**Journal of Information Systems Engineering and Management**
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

**Research Article**

# Decoupling Cloud Security (DCS): A Framework for Data Sovereignty and Cross-Border Cloud Compliance

Suthari Yugandhar Reddy[1], Manam Karthik Babu[2], Roshin Unnikrishnan[3]

[1]Research Student University of the Cumberlands,Williamsburg.

[2]PhD Student University of the Cumberlands, Williamsburg.

[3]Sr Director, Growth and Rev Ops, Cisco Systems Inc.

**ARTICLE INFO**

Received: 12 Dec 2024

Revised: 22 Jan 2025

Accepted: 02 Feb 2025

**ABSTRACT**

The spreading acceptance of Cloud Services across geographically distributed and in different environments has intensified various concerns around data sovereignty, regulatory enforcement and security compliance. Traditionally, the cloud security architectures and integrators are deeply intertwined with cloud service providers and jurisdictional constraints, making it difficult for organizations to maintain control over their data while complying with diverse regulations. This kind of tight coupling introduces various operational inefficiencies, many legal complexities, and security risks, specifically cross-border data processing scenarios and in multi-cloud as well. To address these challenges, this research proposes a Decoupled Cloud Security (DCS) framework that separates security enforcement from cloud infrastructure, enabling dynamic and policy-driven control over data, independent of underlying cloud platforms. The proposed DCS framework take the advantages of distributed cryptographic key management, policy-aware access controls, confidential computing and secure enclaves to provide an abstraction layer which can ensures data security, data integrity, and sovereignty without even constrained by various cloud provider dependencies. Additionally, it incorporates compliance-aware orchestration which are allowing different organizations to automatically enforce jurisdiction-specific security policies and regulations in alignment with various regulatory mandates such as California Consumer Privacy Act (CCPA - USA),, GDPR - EU, Health Insurance Portability and Accountability Act (HIPAA - USA), Personal Data Protection Act (PDPA - Singapore, Thailand, Malaysia), Brazil's Lei Geral de Proteção de Dados (LGPD), China's Personal Information Protection Law (PIPL), India's Digital Personal Data Protection Act (DPDPA), Australia's Privacy Act 1988, and international frameworks such as ISO/IEC 27001, NIST 800-53, Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM), and SWIFT Customer Security Programme (CSP). By using the mechanism to decouple the security mechanisms from cloud service providers, this framework empowers various organizations with support of granular control over security policies, encryption, and access management, irrespective of the cloud infrastructure.

Through theoretical modeling and empirical validation, this research demonstrates how enterprises can achieve regulatory compliance, mitigate vendor lock-in risks, and enhance security postures while maintaining the

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

agility and scalability of cloud services. The findings provide a practical roadmap for enterprises, cloud providers, and regulators to establish a resilient, compliance-driven, and sovereignty-preserving cloud security model.

**Keywords**:Decoupled Cloud Security, Data Sovereignty, Regulatory Compliance, Confidential Computing, Multi-Cloud Security

## INTRODUCTION

As enterprises increasingly adopt various cloud services to ensure regulatory compliance, data sovereignty and security has become a very important and primary concern. Traditional cloud security models are tightly integrated with cloud service providers (**CSPs**), leading to regulatory challenges and operational inefficiencies.

This section explores the adaptation and evolution of cloud security mechanisms and its requirement. Also, it explores various and different key challenges in cross-border and multi-cloud compliance, and the limitations of existing security solution architectures and requirement.

### Evolution of Cloud Security

Early cloud security architectures and solutions are primarily focused on access control lists (ACLs), perimeter-based defenses, relying on firewalls, and virtual private networks (VPNs) to protect cloud workloads [1]. Though, with the rise of multi-cloud environments and geographically distributed data storage, security concerns have moved from perimeter-grounded methods to data-centric models, highlighting encryption, zero-trust frameworks, and confidential computing [2].

The introduction of policy-driven access controls and software-defined security (SDS) both can enabled dynamic enforcement of security policies. Also, they can enable various regulations across different cloud environments [3].

