Towards Global Multi-Cloud Strategies: Insights into AWS and Alibaba Cloud Synergy

Martin G. Zizler*, Malte Prieß†, Christoph P. Neumann*

*Department of Electrical Engineering, Media and Computer Science
Ostbayerische Technische Hochschule Amberg-Weiden, Amberg, Germany
e-mail: {m.zizler1 | c.neumann}@oth-aw.de

†Faculty of Computer Science and Electrical Engineering
Kiel University of Applied Sciences, Germany
e-mail: malte.priess@haw-kiel.de

***Abstract*—Multi-cloud strategies are increasingly adopted by modern enterprises to improve agility and resilience and to reduce vendor lock-in. Integrating workloads across providers, such as Amazon Web Services (AWS) and Alibaba Cloud, remains challenging due to interoperability and migration issues. This paper presents a comparative analysis of AWS and Alibaba Cloud, focusing on architectural, service, and policy differences affecting workload migration. Using both provider-native and open source Infrastructure-as-Code tools, we conduct an exploratory case study about the migration of Internet of Things (IoT) workloads. The results highlight key technical trade-offs and best practices for secure multi-cloud deployments, offering guidance for organizations pursuing AWS and Alibaba Cloud interoperability.**

Keywords-Cloud Computing; Multi-Cloud; AWS; Alibaba Cloud; Infrastructure-as-Code.

I. Introduction

According to Statista analysts, AWS is currently the world's leading Cloud Service Provider (CSP), while Alibaba Cloud ranks fourth worldwide [1]. In contrast, within mainland China, Alibaba Cloud holds the top position, as reported by Canalys [2]. As enterprises expand internationally, region-specific regulations and preferences drive adoption of alternative providers [3]. We specifically selected these two providers because bridging the global market leader (AWS) with the dominant provider in mainland China (Alibaba Cloud) represents a highly relevant, real-world challenge for multinational enterprises that is currently underrepresented in the literature. Multi-cloud strategies enhance agility, cost efficiency, resilience, and compliance [3]–[5], helping businesses mitigate vendor lock-in and address diverse operational needs [6]. However, integrating multiple providers introduces challenges due to differences in architectures, APIs, and services, complicating interoperability and workload portability [7][8]. Although prior research addresses general multi-cloud concepts, practical guidance for migrating workloads specifically between AWS and Alibaba Cloud remains limited. While technical hurdles, such as feature gaps in managed services, can often be solved via replatforming and custom workarounds, the overarching and arguably larger challenge lies in navigating strict, legally binding regulatory environments, including data residency and cross-border transfer restrictions.

This paper presents strategies for deploying and migrating workloads across AWS and Alibaba Cloud, focusing on technical and operational challenges. Section II outlines the state of the art; Section III describes the methodology; Section IV details the comparative analysis and deployments; Section V discusses key findings; Section VI concludes with main contributions and future directions.

II. State of the Art

Prior comparative studies have predominantly focused on AWS, Azure, and Google Cloud [9]–[11], providing quantitative and qualitative benchmarks but often excluding Alibaba Cloud. Zhang et al. [12] addressed this gap through a qualitative case study, identifying core vendor competencies and service delivery mechanisms unique to Alibaba Cloud.

The quantitative and qualitative evaluation methodologies established in these previous studies represent past successes in multi-cloud benchmarking. Our work reuses these foundational approaches but extends them to practical, real-world migration scenarios and technical interoperability involving Alibaba Cloud, which remains underrepresented.

III. Methods

This section details the methodological framework used to analyze, design, and empirically validate a multi-cloud strategy across AWS and Alibaba Cloud. Our approach integrates structured comparative analysis with an exploratory case study, explicitly addressing gaps identified in prior studies and leveraging insights from recent empirical research.

A. Research Design

We employed a mixed-method comparative and exploratory approach, as advocated for cloud provider evaluations [9]. Our methodology combines a targeted literature review to identify technical, operational, and architectural challenges in multi-cloud migration with practical experimentation to ensure findings are empirically grounded.

B. Comparative Framework

Building on the foundational approaches discussed in Section II, our comparative framework evaluates real-world migration scenarios and technical interoperability, emphasizing four domains: Global Infrastructure, Core Service Portfolio, API Usage, and Infrastructure-as-Code (IaC) tooling.

