electronics

MDPI

Article

A Survey: ZTA Adoption in Cross-Domain Solutions—Seven-Pillar Perspective

Yeomin Lee [1,†], Taek-kyu Lee [2,†], Sangkyu Ham [3], Yongjae Lee [3], Yujin Kim [3], Wonbin Kim [4], Ingeol Chun [5] and Jungsoo Park [3,*]

[1] Graduate Department of Computer Engineering, Kangnam University, Yongin-si 16979, Republic of Korea; 1252037@kangnam.ac.kr
[2] Department of Computer, Communication and Security, Chungnam National University (CNU), Daejeon 34134, Republic of Korea
[3] Department of Computer Engineering, Kangnam University, Yongin-si 16979, Republic of Korea; luk2001@kangnam.ac.kr (Y.L.)
[4] Advanced Research Center of Convergence Security, Sangmyung University, Seoul 03016, Republic of Korea; binn.kim29@gmail.com
[5] Artificial Intelligence Computing Research Laboratory, Electronics and Telecommunications Research Institute (ETRI), Daejeon 34129, Republic of Korea
* Correspondence: jspark@kangnam.ac.kr
† These authors contributed equally to this work.

Abstract

This study examines how the seven pillars of ZTA are implemented in a CDS environment that demands high security reliability, similar to the defense and finance sectors, and identifies the technological advancements and integration patterns that emerge during this process. With the introduction of user- and device-centric authentication methods like distributed identity and RF fingerprinting in the Identity and Device areas, there is a growing trend towards strengthening trust even in domains where distrust is prevalent. In the Network and Application domains, the focus is on using micro-segmentation and SDN to segment and control internal traffic flows, while dynamically enforcing the principle of least privilege. In the Data, Visibility, and Orchestration domains, AI analysis is being applied in real-time, leveraging log and visibility data, and orchestration is automating policy execution and response. In conclusion, it is clear that each pillar of ZTA operates in tandem with the others, rather than as isolated components within the CDS environment. This fusion structure demonstrates its ability to function as a unified security strategy that balances trust with comprehensive coverage of diverse domains.

Keywords: Cross Domain Solution; Cross Domain; Zero Trust; Zero Trust Architecture

Check for updates

Academic Editors: Qinghe Du, Zhipeng Cai, Sai Akshita Maradapu Vera Venkata and Chenyu Wang

Received: 31 December 2025
Revised: 20 January 2026
Accepted: 22 January 2026
Published: 28 January 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Today's corporate network environment is becoming increasingly complex due to the growing adoption of cloud and IoT technologies. These changes expose the limitations of the traditional perimeter-based network security model [1]. In today's complex corporate landscape, the "trust no one, verify everything" approach, also known as zero trust, has gained popularity as a strategy to minimize security threats through dynamic and ongoing authentication and verification processes [2,3]. Major US agencies, including the CISA and the Department of Defense (DoD) [4,5], define ZTA as a seven-pillar concept. Within an organization, Identity, Device, Network, Application, and Data are the core pillars of security policy, and through interconnected visibility and orchestration capabilities, ZTA's

overall effectiveness is enhanced. In high-trust environments where data confidentiality and integrity are paramount, such as defense and finance, CDS is gaining attention for its role in ensuring secure information exchange between different security levels. However, existing ZTA research has primarily focused on technical implementation for each pillar, leaving a gap in understanding how ZTA models can be integrated and utilized within systems like CDS. This paper analyzes application cases of each pillar of Zero Trust Architecture (ZTA), focusing on Cross-Domain Solutions/Cross-Domain (CDS/CD) environments. It aims to bridge the gap between the ZTA model and practical integration in high-assurance domains, specifically for information transfer from low-trust domains. The main contributions of this study are as follows.

- **Redefinition of core ZTA elements for CDS environments**
  While prior studies have addressed Zero Trust as a theoretical model in a general IT context, this study reinterprets the requirements of ZTA's seven pillars in CDS environments.
- **Systematic classification framework**
  This paper proposes a new classification framework that categorizes existing technologies based not only on explicit ZTA terminology but also on implicit functional alignment, providing a comprehensive perspective on ZTA adoption in CDS environments.
- **Integrated implementation strategy**
  This paper seeks to organize how the seven core elements interact with one another to ensure continuous verification across heterogeneous security domains.

2. Background

2.1. Concepts and Principles of Zero Trust Architecture

The Zero Trust Architecture is a security architecture proposed to address the limitations of traditional perimeter-based security models, built around the core concept of "trust no one." Unlike traditional models that assume the internal environment is trustworthy, ZTA takes a more cautious approach, questioning the integrity of all objects—users, devices, applications, and data—at every access point, and conducting thorough verification and policy evaluation. ZTA can be broken down into 7 pillars, allowing for a comprehensive analysis from multiple angles. The seven pillars of Identity, Device, Network, Application/Workload, Data, Visibility & Analytics, Automation & Orchestration should work together seamlessly, rather than as separate entities [5–7].

2.1.1. Identity

The Identity Pillar focuses on "who has access". The system creates and manages identities, encompassing not only user accounts but also service accounts and machine IDs. The key is login and authorization. This encompasses strong authentication methods like MFA and FIDO, as well as SSO and federated authentication, and the division of authority into RBAC/ABAC within IAM. In ZTA, identity serves as the foundation of policy, resulting in varying access levels for the same individual based on authentication level, role, and group affiliation [8].

2.1.2. Device

The Device Pillar focuses on "what device you're accessing from" [2,9]. The system checks the status of the device, including whether it is managed by an organization, if the patch is up to date, if the security settings are correct, and if there are any signs of malware [2,10–12]. Typical examples include device registration and inventory management, endpoint security features like EDR, and OS/patch level monitoring [10–13]. In ZTA,

if the device's status is poor, the connection is either blocked or the access is restricted immediately [2,4,9].

2.1.3. Network

Network Pillar is centered on "how to manage connectivity". The key is to break down a large network into smaller, manageable pieces rather than trying to keep everything together as one. Here, you'll find features like micro-segmentation, SDN-based policies, remote access tunnels, and encryption traffic control. The goal is to minimize the use of flat networks and prevent attacks from spreading from within to the sides as much as possible [14,15].

2.1.4. Application

The Application/Workload Pillar focuses on "how to ensure service and workload integrity". The system includes application authentication and authorization, API security, service-to-service communication control via service messaging, CI/CD stage security, and runtime protection. Due to the constant emergence and disappearance of containers or serverless environments, ZTA ensures continuous verification and control of workloads based on identity and policy [6].

2.1.5. Data

Data Pillar is all about "what to protect". Data classification and categorization, labeling, encryption and key management [16], DLP [17], masking and tokenization, access logging, and usage pattern monitoring are all part of the process. In ZTA, all decisions ultimately boil down to "which data can be accessed," and the other Pillars are ultimately connected to the data [18–20].

2.1.6. Visibility & Analytics

Visibility & Analytics is responsible for aggregating logs and events from across the board, providing a real-time view of what is happening right now. This includes SIEM, threat intelligence integration, and AI/ML anomaly detection capabilities. In ZTA, the log is only meaningful if it is accumulated. The goal is to create a context through real-time analysis, identify anomalies, and provide a solid basis for making informed policy decisions [14,21].

2.1.7. Automation & Orchestration

Automation & Orchestration focuses on how quickly and consistently you can respond after detection. SOAR, automated playbook, and API-based policy deployment are typical examples. In the ZTA environment, with numerous access requests and constantly evolving threats, manual operation is no longer feasible. When detected, measures like account blocking, network isolation, and patching are automatically triggered to minimize response time and boost operational efficiency [14].

2.2. Cross Domain Solution (CDS)

Cross Domain Solution (CDS) [11] ensures confidentiality, integrity, and availability by controlling and verifying the flow of information between different security domains when data exchange is required. CDS acts as a secure gateway, safely transmitting only authorized information between trusted and untrusted domains [22,23]. We design the following requirements. First and foremost, information exchange should be possible between networks with different security levels [24]. Second, high-grade sensitive and confidential information must not be leaked to low-grade domains. Third, malicious code or attack traffic originating from the Low domain should not be allowed to flow into the High domain [25]. To meet these stringent security requirements, CDS uses a unique mechanism, such as Data Diodes and Security Guard. Data diodes enforce unidirectional

communication, preventing any return path from low-trust to high-trust domain. Security Guard checks the data payload for malware. The features of these systems prevent the leakage of advanced sensitive information and prevent malicious code from low-grade domains from infiltrating high-grade systems.

2.3. Literature Search Methodology

CDS and Zero Trust have been actively researched as distinct and independent security domains. However, there is a lack of prior research that directly integrates the two technologies to present a comprehensive security model in a high-trust environment. To derive the relationship between the two technologies, a systematic approach to searching for relevant papers was developed.

First, we identify research that directly relates to the security objectives and technical characteristics of each ZTA 7 Pillar principle within the CDS system. In this step, we searched for studies that (i) explicitly mention a given ZTA pillar (or its core objectives) in the context of CDS/CD, and (ii) indirectly align with the pillar, even without explicit terminology—i.e., the research process, control logic, or operational assumptions are functionally similar to the pillar's requirements.

Second, we conduct a more comprehensive search across the entire Cross Domain (CD) space, including ZTA-related research, without limiting the search scope to CDS alone, and secure relevant studies for each pillar. Here, we applied the same two-tier relevance criteria (explicit vs. implicit alignment) to broaden coverage and to avoid missing pillar-relevant evidence that appears outside of "CDS" keyword boundaries.

Third, we identified the key implementation technologies for each ZTA Pillar and analyzed how they were adapted, modified, and expanded to suit the unique characteristics of the CDS/CD environment. When pillar-specific evidence was sparse in CDS/CD literature, we additionally used a technology-driven tracing strategy: for each pillar, we selected representative enabling technologies (e.g., SOAR for the Application pillar) and then searched for studies that apply those technologies in CDS/CD settings. This allowed us to capture how pillar requirements are realized through practical mechanisms, even when the papers do not frame their contributions as "Zero Trust."

This process revealed how the requirements for each ZTA Pillar are being addressed in the CDS/CD study. In addition, we applied explicit inclusion and exclusion criteria during screening. We excluded publications that were purely conceptual or marketing-oriented and lacked concrete technical contributions (e.g., implementable mechanisms, architectures, or evaluation). We also excluded studies in adjacent contexts such as OT/ICS security when they did not establish an explicit linkage to CDS/CD (or equivalent cross-domain separation constructs such as data diodes or information guards). Exceptions were made only when OT/ICS studies implemented or analyzed cross-domain separation mechanisms that are directly transferable to CDS/CD requirements.

Building on the resulting study set, we organize the findings in a pillar-centric manner. In particular, we treat each pillar not as a checklist item, but as a lens for interpreting how trust is constructed, transferred, constrained, and continuously re-validated under cross-domain separation. The following pillar-wise classifications summarize recurring problem statements and solution patterns observed in CDS environments. Each work was assigned to a single primary pillar based on its primary enforcement point (where the policy decision is enforced). Pillar overlap may exist; however, this rule was adopted for analytical consistency. The literature search and screening workflow is summarized in Figure 1.

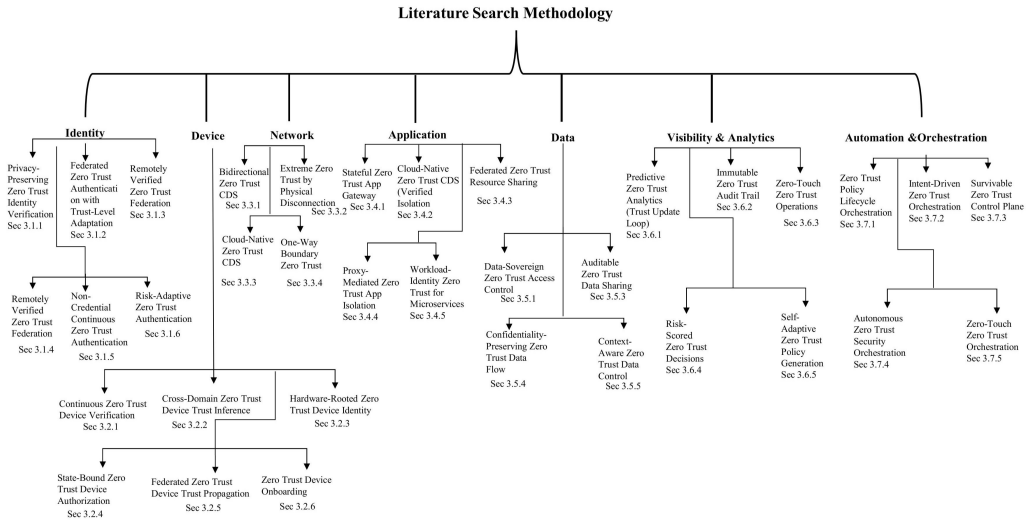


Figure 1. Literature Search Methodology Architecture.

2.3.1. Identity Pillar

Identity in CDS environments is not merely a collection of authentication techniques, but rather an end-to-end process in which identities are created, verified, propagated across domains, and continuously maintained. From this perspective, identity-related studies can be systematically grouped into six categories based on shared problem definitions and functional focus.

- **Privacy-preserving credential verification mechanisms.**
  Several studies emphasize that, in multi-domain settings, the authentication process itself can become a channel for privacy leakage or user traceability. These approaches aim to validate credential legitimacy without disclosing actual identities or attribute values.
- **Trust-level-adaptive federated authentication.**
  Other works point out the limitations of viewing authentication as a one-time operation. Instead, they introduce models in which authentication strength and procedures are adjusted according to evolving trust levels. By incorporating changes in user behavior, device posture, or domain context, these approaches can be grouped as trust-level-adaptive federated authentication.
- **Remote-verified federation.**
  In CDS environments, accepting authentication results generated by external domains without further validation introduces inherent risk. To address this, some studies focus not on the credential itself, but on verifying the integrity and security posture of the environment in which the credential was issued. Because this approach directly tackles cross-domain trust transfer, it is categorized as remote-verified federation.
- **Continuous and context-aware authentication with adaptive authorization.**
  Several studies extend authentication beyond session initiation, arguing that static, entry-point verification is insufficient to prevent privilege abuse or session hijacking. These works continuously reassess identity throughout the session by monitoring contextual information, and are thus classified as continuous and context-aware authentication with adaptive authorization.
- **Non-credential continuous authentication.**
  Another research direction departs from conventional credential-based authentication by leveraging physical-layer signals or behavioral characteristics. Such methods enable ongoing identity verification without explicit credentials, reducing re-authentication overhead in highly mobile and cross-domain CDS environments.

- **Risk-evaluation-driven authentication control.**
  Finally, some studies conceptualize authentication itself as a risk-bearing process. By quantitatively assessing privacy exposure, domain-level uncertainty, or contextual risk during authentication, these approaches dynamically adjust protection mechanisms. Accordingly, they are classified as risk-evaluation-driven authentication control.

Overall, this classification frames Identity not as a static access checkpoint, but as a dynamic trust mechanism that evolves in response to domain boundaries, contextual changes, and risk conditions in CDS environments.

2.3.2. Device Pillar

The Device Pillar in CDS environments is not viewed merely in terms of device presence or registration status. Instead, it is analyzed from the perspective of how devices are defined as trust-bearing entities, how their trustworthiness is verified, and how that trust is maintained and propagated across domains. In large-scale IoT, OT, and edge environments, devices—rather than users—often serve as the primary access subjects. As a result, issues such as device state dynamics, mobility, and heterogeneity emerge as central security challenges in CDS environments. Based on this observation, device-related studies are classified into multiple categories according to shared problem definitions and functional focus.

- **Device profiling-based continuous verification.**
  Some studies treat devices not as static identity objects, but as entities that must be continuously evaluated over time. These approaches aggregate configuration information, integrity measurements, and behavioral characteristics to derive device trust levels, which are then used to dynamically adjust access permissions. This category represents a device-level realization of the Zero Trust principle that trust must not persist beyond verification.
- **Privacy-preserving cross-domain device trust inference.**
  In CDS environments, devices frequently migrate across domains or participate in multiple domains simultaneously. Under such conditions, centralized trust evaluation mechanisms face limitations in scalability and privacy. To address this, some studies propose architectures that infer or transfer device trust without sharing raw device data, reflecting efforts to balance trust continuity with data sovereignty.
- **Hardware- or RF-based device identity establishment.**
  Another research direction focuses on the fundamental problem of device identity itself. Software-based identifiers and key management mechanisms are vulnerable to cloning, theft, and forgery, and are often impractical for resource-constrained devices. Consequently, several studies leverage intrinsic hardware or physical-layer characteristics to establish device identity, distinguishing devices as physical entities rather than purely logical constructs.
- **State-binding zero-trust authorization tokens for distributed enforcement.**
  Some studies concentrate on how verified device states are translated into enforceable access control decisions. These approaches bind device integrity or state verification results to cryptographic tokens or proofs, enabling distributed authorization enforcement without reliance on centralized decision points, thereby addressing scalability and availability concerns in CDS environments.
- **Cross-domain trust propagation and provenance verification.**
  Other studies emphasize the reliability of device trust propagation across domains. Rather than directly accepting device attributes or state information generated by external domains, these approaches verify the provenance and integrity of the systems

that generated such information, reflecting a cautious approach to trust transfer in federated environments.

- **Secure device onboarding and initial trust bootstrapping.**
  Finally, some studies identify device onboarding itself as a cross-domain security problem. These works reject implicit trust in manufacturers or supply chains and instead propose mechanisms that allow users or operators to directly establish initial trust when devices first enter the system.

2.3.3. Network Pillar

The Network Pillar in CDS environments is not treated as a simple mechanism for packet delivery or connectivity. Instead, it is concerned with how communication paths between domains of different trust levels are constructed, constrained, verified, or intentionally removed. In Zero Trust CDS settings, the network itself becomes an enforcement surface where trust boundaries are continuously asserted rather than implicitly assumed. Based on this perspective, network-related studies are classified according to the manner in which inter-domain connectivity is defined and controlled.

- **Bidirectional Zero Trust CDS.**
  Some studies address the challenge of maintaining bidirectional communication under Zero Trust assumptions. Rather than assuming that two-way connectivity is inherently unsafe, these approaches introduce distributed enforcement and state-aware verification mechanisms that independently validate traffic in each direction. By correlating requests and responses and dispersing policy enforcement across multiple nodes, they reduce reliance on a single gateway and limit the impact of reverse-path attacks. This line of work illustrates that bidirectional exchange can be achieved without implicit trust when every transaction is explicitly verified.
- **Extreme Zero Trust by physical disconnection.**
  Other studies adopt the opposite stance, treating the existence of connectivity itself as the primary source of risk. In these approaches, security is achieved by eliminating communication paths altogether through physical or logical disconnection. Air-gapped architectures and extreme isolation models exemplify this perspective, reflecting a Zero Trust interpretation in which risk is mitigated not through verification, but through structural non-connectivity.
- **Cloud-native Zero Trust CDS.**
  A separate body of research focuses on environments where physical separation is impractical, such as hybrid cloud or large-scale distributed systems. These studies redefine network boundaries in logical terms, using workloads, services, or identities as the basis for isolation. Micro-segmentation, service meshes, and continuous verification mechanisms are employed to prevent lateral movement even when infrastructure is shared, emphasizing the shift from hardware-defined boundaries to software-defined, policy-driven network controls.
- **One-way boundary Zero Trust.**
  Another group of studies concentrates on asymmetric communication requirements, where data exchange is necessary but must be strictly limited to a single direction. One-way boundaries and data diode architectures exemplify this approach, prioritizing the elimination of reverse attack paths while still permitting controlled data export. This category represents a practical compromise between complete isolation and bidirectional connectivity, particularly in high-risk operational environments.

This classification does not organize network research by specific technologies or implementations. Instead, it highlights how trust boundaries are enforced at the network level in CDS environments—whether through verified bidirectional communication, complete

disconnection, logical micro-segmentation, or enforced unidirectionality. Through this lens, the Network Pillar is positioned not as a passive transport layer, but as a foundational mechanism for realizing Zero Trust principles across domain boundaries.

2.3.4. Application Pillar

The Application Pillar in CDS environments is not interpreted as a collection of software functions or service implementations. Instead, it concerns how application logic, execution state, and interaction semantics are protected and constrained when applications operate across domains with different trust levels. In a Zero Trust CDS environment, applications cannot rely on network location or deployment context for trust; every interaction must be explicitly verified at the application layer. Based on this perspective, application-related studies are classified according to how trust is enforced and how application behavior is constrained across domain boundaries. Some CDS studies utilize mechanisms like filtering and segmentation at the network layer as auxiliary measures. However, even if network control exists, if the primary control point is application workload identification, request-response semantic validation, or workload arbitration, then these tasks are classified as application-layer.