Despite these advancements, most security solutions remain CSP-dependent, forcing organizations to adopt provider-specific controls, leading to vendor lock-in and compliance complexities [4].

### Key Challenges in Multi-Cloud and Cross-Border Compliance

Organizations operating across multiple jurisdictions face challenges related to:

- In the vendor Lock-In Risks, CSP-native security frameworks make the organization restricted from implementing uniform security policies and procedures across multiple clouds. The process of migrating security configurations and requirements between service providers is very complex and may lead to various security gaps [6].
- Diverse Regulatory Requirements – The various regulations such as GDPR (this is from EU), CCPA (this is from USA), PDPA (from Singapore, Thailand and Malaysia), LGPD (from Brazil), and PIPL (China). The mentioned previously regulatory requirements impose strict requirements on data localization. Also, they impose access control and auditability of the cloud-based application [5]. The compliance requires customized security (modification) implementations and increasing various operational and maintainable complexity.
- Data Residency and Sovereignty Issues – Certain jurisdictions require that sensitive data remain within national borders, making cross-border data transfers legally and technically challenging [7]. Traditional CSP-based security controls do not always provide mechanisms to enforce fine-grained data residency policies.
- Security Management Overhead – Organizations using multi-cloud and hybrid-cloud infrastructures must manage heterogeneous security configurations, increasing administrative burdens and risk exposure [8].

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

**Limitations of Existing Security Architectures**

Despite the widespread adoption of cloud security frameworks, existing models exhibit significant limitations:

- Dependence on Cloud Service Providers – Security solutions designed for Amazon Web Services (AWS), Azure, and Google Cloud are tailored and customized for their specific environments, which restricts interoperability in multi-cloud deployment [9].
- Disjointed Policy Enforcement – Security settings vary between on-premises, cloud, and edge environments, complicating the consistent application of policies.
- Complexity of Compliance – Organizations are required to manually ensure that security implementations adhere to regional regulations, raising compliance burdens and potential legal risks.

To overcome these kinds of complex challenges, a Decoupled Cloud Security Framework (DCS) is proposed in this paper. This paper shows the abstracts security mechanism and methods from different could service provides to ensures consistent security and regulatory compliances which can helps to reduce the risk of vendor lock-in riks. The next section explores the current state-of-the-art approaches in cloud security and their limitations.

## I. State of the Art work

Recently, the Cloud security has evolved significantly which has started incorporating zero-trust architectures and compliance-aware security frameworks. This also have involved secure enclaves and confidential computing.

However, leading to various regulatory and operational challenges, the current security controls and mechanisms remain tightly coupled with cloud providers and integrators.

In this section, we explore the latest advancements in cloud security methos and mechanism which broadly involves like multi-cloud security strategies, policy-driven security frameworks, cryptographic key management solutions, PKI infrastructure, and compliance automation techniques.

### 3.1. Zero-Trust Security in Cloud Environments

Zero-trust security (ZTS) is a standard stint from traditional perimeter-based defenses techniques and mechanism to identity-centric access control mechanisms. Here, the trust is no way assumed and considered but even though the every access request is authenticated and authorized [1].

Various CSPs such as Microsoft Azure, AWS, and Google Cloud have integrated zero-trust architectures into their security models and controls [2].

Despite its benefits of ZTS, its implementation remains CSP-dependent that means there is less dependencies on CSPs where each provider importantly offering proprietary solutions such as AWS Zero Trust, Microsoft Zero Trust, and Google BeyondCorp [3]. This results in inconsistent policy enforcement across multi-cloud environments.

**Confidential Computing and Secure Enclaves**

To improve and enhance data confidentiality and integrity, CSP have introduced confidential computing technologies. These technologies process sensitive data (the data with label “Sensitivity” in detached computing and execution environments called secure enclaves which is also called as security territories. [4].

Leading solutions include:

- Intel Software Guard Extensions (SGX) – Its provides secure enclaves for process of encrypted data without exposing it to the Cloud Service Provider and Operating System (OS) [5].