C. Strategy Development

The comparative insights provided the basis for developing a multi-cloud architectural strategy. Guided by reference architectures in the literature [13, pp. 72–76], we evaluated managed Virtual Machine (VM), container, and serverless models. Reflecting recent empirical work, such as Rajendran et al. [14], which underscores the importance of use-case-driven benchmarking, we selected a representative IoT workload for our Proof of Concept (PoC). A serverless-first strategy was adopted, supplemented by VMs where feature parity was lacking. This means that our approach is more akin to a replatforming approach rather than a simple rehosting or "lift and shift" approach [15]. Replatforming typically requires a higher technical complexity, which means that it can surface deeper migration complexities, involving a higher amount of managed services. To systematically assess migration overhead and feature coverage, we implemented both provider-native—Amazon Web Services Cloud Development Kit (AWS CDK) and Resource Orchestration Service Cloud Development Kit (ROS CDK)—and provider-agnostic (CDK for Terraform) Infrastructure-as-Code (IaC) tools.

D. Proof-of-Concept Development

To test our strategy, we designed and deployed a reference IoT application on AWS using AWS CDK, then migrated and adapted it for Alibaba Cloud with ROS CDK. Parallel definitions using CDK for Terraform provided an agnostic baseline for comparison. The implementation process, informed by best practices in IaC-driven migration [16][17], included:

- Defining and mapping equivalent resources and deployment steps for each provider,
- Adapting configurations and documenting feature gaps,
- Recording manual interventions required for successful migration.

E. Evaluation Methodology

We evaluated each deployment approach using both quantitative and qualitative criteria:

- Portability: Ease of migrating workload definitions and configurations
- Operational Transparency: Ongoing management and troubleshooting
- Maintenance Effort: Codebase maintenance
- Performance: Where measurable, indicative metrics were collected
- Security: Aligning IAM/RAM policies and Authentication

All findings were recorded systematically, with special attention to points of friction and required workarounds, as recommended by prior multi-cloud migration studies [18][19].

IV. Results

This section presents the outcomes of the systematic comparative analysis between AWS and Alibaba Cloud in Section IV-A and the exploratory case study in Section IV-B. The comparative analysis is based on vendor documentation and migration guides, which may introduce bias. To minimize overreliance on these secondary sources, we implemented the practical migration of a representative workload using IaC approaches.

A. Comparative Analysis

1) Global Infrastructure: AWS maintains global reach with 36 regions and 114 availability zones as of mid-2025, delivering strong coverage in North America and Europe [20]. Alibaba Cloud operates 29 regions and 87 availability zones, with its core strength in Greater China [21]. Both providers offer specialized partitions like AWS GovCloud or AWS China [22] to accommodate regulatory or sovereignty requirements.

It is important to note that Alibaba Cloud maintains two distinct infrastructures: AlibabaCloud.com, which serves international regions (e.g., Singapore, Frankfurt, Silicon Valley), and Aliyun.com (e.g., Shanghai, Beijing, Hangzhou), which serves regions within mainland China. In compliance with Chinese regulatory requirements, both Alibaba platforms operate in isolation. While international users can provision or manage resources in mainland China regions through AlibabaCloud.com, they are subject to a different regulatory framework (see also table II, regarding "Cross-border transfer restrictions", "Provider restrictions", and "Data residency").

2) Core Service Portfolio: Both AWS and Alibaba Cloud offer comparable core services across compute, storage, databases, networking, and security, though feature parity is not universal. Figure 1 provides an overview of the matched services and their functional completeness, based on vendor documentation [23][24] and a direct comparison by Alibaba [25]. Key differences are outlined below.

Messaging & API Management: Amazon Simple Queue Service (SQS) offers durable queuing with Standard (at-least-once) and FIFO (First-In-First-Out) modes, including dead-letter queues, short/long polling, and up to 14-day retention. Amazon Simple Notification Service (SNS) enables pub/sub delivery to SQS, Lambda, HTTP, Email, Mobile devices, SMS, Kinesis Data Firehose, and external providers (e.g., MongoDB). Alibaba Cloud Simple Message Queue (SMQ) supports queue-based and topic-based messaging with dead-letter queues, polling, and up to 7-day retention, but lacks FIFO mode. Its topic-based mode supports delivery to SMQ, Function Compute, HTTP, Email, SMS, and mobile endpoints. Both AWS API Gateway and Alibaba Cloud API Gateway are fully managed services that enable secure, scalable client-to-backend communication.