- **Stateful Request–Response Correlation at the Application Layer.**
  Some studies focus on enforcing trust by validating the semantic consistency between application-layer requests and responses. These approaches treat any unsolicited or context-free response as untrusted and enforce strict stateful correlation at the application protocol level. By verifying function codes, sequence information, and execution context, they prevent response injection and replay across domains, emphasizing explicit verification of application state as the primary trust boundary.
- **Virtualized Cloud CDS with Verified Isolation and Least Privilege.**
  Other studies address the challenge of deploying CDS functionality in cloud and virtualized environments while preserving strict isolation guarantees. Rather than relying on perimeter defenses, these works enforce least privilege and isolation through verified microkernels, capability-based access control, and static communication paths. Application components are constrained to predefined privileges that cannot be expanded at runtime, highlighting the role of formally constrained execution environments in applying Zero Trust principles at the application layer.
- **Federated Cross-Domain Resource Sharing with Fine-Grained Policy Enforcement & Automation.**
  A separate group of studies focuses on federated application environments, where resources and services must be shared across domains that do not mutually trust each other. These approaches embed policy enforcement directly into applications or application-adjacent components, enabling fine-grained, resource-level access control that is independent of network location. Policy evaluation and enforcement are automated and consistently applied across domains, reflecting an application-centric model of cross-domain trust enforcement.
- **Proxy-Based Web Component/API Isolation with Runtime Verification.**
  Some studies concentrate on isolating application components and interfaces within complex application ecosystems such as web mashups and API-driven systems. These works reject broad domain-level trust and instead enforce least privilege at the component or interface level using proxies, runtime mediation, and controlled communication paths. Even components within the same application are treated as mutually untrusted, emphasizing fine-grained application-internal trust boundaries.
- **Workload Identity-Centric Zero Trust for Cloud-Native Apps.**
  Another line of research treats workloads themselves as first-class identities and bases

application trust on verifiable workload identity rather than network location. In these approaches, services authenticate and authorize each other using workload identities, mutual authentication, and continuous verification. This enables secure application communication across domains without relying on centralized authentication infrastructure, representing a shift from infrastructure-centric to application-centric trust.

This classification does not organize application-related research by programming models or middleware technologies. Instead, it highlights how trust is enforced at the application layer in CDS environments—through state verification, isolation, policy-driven federation, component-level mediation, and workload identity. Through this perspective, the Application Pillar is positioned as a core mechanism for enforcing Zero Trust principles beyond the network boundary.

2.3.5. Data Pillar

The Data Pillar in CDS environments is not examined merely as a matter of encryption techniques or data storage mechanisms. Instead, it is analyzed from the perspective of how data is protected, transferred, verified, and controlled after its creation. In CDS environments, data frequently traverses domains with different trust levels, or, in some cases, its movement is intentionally restricted altogether. Under such conditions, data-centric security control becomes a core element of Zero Trust enforcement. Based on this observation, data-related studies are classified according to their shared problem statements and differences in control strategies.

- **Data-sovereignty-preserving access control [26].**
  Some studies emphasize that even when inter-domain collaboration is required, moving raw data itself constitutes a significant risk. These approaches preserve data sovereignty by minimizing disclosure, often exchanging only learned models, derived parameters, or summarized information instead of original data [27]. This reflects a Zero Trust interpretation in which data is not allowed to cross trust boundaries unless strictly necessary.
- **Auditability- and traceability-focused data sharing.**
  Other studies focus on scenarios where data movement is unavoidable and identify traceability and accountability—namely, who accessed the data, under what conditions, and when—as the central challenge. These approaches commonly rely on immutable logs or distributed ledgers to enable auditing and verification even in the absence of a trusted central authority.
- **Confidentiality-centric data flow control.**
  Another line of research shifts the center of protection away from networks or gateways and toward the data itself. These studies minimize plaintext exposure across the data lifecycle (storage, transmission, and processing) and enable access control, filtering, or search operations directly over encrypted data, extending the Zero Trust assumption that intermediaries should not be trusted into the data processing layer.
- **Context-aware, data-centric access control.**
  Some studies treat data access decisions not as static policy evaluations, but as dynamic processes driven by context. These approaches combine contextual factors—such as user attributes, environmental conditions, behavioral patterns, and domain state—to determine data access eligibility, while avoiding centralized decision-making and maintaining consistent enforcement in distributed environments.

This classification is not intended to enumerate data-related studies according to specific cryptographic primitives or storage technologies. Rather, it highlights fundamental differences in how data is controlled and protected when crossing trust boundaries in CDS environments. Through this lens, the Data Pillar is positioned not as a supporting

component, but as a core control unit that concretely realizes trust boundaries in Zero Trust CDS architectures.

2.3.6. Visibility & Analytics Pillar

The Visibility & Analytics Pillar is not limited to simple log collection or monitoring functions. In CDS environments, visibility and analytics are directly tied to the problem of how activities and states observed across heterogeneous trust domains can be interpreted and translated into trust judgments and policy decisions. In a Zero Trust environment, where no prior trust is assumed, every access and action must be continuously reassessed based on observable evidence and analytical outcomes. Reflecting these characteristics, related studies are classified according to how visibility is achieved and how analytical results are utilized. Because analytics pipelines impose non-trivial computational and operational overhead—including inference latency and the handling cost of false positives—CDS deployments should apply visibility and analytics in a risk-driven manner, prioritizing high-criticality flows and sensitive data classes rather than enforcing uniform, always-on analytics across all domains [28].

- **Trust-update-centric analytics loops.**
  Some studies focus on directly linking behavior-based observations to immediate trust updates and policy adjustments. These approaches leverage existing security observation tools such as SIEM, IDS, and UBA, but go beyond simple alert generation by dynamically adjusting trust levels based on observed behavior. This category represents an operational realization of the Zero Trust principle of "always verify."
- **Immutable-record-based visibility assurance [29].**
  Some studies question the reliability of visibility itself. Reliance on centralized log repositories or single analysis engines introduces risks such as data tampering and single points of failure. To address this, these studies employ blockchain or distributed ledgers to store behavioral records and analytical outcomes in an immutable form, enabling cross-domain verification. This category extends the Zero Trust assumption to the analytics layer by treating even analytical results as untrusted unless verifiable. However, the blockchain system itself is introducing different attack surfaces and privacy trade-offs. Thus, clear threat and defense mechanisms should be based when utilizing blockchain for auditability and cross-domain verification [29].
- **Analytics-driven automated response.**
  Another research direction treats visibility data not merely as a tool for post-incident analysis, but as input for automated decision-making and response. These studies integrate large-scale logs and operational data into centralized data lakes and apply AI or machine-learning techniques to detect anomalies or automate policy enforcement, enabling sustained Zero Trust operation by compensating for the limits of human intervention in complex multi-domain environments.
- **High-performance trust analytics and decision-making.**
  In CDS environments—particularly in control systems or real-time services—delays introduced during the analytics phase can themselves pose operational risks. To mitigate this, approaches such as parallel processing, optimized policy lookup, and lightweight trust evaluation models have been proposed. These works prioritize processing efficiency and latency reduction while maintaining actionable trust judgments.
- **Self-adaptive analytics and policy generation.**
  Finally, some studies move beyond fixed rules or predefined policies and propose self-evolving analytics and policy generation mechanisms that adapt to contextual changes. By correlating diverse observation data and applying rule learning or evidence fusion

techniques, these approaches derive new policies dynamically, reflecting the evolving nature of threats and inter-domain collaboration patterns in CDS environments.

This classification reframes the Visibility & Analytics Pillar not as a passive observation layer, but as a core mechanism for generating, maintaining, and adjusting trust in Zero Trust CDS environments. Through this perspective, visibility and analytics are positioned not as auxiliary support functions, but as foundational components that dynamically reshape trust boundaries across domains.

2.3.7. Automation & Orchestration Pillar

In this paper, Orchestration does not refer to general service orchestration or business workflow automation. We focus on automating policy enforcement and responses in CDS cross-domain environments. Automation and orchestration in CDS environments are essentially methods for deploying policies across heterogeneous trust domains and executing them in an auditable manner without human intervention. In a zero-trust environment, the policy enforcement process itself may be subject to attack. Maintaining both consistency and reliability in a complex multi-domain environment is difficult when performed manually. Therefore, this paper focuses on how policies propagate across domain boundaries and how automated responses are executed based on event detection results.

- **Policy lifecycle-centric automation.**
  Some studies focus on automating the security policy itself from a lifecycle perspective. Rather than treating policies as static rule sets, these approaches view them as evolving entities that undergo creation, deployment, modification, and retirement. Decision-making at each stage of the policy lifecycle is automated accordingly. This category extends the Zero Trust principle of continuous verification into the policy management and operation phase.
- **Multi-domain collaborative automation.**
  Some studies interpret automation in multi-domain environments as a trust orchestration problem. Instead of unilaterally extending policies from a single domain, these approaches exchange inter-domain trust information and threat intelligence to enable coordinated defense and joint response. This category reinterprets the boundary-control role of traditional CDS as a form of logical and dynamic orchestration rather than static enforcement.
- **Survivable orchestration control structures.**
  Some studies address the resilience and survivability of the automation layer itself as a core concern. Conventional automation systems risk complete security collapse if the centralized control plane is compromised. To mitigate this, these works employ techniques such as distributed consensus, replication, and integrity verification to protect the control plane. This category can be seen as applying Zero Trust principles not only to users and data, but also to the management and control plane.
- **Intelligent security response automation.**
  Another line of research aims to maximize the level of automation in incident response and security operations. Moving beyond static, predefined SOAR playbooks, these approaches propose agent-based automated response mechanisms capable of autonomous situation assessment and decision-making. By replacing or augmenting human analyst judgment, these approaches enable the rapid and repetitive verification and response required in Zero Trust environments.
- **Zero-touch orchestration in trustless environments.**
  Finally, some studies extend automation beyond the scope of a single organization and position it as an infrastructure for collaboration among mutually untrusted parties. These works leverage distributed ledgers, smart contracts, and Trusted Execution

Environments (TEEs) to automate resource allocation, SLA verification, and policy enforcement while minimizing reliance on centralized intermediaries. This category is significant in that it presents automation as a new trust mechanism capable of replacing physical boundaries in CDS environments.

This classification frames the Automation & Orchestration Pillar not as a mere operational layer, but as a core layer that transforms policy into executable trust in Zero Trust CDS environments. Through this perspective, automation is emphasized not as an auxiliary security feature, but as an essential mechanism for sustaining Zero Trust principles in complex multi-domain systems.

3. CDS Application Examples and Analysis by ZTA's 7 Core Principles

3.1. Identity

3.1.1. Privacy-Preserving Zero Trust Identity Verification

Zhao et al. [30] consider the existing authentication model that relies on a centralized trusted authority in a Multi-Trust Domain environment to be a problem. They propose a decentralized anonymous authentication method by integrating blockchain and zk-SNARK. Zhao et al. [30] achieved the anonymity and revocability of zero-trust by decoupling authentication and attestation. The administrator-issued domain provides users with digitally signed authorization credentials for their attributes, which users can then use to create and submit a zero-knowledge proof to the verification domain. In this process, the verification domain can mathematically verify the validity of a user's credentials without needing to verify their actual identity or attribute values. They also propose a Privacy-Preserving Identity Verification model that ensures secure data flow without exposing sensitive internal information in a CDS environment. By posting a signature-based blacklist on the blockchain, administrators can monitor malicious behavior in real-time and revoke the user's anonymous access rights. They also implemented a dynamic security posture that can track and monitor past access history. This enables it to operate in a cross-domain environment while adhering to the principles of zero trust.

Rivera et al. [31] point out that traditional centralized authentication systems have limitations in terms of data leakage and PoF when managing digital identities in a zero-trust environment. To address this issue, the research team proposed a blockchain-based framework for multi-factor authentication that prioritizes user privacy. Rivera et al. [31] designed the Identity Pillar of ZTA as a decentralized structure. The authentication process is designed to be decentralized on Ethereum, ensuring the system's availability even if a specific authentication server is compromised. Furthermore, by integrating zero-knowledge proof technology, a mechanism has been developed that enables users to verify their identity without exposing sensitive data like biometric information or passwords to the network.

Du et al. [32] highlight the issue of privacy leakage and reliance on a centralized trusted third party (TTP) that arises during cross-domain authentication in distributed network environments such as IoT. To address this, they propose an anonymous cross-domain authentication scheme that combines Zero-Knowledge Proof (ZKP) with blockchain technology. Their work focuses on minimizing unavoidable information exposure during authentication when implementing the Identity Pillar of ZTA. They introduce zk-SNARKs (Groth16 algorithm), enabling users to prove legitimate authorization to an agent server using only a proof value, without transmitting actual identities or secret keys over the network. Furthermore, they design agent servers in each domain to participate as blockchain nodes that store authentication records in a distributed manner, preventing data tampering and eliminating single points of failure. This approach is particularly effective in cross-domain (CDS) environments where mutual trust is absent. By enabling consistent trust verification across heterogeneous domains through blockchain, and by completely exclud-

ing sensitive identity information from cross-domain transmission via zero-knowledge proofs, Du et al. [32] demonstrate a decentralized ZTA authentication model that balances privacy protection with system integrity. An overview of the anonymous cross-domain authentication architecture using zk-SNARKs and blockchain is shown in Figure 2.

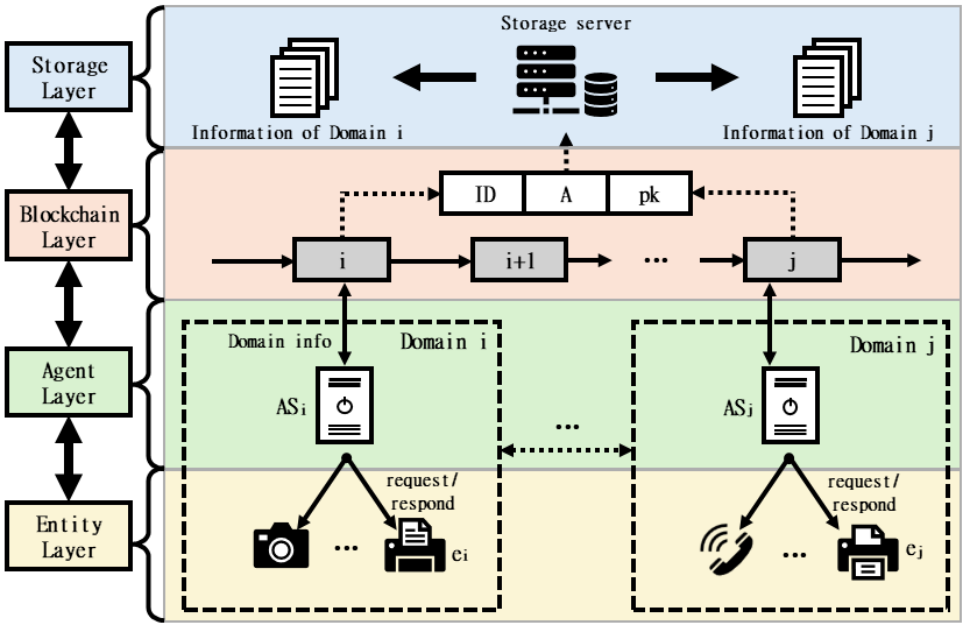


Figure 2. Blockchain-Based Cross-Domain Identity Architecture.

3.1.2. Federated Zero Trust Authentication with Trust-Level Adaptation

Zhu et al. [33] focused primarily on identity verification in existing cross-domain authentication, neglecting the dynamic threats to user terminals and changes in their trustworthiness. To address this, it was proposed to broaden the scope of authentication beyond users to include users, platforms, and domains, and to calculate the Trust Level Evaluation (TLE) by combining these three entities. The TPL uses the TPM to verify the integrity of the system and applications on a terminal that has requested cross-domain access. Furthermore, UTL goes beyond simple identity verification, analyzing users' past behavior and interaction patterns over time to assign dynamic trust levels. To effectively block threats that may arise from malicious domains or untrusted environments, they continuously update the trust relationship through mutual evaluation between DTL domains. To address the vulnerability of authentication based on static credentials in a cross-domain environment, the study proposes a framework that continuously verifies the integrity and behavior patterns of user terminals in real-time. In the CDS environment, it was assessed that integrating ZTA enables dynamic access control to be utilized in collaborative settings across diverse domains.

3.1.3. Remotely Verified Zero Trust Federation

Poirrier et al. [34] noted that traditional identity management systems often rely on implicit trust in authentication information received from other domains in environments where multiple security domains must collaborate. To facilitate secure cross-domain interaction, they propose a remote verification technique grounded in zero-trust principles. Poirrier et al. [34] extend zero trust to the identity provider (IdP) itself and to the integrity of the security infrastructure responsible for authentication and policy enforcement. Before processing incoming requests from external domains, the resource domain verifies the security posture of the requesting domain using remote attestation techniques, ensuring that critical security components have not been compromised. Only after successful verification

is the issued authentication token accepted. Ultimately, their work implements ZTA at the infrastructure level, enforcing the principle that authentication information is trusted only when it is generated within a verified and uncompromised environment.

3.1.4. Continuous Zero Trust Authentication with Context Awareness

Kovacevic [35] pointed out that traditional perimeter-based security is ineffective in environments where multiple devices and diverse protocols coexist. To address this, they proposed a framework for integrated authentication and identity management as a foundation. The core of the model lies in the combination of identity, device, and behavior. To begin with, they established a dual authentication system, where users are authenticated through a software token in addition to their credentials, and devices are verified through a PKI-based digital certificate. The second approach is based on trust scores, which are calculated by integrating user request data, past behavior, and usage patterns to determine trustworthiness. This score is then combined with an ABAC policy to grant access to resources if it exceeds a predetermined threshold. To ensure flexibility through microservices architecture, they can decouple ZTA into independent modules, apply asynchronous communication, and perform continuous verification without compromising performance in a large-scale, distributed environment. The proposed zero trust architecture for integrated authentication and identity management is illustrated in Figure 3.

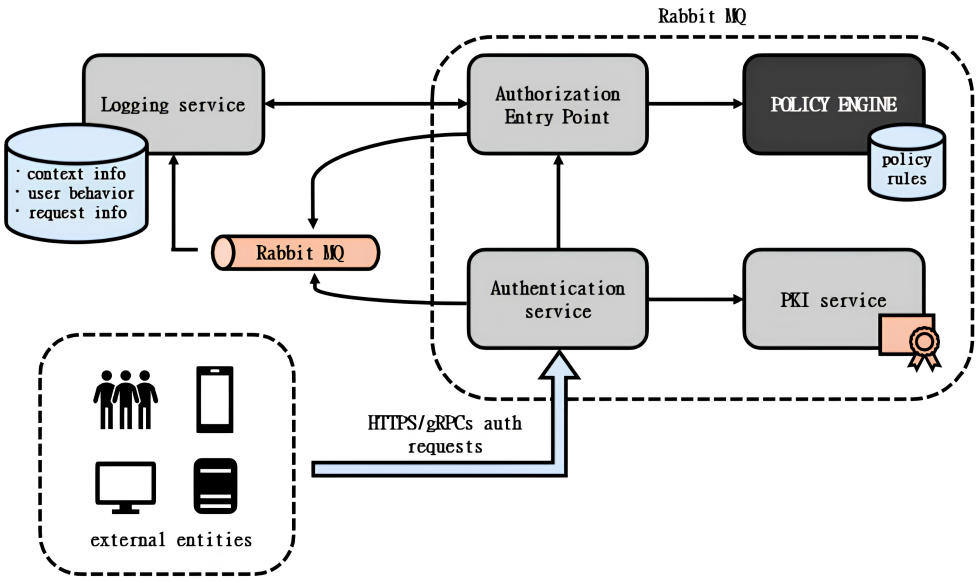


Figure 3. Zero Trust-Based CDS Authentication Architecture.

Ma et al. [36] argue that traditional centralized authentication and simple data sharing methods fall short in terms of confidentiality and efficiency when large-scale IoT devices operate in a domain-hopping environment. They propose a pre-authorization mechanism that enables dynamic verification of cross-domain trust without data transfer by integrating Decentralized Federated Learning (DFL) into a zero-trust architecture. Ma et al. [36] focus on implementing the Identity and Device Pillars of ZTA without directly exchanging sensitive data such as location or access patterns required for verification. Each domain learns a device reliability prediction model using local data and shares only its model parameters with neighboring domains. This allows the target domain to predict device reliability in advance, even without accessing data from external devices. Based on the prediction results, access rights can be dynamically assigned. In a CDS environment lacking mutual trust, their approach demonstrates that ZTA can preserve data ownership while still enabling the continuous verification required for cross-domain operation.

