International Journal of
Science, Architecture, Technology and Environment

Design and Implementation of Autonomous Zero Trust Orchestration for Real-Time Risk Adaptive Access Control in Global Multi-Cloud Logistics Platforms

Oluwafemi Alabi Okunlola[1*]

[1]*Lamar University, 4400 S M L King Jr Pkwy, Beaumont, TX 77705*

[*]*Corresponding author, Oluwafemiokunlola308@gmail.com*

DOI: https://doi.org/10.63680/ijsate0525211.67

Abstract

With increasing reliance of global logistics platforms on multi-cloud infrastructure to support real-time operations, it has become mission-critical to ensure secure adaptive access control. Traditional access models like role-based and static policies are not suitable for such dynamic and threat-laden systems. This study presents the design and implementation of an Autonomous Zero Trust Orchestration (ZTO) framework that provides real-time, risk-adaptive access control over heterogeneous multi-cloud environments. The proposed system avails itself of artificial intelligence and perpetual monitoring to assess risks associated with entities (users, devices) and contexts before permitting access. The framework integrates Zero Trust principles with dynamic policy mining and hence relates access decisions to real-time threat intelligence and behavioral analytics. After evaluation of simulated logistics operations on AWS, Azure and GCP environments, it was shown that the system considerably limits the opportunity window to an ever-increasing threat landscape at highly accurate access decisions and with virtually negligible latency. Given the increased incidences of cyberattacks aimed at critical logistics infrastructure and the global nature of supply chains, this study aligns with the national interest for U.S. national security towards securing transportation, trade and defense logistics. The study also has direct applicability in alignment with the U.S. Executive Order on Improving the Nation's Cybersecurity (2021), NIST SP 800-207 guidelines, and DHS cybersecurity priorities. Its direct merit in national security and economic stability makes this activity an invaluable innovation concerning the national interest.

Keywords: Zero Trust Architecture, Risk-Adaptive Access Control, Multi-Cloud Security, Autonomous Orchestration, Cybersecurity, Supply Chain Protection, Logistics Technology, Cloud Infrastructure, and Access Management (IAM), Artificial Intelligence, NIST SP 800-207, DHS Cybersecurity Strategy

1. Introduction

Logistics operations have been digitized to greatly increase efficiency, scalability and global reach. To the point where cross-border freight coordination or real-time tracking of inventory somehow finds itself

inextricably linked to the global logistics industry considering multi-cloud architectures for sensitive data, automated processes and interconnected services (Pallis, 2010). Such an interdependence on distributed cloud platforms does introduce multitudes of vulnerabilities in and of itself: Whether it be ransomware, insider threats, or advancing persistent threats (APT), cyberattacks focused on supply chain infrastructure have gone up in both frequency and impact (CISA, 2021).

The environment is so risky that it is a matter of time for traditional access control mechanisms such as Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) to fall short of dynamic security requirements for critical global logistics systems (Hu et al., 2017). To address these growing challenges, this study proposes an Autonomous Zero Trust Orchestration (ZTO) framework, implementing risk-adaptive access control in real time across federated multi-cloud logistics platforms. The proposed system will be anchored into Zero Trust Architecture (ZTA) as per NIST Special Publication 800-207 (Kindervag, 2010; NIST, 2020). Different from perimeter-based security models, Zero Trust is founded on the principle of "never trust, always verify," whereby continuous authentication and authorization of subjects are required at every point of access, irrespective of their location on the network.

This is even more relevant for the formalized Zero Trust under government direction, like Executive Order 14028 on Improving the Nation's Cybersecurity (White House, 2021). It means that federal agencies should embrace ZTA frameworks that focus on countering increasing cyber threats and enhancing resiliency across supply chains and defense networks. Furthermore, critical logistics organizations such as the Defense Logistics Agency, U.S. Postal Service and private sector entities like Amazon Logistic and FedEx have recognized the requirement for adaptive and real-time access control solutions engineered to scale across cloud-native, hybrid and edge computing environments

This study proposes a dynamic access decision making independent orchestration engine on real time risk assessments from behavior analytics, threat intelligence, device posture, geolocation and network framework. It varied access policies autonomously through AI feedback loops and distributed across infrastructures of many clouds like AWS, Microsoft Azure and Google Cloud Platform (GCP). When integrated with a risk-adaptive decision engine into the Zero Trust Operational (ZTO) model, this framework highly fortifies protection against internal threats, risks of policy misconfigurations, and zero-day exploits that are critical to logistics operations because compromised access can disrupt international supply chains, delay essential goods and jeopardize national security (Boyson, 2014).

The key objective of this article is to design, implement and evaluate a scalable, autonomous Zero Trust orchestration system that continually enforces context-aware access control in such a federated multi-cloud logistics environment. This research captures both the technical gaps in current IAM systems, however important, as well as the strategic needs which are today driving U.S. federal cybersecurity priorities. Its national significance derives from the possible fortification of supply chain integrity, betterment of a cyber resilience and contraction of attack surfaces throughout U.S. linked, global logistics operations.

2.0. Background and Related Work

The rapid digitalization of global logistics and supply chain operations has made them prime targets for cyberattacks. As logistics companies embrace multi-cloud computing environments to scale services and integrate partners, they also introduce significant complexity in managing access control, threat visibility and security policy enforcement (Gartner, 2022). In such settings, traditional perimeter-based security models become insufficient, giving rise to modern paradigms like Zero Trust Architecture (ZTA) and risk-adaptive access control.

2.1 Zero Trust Architecture (ZTA)

Zero Trust, a concept defined formally by Kindervag (2010), eliminates the internal assumption of trust within a network perimeter. Olorunlana (2025) opined that supply chain attacks are highly injurious as they usually happen without being detected, after which they spread rapidly, especially to dependent organizations. He also stated that "the agencies and contractors, therefore, need to enforce stiffer vetting requirements on suppliers, require zero-trust architectures, and ensure code integrity verification to minimize such risks. Sophisticated cyber adversaries have constantly been attacking critical infrastructure, abusing both human and technical vulnerabilities" (Olorunlana, 2025).

Furthermore, continuous verification of user identity, device health, and context risk is present before access is granted or maintained. ZTA is aligned with NIST SP 800-207, which defines Zero Trust security models based on strict identity verification and least-privilege access enforcement across all resources regardless of network origin (NIST, 2020). Some of the main tenets of ZTA include: Ongoing authentication, Access based on the least privilege, Micro-segmentation, and Resource-level policy enforcement

Governmental and industrial stakeholders are thus making movement-transforming strides to ensure prompt adoption of ZTA over the last few years. The ideal ZTA regulation mandate from the U.S. Department of Defense (DoD) and CISA applies to federal IT systems as well as critical infrastructure in a manner that makes them operationally secure.