Compute: AWS EC2 and Alibaba Cloud ECS provide flexible VM types. AWS Lambda and Alibaba Function Compute offer serverless, event-driven compute with auto-scaling and pay-per-use pricing. AWS EKS and Alibaba Cloud

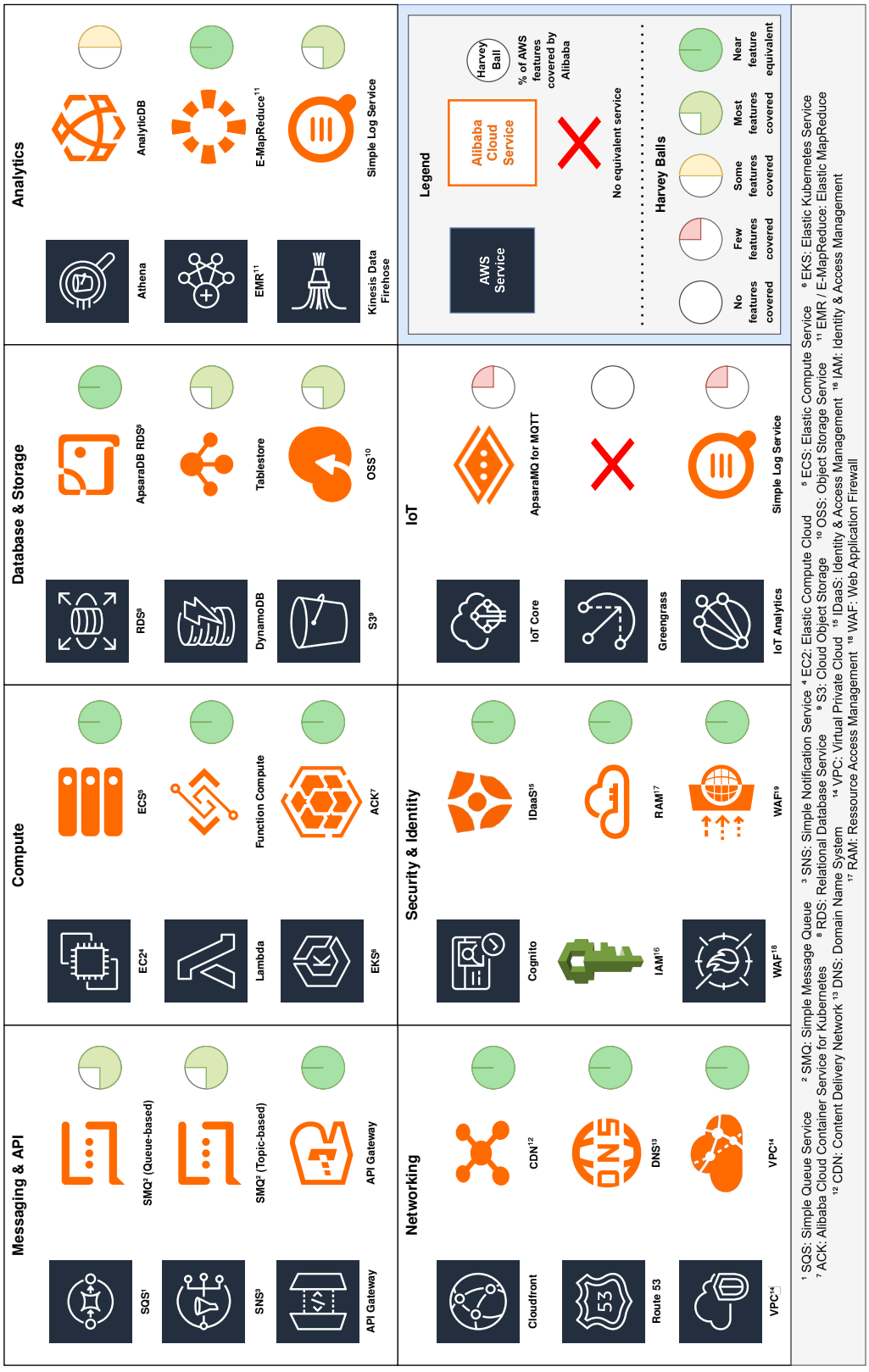

Figure 1. Cloud service overview and comparison between AWS and Alibaba Cloud core offerings, with a substantial gap in the IoT domain.