3.1.5. Non-Credential Continuous Zero Trust Authentication

Existing password-based authentication has a limitation in that it only provides one-time authentication at the start of a session, making it challenging [37] to offer continuous identity verification and fine-grained authentication throughout the session. To address this issue, we propose a solution that continuously authenticates users without disrupting their workflow, leveraging a physical layer-based approach. This paper identifies the scenario where receiver changes lead to performance degradation as a problem, particularly in situations where the registration node and serving node are swapped due to NGN mobility. When transitioning to a different domain, such as from CDS, it is proposed that the same level of identity verification is required each time, and that the same transmitter should be identifiable even if the receiver changes. When a domain shift is detected, the receiver is treated as a different domain. The system is organized around a learning-based approach that minimizes receiver differences, and uses LMMD-based sub-domain alignment to group similar transmitters together. The new receiver adapts solely from the samples, without forcing any labeling. In a dynamic and mobile environment, the identity can be continuously verified from the start of the session, ensuring that ZTA's authentication remains valid throughout.

3.1.6. Risk-Adaptive Zero Trust Authentication

Wu et al. [38] pointed out that the authentication process within the zero-trust framework can ironically become a conduit for confidential information leakage. To address this issue, they proposed Privacy Domain Prevention and Control (PDPC). Wu et al. [38] viewed certification not only as a means of verifying identity, but also as a process that inherently carries potential risks, and conducted a quantitative risk assessment to evaluate these risks. The research team developed the Dynamic Privacy Risk Assessment model by analyzing three types of authentication risks: local, domain, and global. To enhance security, they developed an intelligent risk classification and response system that uses the Analytic Hierarchy Process (AHP) to select the most effective encryption algorithm or protection method in real-time, based on the risk level assessed. This incorporates the ZTA's Identity Pillar into the criteria for assessing the risk of the current authentication attempt. To provide a consolidated view of the studies discussed above, we summarize the key points in Table 1.

Table 1. Summary of Research on the Identity Pillar in CDS Environments. This table summarizes representative CDS-related research based on approaches for establishing and verifying cross-domain identity trust.

Paper Title	Problem Setting in CDS Environment	CDS Application Approach	ZT Utilization Approach	Identity Perspective Core
A Zero-Knowledge-Proof-Based Anonymous and Revocable Authentication Scheme [30]	In a cross-domain environment, when authenticating, the problem of exposure of user/entity privacy and possibility of tracking.	Design of a structure that can combine anonymous authentication and post-hoc tracing without a central trusted party	Credential Verification	Zero-Knowledge Proof-based anonymous and revocable authentication mechanism
A Trust-Level-Based Authentication Mechanism for Crossing Domains [33]	Limitations of existing authentication that treats all entities with the same trust level when accessing between domains.	Dynamically adjust authentication strength and procedures according to trust level	Federated/Cross-Domain Authentication	Trust level-based stepwise authentication framework

Table 1. *Cont.*

Paper Title	Problem Setting in CDS Environment	CDS Application Approach	ZT Utilization Approach	Identity Perspective Core
Authentication and Identity Management Based on Zero Trust Security Model in Micro-Cloud Environment [35]	Single point of failure due to dependence on a central IdP in a multi-domain environment.	Redesign into a continuous verification structure by separating authentication and identity management	Continuous Authentication	ZT-based distributed authentication and ID management structure
Dynamic Authentication and Granularized Authorization with a Cross-Domain Zero Trust Architecture for Federated Learning in Large-Scale IoT Networks [36]	In cross-domain IoT, with session-unit authentication alone, it is not possible to block privilege abuse/lateral movement.	Link context-based authentication/authorization to re-evaluate during the session	Continuous Authentication	Context-aware dynamic authentication mechanism
Receiver-Agnostic Radio Frequency Fingerprint Identification for Zero-Trust Wireless Networks [37]	Session-based cryptographic authentication is not possible for continuous/real-time authentication.	Assist authentication across the entire session with physical-layer fingerprints	Continuous Authentication	Continuous authentication (RFFI) based on receiver-agnostic RF fingerprinting
Dynamic Security Computing Framework With Zero Trust Based on Privacy Domain Prevention and Control Theory [38]	In the authentication process, it is difficult to quantitatively evaluate privacy risks.	Automate risk evaluation → classification → response	Continuous Authentication	Framework based on authentication risk evaluation and prevention-control theory
Building a Zero Trust Federation [34]	In a federated environment, the problem of not being able to trust authentication results issued by other domains.	After verifying the generation environment of the authentication result, accept it for federation	Federated/Cross-Domain Authentication	Federated authentication trust structure based on remote verification
Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication [31]	Dependence on a central MFA server and authentication privacy infringement.	Blockchain-based distributed authenticator structure	Credential Verification	Privacy-preserving MFA based on Blockchain + ZKP

3.2. Device

3.2.1. Continuous Zero Trust Device Verification

Wu et al. [39] noted that the Power Internet of Things (PIoT) environment is limited by its large-scale terminal and network architecture. To address this issue, they propose a dynamic access model that integrates device integrity and behavior-based trust, leveraging a zero-trust approach. A 'Device Portrait' was developed by integrating various attributes, including the terminal's operating system, geographic location, and connection status. Using Device Portrait, they verify the device's unique characteristics to generate a device identifier, which allows us to distinguish between devices accessed by the same user account, even if they are different devices. To verify the integrity of the device, the study employed a file hash-based integrity check method and monitored the device's state changes. In the PIoT environment, it defined a device as a continuously validated entity, and proposed a zero-trust strategy that dynamically adjusts access permissions based on the device's trust status.

3.2.2. Cross-Domain Zero Trust Device Trust Inference

Ma et al. [36] found that existing methods have limitations as cross-domain environments where devices frequently move domains become common in large-scale IoT. Applying security separately for each domain slows authentication and increases privacy

problems in the process of sharing data for trust judgment. So, the researchers proposed a security framework that enables dynamic authentication and detailed authorization without moving original data by combining ZTA and DFL. Ma et al. [36] focus on continuous monitoring of device status and trust-based dynamic verification in the device pillar. Unlike one-time authentication performed only at initial access, device requests and states are continuously observed and evaluated throughout the cross-domain process. As a result, only the minimum access privileges corresponding to the current trust level are granted dynamically. Normal devices are granted only the necessary permissions, while access is immediately reduced or blocked when suspicious behavior is detected. From the CDS point of view, a privacy-preserving trust transfer model is presented. Previously, there was a dilemma that "it is dangerous to share, and it is difficult to judge if not" because it had to receive the original data to evaluate other domain devices. This paper uses a method of exchanging only model parameters learned through federated learning. The target domain can estimate the behavior and reliability of external devices without seeing the data directly. In the end, it can be summarized as an example of extending the strict verification of the zero trust to a cross domain without touching data sovereignty. An overview of the privacy-preserving trust inference framework based on DFL and continuous verification is shown in Figure 4.

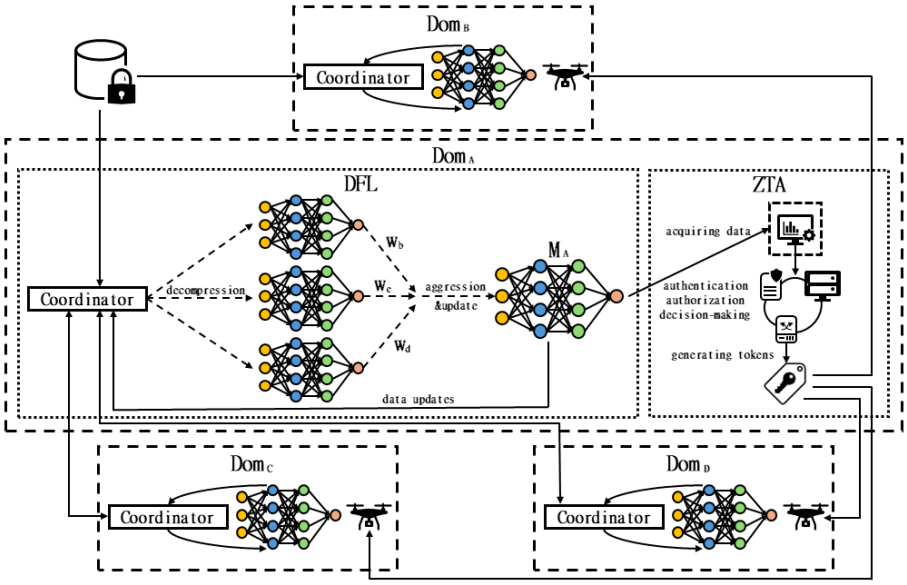


Figure 4. DFL-Based Trust Inference Architecture.Solid arrows indicate request/data flows among components; dashed boxes denote the trust/system boundary separating external entities from internal services; RabbitMQ labels indicate asynchronous message exchanges, and the incoming authentication requests use HTTPS/gRPC.

Wang et al. [40] proposed a blockchain and federated learning-based framework that enables accurate assessment of device reliability in a cross-domain setting with diverse IoT devices, without compromising sensitive data security. To mitigate the risks of a single point of failure and privacy breaches associated with traditional centralized trust management, the research team incorporated a federated learning approach into ZTA's trust evaluation engine, where only local model parameters are shared, without transmitting device data to the outside. Wang et al. [40] go beyond simply calculating the average of model parameters to design a weighted aggregation algorithm that incorporates device attribute information. The authors conduct a comprehensive analysis of devices' resource consumption efficiency and past reliability and apply varying levels of contribution accordingly. Malicious devices are effectively prevented from compromising the global trust model. Furthermore, the

final confidence value is recorded on the blockchain, ensuring that it cannot be tampered with. This implies that the gateway in a cross-domain environment can dynamically manage device access permissions. In conclusion, Wang et al. [40] continuously monitor the dynamic state of devices while meeting the privacy requirements of CDS.

3.2.3. Hardware-Rooted Zero Trust Device Identity

To overcome the limitations of traditional software-based authentication in IoT device environments with limited encryption capabilities and low specifications, Elmaghbub and Hamdaoui [41] proposed a deep learning-based RF hardware fingerprinting technique, dubbed "EPS-CNN". They have developed a unique, unclonable identification system by leveraging the shared RF signal distortion characteristics that occur during the device's hardware manufacturing process. The key difference lies in the fact that existing RF fingerprint technology is susceptible to environmental changes like time and location, which they addressed by developing a new signal representation method called Double-Sided EPS (Envelope Power Spectrum). The proposed framework achieved a time boundary accuracy of over 95% even in cross-domain scenarios where dates or locations are frequently changed. With this, device authentication can be achieved in a domain-agnostic manner, unaffected by specific network environments, allowing devices to be instantly trusted through their hardware uniqueness, regardless of the environment they connect to.

In low-power IoT environments relying on long-distance communication, Hamdaoui and Elmaghbub [41] highlight a critical vulnerability in traditional cryptographic authentication, which is susceptible to key exposure and cloning attacks. They propose a deep learning-based RF device fingerprinting technique and analyze its limitations. Their approach leverages inherent hardware imperfections arising during the device transmission process as a key identifier within the Device Pillar of ZTA. In particular, distortion characteristics in the out-of-band spectrum are exploited. The proposed CNN model achieves a high identification accuracy of over 99% even among devices manufactured using the same process, suggesting that it can provide a robust and virtually unclonable means of identification. However, the key takeaway is that they have identified the limitations of applying this approach in a real-world cross-domain setting. When conducted in a different learning environment or under varying hardware receiver conditions, the identification accuracy significantly decreased. They have found that ZTA technology, which relies on the physical layer, offers robust security within a single domain, but it is highly vulnerable to the Domain Shift issue when devices are moved or in cross-domain environments.

3.2.4. State-Bound Zero Trust Device Authorization

Díaz-Sánchez et al. [42] argue that traditional firewall models, which rely on a centralized Policy Decision Point (PDP), are limited in large-scale IoT environments where numerous devices are connected. They proposed an architecture that leverages Trapdoor Chameleon Hashes to enable decentralized zero-trust tokens. To obtain a token, you must first establish a token generation process that verifies your device's integrity, which is a prerequisite for token issuance. The issued token is cryptographically linked to the device's private key and communication flow. This approach effectively prevents token theft or reuse, and enables conditional access control by allowing communication until the device is in a valid state. In a cross-domain environment, tokens can include verifiable policies and signatures, allowing for independent verification of distributed firewalls or gateways on a per-packet basis, without needing to communicate with a central server.

3.2.5. Federated Zero Trust Device Trust Propagation

Previous studies have primarily utilized blockchain as a simple decentralized storage system, but Li et al. [43] have instead focused on the connectivity issue between blockchains.

They proposed a dual-layered architecture, comprising a local chain and a federated chain, to enable secure authentication credentials to be transferred between different blockchain systems across Cross Domain. Each domain manages device identity through its own independent local blockchain, but when inter-domain interaction is needed, it uses a federated blockchain to exchange only authentication metadata. Specifically, when handling requests from devices in other domains, the system is designed to rely on a distributed authentication and consensus algorithm, rather than a single node's judgment, to ensure cross-validation by multiple nodes based on a predetermined threshold. In a cross-domain environment where trust is not established, it prevents tampering with device authentication information, while in a trusted cross-domain environment, it ensures security is maintained. The dual-layer (local chain–federated chain) architecture for cross-domain device trust propagation is illustrated in Figure 5.

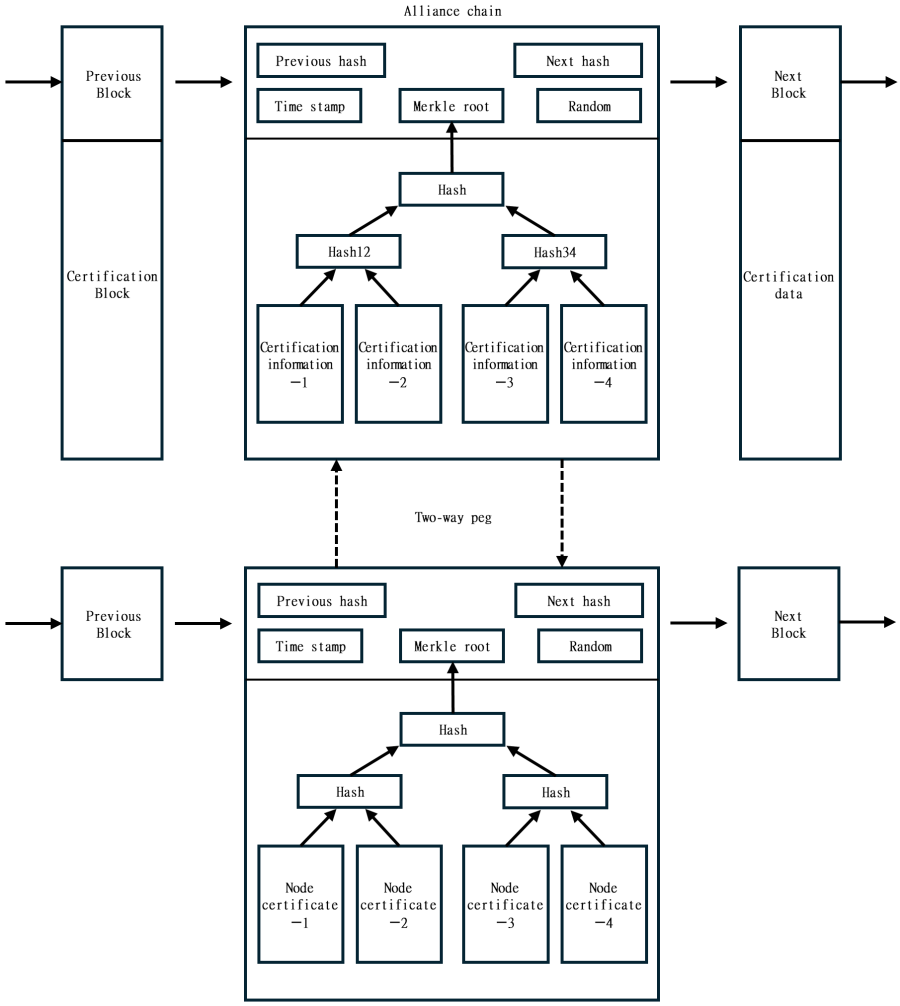


Figure 5. Blockchain-Based Certification Data Structure.

Poirrier et al. [34] pointed out that the existing security model, which relied on device state information provided by other domains in a scenario where multiple independent security domains were interconnected, had a flaw. To address this issue, the research team proposed an architecture that leverages Remote Attestation technology to validate the integrity of a secure infrastructure that generates device state attributes. By implementing the Device Pillar of ZTA, they have moved beyond the traditional approach of forcing agents to be installed on individual devices. However, the security component that monitors and manages the device itself was chosen as the verification target. As a result, a new trust standard was established, which holds that only device information generated from systems with verified

normal operation can be trusted. This means that in a cross-domain environment where trust is lacking, you can technically verify the security operational status of the requesting domain, allowing you to confidently use device attribute information from external sources in your access control policies. In conclusion, Poirrier et al. [34] established a Root that ensures the integrity of device data across the entire federated environment, and provided a foundation for applying consistent ZTA security principles to devices that transcend physical boundaries.

3.2.6. Zero Trust Device Onboarding

Reaz and Wunder [44] argue that traditional zero-trust architectures are effective in verifying device registration, but they have a flaw: they implicitly trust the security posture of manufacturers and supply chains during the onboarding process, when devices first connect to the network. "The problem arises when a supply chain is compromised, rendering all subsequent verification efforts futile." To address this, the research team proposed the ASOP (A Sovereign Device Onboarding Protocol), which enables users to directly verify the identity of a device, thereby bypassing manufacturers and third-party certification bodies. ASOP shifts the trust anchor for device onboarding from manufacturers to end users. It employs FIDO-based authentication and a human-in-the-loop mechanism to ensure that only devices physically verified by users are registered in the cloud. To mitigate man-in-the-middle attacks and manufacturer backdoors, ASOP generates and exchanges ephemeral onboarding keys using quantum-resistant cryptography, rather than relying on manufacturer-embedded initial keys. When implementing the Device Pillar of ZTA, the goal went beyond simply verifying the security status of the device, aiming to ensure its integrity from the production stage onwards. Specifically, the process of moving assets from an untrusted external domain to an internal domain within the operating environment has been redefined as a cross-domain operation. This is seen as a way to prevent potential threats that could arise during the hardware supply phase from contaminating the zero-trust environment. To provide a consolidated view of the studies discussed above, we summarize the key points in Table 2. The ASOP-based device onboarding workflow is illustrated in Figure 6.

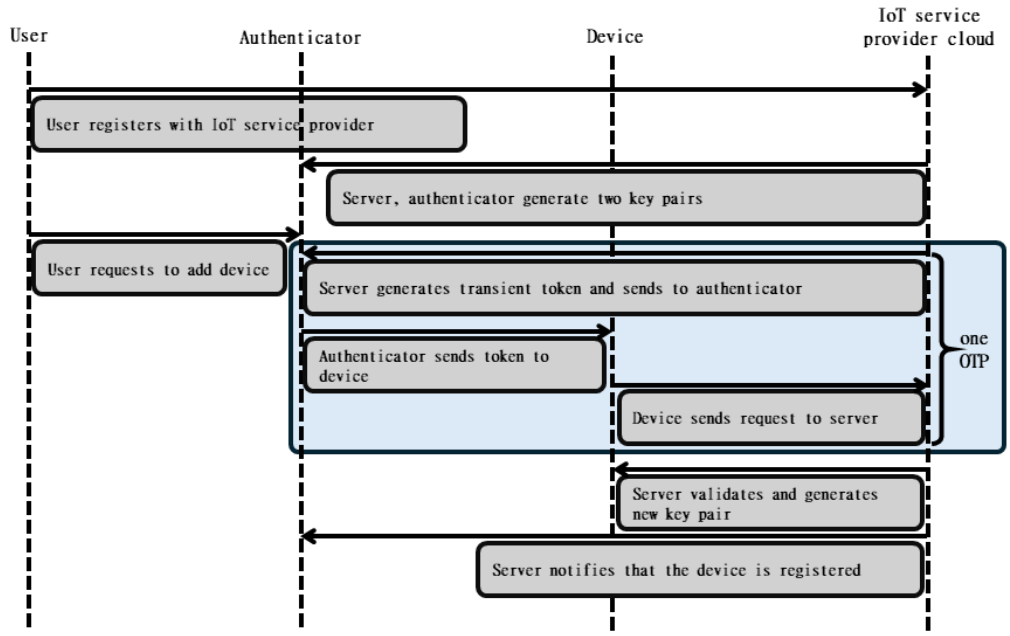


Figure 6. One-Time The vertical dashed lines denote the lifelines of each entity, horizontal arrows indicate message flow, and the shaded region highlights the one-time token (OTT) generation and validation phase.

Table 2. Summary of Research on the Device Pillar in CDS Environments. This table summarizes representative CDS-related research based on approaches for establishing device trust.