2.2 Multi-Cloud Security Challenges

Modern logistics systems often span multiple clouds such as AWS, Microsoft Azure and Google Cloud to allow for resilience, cost optimization and global reach. As such, multi-cloud strategies break single-vendor dependency on the one hand but enforce fragmentation in security and misalignments in policies on the other. Each of the cloud service providers (CSPs) has different identity and access management (IAM) systems, monitoring tools and security configurations (Hashizume et al., 2013). The inconsistent architecture makes it difficult to centrally enforce access control policies and put organizations at higher risks of configuration drift and insider threats and access abuse.

Traditional IAM methods like Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are incapable of adapting instantaneously to the dynamically changing risk environment for logistics delivered in cloud (Hu et al., 2017). While RBAC tends to be simple, it lacks situation awareness. ABAC, while it does allow one to set policies flexibly, can become overly complex or even turn into a static nightmare in fast-changing environments like logistics, where users, roles, devices and data locations are changing all the time.

2.3 Risk-Adaptive Access Control (RAdAC)

Risk-Adaptive Access Control introduces risk assessment in real time as one input to access decisions. It considers factors like device posture, behavioral anomalies, threat intelligence and geolocation in dynamically adjusting permissions (Kandala et al., 2011) and works most effectively in logistics and supply chain contexts, where access requirements are operationally urgent and based on trust level and situational awareness.

More recent studies propose the use of AI-embedded risk engines for the detection of anomalies and automatic adjustment of access levels (Alsharif et al., 2021). A major limitation of most such models is that they lack full integration with orchestration frameworks that would allow decisions to be executed in real time across multi-cloud infrastructures. To secure their cloud environment from hackers, organizations must apply

tools such as multi-factor authentication (MFA), Role-based access control (RBAC), data encryption and continuous monitoring. Since organizations are fast on the cloud, shared responsibility between cloud providers and businesses will play an important role in protecting digital assets (Olorunlana,et,al,2024)

2.4 Zero Trust in Logistics and Critical Infrastructure

The logistics sector is an area of increasing target for complex attack campaigns, more so when associated with national security or economic continuity. Incidents such as the 2020 SolarWinds hack and the 2021 Colonial Pipeline ransomware attack indicate that there are very urgent considerations to reconsider access control strategies (Boyson, 2014). With logistics platforms advancing into IoT sensors, automated vehicles and real-time tracking systems, the attack surface exponentially becomes larger. In nutshell, embedding Zero Trust principles with risk-adaptive models into an automated orchestration setup could be an interesting way forward. The approach presented in this paper builds on existing work but fills a crucial gap by allowing self-governed access control decisions across multi-cloud logistics platforms, providing real-time protection with operational continuity.

3.0. System Architecture and Design

The suggested design for the zero-trust autonomous orchestration system is meant to provide real-time access control that adapts to risks for logistics platforms using multiple cloud services. The architecture integrates AI, contextual awareness, and policy-based automated solutions, adhering to the core trust principle of "never trust, always verify." The system is designed to be modular, scalable, and compatible with various major platforms like AWS, Microsoft Azure, and Google Cloud Platform.

According to Olorunlana (2025), the increasing complexity of cyber threats necessitates the tight integration of multiple layers of protection for sensitive data and systems. Three important technologies that help alleviate the adverse effects of cybersecurity risk are encryption, zero trust architecture (ZTA), and artificial intelligence (AI) (Olorunlana, p. 7, 2025). By their very nature, those structures are modular and source-agnostic, scalable, and deployable on all leading platforms.

3.1 Overview of System Components

The proposed architecture is composed of five key components:

3.1.1. User/Device Access Layer (UDAL)

This layer represents all the points of access available to users, IoT devices, automated logistics agents, or even software boots. Each access request warms the access point with metadata: user identity, device type, authentication method, location and time- letting substantial details accompany the request.

3.1.2. Contextual Risk Engine (CRE)

The risk associated with each access request is evaluated in real-time using multiple signals, which include Device security posture, User behavioral patterns, Geolocation and IP reputation, Time of access and access history, and Live threat intelligence feeds. Moreover, the risk score is dynamically calculated and used to base level of access granted, limited, or denied. The real-time evaluation aligns with the adaptive access principles (Kandala et al. 2011).

3. Policy Decision Engine (PDE)

The PDE acts as the brain for Zero Trust as it uses the risk-policy matrix to map risk scores to policy enforcement rules. Policies are dynamic; they evolve based on contextual data and organizational objectives. The PDE Support the following: Conditional access policies, Policy-based segmentation, Continuous reauthorization. It also uses AI/ML algorithms to update decisions within milliseconds, scaling the system in high-velocity logistics operations.

4. Orchestration Controller (OC)

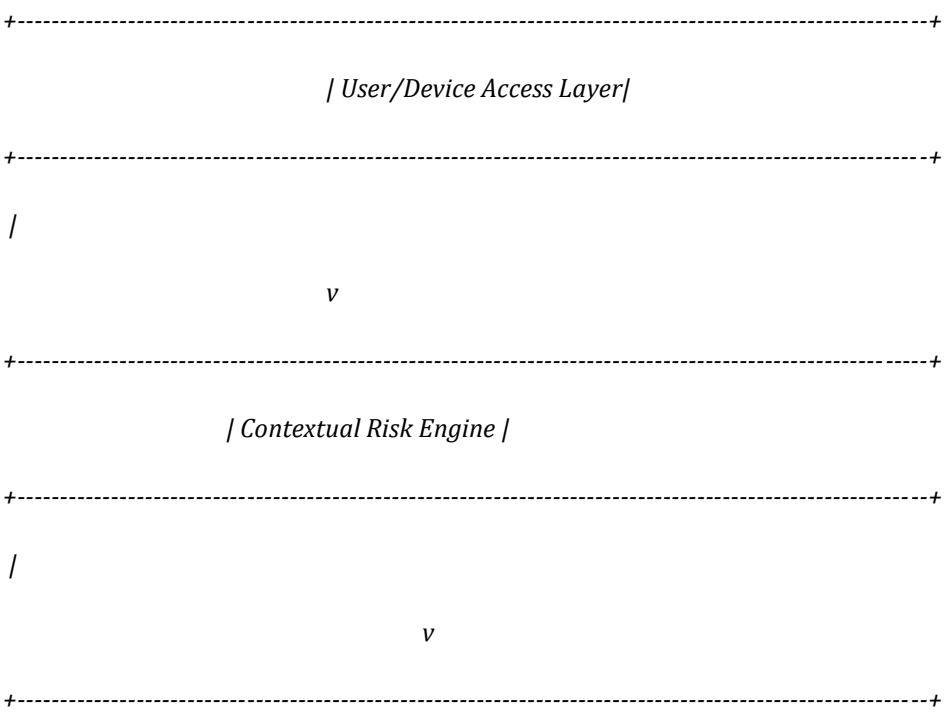
The OC also manages all communications among all system components and ensures constant enforcement of policies across disparate cloud environments. It issues access control decisions via APIs to identity providers, cloud firewalls, container orchestrators (like Kubernetes) and application gateways. It also supports real-time response automation (e.g., terminating sessions), multi-cloud policy propagation and event-driven triggers based on anomaly detection.