ACK deliver managed Kubernetes with high availability and reduced operational overhead.

Database & Storage: AWS Relational Database Service (RDS) and Alibaba Cloud ApsaraDB RDS can manage SQL databases. DynamoDB is a managed, serverless NoSQL database. Table Store delivers comparable features but has no true on-demand capacity mode, as it bills per Compute Unit (CU) instead of per request. AWS S3 and Alibaba Cloud Object Storage Service (OSS) are both fully managed object-storage services. S3 leads in the number of Storage classes.

Analytics: AWS Athena is serverless and lets you run SQL directly on S3 data for fast, ad-hoc analytics with no setup. Alibaba Cloud AnalyticDB provides batch processing and real-time analysis with support for both internal data and OSS, but requires cluster configuration. Athena is simpler to use, while AnalyticDB is more complex. AWS EMR and Alibaba E-MapReduce both run managed Hadoop and Spark clusters for big data processing in the cloud. AWS Kinesis Data Firehose and Alibaba Cloud Simple Log Service (SLS) both handle real-time data ingestion, transformation, and delivery to their cloud platforms. A key difference is that Firehose focuses on streaming data delivery, while SLS also includes built-in log analytics and monitoring features.

Networking: AWS CloudFront and Alibaba Cloud CDN both accelerate web content delivery via edge caching, reducing latency and improving performance. AWS Route 53 and Alibaba Cloud DNS provide scalable, globally distributed DNS management. Both clouds support secure, isolated virtual networks through their Virtual Private Cloud (VPC) services.

Security & Identity: AWS Cognito and Alibaba Cloud IDaaS both provide cloud-based user authentication and access management, integrating with their respective cloud services. AWS Identity and Access Management (IAM) and Alibaba Cloud Resource Access Management (RAM) offer the same core features of access management, including user, group, and role management, as well as permission controls. AWS Web Application Firewall (WAF) and Alibaba Cloud WAF both protect web apps from threats like SQL injection and XSS, offering customizable rules and real-time monitoring.

IoT: AWS IoT Core supports secure device connectivity, flexible protocols, and seamless integration with other AWS services. Alibaba Cloud ApsaraMQ for MQTT provides scalable MQTT messaging but lacks advanced device management and integration features found in IoT Core. AWS Greengrass offers edge computing for IoT, enabling local compute and sync when offline. Alibaba Cloud has no direct equivalent service to Greengrass. AWS IoT Analytics delivers managed pipelines for processing IoT data, while Alibaba Cloud lacks a truly equivalent service. Simple Log Service (SLS) can be used for basic data ingestion and analytics.

3) API Usage: Both clouds expose RESTful APIs and SDKs covering major languages, but slightly differ in endpoint conventions and authentication depending on configuration. The API documentations for both CSPs show that basic API requests are still very similar across both (e.g., Bucket API documentation for Amazon S3 [26] vs. Alibaba OSS [27]).

4) Infrastructure-as-Code Tools: AWS CDK (CloudFormation) and Alibaba ROS CDK provide native IaC tooling. Meanwhile, Terraform or OpenTofu, as well as CDK for Terraform, which are popular for multi-cloud deployments, also support both CSPs [16]. Native IaC tooling generally provides faster support for new resource types and higher levels of abstraction.