Paper Title	Problem Setting in CDS Environment	CDS Application Approach	ZT Utilization Approach	Device Perspective Core
Research on Security Strategy of Power Internet of Things Devices Based on Zero-Trust [39]	In a multi-domain structure where Power IoT is separated into operation, control, and field terminals, the assumption that the inside has the same trust is vulnerable.	Instead of domain/location-based trust, make access decisions based on device attributes, behavior, and traffic	Continuous Verification	Device profiling based on a Device Portrait + EID generation, SDN traffic baseline
Dynamic Authentication and Granularized Authorization with a Cross-Domain Zero Trust Architecture for Federated Learning in Large-Scale IoT Networks [36]	In large-scale cross-domain IoT, when domains move/interconnect, there are limitations of one-time authentication/authorization.	Share learning results by domain to distribute context prediction and dynamic policy decision-making	Continuous Verification	Device context/risk prediction based on DFL and performance/distribution-based weight adjustment
Domain-Agnostic Hardware Fingerprinting-Based Device Identifier for Zero-Trust IoT Security [41]	Due to channel/time/environment changes, the identification consistency of the same device decreases in each domain.	Secure 'domain-independent' identification stability with signal representations robust to domain changes.	Device Identity Establishment	Double-Sided EPS signal representation + EPS-CNN device identification framework
Zero-Trust Token Authorization with Trapdoor Hashes for Scalable Distributed Firewalls [42]	In distributed/multi-domain environments, central authorization/static firewalls have scalability and operational limitations.	Tokenize the device state-attestation results and verify them in distributed firewalls without central dependence	Continuous Verification	State-binding authorization token based on Trapdoor/Chameleon hash + non-interactive verification
Research on Multidomain Authentication of IoT Based on Cross-Chain Technology [43]	In multi-domain environments, device credential verification/sharing is disconnected at domain boundaries.	Perform inter-domain verification/consensus with a local chain–federation (alliance) chain structure	Trust Propagation	Cross-chain authentication structure and threshold-based distributed authentication
ASOP: A Sovereign and Secure Device Onboarding Protocol for Cloud-based IoT Services [44]	Onboarding between manufacturer–supply chain–cloud depends on pre-established trust.	Securely bootstrap device–cloud trust in a user-driven way	Trust Bootstrapping	ASOP onboarding protocol and registration based on one-time/temporary credentials (initial trust establishment)
Deep-Learning-Based Device Fingerprinting for Increased LoRa-IoT Security: Sensitivity to Network Deployment Changes [41]	With LoRa deployment/channel/receiver changes, trust in fingerprint-based identification is shaken.	Experimentally identify fingerprint applicability and 'deployment change sensitivity' (presenting field-application issues)	Device Identity Establishment	DL device fingerprint (CNN) based on OOB (out-of-band) spectrum + deployment-change sensitivity analysis
Building a Zero Trust Federation [34]	In a federation domain, the key issue is the reliability (provenance) of device attributes created by another domain.	Secure provenance trust for attributes by remotely verifying the attribute-issuing entity (IdM/CDM, etc.)	Trust Propagation	Verification of attribute-creation environment/system integrity based on Remote Attestation (provenance verification)
Trust Management for IoT Devices Based on Federated Learning and Blockchain [40]	In cross-domain IoT, malicious devices contaminate the trust model or forge/alter evaluation results.	Distributed learning of the trust model with FL + integrity/sharing of trust scores with blockchain	Continuous Verification	Derive an FL-based Trust Score + record/share via blockchain (ensure reputation/trust immutability)

3.3. Network

3.3.1. Bidirectional Zero Trust CDS

Ansariyan and Doostari [45] found that in a DER environment, IT and OT need to coexist, but existing CDSs struggle to keep pace. A one-way structure can be frustrating for communication, and a centralized structure is vulnerable to collapse if one part fails. They propose a decentralized CDS security architecture that enables secure two-way communication between high-security and low-security domains. Ansariyan and Doostari [45] can be seen as presenting a case of strengthening network segmentation and data protection during transmission, tailored to the CDS environment from the perspective of ZTA. To avoid concentrating security checks on a single perimeter gateway, they have distributed them across multiple nodes. By dividing the network into smaller segments, the attack surface is reduced. Even if a specific node is taken down, the entire domain remains stable. The design aims to enhance resilience. This architecture has moved beyond the traditional reliance on physical one-way transmission devices. They create a two-way secure channel that is strictly controlled and logically secure. Distributed CDS nodes thoroughly inspect traffic content and protocols in both directions. The system demonstrates that efficient data exchange is possible even in a smart grid environment where physical boundaries are blurred, all while adhering to the zero-trust principle of verifying every transaction.

3.3.2. Extreme Zero Trust by Physical Disconnection

Even as cyber threats have become increasingly sophisticated, Na and B [46] reaffirm that physical and logical network separation remains the most effective means of safeguarding critical infrastructure. Their work focuses on network segmentation and attack surface minimization. The extreme isolation model they propose eliminates the possibility of malicious code transmission or remote hacking by physically isolating systems from external networks through a physical air gap. Na and B [46] also clearly demonstrate the connection between CDS and ZTA. While traditional CDSs were primarily designed around physical disconnection, they propose an alternative approach based on logical air gaps and air-fiber technologies that rely on encryption and strict access control. This approach preserves the effect of near-complete isolation while still enabling controlled data exchange when required. In this context, the concept of software-defined boundaries is effectively introduced into the network separation environment. In conclusion, Na and B [46] move beyond simple disconnection when protecting high-trust domains such as SCADA or financial networks. Their approach emphasizes both isolation and controlled connectivity. The significance of their work lies in presenting a practical network separation architecture that integrates logical isolation technologies grounded in zero-trust principles.

3.3.3. Cloud-Native Zero Trust CDS

Gurram [47] identify the challenge of maintaining interoperability and security in hybrid cloud environments that combine public and private infrastructures, where each domain operates under distinct technologies and policies. They propose a comprehensive management architecture that integrates AI-based orchestration, Kubernetes Federation, and a zero-trust security framework. Gurram [47] focus on micro-segmentation at the network pillar layer and integrated networking based on a service mesh. They address the limitation of boundary-based security, which struggles to prevent lateral movement in distributed environments. By dividing the network into workload-level units and continuously verifying each request, the attack surface is significantly reduced. Through the service mesh, traffic management rules and security policies can be applied in a unified manner, even across physically separated domains. From a CDS perspective, Gurram [47] propose a cross-domain integration model that transcends physical boundaries. They observe that

relying on a single point of authentication between cloud providers introduces potential vulnerabilities. To mitigate this, they implement a blockchain-based decentralized identity verification mechanism that enables cross-domain authentication without dependence on a centralized trusted authority, thereby improving resilience against failures. Ultimately, Gurram [47] demonstrate an approach that simplifies operational automation in complex hybrid cloud environments while preserving zero-trust principles. Their work can be summarized as a consolidation strategy that reduces operational complexity without compromising security integrity.

3.3.4. One-Way Boundary Zero Trust

During the replacement of digital instrumentation at the NIST Research Reactor (NBSR), Arneson and Şahin [48] discovered a limitation in which a significant cyber threat to the internal network arises when exporting internal safety sensor data for external analysis. They designed and implemented a physical data diode based on a multi-threaded architecture. Arneson and Şahin [48] focus on removing network segmentation vulnerabilities and attack surfaces from the Network pillar component. They argue that relying solely on software firewalls leaves exploitable vulnerabilities. To eliminate the reverse electrical path, they physically isolate the TX and RX lines of the RS-232 serial cable from each other. As a result, the possibility of external networks infiltrating the internal network is structurally blocked. The Java-based multi-threaded architecture addresses bottlenecks caused by security constraints that had limited parallel processing of multiple sensor data streams. From a CDS perspective, the OT environment highlights the importance of physical reliability in security design. In high-risk facilities, logical verification alone may be insufficient. Their approach treats external networks as potential threats and enforces strict physical unidirectionality to establish a robust security boundary. Their work can be summarized as a hardware-based ZTA implementation that balances data visibility with system safety in critical infrastructure.

Dahlstrom and Taylor [49] discovered that physical air-gaps and software-based high-assurance guards, which were previously used to protect civil-military classified systems, have limitations in cloud analysis and CBM environments. Operational efficiency was declining, and management costs were escalating. They proposed a single FPGA/SoC-based Intelligent Diode architecture. Dahlstrom and Taylor [49] focus on Deep Traffic Inspection and content integrity verification as the core components of the Network Pillar. This structure is not limited to inspecting protocol headers such as Ethernet, IP, and TCP/UDP. The hardware parser implemented within the FPGA performs real-time verification of application-layer formats, including JSON. The architecture enforces packet structure and syntax at the circuit level without software intervention. Ultimately, they demonstrate that verifying all traffic with low latency is feasible even at gigabit speeds. From a CDS perspective, Dahlstrom and Taylor [49] address the limitations of existing HAGs that rely on heavy software stacks such as virtual machines and operating systems. They propose a hardware-centric model that minimizes the trusted computing base (TCB). Their architecture enables secure connectivity to external cloud environments even in high-risk settings. The approach aims to bridge the gap between the security of fully air-gapped systems and the availability of connected systems. Ultimately, their work can be distilled into a practical CDS alternative that applies zero-trust principles through a hardware-centric design.

Borges de Freitas et al. [50] discovered that physical data diodes are widely used in critical infrastructure such as ICSs, but in practice they are hindered by high equipment costs and limited scalability. Many users pointed out that they are difficult to apply to large-scale environments such as cloud or massive IoT systems. They proposed a virtual data diode architecture that leverages SDN to software-enable the one-way functionality traditionally

provided by hardware data diodes. Borges de Freitas et al. [50] employ software-defined boundaries and micro-segmentation within the Network Pillar component. They develop a mechanism to enforce unidirectional flow rules on network switches through SDN controllers, enabling logical one-way communication without physically disconnecting cables. These rules can be decomposed into finer-grained units, such as tenants or service-level segments, allowing more precise enforcement. Ultimately, their architecture enables policy-based control of trust boundaries without relying on physical separation. From a CDS perspective, Borges de Freitas et al. [50] treat CDS functionality as virtualized. They implement one-way security guarantees on general-purpose networking hardware without requiring dedicated diode devices. By removing budgetary and operational constraints, their approach extends zero-trust isolation to environments that previously could not support hardware-based CDS solutions. Their work can be summarized as a practical implementation that combines cloud-native scalability with the strict control requirements of CDS through SDN-based design.

Peter Story [51]—a journalist exposed to sophisticated threats such as state-sponsored hackers—has found that while air-gap workstations are used to protect sources and prevent malware infections, they are not a practical solution due to their limitations. Moving data requires using a USB drive, which is inconvenient and also increases the risk of USB-mediated attacks. While commercial data diodes can be a viable solution, their high cost makes them impractical for individuals or small organizations. He proposed a cost-effective approach to creating DIY data diodes using affordable, off-the-shelf hardware such as the Raspberry Pi. Peter Story [51] focuses on physical network segmentation as the core concept within the Network Pillar component. To prevent reverse communication, the transmission and reception wiring of the Ethernet cable can be physically separated, or an optical Ethernet converter can be used to enforce hardware-level unidirectionality. This method structurally eliminates pathways through which internal data could leak or external attack commands could infiltrate. However, one-way communication introduces challenges where TCP handshaking is not feasible. To enhance reliability, he ensures transmission integrity using pydiode software with forward error correction (FEC) applied. From a CDS perspective, the significance lies in the fact that high-reliability CDS technology has been successfully applied in the private sector. The concept of isolation, previously limited to military or public-sector use, can now be implemented at lower cost. Even NGOs and freelancers with limited budgets can establish strong environments based on physical separation. Ultimately, his work demonstrates that zero trust can be achieved not only through expensive equipment, but also through careful architectural design.

Okhravi and Sheldon [52] pointed out that traditional perimeter security measures, such as firewalls and DMZs, can be vulnerable to security misconfigurations or bypass attacks when integrating ICS with corporate networks. To address this issue, they proposed an architecture that combines data diodes with TPCN. Okhravi and Sheldon [52] focus on network segmentation and entry control as the core components of the Network Pillar component. The data diode physically isolates the control network, thereby eliminating the reverse attack path. At the same time, devices attached to the network are pre-verified through TPCN. The system does not only perform authentication and authorization; it also verifies device integrity and allows access exclusively to equipment that satisfies predefined security requirements. Ultimately, their approach aims to construct a more robust infrastructure by combining physical disconnection with logical device-state verification, rather than relying on blocking alone. From a CDS perspective, Okhravi and Sheldon [52] assume that relying solely on data diodes is insufficient to address all security challenges. Building on the guarantees provided by physical unidirectionality, they incorporate policy-based

verification to achieve a defense-in-depth strategy. The resulting flow physically separates networks while logically verifying and permitting only validated traffic.

Jones and Bowersox [53] found that traditional methods are limited in high-assurance systems, where information disclosure to the outside is necessary, but external access is strictly prohibited. Air-gap systems are cumbersome to operate, and commercial security devices are notoriously complex, making them hard to verify. They proposed a simple data diode design, excluding complex integrated circuits and instead using only optical components like LEDs. Jones and Bowersox [53] focus on physical segmentation and removal of attack surfaces within the Network pillar component. By physically isolating the path that could generate a reverse electrical signal, the attack surface is fundamentally reduced. At the same time, their design is simplified to the extreme, allowing external auditors to verify unidirectional flow without requiring specialized equipment. To minimize the need for trust, they implement a verification-centric principle at the hardware level, with an emphasis on transparency and visibility. From a CDS perspective, Jones and Bowersox [53] suggest that CDS should move away from reliance on vendor guarantees, which often function as black boxes. Instead, they advocate a white-box approach that users can directly verify. In domains where social trust is paramount, such as electoral systems, security outweighs performance considerations, making verifiability essential. Ultimately, their work demonstrates that a CDS with a simple and transparent design can realize the kind of verifiable trust promoted by Zero Trust, where reliability can be independently assessed.To provide a consolidated view of the studies discussed above, we summarize the key points in Table 3.

Table 3. Summary of Research on the Network Pillar in CDS Environments. This table summarizes CDS-related research strategically categorized based on network segmentation centered on bidirectional communication.

Paper Title	Problem Setting in CDS Environment	CDS Application Approach	ZT Utilization Approach	Network Perspective Core
A Novel Bidirectional Distributed Cross Domain Solution Security Architecture [45]	In bidirectional communication between high/low security domains, risk of response forgery, re-injection, and reverse intrusio.	Distributed CDS structure + support for bidirectional data flow + state-based verification	Macro-segmentation, state-based threat response, request-response-based traffic control, distributed structure	Bidirectional CDS based on stateful correlation
A Study on Air-Gap Networks [46]	The external network connection itself is an attack path (if connected, intrusion/exfiltration is possible).	Complete separation of domains with a physical air-gap (remove the connection)	Physical network segmentation (separation), threat mitigation by pre-blocking method	Complete separation that removes communication (blocking type)
Cross-domain integration for hybrid cloud management: Innovations and future directions [47]	In linkage between hybrid clouds, risk of domain boundary collapse and spread.	Logical boundaries at the service/workload unit + policy-based integration (cloud-native)	Micro-segmentation (service), TLS, service-mesh-based traffic control	Logical CDS based on Service Mesh
Cyber Security using Multi-Threaded Architecture Data Diode at the NBSR [48]	Need to block reverse-direction intrusion and remote attacks into key facilities (control network).	Enforce one-way with a data diode + improve export efficiency with system processing (multi-threaded)	Macro-segmentation, reverse-direction blocking (Default Deny), one-way traffic management	Fundamentally block reverse intrusion with a one-way boundary
Protecting Networks with Intelligent Diodes [49]	A simple diode has difficulty blocking the inflow of format-violating/contaminated data.	Intelligent diode including hardware (FPGA)-based packet/payload verification	Default Deny, threat response based on real-time verification, only allowed formats pass, optional encryption	One-way control with format/syntax verification type

Table 3. *Cont.*

Paper Title	Problem Setting in CDS Environment	CDS Application Approach	ZT Utilization Approach	Network Perspective Core
SDN-enabled Virtual Data Diode [50]	Lack of flexibility of physical diodes (difficult to change policy and expand operation).	Implement a virtual diode that enforces one-way via SDN flow rules	SDN-based micro-segmentation (flow), Default Deny, central policy control	Enforce one-way with SDN flow
Building an affordable data diode to protect journalists [51]	Safe outward export in a low-cost environment (prevent reverse intrusion/exfiltration).	Implement one-way export with a DIY/low-cost data diode	Macro-segmentation (physical separation), reverse-direction blocking, one-way traffic management	Low-cost one-way export
Data Diodes in Support of Trustworthy Cyber Infrastructure [52]	To protect ICS/PCN, minimize the risk of connections with corporate networks/outside.	Configure a one-way boundary centered on a diode + DMZ (traditional ICS pattern)	Zone-based macro-segmentation, one-way data flow	Traditional ICS one-way boundary
Secure Data Export and Auditing using Data Diodes [53]	Secure both safe data disclosure and auditability (transparency) at the same time.	One-way transfer + enhance ease of auditing with a simple/visible format (XML)	Complete reverse-direction blocking, one-way traffic management (simplification)	One-way CDS centered on auditability
Secure Data Transfer Guidance for Industrial Control and SCADA Systems [54]	Transfer between ICS/SCADA domains expands the attack surface (direct connection risk).	Transfer architecture guide based on Security Zone/DMZ/whitelist	Macro-segmentation (zone), threat response based on monitoring, encryption recommended, only allowed communications	Zone separation + only allowed communications (guide type)

3.4. Application

Some CDS studies utilize mechanisms like filtering and segmentation at the network layer as auxiliary tools. Therefore, if the primary control point is application workload identification, request-response semantic validation, and workload isolation, we classify these studies as application-level, even if network control is used as an auxiliary tool.

3.4.1. Stateful Zero Trust App Gateway

Choi et al [55] assumes that the High domain is fully under the attacker's control, and that the High domain does not trust any responses from this domain by default, requiring them to be verified through a firewall. This is a direct application of the ZTA premise, which rejects basic trust, regardless of whether it is within or outside the network, at the domain level. The core feature proposed by Choi et al [55] stateful correlation, enables explicit and context-based verification of ZTA application pillars. The system stores the function code, TCP sequence number, segment length, and timestamp of Modbus-TCP request packets sent from the high domain, and only permits them to pass through if the incoming response packets from the low domain match these stored values exactly. All responses that do not match the request are blocked, resulting in a 0% false positive and false negative rate in the experiment. This is an implementation of the ZTA-style implicit deny principle, which holds that all responses are only allowed if they are related to a preceding legitimate request, at the application layer. The bidirectional DPI firewall proposed in the paper also serves as a Policy Enforcement Point (PEP), as described by ZTA. Packet recognizers and analyzers interpret packets based on user-defined protocols, states, and rule sets, and enforce all communications between domains (i.e., sets of applications that do not trust each other) according to a central policy, determining whether to allow or block them. This paper can be summarized as a concrete example of how the principles of

ZTA application pillars (disbelief, least privilege, state and context-based verification, and policy-based filtering) are applied to CDSs situated at the domain boundary.

3.4.2. Cloud-Native Zero Trust CDS (Verified Isolation)

Daughety et al. [56] highlight the limitations of existing CDS systems, which lack a formally verified Trusted Computing Base (TCB), making it impossible to ensure mathematical reliability, and are unsuitable for cloud environments or remote deployment due to their reliance on physical hardware. To address these issues, Daughety et al. [56] propose the vCDS architecture, which leverages the verified seL4 microkernel to ensure reliability and enables execution in cloud environments through virtualization techniques. Daughety et al. [56] designed vCDS to rigorously enforce a least-privilege model at the application level through seL4's capability-based access control mechanism. Within the system, all kernel services and resource access are restricted to pre-defined capability tokens, making it structurally impossible to arbitrarily expand privileges or access unauthorized resources during execution. Furthermore, by utilizing the static nature of the CAmkES framework to fix permissions and communication paths at compile time, Daughety et al. [56] ensure that the creation of new channels or bypass routes at runtime is blocked. This effectively prevents lateral movement by attackers and ensures a transparent communication structure with no hidden paths or implicit privilege escalation from a zero-trust perspective. Daughety et al. [56] also tightly isolated the High and Low sides as separate VMs or processes and strictly controlled data flow. While data flow from Low to High is allowed, data needing to move from High to Low must pass through a Guard, which serves as a Policy Enforcement Point (PEP) to check if the data content violates policy. Additionally, the High side does not blindly trust data received from the Low side; instead, it verifies it through a Blake3-based Integrity Guard and performs additional filtering. Consequently, Daughety et al. [56] emphasize that vCDS ensures consistent, explicit verification of data flows and requests within the system, adhering to the principle that "you can't trust what you can't verify". This architecture breaks away from traditional security methods relying on physical boundaries, faithfully implementing the core requirements of zero-trust applications in the cloud by leveraging mathematically verified software isolation and enforced policy checks.