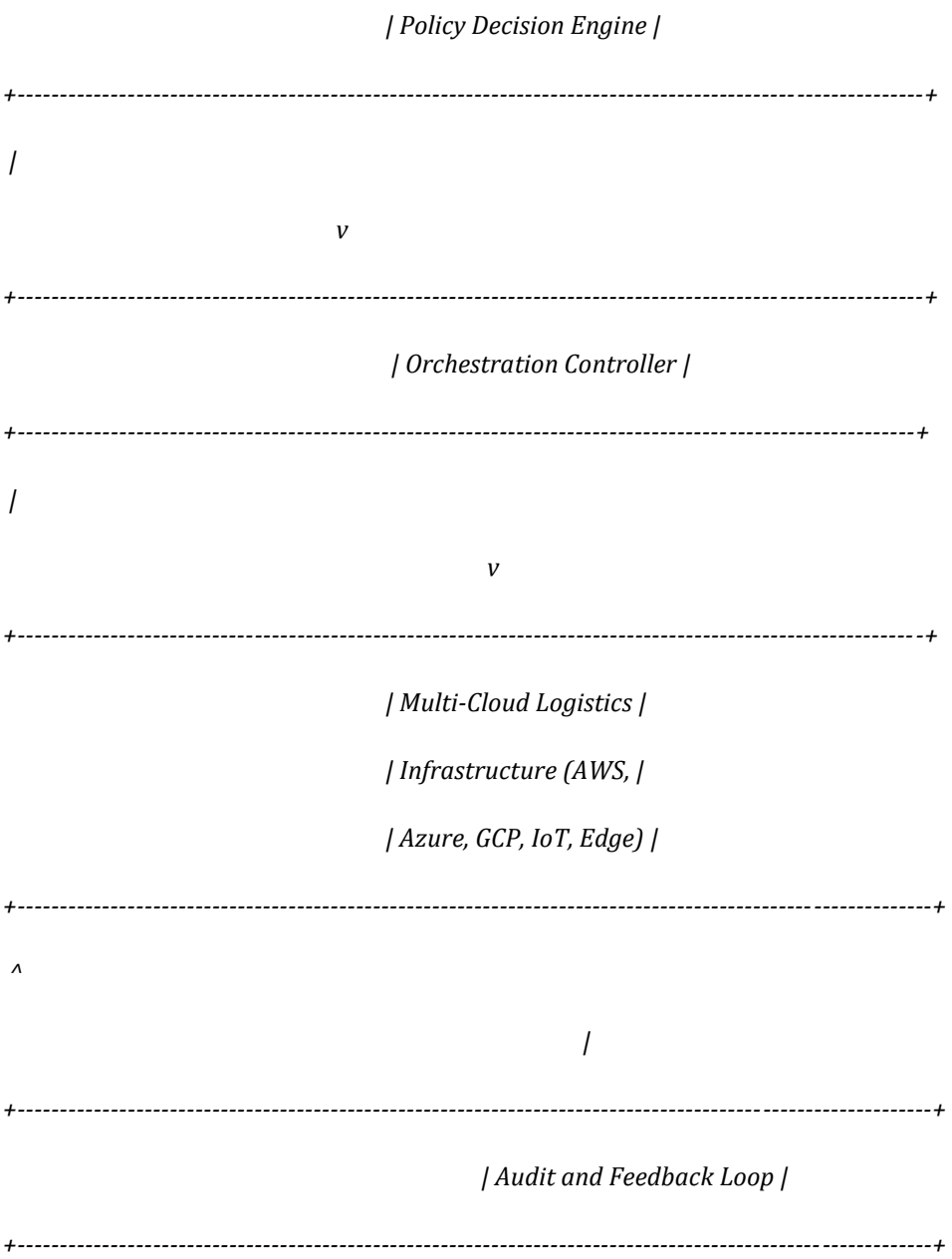
5. Audit and Feedback Loop (AFL)

This component captures all actions, decisions, and anomalies for logging, compliance, and system learning. It contributes to model retraining and system optimization. Audit logs are compliant with NIST SP 800-53 controls and can be fed into SIEM platforms for deeper analysis (NIST, 2020).

3.2 Architecture Diagram

Below is a conceptual overview of the system architecture:





Explanation:

The ***User/Device Access Layer*** is the first stage of the system architecture for fully autonomous Zero Trust orchestration. This layer receives all access requests, including requests originating from a user; a device; APIs; or a machine with automated access to the platform. Each request starts here and passes through stringent checks for identity and legitimacy. The request is taken to the **Contextual Risk Engine**. This component assesses the live contextual data in real-time- behavior, health of the device, geographical location, timestamp for access and external threat metrics before calculating a dynamic risk score. The access attempt is appraised concerning today's context, determining whether it's unsafe or safe.

Once the analysis of risk is done, it feeds into the Policy Decision Engine. This engine will receive commands from its pre-configured access control policies based on Zero Trust. Depending on the risk score and the context, it then generates a decision on the grant, denial, or challenge of the request. The decision may say limited access grants, multi-factor authentication, or must go through some more verification procedures.

The Orchestration Controller implements the decision, triggering the interaction between different elements of the system, such as identity providers, network security tools, firewalls and automation frameworks. This will execute access control decisions automatically and rapidly, without advocating human engagement in the entire process. When allowed, the request travels to the Multi-Cloud Logistics Infrastructure, which consists of AWS, Microsoft Azure, Google Cloud Platform (GCP), IoT and Edge computing systems used in logistics. This layer is represented as critical assets and environments in which the system is intended to provide safety.