B. Exploratory Case Study

1) Workload and Architecture: As a Proof-of-Concept (PoC), a representative IoT workload consisting of compute, storage, and event-driven processing was implemented using both provider-native and agnostic IaC tools for deployment. The workload includes serverless functions, object storage buckets, event triggers, and messaging services, which can be seen in Figure 2. Equivalent resources were used for AWS and Alibaba Cloud. Additional adaptation was required for the AWS IoT Core. While ApsaraMQ for MQTT exists as a potential replacement, it is just a generic MQTT broker with a very sparse feature set (see IV-A). Therefore, Thingsboard was selected as an open alternative and deployed on Alibaba Cloud ECS. Similar to IoT Core, Thingsboard fully supports X.509 Certificate-based mutual authentication, which can be managed by device [28]. It also supports custom Rule Chains to process events. To securely send data from a Thingsboard Rule Chain to other Alibaba Cloud services, a simple Flask server that can get access by utilizing the Alibaba Cloud SDK for Python was also added as an intermediary. Furthermore, an external adapter was set up to show that data can also be retrieved from the CSPs. This adapter was also used to test latency differences depending on deployment location.

2) IaC Implementation: AWS CDK (Python) and Alibaba ROS CDK (Python) were used to define and deploy the stack natively. Most of the resource definitions translated with little adaptation needed, as they have very high overlap, as shown in IV-A. The remaining required manual adaptation is due to differences in parameterization, IAM/RAM policy syntax, or missing features (e.g., managed IoT services).

CDK for Terraform (Python) was used to define stacks utilizing the same Python environment, targeting both AWS and Alibaba Cloud providers, while OpenTofu was used as the underlying IaC tool (open-source Terraform fork). Very similar to the provider-native approach, the Alibaba Cloud code base required provider-specific adaptation in all resources to accommodate differences in event sources and IAM/RAM, as well as configuration.

3) Deployment and Operational Metrics: For these metrics, the Alibaba Cloud equivalent of AWS IoT Core (an ECS-based Thingsboard deployment) is excluded from the IaC line count, as automating this setup would require substantial custom scripting. For fair comparison, AWS IoT Core is also omitted.

Table I summarizes deployment and teardown times, as well as Lines of Code (LoC) required for IaC definitions of each approach. Deployment times were similar between provider-native and provider-agnostic tools within each platform, but Alibaba Cloud was faster. Line counts were measured using