3.4.3. Federated Zero Trust Resource Sharing

Fysarakis et al. [57] acts as a logical CDS, facilitating secure communication between disparate network domains, such as smart homes and smart offices/hospitals, and the internet. Previously, inter-domain communication was not possible relying solely on multicast within the local network. However, with the introduction of the MQTT proxy, local discovery and control messages are captured and converted into MQTT messages, which are then securely transmitted to external domains via an internet broker. They opt for a more integrated approach, embedding security features directly into the application itself, rather than relying on network perimeter defense. By implementing PEP software within individual smart devices, the concept of micro-borders was realized. Instead of controlling access by network IP range, it checks policies on a per-resource basis, comparing the requested action and source ID. Even if they're accessing the same IP, unauthorized users will not be able to access specific application features. Furthermore, XACML enables comprehensive and fine-grained access control across users, resources, and environments, and each time, it verifies communication with the PDP. XSACd is built on CDS technology, which enables connections between different domains without being constrained by physical location. This model goes beyond simple connectivity, embedding PEP within the

device (application), controlling it on a per-feature basis through XACML, and verifying each request, thereby fully adhering to the application pillar of the zero-trust architecture.

Xu et al. [58] discovered that in a 5G and IoT integrated environment, IoT applications need to navigate multiple management domains, but existing approaches fall short. A static security system struggles to keep up with the dynamic nature of changing application requirements, and the issue of trust between domains persists. The research team proposed a dynamic edge resource federation architecture that integrates network slicing and blockchain. Xu et al. [58] center on ensuring application logic integrity and workload-centric access control within the Application Pillar component. Instead of relying on a central authentication server to manage policies, the system has shifted to a blockchain-based smart contract that directly handles access control and resource allocation logic. With policies encoded and becoming harder to tamper with, the transparency and consistency of the logic are ensured. Furthermore, it dynamically creates dedicated network slices tailored to the specific security requirements and quality standards of each IoT application. This is a method of providing a dedicated execution environment that isolates infrastructure to meet the specific needs of applications. From a CDS perspective, the model ensures that services remain uninterrupted even when applications, previously constrained by physical boundaries, are moved across domains. In domains where trust is lacking, people or institutions are often distrusted, but a verified code, such as a smart contract, can serve as a common anchor of trust. The system is designed to automatically handle procedures like authentication and billing on top of that. Ultimately, this research can be summarized as a dynamic federated model based on ZTA, which integrates application mobility and decentralized trust to facilitate cross-domain collaboration.

3.4.4. Proxy-Mediated Zero Trust App Isolation

Hsiao et al. [59] proposes a model that ensures secure communication between components from different sources in a web mashup environment, leveraging Trusted Proxy and HTML5 postMessage. This is a logical CDS technology that also embodies the Zero Trust (ZTA) application security principle. It rejects broad domain-level trust and instead controls access on a fine-grained, element-by-element basis within HTML. The 'minimum privilege principle' is enforced at the application layer, allowing access to only the specific data that has been authorized. Even within the same page, components are not implicitly trusted. The proxy ensures data integrity and confidentiality by explicitly verifying the sender's identity and authority at each communication, through the library it. injects By isolating each component within an IFRAME and limiting communication to a predetermined path, the system structurally prevents the threat from spreading to other sensitive data even if a specific component is compromised. The proposed model is a logical CDS that breaks away from traditional methods that relied on physical boundaries, instead implementing secure cross-platform data transfer through proxy-based policy injection and runtime verification. This technology is considered a key application of the core philosophy of zero-trust architecture, which is based on verification rather than location, in the web application environment.

3.4.5. Workload-Identity Zero Trust for Microservices

As cloud-native environments have become widespread, Rajendran et al. [60] found that the microservices architecture has led to a limitation: traditional perimeter-based security is no longer effective. As East-West traffic within the service grows, visibility and control become increasingly compromised. Building on this, the research team proposed a zero-trust security model based on identity federation, leveraging the SPIFFE/SPIRE and OIDC standards. Rajendran et al. [60] center on mutual authentication between workload

identity and service in the Application pillar component. It does not determine who is who based on location information like IP addresses. The service itself is assigned a unique identifier that is encrypted. Whenever services communicate with each other, mutual authentication is performed using mTLS, and permissions are verified through OAuth 2.0. Ultimately, they have implemented micro-segmentation, breaking down the application layer into service units and verifying each request. From a CDS perspective, they propose a logical trust federation model that enables application connectivity even across physically isolated domains. Microservices from different domains can now exchange trust bundles and verify each other's identities without relying on a central authentication server. It is claimed that this can ensure secure communication of workloads across domain boundaries, even without the need for dedicated physical CDS equipment. Their model demonstrates a direction for applying consistent ZTA policies across hybrid and multi-cloud environments, as it transitions from infrastructure-centric security to application-centric security.

Jonnakuti [61] discovered that managing machine learning pipelines across different clouds, like AWS, Azure, and GCP, can be a significant challenge. To keep pace with the rapid adoption of AI, they need to utilize distributed resources, but as the number of connections between domains grows, so does the attack surface. To safeguard both data privacy and model integrity, they proposed a zero-trust architecture for multi-cloud AI workloads. Jonnakuti [61] center on service unit authentication and workload identity verification as the core components of the Application Pillar section. To move beyond a simplistic approach that relies solely on network boundaries, they verify each time whether the services and containers participating in the learning process are indeed authorized entities. The communication section is secured with end-to-end encryption based on TLS 1.3. The policy enforcement layer ensures that only approved workloads are allowed to participate in learning by verifying the metadata and access context of the learning session. Ultimately, the structure is designed to track who has accessed the learning application from start to finish. From a CDS perspective, this approach presents a way to safeguard data sovereignty in a cross-domain environment that spans multiple clouds. The original data is not transmitted externally, but rather the model parameters are exchanged using a federated learning approach. The goal is to enable domains that do not trust each other to collaborate while adhering to regulations. Ultimately, their work can be summarized as a case where logical CDS is implemented in a way that data remains static while learning occurs simultaneouslyTo provide a consolidated view of the studies discussed above, we summarize the key points in Table 4.

Table 4. Summary of Research on the Application Pillar in CDS Environments. This table summarizes CDS-related research based on cross-domain workload isolation or trusted application mechanisms.

Paper Title	Problem Setting in CDS Environment	CDS Application Approach	ZT Utilization Approach	Application Perspective Core
vCDS: A Virtualized Cross Domain Solution Architecture [56]	Existing CDSs are hard to use in general environments because they focus on defense; remote/cloud distribution is difficult due to reliance on physical equipment; verification is difficult because the inside is a black box. Price and accessibility are also low.	Virtualized CDS, domain-level traffic control	Workload isolation, least privilege	Based on a processor that inspects data flow (e.g., IDS/IPS or firewall), a CDS structure extensible to data sharing and cloud analysis environments is presented.
Cross Domain Solution with Stateful Correlation of Outgoing and Incoming Application-Layer Packets [55]	Industrial protocols follow a 'request → response' pattern, but existing equipment is hard to identify, making it difficult to respond to unsolicited responses.	Stateful CDS, bidirectional packet correlation	Continuous verification, micro-segmentation	Secure cross-communication by enforcing rules such as function code and ordering when communicating with smart grid/ICS control networks.

Table 4. *Cont.*

Paper Title	Problem Setting in CDS Environment	CDS Application Approach	ZT Utilization Approach	Application Perspective Core
XSACd–Cross-domain resource sharing & access control for smart environments [57]	DPWS discovery/communication works mainly within the same network, so it is difficult to use across different domains, imposing major deployment constraints	Federated CDS, multi-cloud resource sharing	Identity-based access control, policy automation	Smart home/IoT shares device resources while extending fine-grained access control across domains.
A Secure Proxy-Based Cross-Domain Communication for Web Mashups [59]	Web browsers limit data exchange between different sources due to SOP, making desired interactions in client mashups difficult	Proxy-based CDS, web API isolation	Request authentication, sessionless verification	Minimizes developer code modification while enabling secure data exchange between sources in mashups.
Zero Trust Security Model Implementation in Microservices Architectures Using Identity Federation [60]	As services increase, communication paths become more complex	Microservice federation, service-to-service trust	Workload identity, continuous authentication	Tokens are obtained from API Gateway/BFF; internal authorization is managed as code via token exchange and OPA.
Zero-Trust Architectures for Secure MultiCloud AI Workloads [61]	Different environments use different authentication and logging methods, making unified security boundaries difficult.	Multi-cloud orchestration, federated identity	Workload protection, continuous monitoring	Bundles cloud-specific policies into common policies and a single flow for observation and response automation.
A Secure Dynamic Edge Resource Federation Architecture for Cross-Domain IoT Systems [58]	It is difficult to operate infrastructure where multiple domains communicate while meeting performance and security requirements.	Edge federation, blockchain-based CDS	Continuous authorization, adaptive access control	Resource orchestration becomes a security perimeter.

3.5. Data

3.5.1. Data-Sovereign Zero Trust Access Control

Ma et al. [36] pointed out that information sharing is essential to assess the trustworthiness of devices from other domains in a cross-domain setting of large-scale IoT networks. However, they found that transmitting the original data in its entirety poses a significant risk of privacy breaches and also leads to increased transmission delays. To enable dynamic authentication and fine-grained authorization, the research team proposed a framework that combines a distributed federated learning approach with a ZTA structure, allowing for seamless cross-domain collaboration without the need to move original data. Ma et al. [36] change the way the target domain retrieves context, such as the state or behavior of external devices, by requesting the original data. The model is designed to share only the learned parameters from the source domain and predict the context of the corresponding device within the target domain. The domain-to-domain control messages and parameter exchange process are safeguarded by an ECC-based encryption channel, thereby enhancing the security of the transmission process. Ma et al. [36] demonstrate demonstrates that data sovereignty can be maintained even in a cross-domain environment where there is no mutual trust, and that sophisticated trust assessments can be made for devices from other domains. With the predicted context as a basis, device-level access rights can be finely adjusted and dynamically assigned based on context, making it a prime example of meeting both privacy requirements and security needs simultaneously. The DFL-based cross-domain zero trust access architecture is illustrated in Figure 7.

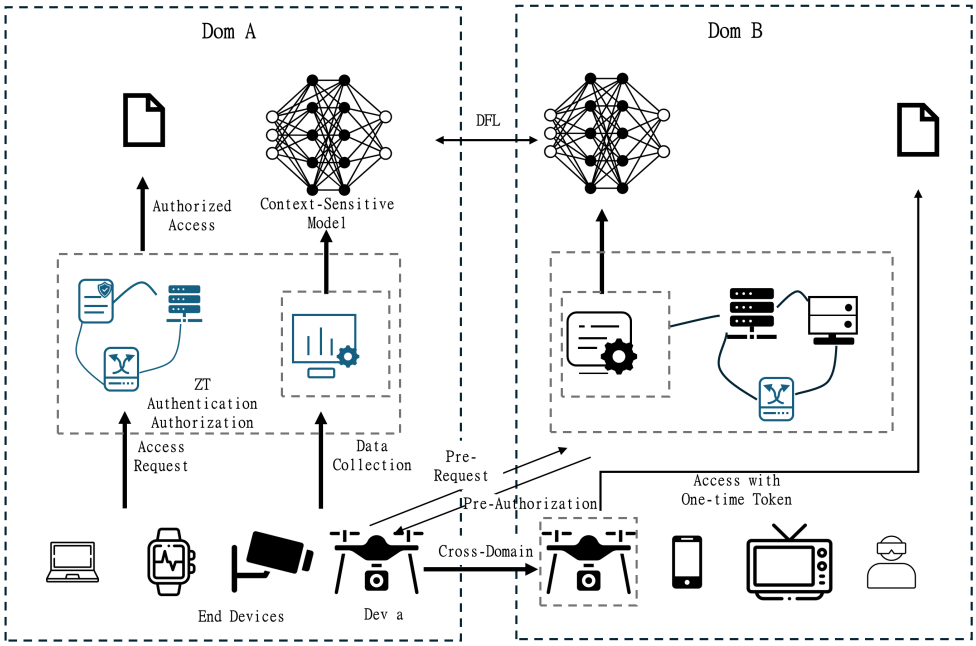


Figure 7. DFL-Based Cross-Domain Zero Trust Access Architecture.

Nguyen et al. [62] found that existing CDS systems are inflexible in environments with multiple security levels, such as the defense and public sectors, where they rely on physical network segregation or dedicated terminals. To facilitate cross-domain data sharing and collaboration, they proposed MYSEA, a cross-domain security architecture built on a cloud-based platform. Although it was researched before the term "zero trust" became widely accepted, it stands out for its clear data-centric control orientation. Nguyen et al. [62] emphasize controlling both the data transmission paths and the inherent properties of the data itself. Initially, they establish a verified tunnel between the terminal and the server, and traffic passing through it is required to be tagged with a security label. As a result, data confidentiality and integrity are preserved. The central server then consistently enforces access control policies based on label information. The system is designed to integrate domains with different security levels into a unified cloud management environment. Ultimately, their architecture does not rely solely on the terminal environment, but instead uses data labels and verified communication paths as the basis for access decisions. The Hyundai ZTA's data-centric control system can be regarded as an early conceptual parallel. Their work can be summarized as demonstrating the feasibility of combining CDS and ZTA principles by migrating high-assurance CDS mechanisms into a more flexible, cloud-based architecture. The multi-level secure cloud architecture is illustrated in Figure 8.

Shonubi [63] has found that traditional perimeter-based security models are no longer viable in environments where the boundaries between organized crime and state-sponsored operations are increasingly blurred, particularly in high-risk settings. Such systems are vulnerable to insider threats and struggle to prevent lateral movement after a breach. Even during prolonged attacks such as APTs, response capabilities remain slow. Shonubi [63] proposed a multi-layered zero-trust architecture as an alternative. Shonubi [63] focus on data-centric security and end-to-end data protection within the Data Pillar of ZTA. The security baseline is shifted from the network perimeter to the data itself. From the moment data is generated, its sensitivity is categorized and labeled. These labels bind security policies, ensuring that control follows the data regardless of its destination. Data loss prevention (DLP) mechanisms tightly regulate data entering and leaving the domain. The architecture is designed to maintain encryption not only during storage and

transmission but also throughout the data processing pipeline. Even if parts of the system are compromised, the design aims to preserve data confidentiality. Shonubi [63] also aim to mitigate the limitations of approaches that rely solely on physical network separation by integrating CDS concepts with ZTA. By incorporating SDP (software-defined perimeter) and SASE (secure access service edge), the architecture establishes logically secure connections that transcend physical boundaries. Cross-domain access histories are recorded on a blockchain, making them resistant to tampering and enabling accountability tracking within a federated environment. Ultimately, this work demonstrates that a cloud-native combination of technologies can create a highly secure and reliable federated security environment without the constraints imposed by physical isolation.

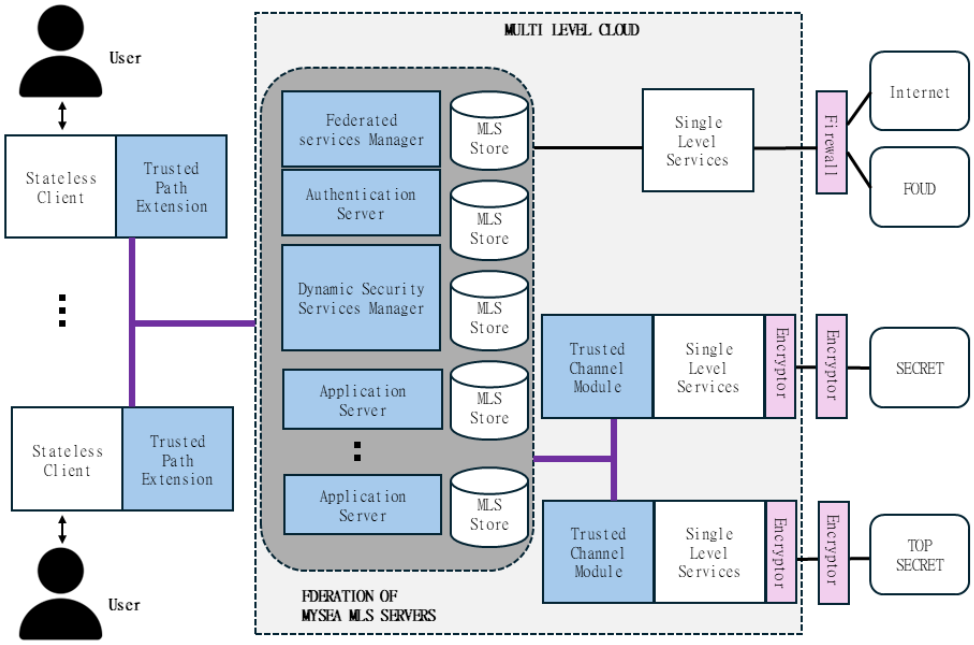


Figure 8. Multi-Level Secure Cloud Architecture.

3.5.2. Auditable Zero Trust Data Sharing

Liu et al. [64] discovered that traditional centralized data sharing methods are limited in large-scale networks where cloud, edge, and end devices are integrated. In situations where strict verification is required every time, as in zero-trust approaches, performance suffers and scalability becomes increasingly difficult as the system grows. They proposed a data-sharing framework that enables multiple domains to collaborate on a shared data structure, built on a sharding blockchain, with the goal of maintaining security while accelerating cross-domain sharing. Liu et al. [64] focus on balancing performance and fairness. Each domain independently processes consensus within its own shard, enabling parallel processing and reducing overall performance bottlenecks. In environments where trust is limited, they employ Merkle tree-based policy attestation to accelerate verification. In scenarios where no trust exists at all, Liu et al. [64] introduce stronger enforcement mechanisms. They utilize smart contracts deployed on public blockchains to prevent unfair behavior by requiring security deposits, and the system is designed to penalize participants who deliberately deny data reception or disrupt data sharing. In essence, Liu et al. [64] eliminate the need for a centralized trusted authority that traditionally acts as a bottleneck in CDS environments, instead distributing trust through blockchain-based consensus. Their results suggest that a scalable data-sharing model capable of handling large-scale traffic is feasible under zero-trust assumptions.

Jiang et al. [65] pointed out that as production processes expand into cross-domain IIoT environments, data sharing becomes a necessity. However, they observe that many domains do not trust each other, and reliance on third-party cloud storage raises concerns about potential privacy breaches. To address these challenges, Jiang et al. [65] propose a CDAS data-sharing scheme that integrates a multi-layer blockchain with IPFS. Their system is designed to enable efficient data sharing while adhering to zero-trust principles, even in resource-constrained device environments. From the perspective of ZTA's Data Pillar, Jiang et al. [65] focus on dynamic access control and decentralized integrity verification enabled through smart contract-based mechanisms. Access control is implemented as a smart contract enforcing ABAC policies, allowing permissions to be automatically verified on-chain without relying on a centralized authentication server. If policy conditions are not satisfied, access is immediately denied. Data are encrypted using symmetric keys and stored on IPFS, while only hashes and indices are recorded on the blockchain. In this way, data confidentiality is preserved while integrity remains verifiable through hash-based validation. Jiang et al. [65] also explore performance bottlenecks that arise when combining CDS and ZTA in IIoT environments. Because resource-constrained devices cannot efficiently handle intensive cryptographic operations and transaction processing, edge servers are introduced to construct an edge blockchain layer and the majority of computational overhead. This design enables the architecture to scale effectively even under massive traffic loads. In conclusion, Jiang et al. [65] move beyond traditional models that rely on a single centralized gateway by decentralizing both consensus and processing. Their work demonstrates that even in environments characterized by mutual distrust, seamless cross-domain collaboration can be achieved while maintaining data confidentiality and integrity. The CDAS multi-layer blockchain–IPFS architecture is illustrated in Figure 9.

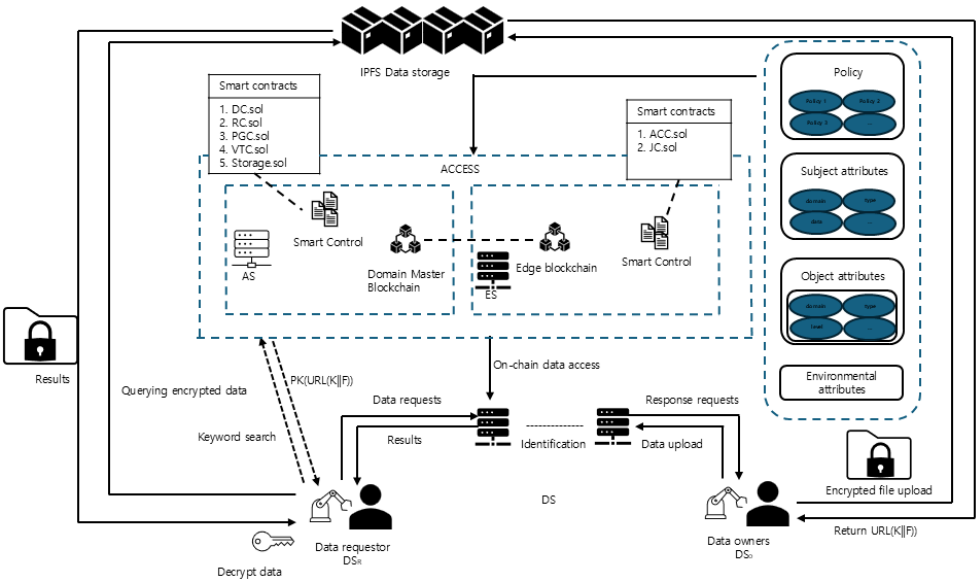


Figure 9. Blockchain-Based Zero Trust Data Access Architecture.