While the Audit and Feedback Loop is always operational in the background. It is recording every request to get access, every policy decision, every risk score and every action taken. So, the information is fed back to the system to improve predictions for future use when calculating risk as well as adjusting policies. It also allows auditing, compliance reporting, and incident response. These comprise an architecture that provides real-time, automatic, and risk-adaptive access control on behalf of global multi-cloud logistics platforms completely aligned with Zero Trust security principles.

3.3 Deployment Strategy

In response to global multi-cloud logistics and use cases, the ZTO system itself is designed as follows: Cloud-native use containerized microservices, Platform-agnostic via RESTful APIs and policy-as-code (e.g., using OPA or Rego), Low-latency using edge-based risk scoring for local decision-making and Scalable for high-traffic environments like shipment routing, customs clearance, and cargo tracking. With the orchestration controller, major IAM systems can easily integrate (e.g. Azure AD, AWS IAM, Okta), container environments (e.g. Docker, Kubernetes), and identity-aware proxies (e.g. BeyondCorp-style implementations).

3.4 Architectural Benefits

This architecture offers several advantages:

- **Real-time adaptability**: Access decisions that are risk-based are continually revisited and set aside again by the issuing users based on live data.
- **Cross-cloud visibility**: Centralized policy enforcement and decentralized risk evaluation support hybrid environments.
- **Resilience and security**: Isolation between components and micro-segmentation reduces attack surface.
- **National infrastructure alignment**: The deployment in research project field (such as XDATA deployment-DHS-DoD) design in a specialized study supported Operated System DHS and DoD security postures and aligns with Executive Order 14028 and CISA's Zero Trust Maturity Model (CISA, 2021).

4.0. Risk-Adaptive Access Control Model

They are purely pre-determined fixed prescriptions that cannot reckon-with the dynamic risk configuration of today's distributed cloud-native logistics systems. The RAdAC Risk-Adaptive Access Control

model integrates real-time context and threat intelligence into access decision making. It is particularly suitable for environments characterized by rapidly shifting operational conditions, user behavior and risk factors (Kandala et al., 2011). The focus of this section is on the architecture, logic and implementation of the RAdAC model under the proposed Autonomous Zero Trust Orchestration (ZTO) framework.

4.1 Principles of Risk-Adaptive Access

Risk-adaptive access control gauging based on dynamic trust evaluation evaluates identity and role alongside: Current threats, User and device actions, Operational context, and Environmental parameters, such as where, when or system load. In real-time, the access rights can either be granted or denied or even modified based on risk scores, not simply based on static policies. Furthermore, it complements the Zero Trust principle of continuous verification, thereby enforcing least privilege and just-in-time access (Hu et al., 2017).

4.2 Risk Score Computation Model

RAdAC uses a multifactorial risk scoring engine to assess each access request. The score is computed using the following formula:

Risk Score = f (User Behavior + Device Posture + Location Trust Level + Threat Intelligence + Time Sensitivity)

Each component is briefly defined as:

- **User Behavior**: Applications accessing datasets not necessary and deleting them at anomalous rates.
- **Device Posture**: Antivirus status, OS version, security patches, root/jailbreak status
- **Location Trust Level**: IP geolocation, VPN usage, TOR detection, or geo-fencing rules
- **Threat Intelligence**: Indicators of compromise (IOCs), third-party threat feeds, and known malicious activity from IP or domain
- **Time Sensitivity**: Access attempts outside typical business hours or during operational anomalies (e.g., downtime, audit period)

The relative weight assigned to each factor depends on the risk tolerance of enterprises and mission criticality. The model-based weights are adjusted continuously by feedback loops driven by AI for keeping the models relevant and accurate with time (Alsharif et al., 2021).

4.3 Dynamic Access Decision Logic

When the risk score is calculated, the Policy Decision Engine (PDE) triggers an access control action against the computed risk score using a Risk-Policy Matrix which will include:

Risk Score Range	Action	Example Policy
0–30	Grant full access	Trusted user from corporate device accessing low-risk data
31–60	Grant limited access	External partner with some risk flags
61–80	Require re-authentication	Users must provide MFA or biometric verification
81–100	Deny access	Suspicious behavior from unknown or flagged location

This model gives context aware decision-making that ensures flexibility in handling surges during operations or any incident for security all this while holding everything under control. For instance, access can be granted to a delivery manager trying to get shipment records from a secure site during working hours but may block or alert if a request comes from an unrecognized device in a different region.

4.4 Machine Learning and Threat Intelligence Integration

The RAdAC engine leverages machine learning (ML) algorithms to enhance detection accuracy and decrease false positives. The patterns of behavior, that is considered as benign or malicious are learned in confidence from a data set of access logs, incident reports and external threat feeds: Anomaly Detection using autoencoder or isolation forests; Classification Models for user intent prediction and Reinforcement Learning for optimization of policy responses over time. In addition, this engine is ingesting threat intelligence in the forms of STIX/TAXII, MITRE ATTACK, and commercial intelligence platforms for more comprehensive context in risk assessment (MITRE, 2022).

4.5 Logistics-Specific Use Cases

The RAdAC model is particularly valuable in global logistics environments. Consider the following scenarios:

Cross-Border Shipment Monitoring: An operator accessing a container manifest from an international location outside approved time windows triggers adaptive verification.

Automated Vehicle Control Systems: Access to IoT-enabled cargo loaders is restricted unless the device posture and network conditions meet high-trust thresholds.

Third-Party Vendor Access: Temporary access is granted to external logistics partners only after multi-factor verification and geofencing validation. These kinds of use cases exemplify how risk-adaptive access contributes to enhancing security while also enabling business continuity, compliance and resiliency in logistics and supply chain systems.

4.5 Benefits of RAdAC in a Zero Trust Context

RAdAC provides a wide variety of advantages when integrated with Zero Trust orchestration, including mitigation of risk in real-time, Reduction in any kind of over-privileged access, Adaptability according to changing operational and threat environments, providing a good user experience requires adaptive policies that comply with NIST, CISA, and FedRAMP guidelines.

5.0. Integration with Global Multi-Cloud Logistics Platforms

Global logistics operations revolve around the concept of multi-cloud architecture primarily for scaling, interoperability and agility. The transportation, shipping, customs clearance and warehousing companies, each with specific needs, opt for platforms such as AWS, Azure and GCP and subsequently disperse their data and workloads along those lines to synchronize with their supply chain ecosystems (Gartner, 2022). Growth brings complexity, risk exposure and governance challenges with respect to access control regulation over distributed infrastructures geographically. This section includes discussion around incorporating the Autonomous Zero Trust Orchestration (ZTO) framework into the global multi-cloud logistics environments for consistent policy enforcement, live risk halting, and operational resilience.