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- AMD Secure Encrypted Virtualization (SEV) – It provides hardware-based encryption for virtualized workloads, which is very secure way to reduce cloud provider access (or access mechanism security) to customer data which can be sensitive [6].
- Google Cloud Confidential VMs – Allows its all customers to encrypt their data during date processing using the mechanism developed by themselves called confidential computing capabilities [7].

While different mechanisms of confidential computing, addresses data exposure risks, and importantly, these kinds of solutions remain straightforward cloud-specific, limiting cross-cloud interoperability issues and challenges.

**Cryptographic Key Management and Data Control**

Normally, various organizations increasingly rely and depend on third party and externalized key management solutions (KMS) to take the security control over the encryption keys while using cloud services and micro services. Common solutions include:

- Bring Your Own Key (BYOK) – Allows enterprises to manage encryption keys externally while using cloud storage [8].
- Hold Your Own Key (HYOK) – It provides the entire control over encryption keys (for symmetric and asymmetric), to ensure that CSPs cannot access encrypted data [9].
- Cloud-Hardware Security Modules (Cloud-HSM) – AWS, Azure, and Google Cloud provide HSM-based key management, but they are still integrated into CSP ecosystems [10].

A key limitation and challenges of existing and current cryptographic key management methos is the lack of incorporated, cross-cloud encryption standard which makes multi-cloud security more challenging and complex.

**Policy-Driven Security and Compliance Automation**

To streamline regulatory compliance, CSPs have introduced a policy-driven security frameworks which controls security configurations in align with legal requirements. Examples include:

- **AWS Security Hub and Azure Policy** – The predefined compliance templates and requirements are based on the Automate security governance which are provided by service providers. [11].
- **Cloud Security Alliance (CSA)** Cloud Controls Matrix (CCM) – It provide a mapping of regulatory frameworks to the security controls of cloud [12].
- **Automated Compliance-as-Code (CaC)** Frameworks – There are various tools like HashiCorp , Open Policy Agent (OPA) which can helps us to enable programmatic enforcement of security policies [13].

However, compliance automation solutions remain CSP-centric, requiring organizations to manually align policies across multiple cloud environments.

**Limitations of Current Approaches:**

Even with progress, current cloud security mechanisms show critical shortcomings:

- **Cloud Provider Dependence** – Security controls are bundled into CSP architectures, thus limiting interoperability in multi-cloud environments [14].
- **Fragmented security models** – every cloud provider builds their own security solutions, so policy enforcement is not consistent [15].
- **Absence of Unified Compliance Frameworks** – Although compliance automation tools exist, they demand cloud-specific configurations resulting in increased operational complexity [16].

To bridge these gaps, this paper proposes the **Decoupled Cloud Security (DCS)** framework which decouples security enforcement from cloud infrastructure, allowing for the enforcement of consistent

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

security and compliance policies in multi-cloud environments. The following section describes both the DCS framework that was proposed and its main components.

## II. PROPOSED APPROACH

In order to overcome the limitations of traditional cloud security models, we introduce Decoupled Cloud Security (DCS) framework, which decouples security enforcement from cloud service providers (CSPs), enabling a dedicated security environment on-top of third-party services. Contrary to traditional approaches that depend on provider-specific security controls (such as IAM policies, S3 bucket policies, etc.), the DCS framework spearheads an independent, policy-driven security architecture that upholds data sovereignty, compliance, and cross-cloud security governance. The proposed approach is shown in Fig. 1.

### Key Design Principles

The DCS framework is structured on the following four principles: **Security Independence from CSPs** – As suggested by the current structure, security controls should not be integrated into cloud provider infrastructure but act as an externalized security layer [1]. **Policy-Aware Data Governance** In this stage, security policies are enforced dynamically, based on jurisdiction-specific regulations and organizational security requirements [2]. **Distributed Cryptographic Control** – Organizations must maintain total control over encryption keys and data protection mechanisms independent of the CSP-managed encryption [3]. **Data Isolation mean with Confidential Computing** — Secure enclaves and trusted the execution environment (TEE) should keep the data always encrypted—including while it is being processed. [4]. **Cross-Border Compliance Automation** – Security configurations need to be modified automatically to achieve compliance with regional data protection laws [5]

### DCS Framework Architecture:

The DCS framework consists of four primary components:

**Distributed Cryptographic Key Management:** The DCS framework implements an externalized key management system (EKMS) that enables: Unlike CSP-integrated key management solutions.