As industrial Internet has spread, Luo et al. [66] observed that there is a growing need for data collaboration across different trust domains. However, they found that the varying attribute systems and access policies across domains make it challenging to achieve secure sharing with a single-domain CP-ABE approach. The investigation also found that existing encryption methods make it hard to track down who leaked the key, even if it is compromised, which makes it difficult to ensure accountability. To address this challenge, the research team proposed a TE-CP-ABE method that balances traceability with efficiency, and integrated it with proxy re-encryption to create a data sharing scheme

tailored to cross-domain environments. In this architecture, the domain proxy does not decrypt the data owner's ciphertext into plaintext. The role is to convert the ciphertext according to the attribute policy of the target domain. Despite the domains being different, confidentiality is maintained. This can be seamlessly integrated with a fine-grained access control policy. The key is that it has successfully integrated data-driven control and accountability tracking. They implemented fine-grained access control at the data level by encrypting access permissions tied to attributes. With white-box traceability, users can now track and block any decryption key leaks or misuse. In conclusion, this approach can be summarized as a model that ensures not only the secure flow of data in a cross-domain environment, but also post-audit assurance.

3.5.3. Confidentiality-Preserving Zero Trust Data Flow

Guo et al. [67] found that in open networks, the need for data sharing across domains conflicts with the need for protection, such as confidentiality, and the need for utility, like search functionality. They also thought that the centralized approach, where one entity controls everything, has its limitations due to scalability and trust issues. The research team proposed a CD-ABSE scheme that combines attribute-based searchable encryption with blockchain technology. The data is designed to be shared across domains, even when it is hidden. The key finding is that it enables searching in a cryptic or encrypted state. In the past, decrypting data was a necessary step, which inevitably compromised confidentiality. In contrast, CD-ABSE enables keyword search in a cryptic state, keeping confidentiality intact until the data is actually accessed. To implement the principle of least privilege at the data level, they have added a structure that allows access to be controlled based on user attributes. Data can only be accessed when certain conditions are met. This scheme also addresses the challenge of domains having a hard time trusting each other, by leveraging blockchain technology. Data access and sharing processes are recorded on the blockchain, making it difficult to tamper with or alter the information. Even without a central trust authority, tracking and auditing become possible. In conclusion, this study can be summarized as a data-centric ZTA model that ensures secure cross-domain movement by encrypting data and enforcing attribute policies, rather than relying on physical boundaries.

Tinker et al. [68] discovered that existing CDSs have a limitation in that they need to decrypt plaintext at the gateway before performing data filtering. Once a gateway is compromised, sensitive data can be exposed at that point. The researchers proposed a structure that enables the gateway to make routing and filtering decisions without seeing the plaintext, by applying homomorphic encryption to the CDS filtering process. This proposal breaks down the role of cryptographic technology into separate components. The data is protected by a block cipher like AES or SIMON. The operations required for filtering determination are implemented concurrently in the YASHE-based homomorphic encryption environment. The intermediate gateway applies a pre-defined filtering operation to encrypted packets. It only generates results based on judgments like pass or block. The final routing decision is made by the router after receiving the result. In conclusion, this approach undermines the underlying structure that relies on the gateway's trustworthiness. The gateway demonstrates that policy enforcement can be achieved without exposing plaintext, even in the most challenging scenarios. In the CDS environment, it can be summarized as an effort to balance the need for zero trust and data protection simultaneously.

3.5.4. Context-Aware Zero Trust Data Control

Smith et al. [69] proposes a framework that systematically decomposes and analyzes existing access control mechanisms to address the challenge of ensuring confidentiality by placing security closest to the data itself from a data-centric security (DCS) perspective,

where dynamic and distributed access control is essential. The paper begins by outlining the objectives and security guidelines of DCS, and then breaks down the DCS infrastructure into three key components: policy, data, and roles. Smith et al. [69] further break down major access controls into sub-concepts such as authorization, activation, access decision, change/revoke, policy change, and context change, and further breaking down sub-divisional concepts like key generation, authority assignment, authority revocation, access decision, encryption/decryption, context management, and data storage/protect into sub-concepts like data storage/protect, and categorizing each study's coverage in a table format. This paper aligns with the operational perspective of data filas, which centers on data classification and labeling, policy integration, and authority/role-based least privilege, as seen in DCS's policy and data filas. It also extends dynamic access decisions to include zero-trust always-verifying access, as well as context-based elements, such as MLS cases.

Feng et al. [70] discovered that in a cross-domain data-sharing environment with multiple layers and complex structures, relying solely on predefined rules is insufficient. Threats continuously evolve, and collaboration patterns vary depending on context. When rigid rules are enforced, system responses become slow to adapt. Building on zero-trust principles, they proposed the FlexiGuard framework, which enables policies to learn and adapt autonomously. The FlexiGuard architecture is illustrated in Figure 10. They employ inductive logic programming (ILP) and Dempster–Shafer evidence theory to achieve this goal. FlexiGuard advances data-driven control by continuously collecting contextual information, including user behavior, network status, and device integrity. The framework extracts recurring patterns using ILP and structures them into security rules. When trust assessments from heterogeneous sources conflict, FlexiGuard reconciles them into a unified decision using evidence theory. Its decision-making and data-processing components operate within a trusted execution environment (TEE), thereby protecting internal computations. Feng et al. [70] further strengthen domain authentication and communication mechanisms. To address future threats, they aim to integrate blockchain-based decentralized identities (DID) and incorporate post-quantum cryptography and quantum key distribution techniques. In conclusion, FlexiGuard is designed not only to ensure secure data transfer but also to adapt dynamically to changes in access subjects, contexts, and operating conditions. Feng et al. [70] demonstrate a concrete example of applying context-based verification in a CDS environment through an adaptive, learning-based zero-trust architecture. The key points discussed above are summarized in Table 5.

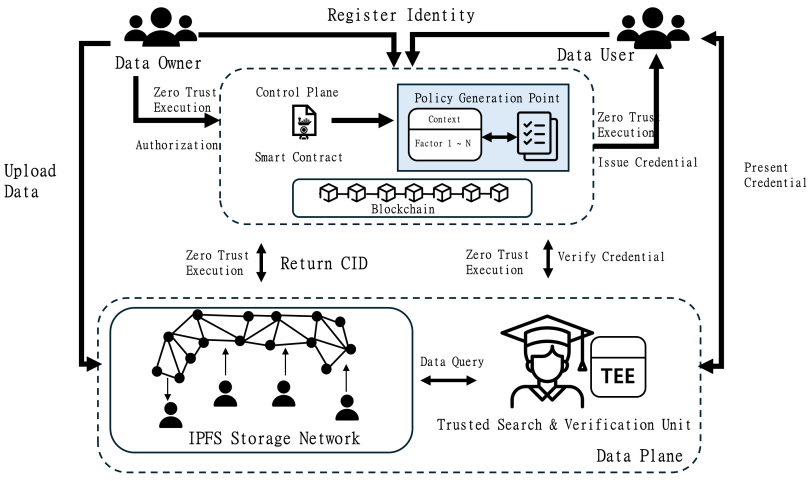


Figure 10. Enterprise Zero Trust Authentication Architecture. Arrows indicate the direction of data/credential flows (upload, query, verification, and return of the CID); dashed boxes denote functional boundaries (e.g., policy/control components, storage network, and data-plane verification); the blockchain represents an append-only audit/credential ledger, and the TEE denotes a trusted execution environment used for secure verification.

Table 5. Summary of Research on the Data Pillar in CDS Environments. This table summarizes CDS-related research based on data-centric protection mechanisms.

Paper Title	Problem Setting in CDS Environment	CDS Application Approach	ZT Utilization Approach	Data Perspective Core
Dynamic Authentication and Granularized Authorization with a Cross-Domain Zero Trust Architecture for Federated Learning in Large-Scale IoT Networks [36]	Continuous verification is needed for movement/access between domains, but context sharing (privacy, latency, overhead) is a bottleneck.	The boundary controls with an encrypted request → prior authorization → a one-time token	For every request, always verify with authentication + risk assessment + policy decision; implement least privilege	Minimize disclosure of the original data + protect with encryption, signatures, and one-time tokens
A Cloud-Oriented Cross-Domain Security Architecture [62]	Even with low-trust clients, inter-domain information flow (MAC) must be enforced.	Provide cross-domain services with a MYSEA (MLS) federation + a community cloud	Endpoints are less trusted; operate with policy-based access control + SSO/QoSS	By controlling data flows, secure convenience and policy compliance/QoSS at the same time
CD-ABSE: Attribute-Based Searchable Encryption Scheme Supporting Cross-Domain Sharing on Blockchain [67]	Securely support cross-domain sharing + search/access control at the same time.	Store in IPFS + manage the sharing flow with blockchain (contracts/index)	Use attribute-based policies for least privilege; strengthen auditability with the chain	Search over ciphertext (trapdoor) keeps plaintext undisclosed; aims at lattice-based security
Exploring the Application of Homomorphic Encryption to a Cross Domain Solution [68]	An untrusted gateway must route between domains without exposing the data/destination.	With homomorphic encryption, evaluate gateway bypass/routing conditions in the ciphertext state	Intermediaries are untrusted; even routers are assumed semi-trusted to minimize trust	Data is always encrypted; attach only required attributes and handle via ciphertext computation
Secure and Scalable Cross-Domain Data Sharing in Zero-Trust Cloud-Edge-End Environment Based on Sharding Blockchain [64]	Solve security fairness and scalability problems of untrusted cross-domain data sharing in a cloud-edge-end environment.	Distribute policy/transactions with a sharding-blockchain-based multi-domain architecture	Under the premise of mutual distrust, enforce sharing with partial-trust / full Zero Trust protocols	With Plaintext-Checkable Encryption for lightweight devices, verify ciphertext validity + protect data
Analyse des mécanismes de contrôle d'accès pour une approche dynamique et décentralisée du data-centric security (DCS) [69]	To protect everywhere in a data-centric security (DCS) way, dynamic + decentralized access control is needed, but existing methods only partially satisfy it.	Using requirements for dynamism/decentralization, classify candidates that combine access control, crypto-based methods, blockchain, etc.	A direction of data-proximate control that makes per-request decisions based on context and attributes, without assuming trust in the network/central authority	Protection unit = data; decentralization mitigates availability/single point of failure
FlexiGuard: Self-adaptive and Dynamic Context-based Access Control for Cross-domain Data Sharing [70]	For dual-level (governance/user) dynamic sharing, static models and continuous-verification performance are limited.	On DID + IPFS (CID) + chain, enforce with ILP rule learning, DS fusion, and VC + TEE	Update rules with behavior, network, and device context to always verify / granularly authorize	Bind (S,O,Op,C) rules + on-chain CID integrity/traceability + TEE confidential processing
Multi-Layered Zero Trust Architectures for Cross-Domain Data Protection in Federated Enterprise Networks and High Risk Operational Environments [63]	In a federated (multi-domain) environment, perimeter security is limited because of insiders, lateral movement, and APTs.	Use SDP + SSE + DID + a federated Trust Broker for inter-domain interoperability/policy enforcement	Context-based continuous verification + least privilege + micro-segmentation/behavior analysis	Protect data to where it goes with classification, tagging, encryption, and monitoring
Efficient and secure cross-domain data sharing scheme with traceability for Industrial Internet [66]	Because of attribute/policy mismatches by domain, single-domain ABE makes cross-domain sharing difficult; there are privacy and unauthorized-access risks.	Perform policy (attribute) transformation with TE-CP-ABE + proxy re-encryption, and a Domain Proxy relays cross-domain sessions	Proceed with the re-encryption/decryption flow only after mutual DP ID authentication + policy-based fine-grained control	Use hybrid encryption so only policy-satisfying parties can access + trace key misuse
CDAS: A Secure Cross-Domain Data Sharing Scheme Based on Blockchain [65]	In IIoT cross-domain sharing, trust between domains + security/privacy are the core hard problems.	Process sharing with an edge-proximate multi-layer blockchain + smart-contract ABAC/anonymous registration	Re-verify authorization for every request and block illegal access/duplicate requests with a minimum-trust approach	Store ciphertext data in IPFS + searchable encryption to search/transmit without exposing plaintext

3.6. Visibility & Analytics

3.6.1. Predictive Zero Trust Analytics (Trust Update Loop)

Li et al. [71] found that in a 5G-based MDW environment where the five domains of land, sea, air, space, and cyber are hyper-connected, the threat of an attacker exploiting stolen privileges to facilitate domain-to-domain lateral movement is particularly severe. To address this, they proposed the DD-ZTD framework. Li et al. [71] elevate the Visibility and Analytics Pillar component to a predictive analytics capability in the context of information asymmetry. The 5G network's vastness poses a problem, as defenders cannot keep an eye on all threats. They designed a trust engine that can make judgments based solely on partial observational data collected from IDS and SIEM. At this point, they combine game theory and Bayesian inference to analyze the data. This enables not only observation of ongoing actions, but also probabilistic inference of attacker intent and strategy, allowing for dynamic evaluation of trustworthiness. From a CDS perspective, the MDW environment is viewed as a massive, cross-domain platform. The problem is that static boundary equipment alone is insufficient to prevent cross-domain threat transfer when physical boundaries are blurred. Before the kill chain is fully formed, DD-ZTD makes a defensive decision based on the results of visibility analysis. This is a method of securing a decisive advantage and proactively blocking it in the domain connection section.

Following OIF, Plyler et al. [72] observed that the tactical edge environment underwent a significant shift, revealing the limitations of traditional CDS. The approach that relies on physical isolation and hardware equipment is impractical for meeting data sharing demands in environments with high SWaP requirements and high mobility. To move beyond the traditional hardware-centric static security model, the research team proposed a next-generation tactical CDS framework based on Service-Oriented Architecture (SOA). Ref. [72] focus on asset visibility through service search and metadata-driven content analysis as the core of the Visibility and Analytics pillar component. It does not assume a fixed physical connection. They create visibility by identifying and monitoring security services and resources in real-time within the network, and checking their status. At the same time, it attaches metadata to data packets, which includes security ratings and content information, and uses this metadata to enforce policies. The structure is based on what the data is, rather than where the traffic is flowing. From a CDS perspective, they redefine CDS as a visible, on-demand security service, rather than a black-box hardware gateway. They have broken down the security check function into a software service, making it location-independent. With this, logical isolation becomes possible regardless of physical location, thanks to metadata. Ultimately, this research can be distilled into an early ZTA-CDS model that addresses location irrelevance and continuous verification in a tactical environment through a service-oriented approach.

3.6.2. Immutable Zero Trust Audit Trail

Wang et al. [73] found that in an aircraft-based wireless sensor network environment, the coexistence of the flight control domain and the information service domain leads to significant insider threats and the challenges of lateral movement. To address this issue, they proposed DzTrust, a decentralized zero-trust framework. Wang et al. [73] focus on strengthening the Visibility and Analytics Pillar component. The research team has implemented RBD Chain, a blockchain technology, to log behavioral data, including node communication patterns and resource usage, on the blockchain. The goal is to ensure visibility in a form that is resistant to tampering. The accumulated data is analyzed in real-time to provide node reliability. It is essentially a dynamic authentication mechanism. They proposed a data-driven trust evaluation model that goes beyond simply accumulating logs, instead using past behavior history to inform the next level of access. From a CDS

perspective, the issue is that centralizing all decision-making in a central gateway can lead to performance bottlenecks. As a result, they adopted a distributed deployment structure for the ZT engine. When data is exchanged between the control domain and the service domain, it enables cross-validation to be performed directly at the edge stage, bypassing the central server. This research can be summarized as a decentralized ZTA-CDS model that integrates blockchain-based visibility data with a distributed verification engine, enabling secure data exchange and real-time threat blocking across domains, even in limited aviation networks.

Xu et al. [58] found that in large-scale IoT environments like 5G-based smart cities, where cross-domain resource sharing is crucial, existing approaches fall short. As a centralized infrastructure grows in size, it becomes increasingly bottlenecked, and static perimeter security can be challenging to adapt to changing circumstances. The research team proposed a dynamic edge resource federation architecture that integrates network slicing and blockchain. Ref. [58] center on blockchain-based immutable visibility as a core component of the Visibility and Analytics pillar. The federation ledger records resource access requests, transactions, and policy changes that occur across domains. The goal is to create a global audit trail that is resistant to tampering, even without a central administrator. In real-time, it monitors and analyzes the status of edge resources, dynamically allocating the optimal slice. Ultimately, it is a system that intelligently manages resources based on visibility data. From a CDS perspective, they view CDS, which was previously tied to physical boundaries, as a software-defined federated approach. With network slicing, they create a logical isolation channel on demand for cross-domain transmissions. With this, authority verification and policy enforcement are automated through a smart contract-based approach. This has enabled scalable collaboration that adheres to the principle of micro-segmentation, even without physical equipment. their work can be summarized as a case of implementing a flexible ZTA-CDS collaboration model using slicing and blockchain technology.

3.6.3. Zero-Touch Zero Trust Operations

Carrozzo et al. [74] found that as 5G expands into an ecosystem involving multiple operators and multiple stakeholders, traditional approaches are proving to be limiting. In a model where businesses enter into bilateral agreements and manually manage operations, dynamic resource sharing is challenging to implement. Maintaining end-to-end security consistently is a challenging task. A lack of trust among business operators is a major obstacle to data sharing and AI-driven automation. The research team proposed a conceptual architecture for 5GZORRO, which integrates AI-based zero-touch automation with distributed ledger technology. Carrozzo et al. [74] introduce a 5G operation data lake as a key component of the Visibility and Analytics Pillar. By consolidating operational data scattered across domains and technology layers into a single location, global visibility is ensured. The collected data is then analyzed using AI/ML to assess the network's status. As a result, they have developed a cognitive management framework that automates resource management. The ultimate goal is to automate the operation, which was previously managed manually, using data-driven approaches. From a CDS perspective, a large cross-domain platform is seen as a collaborative environment where multiple operators who do not trust each other work together. The assumption is that relying solely on physical gateways to define boundaries is not a viable way to quickly drive collaboration. They aim to establish trust through blockchain and smart contracts by leveraging technology. Resource sharing processes like spectrum trading and network slicing are recorded and verified on a distributed ledger. It is designed to be transparent and automated, without the need for a central intermediary. Ultimately, this research can be distilled into a decentralized CDS model that enables automated collaboration even in untrusted, multi-party environments.

3.6.4. Risk-Scored Zero Trust Decisions

Li et al. [75] found that applying ZTA in large-scale cross-domain environments, such as Power IoT, raises practical challenges. As they constantly evaluate trust and match policies for every access request, our system is becoming increasingly bottlenecked and experiencing longer access delays. The research team proposed a parallel pipeline processing approach and a policy search algorithm based on multi-index hashing. The goal is to enhance access processing efficiency while maintaining security. Li et al. [75] focus on the efficiency of the analysis engine as a core aspect of the Visibility and Analytics Pillar. Existing research has primarily focused on collecting and analyzing specific data. In contrast, this paper focuses on how quickly context can be analyzed and decisions made in the context of high-volume traffic. They process trust evaluation and authority checks in parallel, rather than in sequence. Simultaneously, policy search is optimized using a hashing-based approach to minimize query time. The goal is to minimize the delays inherent in the Analytics stage and achieve high-performance real-time dynamic authorization. From a CDS perspective, the performance degradation is tackled head-on. In areas where delays are not tolerated, like control systems, slow verification can quickly become a operational issue. The proposed technique enables continuous verification to run smoothly even with high concurrent connections. Ultimately, this study can be summarized as providing a practical technical foundation for realizing high-performance ZTA-CDS.

3.6.5. Self-Adaptive Zero Trust Policy Generation

Feng et al. [70] discovered that relying solely on static rules is insufficient in a cross-domain environment where multiple organizations operate independently and share data. When threats and collaborative situations are constantly evolving, having a fixed policy can hinder our ability to respond effectively. Building on this, the research team proposed FlexiGuard, a system that integrates ILP and Dempster-Shafer evidence theory to autonomously learn and adapt policies based on contextual information. [70] center on deep contextual visibility and intelligent policy analysis as the core of the Visibility and Analytics Pillar component. The system collects and aggregates real-time data from various sources, including user behavior, network conditions, and device status, to provide a comprehensive view. They then analyze this data using ILP to generate dynamic access control rules tailored to the current situation. When multiple context sources are at odds, the reliability is integrated through evidence theory to reach a unified conclusion. Ultimately, it is a structure that refines decision-making through data-driven approaches. From a CDS perspective, they an intelligent trust mediator model that overcomes the limitations of traditional gateways, which are based on fixed policies. Despite varying security standards across domains, FlexiGuard continuously monitors context changes and dynamically adjusts its access permissions accordingly. This direction ensures secure data flow between domains without disrupting it. Ultimately, this research can be summarized as a flexible ZTA-CDS architecture that adapts to changing circumstances. The key points discussed above are summarized in Table 6.