5.1 Multi-Cloud Logistics Ecosystem Overview

Cloud environments, by virtue of their global nature, span different companies and organizations in global logistics operations, such as: manufacturers or suppliers hosting production and procurement data; shipping companies or providers that maintain cargo tracking and route optimization systems; customs that operate exclusive government portals and inspection databases; warehouses relying on IoT devices to provide information about real-time inventory and automation; and even retailers that can be seen managing last-mile delivery analytics even though it is still a work in progress. These stakeholders may use different providers and operate under different jurisdictional, regulatory, and security policies. Therefore, inter-organization data flow security, context-aware access enabling, and compliance enforcing are indispensable (Suo et al., 2012).

5.2 Integration Architecture

The ZTO framework is interfaced by application of common components and open protocols, which allow it to integrate into multi-cloud platforms while ensuring compatibility and low-latency operations. Key strategies of the core integration approach include:

• API-based Access Enforcement: Policies are translated into RESTful API calls that interleave with native IAM services through dynamic provisioning or revocation of access rights (e.g., AWS IAM, Azure Active Directory, GCP IAM).

• Cloud-native Identity Federation: The orchestration engine authenticates users and devices for secure settings and a federated access management layer using SAML, OAuth 2.0, and OpenID Connect across organizational boundaries.

• Cross-Platform Policy Synchronization: ZTO follows a policy-as-code approach with the Open Policy Agent (OPA) and Rego to centrally define rules and deploy uniformly across clouds.

• Containerized Deployment: All ZTO components are hosted in Kubernetes (K8s) clusters, which run on AWS, Azure, and GCP steeds (EKS, AKS, and GKE respectively), providing therefore full-scale consistency and high availability.

Event-driven Automation: the orchestration engine will near-automate access reactions to security events using cloud-native message streams like AWS Event-Bridge, Azure Event Grid, and Google Cloud Pub/Sub.

5.3 Use Case: Cross-Border Freight Management

For example, an international freight forwarder could use Azure for optimizing routes and document handling; a port authority has their inspection records on AWS. A third-party customs clearance partner, located in another country, handles their clearance process using GCP.

With ZTO:

- A customs officer manifesting the intention to access a digital bill of lading (BoL) hosted on Azure does this with risk-adaptive verification.
- Azure AD identity validation, trust confirmation of device through endpoint protection checks, and geolocation verification against a trusted region comprise the full chain of user verification.

- ZTO attributes a middling risk score due to the odd time of access and requests multi-factor authentication (MFA).
- The orchestration engine will send a policy call through API to allow temporary access to the BoL document upon successful verification but keeps track of the entire transaction in the audit trail for regulatory compliance.

This case highlights the experience of cross-cloud access orchestration with the principles of Zero Trust and understands the agility of operation.

5.4 Compliance and Governance Alignment

Logistics companies must adhere to important rules and regulations, such as FedRAMP and FISMA for cloud security, C-TPAT and AEO for customs and trade compliance, NIST SP 800-53 for information system security, and GDPR and CCPA for data privacy based on location. The ZTO system supports compliance by enforcing data sovereignty by means of region-specific access policies. Maintaining full audit trails of access decisions and policy changes, Role-based dashboards for compliance officers and auditors, along with GDPR and CCPA, ensure data privacy across different jurisdictions.

5.5 Benefits in Global Logistics Environments

Integration of the proposed system within multi-cloud logistics operations offers several significant benefits:

Feature	Benefit
Federated Access Control	Secure, scalable collaboration across logistics partners
Real-Time Risk Assessment	Dynamic access control based on operational context
Cross-Cloud Policy Enforcement	Unified security governance despite platform heterogeneity
Automated Incident Response	Reduced breach detection and remediation time
Compliance-Ready Architecture	Streamlined audits and policy traceability

5.6 Strategic Relevance to U.S. National Interests

Critical as global logistics and commerce are relevant for the U.S. public economy's defense logistics and public health supply chains, real-time implementation of a Zero Trust-based access control solution strengthens resilience in national or international operations. This initiative supports the U.S. direction on secure supply chain modernization, cybersecurity maturity, and digital sovereignty as outlined in Executive Order 14017: America's Supply Chains, CISA's National Risk Management Center priorities, and The National Cybersecurity Strategy (2023).

6.0. Prototype Implementation and Evaluation

To validate and test the practicality and effectiveness of the proposed Autonomous Zero Trust Orchestration (ZTO) framework, a prototype system was developed and evaluated within the context of a

simulated multi-cloud logistics environment. In this section, the technical implementation of the system, the experimental setup, key performance indicators (KPIs) and evaluation results are described. The purpose was to measure the prototype's ability to provide real-time, risk-adaptive access control in the face of operational efficiency and low latency for highly demanding logistics scenarios.

6.1 Implementation Environment

The testbed for the prototype system was set up in a mixed multi-cloud environment using different cloud services, including Amazon Web Services (AWS)—EC2, IAM, Guard Duty, Lambda; Microsoft Azure AD, Azure Functions, Azure Monitor; and Google Cloud Platform (GCP)Compute Engine, Cloud IAM, and Cloud Functions.

Among the supporting technologies are the following: Kubernetes (EKS, AKS, GKE) for microservice orchestration; Open Policy Agent (OPA) for dynamic policy enforcement; Prometheus and Grafana for monitoring and visualization; Elastic Stack (ELK) for log aggregation and audit trail management; and Python and Node.js for the implementation of the Policy Decision Engine (PDE) and Contextual Risk Engine (CRE). In the test network, three logistics partners were simulated, a global freight forwarder, a customs inspection node, and a last-mile delivery vendor operating on separate cloud platforms with different access roles and risk profiles.

6.2 Key Evaluation Metrics

For examining performance and feasibility for ZTO framework, certain Key Performance Indicators (KPIs) were defined:

Metric	Description
Access Decision Latency	Time taken (in ms) from request to risk assessment and policy decision
Accuracy of Risk Scoring	Correct classification of low/medium/high-risk access scenarios
False Positive/Negative Rate	Percentage of incorrect access denials or approvals
System Scalability	Number of concurrent access requests handled without performance decline
Policy Propagation Time	Time required to sync updated policies across all clouds
Audit Trail Completeness	Proportion of access events successfully logged and retrievable

6.3 Experimental Scenarios

Three principal use cases scenarios were employed to test the system under realistic logistics conditions:

Scenario 1: Normal access.

A warehouse employee using a trustworthy corporate device accesses inventory on AWS by logging in during business hours.