- Bring Your Own Key (BYOK)/ Hold Your Own Key (HYOK) – Organizations are able to maintain encryption keys outside of CSP control on-premises or in third-party HSMs [6]
- Threshold Cryptography & Multi-Party Computation (MPC) – Guarantees single entity (such as CSPs) will not have full access to encryption keys [7].
- Post-Quantum Cryptography (PQC) Readiness – shields against future dangers introduced by quantum computing concerning ciphering algorithms [8].

To that end, the framework employs a decentralized policy enforcement layer that combines attribute-based access control (ABAC) and fine-grained policy definitions [9]. Features include:

- **Geofencing & Jurisdiction**-Aware Access Control – Enforces data residency policies derived from region-specific regulatory requirements (e.g., GDPR, CCPA, PDPA) [10].
- **Decentralized Identity Management (DID)** – Uses blockchain-based identity verification to secure tamper-resistant authentication [11].
- **Federated Security Policy Enforcement** – Allows cross-cloud security enforcement via interoperable policy definitions [12].

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

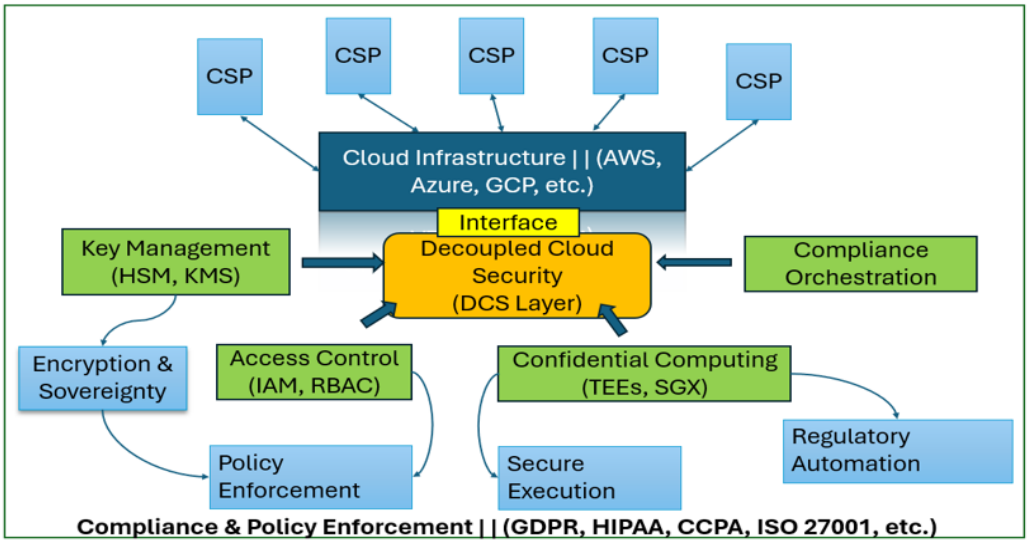


Fig. 1 Proposed Approach (DCS)

**Confidential Computing for Secure Processing**

To address the risks associated with CSP access to sensitive data, the DCS framework overlays confidential computing using:

- Intel SGX & AMD SEV for Secure Enclaves — Keeps sensitive data invulnerable in an encrypted state even when it is processed, minimizing the risk of insider threats [13].
- Confidential Virtual Machines (CVMs) – Unlike your VMs, this prevents your cloud service provider from seeing runtime and memory data [14].
- Privacy-Preserving Computation our (PPC) Referral uses homomorphic encryption deploys (HE) and secure multi-party computation (SMPC) to process encrypted data without decrypting it [15].