Table 6. Summary of Research on the Visibility & Analytics Pillar in CDS Environments. This table summarizes CDS-related research based on cross-domain remote data collection and audit/log visibility and analytics capabilities.

Paper Title	Problem Setting in CDS Environment	CDS Application Approach	ZT Utilization Approach	Visibility & Analytics Perspective Core
Decision-Dominant Strategic Defense Against Lateral Movement for 5G Zero-Trust Multi-Domain Networks [71]	In a multi-domain environment, attacks (such as lateral movement) must be blocked with only partial observation.	Observation(logs/IDS/SIEM, etc.) → trust level update → dynamic defense loop leading to grant/deny	Activity logs, SIEM, threat analysis, UBA, dynamic policy	Observation-based trust update + dynamic policy
A distributed zero-trust scheme for airborne wireless sensor networks using dynamic identity authentication [73]	In airborne WSNs, trust collapses due to node compromise/spoofing.	Behavior data collection + RBD_chain (blockchain) immutable record + dynamic trust evaluation + SDP blocking	Activity logs, SIEM, threat analysis, UBA, dynamic policy	Behavior-based trust evaluation + immutable logs
AI-driven Zero-touch Operations, Security and Trust in Multi-operator 5G Networks: a Conceptual Architecture [74]	In multi-operator 5G, automation of trust/security/operations is needed.	Operational Data Lake + AI-based analysis + zero-touch automation (conceptual architecture)	Activity logs, SIEM, threat analysis, UBA, dynamic policy	Data Lake-based operational visibility + automation
Enhancing Cross-Domain Access Efficiency in Zero-Trust Scenarios Oriented to the Access Process [75]	The ZT access process is slow, causing efficiency/latency issues.	Trust calculation based on behavior, environment, and history attributes + grant/deny with a risk penalty	Activity logs, threat analysis, UBA, TI, dynamic policy	Trust calculation with behavior + environment + external TI
FlexiGuard: Self-adaptive and Dynamic Context-Based Access Control for Cross-Domain Data Sharing [70]	Policies break due to context changes, causing misuse/exposure.	Context collection → ILP rule learning → D–S evidence fusion → dynamic policy generation (blockchain management)	Activity logs, SIEM, threat analysis, UBA, dynamic policy	Context correlation/fusion → automatic policy generation
Tactical Cross-Domain Solutions: Current Status and the Need for Change [72]	Tactical CDS is manual/opaque/static policy, so speed, scalability, and auditability are lacking.	Need risk-aware processing + dynamic policy updates(improvement required)	Activity logs, threat analysis, UBA, TI, dynamic policy	Static CDS → demand for risk-based dynamic policy
A Secure Dynamic Edge Resource Federation Architecture for Cross-Domain IoT Systems [58]	Ensure integrity, audit, and trust in edge resource/slice federation.	Immutable records with an intra/inter-domain ledger + slice lifecycle management	Activity logs, threat analysis, UBA, dynamic policy	Ledger-based audit/traceability centered

3.7. Automation & Orchestration

3.7.1. Zero Trust Policy Lifecycle Orchestration

Yin et al. [76] propose a framework that systematically decomposes and analyzes existing access control mechanisms to address the challenge of ensuring confidentiality by placing security closest to the data itself, from a Data-Centric Security (DCS) perspective where dynamic and distributed access control is essential. They begin by outlining the objectives and security guidelines of DCS, and then decompose the DCS infrastructure into three key components: policy, data, and roles. The authors further break down major access controls into sub-concepts such as authorization, activation, access decision, change/revocation, policy change, and context change. These are subsequently divided into granular concepts—including key generation, authority assignment, authority revocation, access decision, encryption/decryption, context management, and data storage/protection—and they categorize each study's coverage in a tabular format. Yin et al. [76] align their analysis with

the operational perspective of the Data Pillar, centering on data classification and labeling, policy integration, and authority/role-based least privilege [26], as seen in DCS's policy and data components. They also extend dynamic access decisions to include Zero Trust 'always-verifying' access, as well as context-based elements such as Multi-Level Security (MLS) cases.

3.7.2. Intent-Driven Zero Trust Orchestration

Ghoraishi et al. [77] examines the iTrust6G framework, proposed to address the limitations of traditional perimeter-based security in the 6G environment, and explores its integration with cross-domain solutions (CDS) and zero-trust architectures (ZTA) through orchestration. iTrust6G proposes a ZTA-type orchestration framework that leverages decentralized trust management to dynamically verify trust across multiple domains and automate policy enforcement. First, whereas traditional CDS controlled data flow between physical networks, iTrust6G extends CDS to a "trust broker" by exchanging and verifying inter-domain trust scores in real-time through ZTA orchestration. To achieve multi-domain joint defense, they introduce a collaborative threat intelligence sharing mechanism, enabling the ZTA orchestrator to function as a security pipeline for CDS. Third, by having AI interpret and enforce the administrator's high-level intentions through intent-based security policies, it ensures consistency and automatic responsiveness across domains. iTrust6G integrates the cross-domain control structure of CDS and the orchestration pillars of ZTA, ultimately presenting a direction for realizing intelligent and automated trust management and security orchestration in the 6G environment.

3.7.3. Survivable Zero Trust Control Plane

Although not explicitly referring to CDS, the Survivable ZTA architecture proposed by Magnanini et al. [78] is closely tied to a logical CDS orchestration model. Given that CDS regulates data exchange between disparate security domains, this architecture achieves logical domain separation through encryption and validation rather than physical network separation. Magnanini et al. [78] designed the Access Proxy to initially receive external traffic, ensuring internal data is not compromised, while the Resource Proxy enforces the final policy in front of the High Domain (DB, server). Traffic is blocked without a collective signature from the Access Control Engine (ACE), simultaneously providing effective security controls. The ACE, which Magnanini et al. [78] position as the core orchestration engine, serves a similar purpose to the CDS policy decision engine but with the added assurance of reliability provided by the Byzantine Fault Tolerance (BFT) algorithm. To prevent a single point of failure, Magnanini et al. [78] utilize multiple replicas that collaborate to agree on a policy; this policy is then validated by a collective signature generated by the replicas before the Resource Proxy can open the data. This process of rigorous integrity verification during data transmission can be viewed as an advanced form of a cloud-based distributed environment. Furthermore, while the Access Proxy acts as a relay during data transmission, Magnanini et al. [78] ensure that the response data sent by the resource is encrypted with the user's device public key, making it inaccessible even to the Access Proxy. To ensure that high-domain data remains confidential even if the orchestration layer is compromised, Magnanini et al. [78] implemented this approach to prevent data plane confidentiality from being breached. The survivable zero trust control-plane architecture is illustrated in Figure 11.

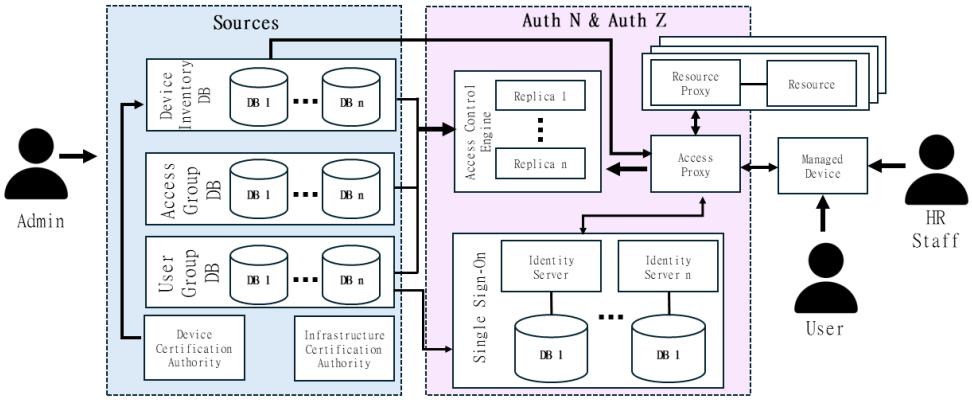


Figure 11. Smart Contract-Based Zero Trust Data Access Framework.

3.7.4. Autonomous Zero Trust Security Orchestration

Ismail et al. [79] propose an IVAM (Investigation-Validation-Active Monitoring) framework that leverages LLM-based Agentic AI to address the limitations of traditional static playbook-based SOAR. Ismail et al. [79] designed this system as a hyper-automated SOAR architecture that integrates threat analysis, response verification, and active monitoring, minimizing human intervention while continuously refining response accuracy through feedback. From the ZTA perspective, Ismail et al. [79] effectively implement dynamic policy execution and ongoing verification through this framework. Agentic AI enhances ZTA's PDP by dynamically applying a minimum authority policy and automatically generating response scenarios in real-time, leveraging threat analysis. Furthermore, through ongoing quantitative risk assessments and active monitoring, Ismail et al. [79] continuously verify the effectiveness and reliability of responses, thereby strengthening the ongoing trust verification of ZTA. From a CDS/CD perspective, Agentic SOAR serves as a cross-domain security orchestration platform that integrates and orchestrates security across different domains. The Agent Router and Executor modules integrate and manage a range of security tools, including SIEM, EDR, and MFA, to ensure secure data exchange and context transfer between disparate security domains. Moreover, Ismail et al. [79] utilize LLM-based dynamic code generation to ensure interoperability and scalability in complex cross-domain environments. Ismail et al. [79] conclude by proposing the evolution of rule-based SOAR into agentic AI SOAR, which enables autonomous decision-making and response capabilities, presenting a next-generation security automation model that integrates intelligent orchestration of ZTA with cross-domain control of CDS.

3.7.5. Zero-Touch Zero Trust Orchestration

Carrozzo et al. [74] highlight that current 5G network standards and deployment methods fall short in supporting services that prioritize specific data, ensuring performance levels such as speed and reliability (QoS), and are limited in terms of security and automation. They argue that for 5G to reach the production stage, the adoption of AI for zero-touch automation and cognitive network management is crucial. Consequently, Carrozzo et al. [74] propose a cross-domain security and trust orchestration architecture that ensures security and trust in multi-stakeholder environments by integrating AI-based zero-touch operations with Distributed Ledger Technology (DLT) through the 5GZORRO project. To facilitate collaboration between non-trusted parties in the proposed cross-domain environment, Carrozzo et al. [74] adopted a method that integrates blockchain-based smart contracts and Trusted Execution Environments (TEEs) into the orchestration process. Furthermore, Carrozzo et al. [74] establish a mutual domain layer to facilitate cross-domain resource discovery, spectrum trading, and SLA monitoring. In this setup,

they ensure a zero-trust environment by cryptographically verifying data governance and multi-party trust through DLT. Carrozzo et al. [74] also designed the system so that operational data collected from each domain is logically stored in the Operational Data Lake and leveraged for AI analysis, ensuring the reliability of the orchestration by strictly controlling data access. Ultimately, through the 5GZORRO architecture, Carrozzo et al. [74] have addressed the challenge of intelligent third-party resource selection and provisioning by automating it across physical and logical boundaries between different operating entities.

Xu et al. [60] discovered that in the next-generation network environment where 5G and AI converge, IoT applications need to navigate multiple management domains, but existing approaches fall short. A static infrastructure structure struggles to keep pace with rapidly evolving service demands, and resolving cross-domain trust issues is equally challenging. The research team proposed a dynamic edge resource federation architecture that integrates network slicing and blockchain. Xu et al. [60] focus on the core aspect of Automation & Orchestration, specifically the Pillar component. When an IoT device request is received, the system automatically sets up a dedicated secure path by logically isolating network resources. To minimize human intervention, domain access control and SLA verification are now handled through smart contracts. Ultimately, it enables rapid response in large-scale IoT by automating the application of security policies and resource allocation in real-time. From a CDS perspective, they view the traditional structure that relied on physical boundaries as a dynamic, software-defined, and federated model. When domains that do not trust each other collaborate, they rely on blockchain as a trusted anchor, rather than a central authority. By leaving a transparent record of access history and verification processes, it enables audits and certifications to be conducted. Furthermore, slicing logically isolates traffic between domains. Ultimately, this research can be distilled into an IoT security model that leverages automated orchestration to simplify cross-domain environments and extend ZTA security to the edge.The key points discussed above are summarized in Table 7.

Table 7. Summary of Research on the Automation & Orchestration Pillar in CDS Environments. This table summarizes representative CDS-related research based on automation and orchestration capabilities, such as cross-domain automated patching and workflows.

Paper Title	Problem Setting in CDS Environment	CDS Application Approach	ZT Utilization Approach	Automation & Orchestration Perspective Core
ACROSS: Automated zero-touch cross-layer provisioning framework for 5G and beyond vertical services [76]	The management system is too complex to operate as a whole. Events flood in, and automation is insufficient.	Multi-domain integrated orchestration with end-to-end telemetry and AI-driven zero-touch provisioning	Trusted execution + policy-based security to enforce secure orchestration decisions	Monitoring data → AI detects anomalies or predicts signals → triggers automatic actions; also classifies task types and defines what should be automated
iTrust6G: Zero-Trust Security for 6G Networks [77]	Existing 6G security manages trust in one central place, which makes automated response difficult.	Distributed trust management across domains with AI-driven orchestration and intent-based policy control	Continuous verification with least privilege and micro-segmentation enforced dynamically.	AI observes threats and automatically performs response and recovery

Table 7. *Cont.*

Paper Title	Problem Setting in CDS Environment	CDS Application Approach	ZT Utilization Approach	Automation & Orchestration Perspective Core
Survivable zero trust for cloud computing environments [78]	Prior ZT research assumes the management/control system is safe, but an attacker can also compromise the management system.	Survivable control plane by distributing management functions and protecting policy/state storage and signaling	Apply ZT to the control plane itself, not only the data plane	Even if automatic configuration and policy deployment are attacked, the system can recover and keep operating
Toward Robust Security Orchestration and Automated Response with a Hyper-Automation Approach Using Agentic AI [79]	SOC needs automated response, but existing SOAR is tied to fixed playbooks; it struggles with complex cases and becomes hard to manage at scale.	Agentic AI generates and runs security workflows across tools instead of fixed playbooks	Validation + continuous monitoring to keep automated response accountable and controlled	Orchestrates multiple security tools together and reduces long procedures into a few core actions to improve operational efficiency
AI-driven Zero-touch Operations, Security and Trust in Multi-operator 5G Networks: a Conceptual Architecture [74]	In multi-operator 5G, it is hard to manage services end-to-end. Security, trust, and automation are still limited, so it is difficult to reach production-grade operations.	Cross-operator coordination using DLT + AI-driven service lifecycle automation.	Trust without a central party via ledger-based verification and automated policy execution	AI performs automation based on monitoring; also automates resource inventory and SLA checking
Zero Trust Security Model Implementation in Microservices Architectures Using Identity Federation [60]	In an AI network environment, IoT applications are hard to manage.	Multi-domain microservices	Continuous authorization	Policy automation.

4. Future Work

This survey is based on published literature and does not include large experimental measurements in operational CDS deployment environments. Therefore, quantitative grounds for end-to-end feasibility such as latency overhead, resource cost, and scalability under continuous analysis and coordination may be limited.

To address these limitations, we consider rigorous performance evaluation and conducting empirical experiments as top priorities in future studies. Specifically, follow-up studies will focus on: (i) quantifying latency and resource overhead under realistic cross-domain operating conditions, and establishing an evaluation and benchmarking methodology for ZTA-based CDS; (ii) developing deployment strategies that minimize latency while maintaining verifiability based on quantitative experimental results; and (iii) addressing interoperability issues with existing systems and heterogeneous operating technologies through stepwise introduction and compatibility layers.

5. Conclusions

In high-assurance Cross Domain Solution (CDS) environments such as defense and finance, this paper summarizes how the seven pillars of Zero Trust Architecture (ZTA) are applied and converged, and analyzes both the technological evolution and practical feasibility of their adoption. The findings show that CDS is moving beyond traditional security models based on physical network separation and fixed, policy-driven controls, and is evolving toward a more intelligent and dynamic security paradigm [80].

The security boundary in CDS is transitioning from a physically isolated, air-gapped structure to a Software-Defined Perimeter (SDP) that combines virtualization with data-diode technologies. In addition, to address the limitations of centrally managed trust across domains, blockchain-based distributed trust models are being introduced to provide stronger authentication and integrity guarantees. A further trend is the emergence of zero-touch operations in which artificial intelligence (AI) autonomously detects threats and adaptively adjusts response policies.

From a pillar-by-pillar perspective, the Identity and Device domains increasingly adopt user-centric, physically grounded authentication approaches—such as blockchain-based decentralized identity (DID), RF fingerprint-based authentication, and sovereign onboarding protocols—enabling robust trust establishment even in cross-domain, low-trust conditions. In the Network and Application domains, dynamic boundary-control technologies including microsegmentation, software-defined networking (SDN), and service mesh architectures are receiving growing attention, proving effective in enforcing the principle of least privilege even within internal networks.

In the Data and Visibility & Orchestration domains, emphasis is placed on continuous and autonomous policy enforcement mechanisms, such as real-time security log analytics, AI-driven anomaly detection, and policy orchestration. This indicates that security control in CDS environments is evolving from isolated functional capabilities to organization-wide, automated security strategies.

Overall, the study empirically demonstrates that the ZTA pillars do not operate in isolation within CDS environments; rather, they function in an interconnected and convergent manner. This convergence can serve as an integrated security strategy that minimizes trust across multiple heterogeneous domains.

Author Contributions: Conceptualization, Y.L. (Yeomin Lee), T.-k.L. and J.P.; methodology, J.P.; investigation, Y.L. (Yeomin Lee), T.-k.L., S.H., Y.L. (Yongjae Lee), Y.K., W.K. and I.C.; resources, J.P.; data curation, S.H., Y.L. (Yongjae Lee), Y.K., W.K. and I.C.; writing—original draft preparation, Y.L. (Yeomin Lee) and T.-k.L.; writing—review and editing, Y.L. (Yeomin Lee), T.-k.L. and J.P.; visualization, S.H., Y.L. (Yongjae Lee), Y.K., W.K. and I.C.; supervision, J.P.; project administration, Y.L. (Yeomin Lee) and T.-k.L.; funding acquisition, J.P. All authors have read and agreed to the published version of the manuscript.

Funding: Coummunications Technology Planning & Evaluation—ITRC (Information Technology Research Center) grant funded by the Korean government (Ministry of Science and ICT) (IITP-2025- RS-2020-II201602). This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (RS-2025-25453740, Development of a large-scale mixed device control and management platform for edge AI server systems).