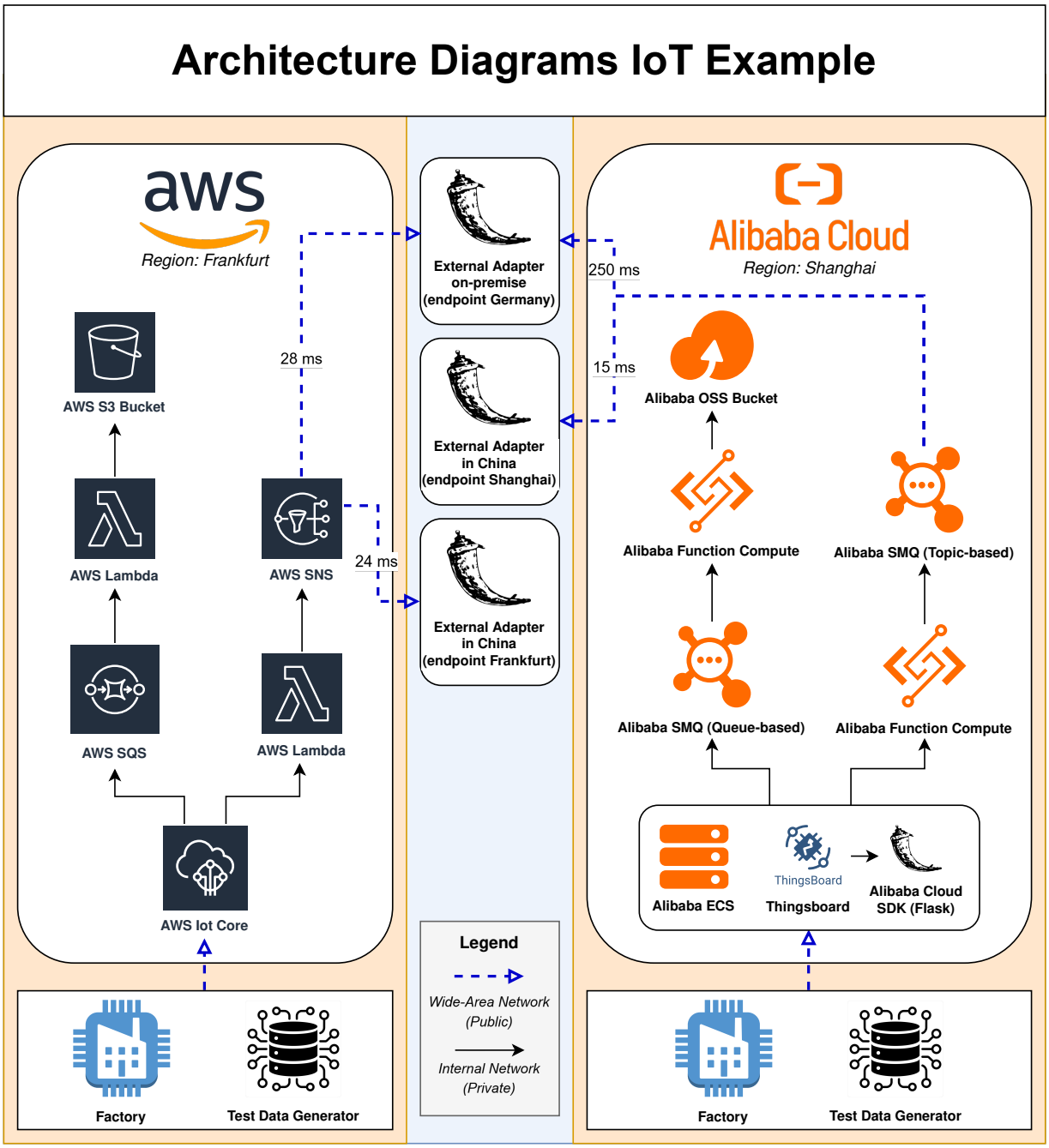

Figure 2. Architecture diagram showing resource mapping and data flow of a basic IoT Stack.

VS Code Counter with code formatted via Black to ensure consistency. Notably, the AWS CDK for Terraform (CDKTF) implementation required substantially more code than alternative approaches, primarily due to AWS's detailed IAM model and the need for explicit resource linking. In contrast, the AWS CDK benefits from high-level constructs, resulting in a more concise codebase. Differences in code length among Alibaba Cloud tools were comparatively minor.

TABLE I. DEPLOYMENT TIMES, TEARDOWN TIMES, AND IAC LINE COUNTS OF IOT STACK.

Platform	Tool	Deploy	Destroy	Lines
AWS	CloudFormation	1m 15s	56s	75
AWS	CDKTF	1m 11s	30s	184
Alibaba Cloud	ROS	24s	26s	146
Alibaba Cloud	CDKTF	19s	26s	143

The architecture diagram in Figure 2 also provides some latency numbers, annotated to the blue dashed arrows for wide-area networks. Network transfers within the same country (Germany to Germany or China to China) have low latency.

Cross-border egress (from Alibaba in Shanghai to the external adapter in Germany) introduces a latency about ten times higher. We provide an extended set of quantitative benchmarking in a publicly available Master's thesis [29].

V. Evaluation

This section summarizes the main findings from our comparative analysis and exploratory case study, highlighting key trade-offs of native versus agnostic IaC approaches.

A. Interpreting the Comparative Analysis

AWS and Alibaba Cloud both offer mature core services, but differ in regional coverage, service completeness, and compliance. IoT-heavy workloads on Alibaba Cloud require additional custom or third-party solutions to address service gaps, whereas AWS provides more integrated support.

B. Evaluating the PoC

The deployments allow evaluation of the following criteria:

1) **Portability**: Provider-native IaC (AWS CDK, ROS CDK) offers rapid access to new features and high-level constructs, but poor cross-provider code reuse. Agnostic IaC (OpenTofu) enables a unified code base, but still needs extensive provider-specific adjustments.
2) **Operational Transparency**: Native tools integrate better with CSP management interfaces, offering richer diagnostics and control, unlike OpenTofu-based stacks.
3) **Maintenance Effort**: Unified CDK for Terraform code bases can reduce duplication but increase maintenance for provider plugin updates. Native stacks benefit from vendor-managed updates but require managing separate pipelines.
4) **Performance**: Deployment times for Alibaba Cloud seem to be a bit faster (see Table I).
5) **Security**: Ensuring least-privilege access required manual effort to align IAM (AWS) and RAM (Alibaba Cloud) policies. For instance, AWS CDK provides high-level abstractions for granting permissions (e.g., allowing Lambda to write to S3), whereas ROS CDK often necessitates explicit role and policy configuration. Additionally, synchronizing certificate-based authentication across providers involved adapting identity management to maintain secure communication over wide-area networks.