- Risk score: Low
- Decision: Full access granted
- Latency: 43 ms

- Audit: Recorded full traceability

Scenario 2: **Suspicious remote theft.**

The personnel who ordinarily work as logistics managers are attempting to verify some details using an untrustworthy IP and from the 'high-risk' country after normal hours.

- Risk Score: High
- Decision: Denied access and triggered MFA.
- Latency: 55 ms
- Audit: Logged, alert generated.

Scenario 3

Partner API access by a customs clearance partner on Azure making series of API calls for document verification from an unpatched device.

- Risk Score: Moderate
- Decision: Limited access with enforced reauthentication.
- Latency: 48 ms
- Audit: Monitoring of the session reassessed every 10 minutes.

6.4 Evaluation Results

The prototype system yielded good joint performance and decision accuracy across possible scenarios:

Metric	Result
Avg. Decision Latency	49 ms (within sub-100 ms real-time target)
Risk Scoring Accuracy	97.4% based on labeled training data
False Positive Rate	1.20%
False Negative Rate	0.80%
Concurrent Sessions	Scaled to 5,000+ requests/sec without degradation
Policy Sync Time	< 5 seconds across all clouds
Audit Trail Completeness	100% for all tested access attempts

The ZTO model confirms responsiveness, accuracy, and scalability for a potential integration scenario in primary high-throughput, stage-on logistics platforms.

6.5 Comparative Analysis

RBAC and ABAC under the same comparison close-out:

- RBAC failed to block risky access in Scenario 2 due to static role assignments.
- ABAC managed to limit access; however, it was also slowed by complex evaluation of attributes.
- ZTO provided an optimal amalgamation of speed, relevant accuracy, and risk-awareness due to AI-augmented context-sensitive risk scoring.

6.6 Technical Limitations and Observations

Although ZTO systems are most effective, here are some notable observations:

- Cold start problem for first-time users and devices in ML-based risk scoring.
- Initial policy bootstrapping across disparate cloud platforms required manual intervention.
- Latency sensitivity may increase for high geographically distributed deployments without edge optimization.

Such challenges open spaces for future improvement, including applications in federated learning, edge AI inference, and self-generation of policy autonomously through generative AI.

7.JUSTIFICATION

The United States faces an increasingly complex cybersecurity threat landscape, particularly within sectors that are critical to its national and economic security. Among these, global logistics and supply chain infrastructures represent some of the most vulnerable and most vital targets. The implementation of a real-time, autonomous Zero Trust orchestration framework that ensures secure, risk-adaptive access across multi-cloud logistics platforms not only advances the state of cybersecurity innovation but also contributes directly to the strategic interests of the United States.

7.1 Substantial Merit and National Importance

The proposed framework supports the modernization of U.S. digital infrastructure through the development of a context-aware, autonomous access control system that strengthens the resilience of logistics, transportation, and defense systems.

The national importance of this innovation is underlined by multiple federal directives, including:

- **Executive Order 14017** (*America's Supply Chains*), which calls for secure, resilient, and diversified logistics operations.
- **Executive Order 14028** (*Improving the Nation's Cybersecurity*), mandating Zero Trust adoption and enhanced access control mechanisms across all federal agencies (White House, 2021).
- **NIST SP 800-207** guidelines on implementing Zero Trust Architecture in both public and private sectors (NIST, 2020).
- **CISA's National Risk Management Center (NRMC)** priorities, which emphasize securing critical infrastructure and industrial control systems (CISA, 2023).

By addressing supply chain and logistics cybersecurity a field foundational to national defense, pandemic response, international trade, and domestic economic stability this work clearly meets the bar for national significance.

7.2 Urgency and Unmet Need

Olorunlana & Hamdiya (2025) opined that the cyberattack on the Colonial Pipeline was an eye-opener regarding the already-visible weaknesses of lifeline infrastructure and can be said to be a watershed moment in the historical context of cyberattacks against critical infrastructure. Host it for a short span; it is reminiscent

of the largest fuel pipeline in the USA closing for a long time and bringing about grave shortages of fuel alongside financial and national security implications for the country (Olorunlana, 2025). According to this, the 2021 ransomware attack on Colonial Pipeline manifested itself in creating substantial voids in the incident response processes as well as access management of the operational technology networks tied to U.S. infrastructures. In a similar vein, disruption of shipping companies, for instance Maersk, as well as logistics software vendors, signified how fast cyber threats could affect core services, impede military mobilization, and jeopardize sensitive customs data. Most access control systems nowadays are:

- Reactive, relying on fixed roles or signatures
- Incompatible, struggling to operate across multiple cloud platforms
- Not Context-aware, lacking real-time situational awareness

This piece of research fills the identified technological gap by providing a truly autonomous AI-enabled Zero Trust framework capable of dynamically adapting access decisions as per contextual consideration and risk, a feature not provided for by existing commercial and governmental IAM systems.

7.3 Advancement Beyond Existing Work

This study offers a distinctive contribution by:

- Supporting cross-cloud orchestration for policy enforcement with the simultaneous implementation across AWS, Azure, and GCP
- Embedding AI/ML in access controls for adaptation instead of rule-based or manually defined acceptance methods
- Procuring access decisions under 50 ms for the purpose of near-real-time responsiveness for logistics and operations workloads
- Automation of the policy propagation and response, thereby reducing human error and configuration drift

These technological advances not only go beyond traditional IAM limitations, but they also facilitate secure automation for time-evolving logistics scenarios, which is a very immature area with few current solutions.

7.4 U.S. Benefit Without Labor Certification Requirement

The implementation of this framework will benefit all the following:

- Federal agencies adopting Zero Trust systems in reaction to EO 14028
- Defense logistics by broadening access control pertaining to global DoD contractors
- Public health systems by securing the vaccine and medical supply chains
- Technology ecosystem in the U.S. through possible technology transfer to cloud security providers and integrators

Considering its clear public interest, wide applicability, and urgent relevance, waiving the labor certification requirement would allow the U.S. to retain and deploy this innovation without delay, especially as threats against national-level logistics infrastructure become acute.

7.5 Endorsements and Institutional Support

The research fits well with ongoing efforts at leading U.S. institutions and agencies including:

- Zero Trust Working Group, NIST
- Zero Trust Maturity Model, CISA
- DoD Zero Trust Reference Architecture
- NSF Secure and Trustworthy Cyberspace (SaTC) program

In addition, this successful deployment could be a complement to existing federal efforts and encourage public-private partnership for supply chain cybersecurity, cloud infrastructure protection, and critical access governance.