**Compliance-Aware Security Orchestration**

DCS framework includes an automated compliance engine that maps security configurations with regional regulatory requirements. Features include:

- Dynamic Compliance Enforcements – Complies with dynamic changes in security based on evolving regulatory landscapes (e.g. GDPR, HIPAA, LGPD) [16]
- Cross-Cloud Security Posture Management (CSPM) — Supplies a universal security governance layer that runs across several clouds [17].
- Regulatory Changes Detection & Policy Updates – Utilizes AI driven monitoring to adjust security policies when the legal frameworks change [18].

**Implementation Feasibility and Challenges**

Though the DCS framework provides a scalable and flexible solution, its deployment faces a number of challenges:

- **Interoperability with Existing Cloud Infrastructures** – [19] still shows as a technical challenge to standardize the security controls among CSPs.
- **Performance Overhead of Confidential Computing** – Secure enclaves incur computational costs and may degrade processing speeds [20].
- **Regulatory Complexity in Multi-Jurisdictional Environments** – It requires constant monitoring and updates to adapt the policies to the various global compliance mandates [21].

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

**Summary**

The DCS framework delivers vendor agnostic, compliance based and sovereignty preserving security architecture. Separation of Security Enforcement from CSPs It then enables organizations to:

- Data Security What are the data security capabilities?
- Enforce jurisdiction-specific security policy dynamically
- Explore Secure Data Processing with Confidential Computing
- Cross-cloud interoperability and compliance automation

## III. COMPARATIVE ANALYSIS

To evaluate the effectiveness of the **Decoupled Cloud Security (DCS) framework**, this section compares it against traditional cloud security models and emerging security architectures in terms of data sovereignty, compliance, cryptographic control, and cross-cloud security governance.

### Comparative Dimensions

The comparison is structured around four key dimensions:

- Data Sovereignty and Compliance – Enforcing jurisdictional policies and data residency.
- Cryptographic Control and Key Management – Whether encryption keys are retained within a customer control and not CSP-managed.
- Security Enforcement Model – One or more layers of dependency on CSP versus externalized, vendor agnostic security.
- Cross-Border Security Governance – The ability to dynamically adjust security controls in various cloud environments.

**The comparison with Traditional Cloud Security Models shows in Table 1.**

TABLE I

TRADITIONAL CLOUD SECURITY MODELS

| **Feature** | **Traditional Cloud Security** | **DCS Framework** |
|---|---|---|
| **Data Sovereignty** | Limited; Data residency often controlled by CSP [1] | Ensures strict **policy-aware enforcement** with **geofencing** [2] |
| **Compliance Automation** | CSP-driven; Not fully adaptable to evolving laws [3] | Dynamic **regulatory compliance mapping** [4] |
| **Encryption Key Control** | CSP-hosted key management (e.g., AWS KMS, Azure Key Vault) [5] | Customer-controlled **Bring Your Own Key (BYOK) / Hold Your Own Key (HYOK)** [6] |

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

| | | |
|---|---|---|
| **Confidential Computing** | Limited support for **secure enclaves** [7] | Integrates **Intel SGX, AMD SEV, and homomorphic encryption** [8] |
| **Cross-Cloud Interop.** | CSP-specific security silos [9] | Vendor-agnostic **federated security policy enforcement** [10] |
| **Policy-Driven Security** | Dependent on CSP security tools [11] | Independent, **externalized policy enforcement layer** [12] |

**Comparison with Emerging Security Architectures**

***DCS vs. Cloud Security Posture Management (CSPM)*: Cloud Security Posture Management (CSPM)** solutions provide **automated risk assessments and compliance checks**, but they still **operate within CSP-managed environments** [13]. The DCS framework extends beyond CSPM by **enabling externalized policy enforcement and independent cryptographic control**.

TABLE II

COMPARISON WITH CSPM VS DCS FRAMEWORK

| Feature | CSPM [14] | DCS Framework |
|---|---|---|
| **Scope of Control** | CSP-managed | Customer-managed |
| **Security Enforcement** | Cloud-native tools | External, cross-cloud enforcement |
| **Key Management** | CSP-controlled | Customer-controlled (BYOK/HYOK) |
| **Compliance Adaptability** | Reactive | Dynamic, proactive enforcement |

**DCS vs. Zero Trust Architecture (ZTA)**

**Zero Trust Architecture (ZTA)** promotes **continuous authentication** and **least-privilege access** but does not directly **address cloud vendor dependence** [15]. The **DCS framework complements ZTA** by extending trust boundaries across **multiple cloud providers** while enforcing **cross-border compliance**.

