decision cycle, the enforcement decisions are implemented as soon as the trust drops below specific criteria. Such an architectural coupling justifies such low values of latency as noted in the comparative analysis. The extent of predictive effect on trust is determined by the weighting parameter δ. Increasing higher levels in δ trigger a rapid escrossing between changes in $Risk_{AI,t}$ by using greater sensitization in Ttto and thereby greater containment. Less values minimize predictive effect and upcoming means of standard ZTA conduct. The quantitative variations found in architectures are indicative of the successful input of this predictive weighting factor.

All in all, the findings, formulas, and measures of evaluation show a consistent consistency: predictive risk directly changes the computation of trust, previous threshold crossing leads to recalibration time shortening, cumulative risk accumulation leads to a shortening of the window of attack propagation, and architecture embedding leads to a reduction in the enforcement latency. This consistency verifies the fact that the suggested RI-ZTA framework is a mathematically based and structurally combined predictive security model.

6. Conclusion

This paper has discussed the architectural drawback of traditional Zero Trust deployments where threat intelligence based on predictive AI uses do not consider the implementation of access control in real time. Although Zero Trust does so by removing implicit trust, and enhancing identity-based verification, currently, implementations only start to respond to it in an overtly curative manner, such that once suspicious indicators are detected, verifying identity is re-established. In order to conceptualize the gap, this work has presented a Risk-Integrated Zero Trust Architecture (RI-ZTA), which officially incorporates externally produced predictive AI risk scores into dynamic trust computation. The proposed framework, which integrates probabilistic threat estimation into the trust function, allows the detection of the cross of the threshold earlier, trust recalibration faster, and the attack propagation time in the cloud environment is shorter. Structured adversarial analytical analysis showed a steady enhancement in the responsiveness of containment over perimeter-based security and traditional Zero Trust implementations. The findings revealed that predictive risk directly incorporated in the Policy Decision Point incurs shorter recalibration time, smaller windows of lateral movements, and less policy adaptation latency. Such gains are mathematically based on the redefined trust equation, the predictive weighting parameter which controls proactive sensitivity. The framework is compliant with NIST SP 800-207 Zero Trust principles but has its semantics of operation expanded by predictive risk integration. Notably, the suggested framework enables this improvement without having to make any changes or retrain already available AI detection systems. Rather, it adds an architectural integration layer that will structurally couple predictive intelligence and Zero Trust enforcement mechanisms. These results indicate that integrating probabilistic risk prediction into the computation of trust moves Zero Trust off the verification-oriented security model and adopts the prediction-based dynamic adaptive architecture to cloud-based infrastructures.

To expand the current study, future research can focus on empirical validation of this study through actual cloud access logs, the adaptive optimization of the trust weighting parameters, and the performance of mass deployment when using the multi-cloud environments.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," 2010 IEEE Second International Conference on Cloud Computing Technology and Science, 2010.

[2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, 2020.

[3] J. Kindervag, "Build security into your network's DNA: The zero trust network architecture," Forrester Research, 2010.

[4] MITRE Corporation, "MITRE ATT&CK Framework," 2023. [Online]. Available: https://attack.mitre.org/

[5] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Computer Networks, vol. 51, no. 12, pp. 3448–3470, 2007.

[6] M. A. Ferrag, L. Maglaras, A. Ahmim, et al., "Deep learning for cybersecurity intrusion detection: Approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 50, 2020

[7] R. Sandhu and S. Samarati, "Access control: Principle and practice," IEEE Communications Magazine, vol. 32, no. 9, pp. 40–48, 1994.

[8] D. Ferraiolo, D. Kuhn, and R. Chandramouli, Role-Based Access Control, Artech House, 2003.

[9] J. Park and R. Sandhu, "The UCONABC usage control model," ACM Transactions on Information and System Security, vol. 7, no. 1, pp. 128–174, 2004.

[10] E. Yuan and J. Tong, "Attributed based access control (ABAC) for web services," IEEE International Conference on Web Services, 2005.

[11] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems," NIST SP 800-94, 2007.

[12] W. Wang et al., "HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection," IEEE Access, vol. 6, 2018.

[13] M. Eberle and J. Holder, "Insider threat detection using graph-based approaches," Cybersecurity Applications & Technology Conference, 2009.

[14] H. Xu and X. Zhang, "Adaptive access control using reinforcement learning," Computers & Security, vol. 92, 2020.

[15] R. McGraw, "Risk-adaptive access control (RAdAC)," NIST Workshop on Attribute Based Access Control, 2010.

[16] P. Ammann, D. Wijesekera, and S. Kaushik, "Scalable, graph-based network vulnerability analysis," ACM CCS, 2002.

[17] M. Albanese et al., "Attack graph generation and analysis," ACM Transactions on Information and System Security, vol. 14, no. 1, 2011.

[18] E. Hutchins, M. Cloppert, and R. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns," Leading Issues in Information Warfare & Security Research, 2011.