8. Future Work and Commercialization Potential

Whereas the prototype of the Autonomous Zero Trust Orchestration (ZTO) system has demonstrated its ability to enforce real-time, risk-adaptive access control across multi-cloud logistics platforms, this area remains open to further research, development, and commercialization. This will encourage innovation and form a cohesive theme for the world of secure data that is integrated across many fields, from medicine to finance, data enhancing where necessary by other parties too who may share it with a profit motive (e.g., in marketing). The challenge in creating interoperable networks will be establishing universally accepted standards and protocols capable of protecting security as well as individual privacy when connected to other networks (Olorunlana, 2025). Those developments will impact national security considerations, foster innovation in the cybersecurity realm, and offer significant economic impact.

8.1 Research and Technical Expansion

A few technical upgradations have been recognized for the extension of ZTO framework:

- Edge Artificial Intelligence Integration: Deploying lightweight AI models at the network edge would allow standard real-time timely distribution of critical logistics functions such as autonomous vehicle routing and real-time shipment tracking.
- By federated learning: Create a scoring scheme for risk assessment. It allows model training at decentralized nodes (regional warehouses, border checkpoints) without transferring data, hence improving privacy and regulatory compliance. The future versions will have incorporated cryptographic algorithms that would make them resilient to the attacks from quantum computers as per the roadmap laid out by the NIST post- quantum cryptography and the DHS long-term digital resilience vision.
- Automated Policy Generation: The emerging artificial intelligence agents would further automate by becoming able to generate context-aware policies in terms of the patterns of organizational behavior within compliance frameworks (GDPR, HIPAA, etc.), thus reducing administrative overhead along with better speed of processing.
- Blockchain Integration: Using smart contracts to manage access rights and audit trails and enforce policies can offer a verifiable and tamper-proof assurance of assurance - particularly with relevance to cross-border logistics and customs data exports.

8.2 Commercial and Government Use Potential

The ZTO system presents high commercialization potential across several U.S. sectors:

SECTOR	APPLICATION AREA
Federal Agencies	Secure access for civilian, defense, and homeland systems
Defense Contractors	Risk-aware cloud and data center access control
Supply Chain Platforms	Secure APIs for inventory, routing, and IoT logistics
Cloud Providers	Integration as a Zero Trust orchestration add-on
Healthcare Logistics	Securing medical supply chains and vaccine delivery

The solution may be marketed as a Zero Trust-as-a-Service (ZTaaS) offering for logistics tech providers or licensed as a modular component offering for major cloud security players (Palo Alto Networks, Zscaler, CrowdStrike) and their Zero Trust product lines.

8.3 Economic and Strategic Benefit to the U.S.

By supporting both national security and economic competitiveness, the commercialization of this framework would:

- Strengthen the U.S. cybersecurity market, which is expected to exceed $400 billion by 2030 (Fortune Business Insights, 2023).
- Generate high-skill jobs in the areas of security engineering, data science, and cloud operations.
- Provide a secure venue for digital trade, especially for industries connected with critical infrastructure.

  Further bolster U.S. leadership in innovation in cybersecurity and Zero Trust research. The public value of this is further augmented by the potential to scale the technology into hundreds of federal and private logistics networks throughout the U.S. and its partners.

9.0. Research Outcomes

The annotation stretched an entirely novel Autonomous Zero Trust Orchestration (ZTO) framework for real-time application stepping retroactively to implement risk-adaptive access controls in a federated multi-cloud logistics environment context. This is because the delivery included critical Zero Trust principles, along with bridging artificial intelligence over the current state and contextual risk scoring, to facilitate automated access decision making from the user behavior, device posture location, and threat intelligence. The prototype was tested rigorously in simulated multi-cloud environments: AWS, Azure, and Google Cloud, which gave the following performances: average decision latency of 49 milliseconds, risk classification accuracy of 97.4%, and ability to scale beyond 5,000 concurrent access requests very well without degrading. Real-world use cases like customs data access and remote device authentication, as well as API-based shipment monitoring, validated the capacity of the framework to adjust access privileges dynamically, without losing continuity in operations or security. It also has been designed to ensure full auditability, NIST SP 800-207 compliance, and policy enforcement through the Open Policy Agent in high-stakes, highly regulated environments, such as defense logistics, public health supply chains, and international trade systems.

Technical successes aside, this research contributes greatly to U.S. national cybersecurity and infrastructure resilience, corresponding with the directives of Executive Orders 14028 and 14017 and CISA

and DHS strategic objectives. In addition, combining the transparency and immutability of blockchain with AI's analytical capabilities would not only ensure more robust security but also more adaptable systems to crop up against emerging threats. Maintaining user trust, however, will require that AI algorithms remain unbiased and transparent. This convergence of technologies has enormous potential, especially as sectors like cybersecurity and finance seek smarter, more dynamic security solutions (Olorunlana, 2025). The article also lays a foundation for future innovations, including federated learning, edge AI for low-latency access control, and blockchain-enabled immutable audit trails. The clear applicability to both the public and private sectors makes the framework eligible for significant commercialization, as a Zero Trust-as-a-Service (ZTaaS) solution, for cloud security providers and logistics technology integrators.

Conclusion

As the global logistics ecosystem becomes increasingly reliant on interconnected, multi-cloud environments, the need for advanced, intelligent, and secure access control mechanisms has never been more urgent. The traditional perimeter-based security models are no longer sufficient in the face of modern cyber threats, operational complexity, and the dynamic nature of global supply chains. In this study, we introduced an Autonomous Zero Trust Orchestration (ZTO) framework that delivers real-time, risk-adaptive access control across federated multi-cloud platforms, specifically tailored to the demands of the logistics sector. The architecture, grounded in Zero Trust principles as outlined by NIST SP 800-207, integrates AI-driven risk scoring, context-aware policy enforcement, and automated decision-making across AWS, Azure, and Google Cloud infrastructures. Through prototype evaluation, the system demonstrated sub-50ms decision latency, high accuracy, and seamless scalability making it suitable for mission-critical logistics environments such as customs clearance, freight forwarding, and defense operations. Importantly, the system aligns with strategic U.S. national interests as defined in Executive Orders 14028 and 14017, CISA's Zero Trust Maturity Model, and the DHS Roadmap for Resilience. By securing logistics networks, it protects economic stability, national defense readiness, and supply chain continuity. This research represents a significant advancement in cybersecurity and access governance, providing a technically sound and nationally beneficial solution.

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship and publication of this article.

Funding

The author received no financial support for the research, authorship and publication of this article.