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

TABLE III

ZTA VS. DCS FRAMEWORK

| Feature | ZTA [16] | DCS Framework |
|---|---|---|
| **Access Control** | Dynamic, continuous authentication | Policy-aware, **jurisdiction-based enforcement** |
| **Data Sovereignty** | Not a primary focus | Ensures **compliance with local regulations** |
| **Cloud Security Model** | Cloud-dependent | **Vendor-agnostic** |

### 6.3.3 DCS vs. Confidential Computing Frameworks

**Confidential computing frameworks** such as **Google Confidential VMs** and **Azure Confidential Computing** focus on **data protection during processing** but remain tightly integrated with CSP infrastructure [17].

The DCS framework extends these concepts by **offering an independent, cross-cloud security layer**.

TABLE IV

CONFIDINTIAL COMPUTING VS. DCS FRAMEWORK

| Feature | Confidential Computing [18] | DCS Framework |
|---|---|---|
| **Secure Data Processing** | Yes | Yes |
| **Security Control Location** | CSP-managed | Customer-controlled |
| **Cross-Cloud Interoperability** | No | Yes |

**Strengths and Trade-Offs of the DCS Framework**

**Strengths:**

- **Improved Data Sovereignty:** The DCS model ensures that customers maintain complete control over security policies and encryption keys, in contrast to a CSP-dependent model [19].

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- **Adaptive Regulatory Compliance:** the automated compliance engine adapts to continuously evolving global regulations [20].
- **Cross-Cloud Security Management** The DCS framework allows security governance in multiple cloud environments as opposed to conventional CSP silos [21].

### 6.4.2 Trade-Offs

- **Integration Complexity:** The externalized security layer is based on interacting with different CSP environments, which may introduce operational complexity [22].
- **Confidential Computing Performance Overhead:** Secure enclaves and homomorphic encryption incur computational overheads [23].
- **Interoperability Challenge:** Security policies standardization across cloud providers is a technical challenge [24].

### 6.5 Summary

This comparative analysis highlights that the DCS framework offers a vendor-neutral, compliance-first, and sovereignty-preserving security architecture. Although traditional CSP security models and new security paradigms solve some cloud security problems, they only partially decouple security enforcement from CSP infrastructure. The DCS framework avoids these limitations by guaranteeing:

1. Multi-cloud security control and policy enforcement
2. It was also the last thing that allowed for key ownership with customer-managed encryption—removing dependence on CSP.
3. Intelligent compliance, dynamic, jurisdiction- aware in real time, compliant with global regulations.

## IV. Conclusion AND future work

To compound the problem, the widespread adoption of cloud computing in every sector has raised issues of data sovereignty, regulatory compliance, and cross-border security governance. Traditional cloud security assumes CSP-managed security controls which can lead to risks of vendor lock-in and restrictions for organizations on enforcing independent security policies. To tackle these issues, this paper presents the Decoupled Cloud Security (DCS) framework that adds a vendor-agnostic security layer which:

- Decouples security enforcement from cloud service providers so that you have sovereign control over your security policies.
- Provides separate cryptographic capabilities and unique keys, enabling customers to administer encryption keys in a location separate from CSPs.
- Supports automatic enforcement of compliance by dynamically responding to governance changes
- Improves cloud security between borders with standardized governance between different CSPs

### Future Work

Still, the DCS architecture resolves many cloud security decoupling issues, albeit the efficacy of its operability, scalability, and interoperability needs to be investigated in future research. Future directions include:

### Standardization of Interoperable Security Policies

This becomes a significant hurdle to enforce cross-cloud security policy because there is no unified security policy standard across CSPs. Future Enhanced work on policy formats should be agnostic of the models and use frameworks like OASIS XACML and NIST Zero Trust [1].