C. Compliance Considerations

Compliance challenges are increased by regional regulations. For example, Alibaba Cloud's mainland China partition is subject to local laws like the China Cybersecurity Law, requiring data residency and stricter controls on cross-border flows [46]. AWS China and Alibaba's specialized regions address sovereignty but require careful architectural planning.

To further classify the regulatory requirements, table II shows examples of compliance constraints derived from international legal sources and industry-specific standards. The analysis does not aim to provide a concluding legal evaluation of regulatory frameworks; rather, it offers a first technical abstraction of selected requirements. From an architectural perspective, it illustrates how regulatory requirements, such as the GDPR, the German IT Security Act 2.0, PIPL, or the CLOUD Act, may translate into concrete technical design decisions, including role-based access control, client separation, and data localization.

Due to the limited harmonization of international regulations, globally uniform cross-country infrastructures remain challenging. A more realistic horizon lies in compliance-aware, modular architectures that enable controlled interoperability while respecting regional legal constraints.

D. Lessons Learned & Best Practices

- Utilize a service mapping matrix to track equivalences.
- Use provider-native IaC services to make use of high-level abstraction and have a higher operational transparency. Use cloud-agnostic IaC to achieve more equal code bases between different CSPs.
- Plan for manual adaptation where services don't match.
- Leverage native security tools and audit access policies.

E. Threats to Validity

Our PoC focused on a basic IoT stack; results may not generalize to large-scale data processing, or CSP-specific managed services outside the evaluated scope. Pricing and performance data are indicative; real-world figures will vary by workload size, region, and time. Finally, CSP feature sets evolve rapidly, so this mid-2025 snapshot may differ from future states.

VI. Conclusion and Future Work

Our analysis compared AWS and Alibaba Cloud across infrastructure, services, Infrastructure-as-Code tools, and regulatory frameworks, with the findings validated through a small-scale IoT proof of concept. AWS has a more mature service portfolio and leads in innovation speed. This can make it harder to develop a true multi-cloud strategy based on using serverless services. Our comparative analysis extends previous studies to real-world migration scenarios and technical interoperability. In conclusion, the paper closes several gaps in multi-cloud literature for global approaches that comprise China and Alibaba Cloud.

Several opportunities for further investigation present themselves moving forward:

- Broader workloads with other managed services.
- Performance and cost benchmarking at scale.
- Explore integration of multi-cloud management platforms.
- Assess interoperability with third-party SaaS offerings.
- Evaluate specific privacy and security implications of using CSPs governed by distinct national legal frameworks (e.g., data sovereignty and state access concerns regarding Alibaba Cloud).

By advancing these areas, future work can further reduce operational friction and enhance the robustness of global multi-cloud deployments.

TABLE II. EXAMPLES OF COMPLIANCE CONSTRAINTS DERIVED FROM INTERNATIONAL LEGAL SOURCES AND INDUSTRY-SPECIFIC STANDARDS.