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Huang, Y.; Li, Y.J.; Cai, Z. Security and Privacy in Metaverse: A Comprehensive Survey. *Big Data Min. Anal.* **2023**, *6*, 234–247. [CrossRef]
2. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. *Zero Trust Architecture*; NIST Special Publication 800-207; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. Available online: https://csrc.nist.gov/publications/detail/sp/800-207/final (accessed on 15 January 2026)
3. Chandramouli, R.; Butcher, Z. *A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Location Environments*; NIST Special Publication 800-207A; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023. Available online: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207A.pdf (accessed on 31 December 2025).
4. Department of Defense (DoD). *Zero Trust Reference Architecture*; Version 2.0; Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team: Fort Meade, MD, USA, 2022.
5. Cybersecurity and Infrastructure Security Agency (CISA). *Zero Trust Maturity Model*; Version 2.0; CISA: Washington, DC, USA, 2023. Available online: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf (accessed on 15 January 2026).
6. National Institute of Standards and Technology (NIST). *Implementing a Zero Trust Architecture*; Special Publication 1800-35; National Cybersecurity Center of Excellence (NCCoE), NIST: Gaithersburg, MD, USA, 2025. Available online: https://csrc.nist.gov/pubs/sp/1800/35/final (accessed on 15 January 2026).
7. U.S. General Services Administration (GSA). *Zero Trust Architecture (ZTA) Buyer's Guide*, 3rd ed.; GSA: Washington, DC, USA, 2024. Available online: https://www.gsa.gov/system/files/ZTA%20Buyer%27s%20Guide%20v3.2%20June%202025%20508%20reviewed.pdf (accessed on 15 January 2026).
8. Cybersecurity and Infrastructure Security Agency (CISA). *Applying Zero Trust Principles to Enterprise Mobility*; CISA: Washington, DC, USA, 2022. Available online: https://www.cisa.gov/sites/default/files/publications/Zero_Trust_Principles_Enterprise_Mobility_For_Public_Comment_508C.pdf (accessed on 15 January 2026).
9. National Security Agency (NSA). *Advancing Zero Trust Maturity Throughout the Device Pillar*; Cybersecurity Information Sheet (CSI); National Security Agency (NSA): Fort Meade, MD, USA, 2023. Available online: https://media.defense.gov/2023/Oct/19/2003323562/-1/-1/0/CSI-DEVICE-PILLAR-ZERO-TRUST.PDF (accessed on 31 December 2025).
10. National Institute of Standards and Technology (NIST). *Guide to Enterprise Patch Management Planning and Implementation*; NIST Special Publication 800-40 Revision 4; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2022. Available online: https://csrc.nist.gov/pubs/sp/800/40/r4/final (accessed on 31 December 2025).
11. National Institute of Standards and Technology (NIST). *Security and Privacy Controls for Information Systems and Organizations*; NIST Special Publication 800-53 Revision 5 (Update 1); National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2020. Available online: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (accessed on 31 December 2025).
12. Cybersecurity and Infrastructure Security Agency (CISA). *BOD 23-01: Implementation Guidance for Improving Asset Visibility and Vulnerability Detection on Federal Networks*; Cybersecurity and Infrastructure Security Agency (CISA): Washington, DC, USA, 2022. Available online: https://www.cisa.gov/news-events/directives/bod-23-01-implementation-guidance-improving-asset-visibility-and-vulnerability-detection-federal (accessed on 31 December 2025).
13. Cybersecurity and Infrastructure Security Agency (CISA). *Continuous Diagnostics and Mitigation (CDM) Program Technical Capabilities Volume 2 (v2.5)*; Cybersecurity and Infrastructure Security Agency (CISA): Washington, DC, USA, 2023. Available online: https://www.cisa.gov/sites/default/files/2023-08/CDM_Tech%20Volume2_v2.5.pdf (accessed on 31 December 2025).
14. U.S. Department of Defense (DoD). *Zero Trust Execution Road Map v1.1 (Data Tables)*; U.S. Department of Defense: Washington, DC, USA, 2022. Available online: https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-CapabilitiesActivities.pdf (accessed on 15 January 2026).
15. Department of Defense (DoD). *Department of Defense Zero Trust Overlays*; Version 1.1; Department of Defense: Washington, DC, USA, 2024. Available online: https://dodcio.defense.gov/Portals/0/Documents/Library/ZeroTrustOverlays.pdf (accessed on 15 January 2026).
16. National Institute of Standards and Technology (NIST). *Recommendation for Key Management: Part 1—General*; NIST Special Publication 800-57 Part 1 Revision 5; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2020. [CrossRef]
17. National Institute of Standards and Technology (NIST). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*; NIST Special Publication 800-122; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2010. [CrossRef]
18. Federal CIO Council; Federal CISO Council; Federal CDO Council. *Federal Zero Trust Data Security Guide*; Executive Office of the President: Washington, DC, USA, 2024. Available online: https://www.cio.gov/assets/files/Zero-Trust-Data-Security-Guide_Oct24-Final.pdf (accessed on 31 December 2025).

19. National Security Agency (NSA). *Advancing Zero Trust Maturity Throughout the Data Pillar*; Cybersecurity Information Sheet (CSI); NSA: Fort Meade, MD, USA, 2024. Available online: https://media.defense.gov/2024/Apr/09/2003434442/-1/-1/0/CSI_DATA_PILLAR_ZT.PDF (accessed on 31 December 2025).
20. National Institute of Standards and Technology (NIST). *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800-60 Volume I Revision 1; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2008. Available online: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-60v1r1.pdf (accessed on 31 December 2025).
21. National Institute of Standards and Technology (NIST). *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*; NIST Special Publication 800-137; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2011. Available online: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf (accessed on 31 December 2025). [CrossRef]
22. National Security Agency (NSA). National Cross Domain Strategy & Management Office (NCDSMO): Raise the Bar. Available online: https://www.nsa.gov/Cybersecurity/Partnership/National-Cross-Domain-Strategy-Management-Office/ (accessed on 31 December 2025).
23. National Institute of Standards and Technology (NIST). *The NIST Cybersecurity Framework (CSF) 2.0*; NIST CSWP 29; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, 2024. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (accessed on 31 December 2025).
24. National Institute of Standards and Technology (NIST). Cross Domain Solution (CDS). CSRC Glossary. Available online: https://csrc.nist.gov/glossary/term/cross_domain_solution (accessed on 31 December 2025).
25. Committee on National Security Systems (CNSS). *CNSS Instruction (CNSSI) No. 4009*; CNSS: Fort Meade, MD, USA, 2022.
26. Zhang, K.; Tian, Z.; Cai, Z.; Seo, D. Link-Privacy Preserving Graph Embedding Data Publication with Adversarial Learning. *Tsinghua Sci. Technol.* **2022**, *27*, 244–256. [CrossRef]
27. Pang, J.; Li, J.; Xie, Z.; Huang, Y.; Cai, Z. Collaborative City Digital Twin for the COVID-19 Pandemic: A Federated Learning Solution. *Tsinghua Sci. Technol.* **2021**, *26*, 759–771. [CrossRef]
28. Hou, Q.; Han, M.; Cai, Z. Survey on Data Analysis in Social Media: A Practical Application Aspect. *Big Data Min. Anal.* **2020**, *3*, 259–279. [CrossRef]
29. Chen, Y.; Chen, H.; Zhang, Y.; Han, M.; Siddula, M.; Cai, Z. A Survey on Blockchain Systems: Attacks, Defenses, and Privacy Preservation. *High-Confid. Comput.* **2022**, *2*, 100048. [CrossRef]
30. Zhao, X.; Xia, F.; Xia, H.; Mao, Y.; Chen, S. A Zero-Knowledge-Proof-Based Anonymous and Revocable Scheme for Cross-Domain Authentication. *Electronics* **2024**, *13*, 2730. [CrossRef]
31. Diaz Rivera, J.J.; Muhammad, A.; Song, W.-C. Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication. *IEEE Open J. Commun. Soc.* **2024**, *5*, 2792–2814. [CrossRef]
32. Du, R.; Li, X.; Liu, Y. A Cross-Domain Authentication Scheme Based on Zero-Knowledge Proof. In *Algorithms and Architectures for Parallel Processing*; Lai, Y., Wang, T., Jiang, M., Xu, G., Liang, W., Castiglione, A., Eds.; Lecture Notes in Computer Science; Springer International Publishing: Cham, Switzerland, 2022; Volume 13156, pp. 647–664.
33. Zhu, Q.; Chang, Y.; Zhao, K.; Zha, Y. A trust level based authentication mechanism crossing domains. In *2014 International Conference on Information and Communications Technologies (ICT 2014)*; IET: Stevenage UK, 2014. [CrossRef]
34. Poirrier, A.; Cailleux, L.; Heide Clausen, T. Building a Zero Trust Federation. *IEEE J. Sel. Areas Commun.* **2025**, *43*, 2113–2125. [CrossRef]
35. Kovacevic, I.; Stojkov, M.; Simic, M. Authentication and Identity Management Based on Zero Trust Security Model in Micro-cloud Environment. In *Disruptive Information Technologies for a Smart Society (ICIST 2023), Kopaonik, Serbia, 12–15 March 2023*; Trajanovic, M., Filipovic, N., Zdravkovic, M., Eds.; Lecture Notes in Networks and Systems; Springer: Cham, Switzerland, 2024; Volume 872, pp. 481–489. [CrossRef]
36. Ma, X.; Fang, F.; Wang, X. Dynamic Authentication and Granularized Authorization with a Cross-Domain Zero Trust Architecture for Federated Learning in Large-Scale IoT Networks. *arXiv* **2025**, arXiv:2501.03601.
37. Li, K.; Bao, J.; Xie, X.; Hong, J.; Hua, C. Receiver-Agnostic Radio Frequency Fingerprint Identification for Zero-Trust Wireless Networks. *IEEE J. Sel. Areas Commun.* **2025**, *43*, 1981–1997. [CrossRef]
38. Wu, X.; Zou, B.; Lu, C.; Wang, L.; Zhang, Y.; Wang, H. Dynamic Security Computing Framework With Zero Trust Based on Privacy Domain Prevention and Control Theory. *IEEE J. Sel. Areas Commun.* **2025**, *43*, 2266–2278. [CrossRef]
39. Wu, K.; Shi, J.; Guo, Z.; Zhang, Z.; Cai, J. Research on Security Strategy of Power Internet of Things Devices Based on Zero-Trust. In *Proceedings of the 2021 International Conference on Computer Engineering and Application (ICCEA), Kunming, China, 25–27 June 2021*; IEEE: Piscataway, NJ, USA, 2021; pp. 79–83.
40. Wang, L.; Li, Y.; Zuo, L. Trust Management for IoT Devices Based on Federated Learning and Blockchain. *J. Supercomput.* **2025**, *81*, 232. [CrossRef]

41. Elmaghbub, A.; Hamdaoui, B. Domain-Agnostic Hardware Fingerprinting-Based Device Identifier for Zero-Trust IoT Security. *IEEE Wirel. Commun.* **2024**, *31*, 42–48. [CrossRef]
42. Díaz-Sánchez, D.; Almenarez-Mendoza, F.; Campo-Vázquez, C.; García-Rubio, C. Zero-Trust Token Authorization with Trapdoor Hashes for Scalable Distributed Firewalls. *Future Gener. Comput. Syst.* **2026**, *176*, 108227. [CrossRef]
43. Li, D.; Yu, J.; Gao, X.; Al-Nabhan, N. Research on Multidomain Authentication of IoT Based on Cross-Chain Technology. *Secur. Commun. Netw.* **2020**, *2020*, 6679022. [CrossRef]
44. Reaz, K.; Wunder, G. ASOP: A Sovereign and Secure Device Onboarding Protocol for Cloud-Based IoT Services. *arXiv* **2024**, arXiv:2403.13020.
45. Ansariyan, S.; Doostari, M. A Novel Bidirectional Distributed Cross Domain Solution Security Architecture. In *Proceedings of the 2024 11th International Symposium on Telecommunications (IST), Tehran, Iran, 9 October 2024*; IEEE: Piscataway, NJ, USA, 2024; pp. 627–636.
46. Na, M.R.; Sundharakumar, K.B. A Study on Air-Gap Networks. In *Proceedings of the 2024 5th International Conference on Innovative Trends in Information Technology (ICITIIT), Kottayam, India, 15 March 2024*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–6.
47. Gurram, S. Cross-Domain Integration for Hybrid Cloud Management: Innovations and Future Directions. *World J. Adv. Eng. Technol. Sci.* **2025**, *15*, 1755–1761. [CrossRef]
48. Arneson, S.; Şahin, D. *Cyber Security Using Multi-Threaded Architecture Data Diode at the NBSR*; *Technical Report*; American Nuclear Society: La Grange Park, IL, USA, 2017.
49. Dahlstrom, J.; Taylor, S. Protecting Networks with Intelligent Diodes. *Proc. Int. Conf. Cyber Warfare Secur. (ICCWS)* **2022**, *17*, 45–54. [CrossRef]
50. Borges de Freitas, M.; Rosa, L.; Cruz, T.; Simões, P. *SDN-Enabled Virtual Data Diode*; Springer International Publishing: Cham, Switzerland, 2018.
51. Story, P. Building an Affordable Data Diode to Protect Journalists. In *Proceedings of the Workshop on Privacy Engineering in Practice (PEP '23), Anaheim, CA, USA, 6 August 2023*; USENIX Association: Berkeley, CA, USA, 2023.
52. Okhravi, H.; Sheldon, F.T. Data Diodes in Support of Trustworthy Cyber Infrastructure. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, TN, USA, 21 April 2010*; ACM: New York, NY, USA, 2010; pp. 1–4.
53. Jones, D.W.; Bowersox, T.C. Secure Data Export and Auditing Using Data Diodes. *Tech. Rep.* **2006**, *6*, 7.
54. Mahan, R.E.; Fluckiger, J.D.; Clements, S.L.; Tews, C.W.; Burnette, J.R.; Goranson, C.A.; Kirkham, H. *Secure Data Transfer Guidance for Industrial Control and SCADA Systems*; Report No. PNNL-20776; Pacific Northwest National Laboratory (PNNL): Richland, WA, USA, 2011
55. Choi, H.; Lee, J.; Lee, W.; Kwon, Y.; Myoung, N.; Park, M.; Song, J.-J. Cross Domain Solution With Stateful Correlation of Outgoing and Incoming Application-Layer Packets. *IEEE Access* **2024**, *12*, 26830–26838. [CrossRef]
56. Daughety, N.; Pendleton, M.; Xu, S.; Njilla, L.; Franco, J. vCDS: A Virtualized Cross Domain Solution Architecture. In *MILCOM 2021—2021 IEEE Military Communications Conference (MILCOM), San Diego, CA, USA, 29 November 2021*; IEEE: Piscataway, NJ, USA, 2021; pp. 61–68.
57. Fysarakis, K.; Soultatos, O.; Manifavas, C.; Papaefstathiou, I.; Askoxylakis, I. XSACd—Cross-Domain Resource Sharing & Access Control for Smart Environments. *Future Gener. Comput. Syst.* **2018**, *80*, 572–582. [CrossRef]
58. Xu, R.; Chen, Y.; Li, X.; Blasch, E. A Secure Dynamic Edge Resource Federation Architecture for Cross-Domain IoT Systems. In *Proceedings of the 2022 International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 25–28 July 2022*; IEEE: Piscataway, NJ, USA, 2022; pp. 1–7.
59. Hsiao, S.-W.; Sun, Y.S.; Ao, F.-C.; Chen, M.C. A Secure Proxy-Based Cross-Domain Communication for Web Mashups. In *Proceedings of the 2011 IEEE Ninth European Conference on Web Services (ECOWS), Lugano, Switzerland, 14–16 September 2011*; IEEE: Piscataway, NJ, USA, 2011; pp. 57–64.
60. Rajendran, R.N.; Anumula, S.K.; Rai, D.K.; Agrawal, S. Zero Trust Security Model Implementation in Microservices Architectures Using Identity Federation. *arXiv* **2025**, arXiv:2511.04925. [CrossRef]
61. Jonnakuti, S. Zero-Trust Architectures for Secure Multi-Cloud AI Workloads. *Int. J. Lead. Res. Publ.* **2021**, *2*, 88–97.
62. Nguyen, T.D.; Gondree, M.A.; Shifflett, D.J.; Khosalim, J.; Levin, T.E.; Irvine, C.E. A Cloud-Oriented Cross-Domain Security Architecture. In *Proceedings of the IEEE Military Communications Conference (MILCOM 2010), San Jose, CA, USA, 31 October–3 November 2010*; IEEE: Piscataway, NJ, USA, 2010; pp. 441–447. [CrossRef]
63. Shonubi, J.A. Multi-Layered Zero Trust Architectures for Cross-Domain Data Protection in Federated Enterprise Networks and High-Risk Operational Environments. *Int. J. Adv. Res. Publ. Rev.* **2025**, *2*, 146–169. [CrossRef]
64. Liu, Y.; Xing, X.; Tong, Z.; Lin, X.; Chen, J.; Guan, Z. Secure and Scalable Cross-Domain Data Sharing in Zero-Trust Cloud-Edge-End Environment Based on Sharding Blockchain. *IEEE Trans. Dependable Secur. Comput.* **2024**, *21*, 2603–2618. [CrossRef]
65. Jiang, J.; Pei, T.; Chen, J.; Hou, Z. CDAS: A Secure Cross-Domain Data Sharing Scheme Based on Blockchain. *Information* **2025**, *16*, 394. [CrossRef]

66. Luo, W.; Lv, Z.; Lai, C.; Yang, T. Efficient and secure cross-domain data sharing scheme with traceability for Industrial Internet. *Comput. Netw.* **2025**, *260*, 111117. [CrossRef]
67. Guo, K.; Han, Y.; Wu, R.; Liu, K. CD-ABSE: Attribute-Based Searchable Encryption Scheme Supporting Cross-Domain Sharing on Blockchain. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 6719302. [CrossRef]
68. Tinker, C.; Millar, K.; Kaminsky, A.; Kurdziel, M.T.; Lukowiak, M.; Radziszowski, S.P. Exploring the Application of Homomorphic Encryption to a Cross Domain Solution. In *MILCOM 2019—2019 IEEE Military Communications Conference (MILCOM), Norfolk, VA, USA, 12–14 November 2019*; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6. [CrossRef]
69. Lemonnier, E.; El Hachem, J.; Touseau, L.; Buisson, J.; Belloir, N.; Wiorek, J.-F. Analysis of Access Control Mechanisms for a Dynamic and Decentralized Approach of Data-Centric Security (DCS). In Proceedings of the C&ESAR'24: Computer & Electronics Security Application Rendezvous, Rennes, France, 20–21 November 2024. Available online: https://2024.cesar-conference.org/program-media/CESAR-2024_paper-8811.pdf (accessed on 30 December 2025).
70. Feng, Z.; Chen, Y.; Zhang, B.; Bu, F.; Wang, S.; Shao, Z.; Yu, Z. FlexiGuard: Self-Adaptive and Dynamic Context-Based Access Control for Cross-Domain Data Sharing. In Proceedings of the 20th International Conference on Mobility, Sensing and Networking (MSN 2024), Harbin, China, 20–22 December 2024; pp. 754–761. [CrossRef]
71. Li, T.; Pan, Y.; Zhu, Q. Decision-Dominant Strategic Defense Against Lateral Movement for 5G Zero-Trust Multi-Domain Networks. In *Network Security Empowered by Artificial Intelligence*; Chen, Y., Wu, J., Yu, P., Wang, X., Eds.; Advances in Information Security; Springer Nature Switzerland: Cham, Switzerland, 2024; Volume 107, pp. 25–76.
72. Plyler, K.; Tague, B.C.; Thomas, R.; Tsang, S. Tactical Cross-Domain Solutions: Current Status and the Need for Change. In *MILCOM 2009–2009 IEEE Military Communications Conference, Boston, MA, USA, 18–21 October 2009*; IEEE: Piscataway, NJ, USA, 2009; pp. 1–7.
73. Wang, K.; Hong, Y.; Li, Y.; Yan, R.; Feng, J. A Distributed Zero-Trust Scheme for Airborne Wireless Sensor Networks Using Dynamic Identity Authentication. *Sci. Rep.* **2025**, *15*, 8036. [CrossRef]
74. Carrozzo, G.; Siddiqui, M.S.; Betzler, A.; Bonnet, J.; Perez, G.M.; Ramos, A.; Subramanya, T. AI-Driven Zero-Touch Operations, Security and Trust in Multi-Operator 5G Networks: A Conceptual Architecture. In *Proceedings of the 2020 European Conference on Networks and Communications (EuCNC), Dubrovnik, Croatia, 15–18 June 2020*; IEEE: Piscataway, NJ, USA, 2020; pp. 254–258.
75. Li, X.; Zhang, S.; Zeng, J.; Li, S.; Yang, R. Enhancing Cross-Domain Access Efficiency in Zero-Trust Scenarios Oriented to the Access Process. In *Proceedings of the 2025 International Conference on Electrical Automation and Artificial Intelligence (ICEAAI), Guangzhou, China, 10 January 2025*; IEEE: Piscataway, NJ, USA, 2025; pp. 1400–1405.
76. Giannopoulos, D.; Katsikas, G.P.; Trantzas, K.; Klonidis, D.; Tranoris, C.; Denazis, S.; Gifre, L.; Vilalta, R.; Alemany, P.; Muñoz, R.; et al. ACROSS: Automated Zero-Touch Cross-Layer Provisioning Framework for 5G and Beyond Vertical Services. In *Proceedings of the Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Gothenburg, Sweden, 6–9 June 2023*; IEEE: Piscataway, NJ, USA, 2023; pp. 735–740. [CrossRef]
77. Ghoraishi, M.; Siddiqui, M.S.; Compastié, M.; Mhiri, S.; Ntantos, C.; Kontoulis, M.; López, D.R.; Lioy, A.; Markakis, E.; Baskaran, S.B.M. iTrust6G: Zero-Trust Security for 6G Networks. In *Proceedings of the 2024 IEEE Future Networks World Forum (FNWF), Dubai, United Arab Emirates, 15–17 October 2024*; IEEE: Piscataway, NJ, USA, 2024; pp. 411–416.
78. Ferretti, L.; Magnanini, F.; Andreolini, M.; Colajanni, M. Survivable Zero Trust for Cloud Computing Environments. *Comput. Secur.* **2021**, *110*, 102419. [CrossRef]
79. Ismail; Kurnia, R.; Brata, Z.A.; Nelistiani, G.A.; Heo, S.; Kim, H.; Kim, H. Toward Robust Security Orchestration and Automated Response in Security Operations Centers with a Hyper-Automation Approach Using Agentic Artificial Intelligence. *Information* **2025**, *16*, 365. [CrossRef]
80. Sai, A.M.; Wang, C.; Cai, Z.; Li, Y. Navigating the Digital Twin Network Landscape: A Survey on Architecture, Applications, Privacy and Security. *High-Confid. Comput.* **2024**, *4*, 100269. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.