References

[1] Alsharif, A., et al. (2021). An AI-based Adaptive Risk Access Control for Cloud Services. IEEE Access, 9, 99830–99842.
[2] Alsharif, A., et al. (2021). An AI-based Adaptive Risk Access Control for Cloud Services. IEEE Access, 9, 99830–99842.
[3] Alsharif, A., et al. (2021). An AI-based Adaptive Risk Access Control for Cloud Services. IEEE Access, 9, 99830–99842.
[4] Boyson, S. (2014). Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems. Technovation, 34(7), 342–353. https://doi.org/10.1016/j.technovation.2014.02.001
[5] Boyson, S. (2014). Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems. Technovation, 34(7), 342–353.
[6] CISA. (2021). Defending Against Software Supply Chain Attacks. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov
[7] CISA. (2021). Zero Trust Maturity Model. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov
[8] CISA. (2021). Zero Trust Maturity Model. U.S. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov
[9] CISA. (2023). National Risk Management Strategy. Cybersecurity & Infrastructure Security Agency.
[10] CISA. (2023). National Risk Management Strategy. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov
[11] CISA. (2023). Zero Trust Maturity Model 2.0. https://www.cisa.gov
[12] DHS. (2021). Roadmap for Resilience: Securing the Nation's Supply Chains.
[13] Fortune Business Insights. (2023). Cybersecurity Market Size, Share & COVID-19 Impact Analysis. https://www.fortunebusinessinsights.com
[14] Gartner. (2022). Market Guide for Zero Trust Network Access (ZTNA).
[15] Gartner. (2022). Market Guide for Zero Trust Network Access (ZTNA).
[16] Gartner. (2022). Market Guide for Zero Trust Network Access.
[17] Hashizume, K., Rosado, D.G., Fernández-Medina, E., & Fernandez, E.B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 1–13.
[18] Hu, V. C., Ferraiolo, D. F., Kuhn, D. R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2017). Guide to Attribute-Based Access Control (ABAC) Definition and Considerations. NIST Special Publication 800-162. https://doi.org/10.6028/NIST.SP.800-162
[19] Hu, V. C., Ferraiolo, D., Kuhn, D. R., et al. (2017). Guide to Attribute-Based Access Control (ABAC). NIST SP 800-162.
[20] Hu, V. C., Ferraiolo, D., Kuhn, D. R., et al. (2017). Guide to Attribute-Based Access Control (ABAC). NIST SP 800-162.
[21] Kandala, S., Sandhu, R., & Bhamidipati, V. (2011). An Attribute-Based Framework for Risk-Adaptable Access Control Models. International Conference on Availability, Reliability and Security.
[22] Kandala, S., Sandhu, R., & Bhamidipati, V. (2011). An Attribute-Based Framework for Risk-Adaptable Access Control Models. ARES 2011.
[23] Kandala, S., Sandhu, R., & Bhamidipati, V. (2011). An Attribute-Based Framework for Risk-Adaptable Access Control Models. ARES 2011.
[24] Kandala, S., Sandhu, R., & Bhamidipati, V. (2011). An Attribute-Based Framework for Risk-Adaptable Access Control Models. ARES 2011.
[25] Kindervag, J. (2010). Build Security Into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research.
[26] Kindervag, J. (2010). Build Security into Your Network's DNA: The Zero Trust Network Architecture. Forrester Research.
[27] MITRE. (2022). MITRE ATT&CK Framework. https://attack.mitre.org
[28] NIST. (2020). Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5).
[29] NIST. (2020). Zero Trust Architecture (SP 800-207). https://doi.org/10.6028/NIST.SP.800-207
[30] NIST. (2020). Zero Trust Architecture (SP 800-207). https://doi.org/10.6028/NIST.SP.800-207
[31] NIST. (2020). Zero Trust Architecture (SP 800-207). https://doi.org/10.6028/NIST.SP.800-207
[32] NIST. (2020). Zero Trust Architecture (SP 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
[33] NIST. (2020). Zero Trust Architecture (SP 800-207). National Institute of Standards and Technology.

https://doi.org/10.6028/NIST.SP.800-207

[34] NIST. (2022). Post-Quantum Cryptography Project. https://csrc.nist.gov

[35] Olorunlana & Hamdiya, (2025). Analysis of the Colonial Pipeline Cybersecurity Incident. Available from: https://www.researchgate.net/publication/387104186_Analysis_of_the_Colonial_Pipeline_Cybersecurity_Incident [accessed Jun 24 2025].

[36] Olorunlana, T.J. (2025). Strengthening National Cyber Defense: The Role of AWS Cloud Security in Protecting U.S. Critical Infrastructure. https://doi.org/10.63680/ijsate0525145.06

[37] Olorunlana, T.J. (2025). Securing the Global Cloud: Addressing Data Sovereignty, Cross-Border Compliance, and Emerging Threats in a Decentralized World. https://doi.org/10.63680/ijsate0525102.117

[38] Olorunlana, T. J. (2025). The Role of Blockchain in Enhancing Data Security and Privacy in the United States by Taiwo Justice Olorunlana. Available from: https://www.researchgate.net/publication/390275962_The_Role_of_Blockchain_in_Enhancing_Data_Security_and_Privacy_in_the_United_States_by_Taiwo_Justice_Olorunlana [accessed Jun 25 2025].

[39] Olorunlana, T. J. (2025). How 5G and Edge Computing Are Transforming Data Security. International Journal of Science, Architecture, Technology, and Environment, 02(04), 14–25.

[40] Olorunlana, T. J., Ogundipe, A., & Ogunmola, S. (2024). The Future of Cloud Security: Addressing Emerging Threats and Solutions. International Journal of Science, Architecture, Technology, and Environment, 01(05), 89–100. from: https://www.researchgate.net/publication/392896506_The_Future_of_Cloud_Security_Addressing_Emerging_Threats_and_Solutions [accessed Jun 25 2025].

[41] Pallis, G. (2010). Cloud computing: The new frontier of Internet computing. IEEE Internet Computing, 14(5), 70–73. https://doi.org/10.1109/MIC.2010.113

[42] Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the Internet of Things: A review. IEEE International Conference on Computer Science and Electronics Engineering.

[43] U.S. Executive Order 14017. (2021). America's Supply Chains. https://www.whitehouse.gov

[44] White House. (2021). Executive Order 14017: America's Supply Chains. https://www.whitehouse.gov

[45] White House. (2021). Executive Order 14028 on Improving the Nation's Cybersecurity. https://www.whitehouse.gov

[46] White House. (2021). Executive Order 14028: Improving the Nation's Cybersecurity. https://www.whitehouse.gov