Journal of Information Systems Engineering and Management
2025, 10(4)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

### Performance Optimization in Confidential Computing

While confidential computing is integrated into the DCS framework (for example, Intel SGX, AMD SEV, and homomorphic encryption [2]), these approaches incur performance overhead. Future work may investigate light-weight cryptographic methods and secure enclave specific optimizations to decrease computational overhead with a retained security guarantee.

### AI-Driven Dynamic Compliance Adaptation

Future research could investigate machine-learned compliance frameworks that auto-tune policies given changing jurisdictional information [3].

### Cross-Border Data Flow Optimization

Through operating in multiple geographies, organizations continue to face a challenge of looking at their data flows. It should be followed by future work on conducting different privacy-preserving mechanisms like secure multi-party computation (SMPC) and federated learning for optimizing cross-border data sharing with regulatory conformations [4].

### Blockchain-Enabled Trust Management

Incorporating decentralized blockchain-based IAM is another way to establish multi-cloud security governance with trust. Future research proposals must focus upon the integration of smart contracts as means of automated enforcement of policies and verification [5].

## V. References

[1] National Institute of Standards and Technology (NIST), “Zero Trust Architecture,” NIST Special Publication 800-207, 2020.

[2] V. Costan and S. Devadas, “Intel SGX Explained,” Cryptology ePrint Archive, Rep. 2016/086, 2016.

[3] NIST, “NIST AI Risk Management Framework,” 2023.

[4] R. Shokri *et al.*, “Privacy-Preserving Distributed Machine Learning,” in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, 2015.

[5] G. Zyskind, O. Nathan, and A. Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” in *Proc. IEEE Secur. & Priv. Workshops*, 2015.

[6] Cloud Security Alliance (CSA), “Cloud Controls Matrix (CCM) v4,” 2021.

[7] European Commission, “General Data Protection Regulation (GDPR),” 2016.

[8] California Legislative Information, “California Consumer Privacy Act (CCPA),” 2018.

[9] U.S. Department of Health & Human Services, “Health Insurance Portability and Accountability Act (HIPAA),” 1996.

[10] Singapore Personal Data Protection Commission, “Personal Data Protection Act (PDPA),” 2012.

[11] Brazilian Government, “Lei Geral de Proteção de Dados (LGPD),” 2020.

[12] The National People’s Congress of China, “Personal Information Protection Law (PIPL),” 2021.

[13] Government of India, “Digital Personal Data Protection Act (DPDPA),” 2023.

[14] Australian Government, “Privacy Act 1988,” 1988.

[15] ISO/IEC, “ISO/IEC 27001: Information Security Management Systems,” Int. Org. Standardization, 2022

Research Article

[16] National Institute of Standards and Technology (NIST), “Security and Privacy Controls for Federal Information Systems and Organizations,” NIST SP 800-53 Rev. 5, 2020.

[17] SWIFT, “Customer Security Programme (CSP),” 2022.

[18] IBM, “Confidential Computing for Secure Cloud Workloads,” IBM Research, 2021.

[19] A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption,” in *Proc. Int. Conf. Theory Appl. Cryptographic Technol.*, 2005.

[20] K. Kent and M. Souppaya, “Guide to Computer Security Log Management,” NIST SP 800-92, 2006.

[21] S. Pearson, “Taking Account of Privacy when Designing Cloud Computing Services,” in *Proc. IEEE Int. Conf. Cloud Comput. (CLOUD)*, 2009.

[22] K. D. Bowers, A. Juels, and A. Oprea, “HAIL: A High-Availability and Integrity Layer for Cloud Storage,” in *Proc. ACM CCS*, 2009.

[23] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, “Hey, You, Get Off My Cloud: Exploring Information Leakage in Third-Party Compute Clouds,” in *Proc. ACM CCS*, 2009.

[24] D. Boneh, B. Lynn, and H. Shacham, “Short Signatures from the Weil Pairing,” J. Cryptol., 2004.

[25] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” in *Proc. Int. Conf. Financial Cryptogr. Data Secure, 2010