Constraint type		Source	Significance for multi-cloud
Data residency	Transfer of personal data to third countries (outside the EU/EEA) is only permitted under specific conditions.	GDPR Art. 44–49 [30]	Storing EU personal data in Alibaba Cloud Mainland may breach GDPR; transfers require adequacy decisions, SCCs, or legal exceptions.
Cross-border transfer restrictions	Data exports from China may require prior security assessment and government approval.	DSL Art. 31–37 [31], CSL Art. 37 [32], MLPS 2.0 [33]	Transfers from Alibaba Cloud Mainland to AWS Frankfurt may require CAC approval and data export security review.
Tenant isolation	Data belonging to different customers, departments, or patients must be kept logically and technically separated.	GoBD 2020 [34], SOX §404 [35], HIPAA 164.308(a)(4) [36]	IaC should enforce resource separation (e.g., VPCs, IAM roles, storage buckets) per tenant to prevent data leakage.
Auditability	Access to systems must be traceable and securely logged for compliance and incident analysis.	BSI C5:2020 (e.g., OPS-07) [37], ISO 27001 8.15 (Logging) [38], GDPR Art. 30, 33 [30]	Cloud-native logging (e.g., AWS CloudTrail, Alibaba ActionTrail) should be enabled, retained, and protected.
Classification requirements	Operators of critical infrastructure must classify systems and apply tiered protection accordingly.	NIS 2 (EU 2022/2555, Art. 21) [39], BSIG §8a [40] & IT Security Act [41], MLPS 2.0 [33]	Selection of certified services only (e.g., BSI C5) and onshore deployment; additional monitoring and emergency mechanisms if necessary; classification as a necessary prerequisite for protective measures.
Provider restrictions	A cloud provider may be subject to foreign government access demands (e.g., US CLOUD Act, CN national laws).	CLOUD Act [42], GDPR Art. 48 [30], BSIG §9b [40] & IT Security Act [41], Gaia-X standards, if applicable [43][44]	Onshore providers preferred to avoid extraterritorial access; regulatory context may disqualify US/CN providers for critical workloads; clarification on who can enforce access to data is essential.
Access and identity control	Only authorized users should access data, using strong authentication and role-based access control.	GDPR Art. 32(1)(b) [30], ISO 27001 8 (Technological controls) [38], BSI C5 (e.g., IDM-09) [37], CSL Art. 21 [32]	IAM (AWS) and RAM (Alibaba) should enforce RBAC, MFA, and auditable access policies.
Data minimization & purpose limitation	Only necessary data may be processed and stored for clearly defined purposes.	GDPR Art. 5(1)(c) [30], PIPL Art. 6 [45]	IaC and pipelines should be limited to minimal datasets and clearly scoped processing goals.

REFERENCES

[1] F. Richter, "Amazon and Microsoft stay ahead in global cloud market," 2025, Accessed: 2025-03-18. [Online]. Available: https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/.

[2] D. Singh, "Canalys: Global Cloud Infrastructure Spending Rose 22% In Q2 2025," 2025, Accessed: 2025-09-11. [Online]. Available: https://channelpostmea.com/2025/09/11/canalys-global-cloud-infrastructure-spending-rose-22-in-q2-2025/.

[3] D. Seth, M. Najana, and P. Ranjan, "Compliance and regulatory challenges in cloud computing: A sector-wise analysis," *International Journal of Global Innovations and Solutions (IJGIS)*, vol. 3, Jun. 2024, https://ijgis.pubpub.org/pub/n5sgt1c7. DOI: 10.21428/e90189c8.68b5dea5.

[4] J. Alonso et al., "Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review," *Journal of Cloud Computing*, vol. 12, p. 6, Jan. 2023. DOI: 10.1186/s13677-022-00367-6.

[5] G. Chatzithanasis, E. Filiopoulou, C. Michalakelis, and M. Nikolaidou, "Exploring cost-efficient bundling in a multi-cloud environment," *Simulation Modelling Practice and Theory*, vol. 111, p. 102 338, May 2021. DOI: 10.1016/j.simpat.2021.102338.

[6] D. Petcu, "Multi-cloud: Expectations and current approaches," in *Proceedings of the 2013 International Workshop on Multi-Cloud Applications and Federated Clouds*, ser. MultiCloud '13, Prague, Czech Republic: Association for Computing Machinery, 2013, pp. 1–6. DOI: 10.1145/2462326.2462328.

[7] R. Ranjan, "The cloud interoperability challenge," *IEEE Cloud Computing*, vol. 1, no. 2, pp. 20–24, 2014. DOI: 10.1109/MCC.2014.41.

[8] V. Munteanu, C. Sandru, and D. Petcu, "Multi-cloud resource management: Cloud service interfacing," *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 3, p. 3, Dec. 2014. DOI: 10.1186/2192-113X-3-3.

[9] A. Li, X. Yang, S. Kandula, and M. Zhang, "CloudCmp: Comparing public cloud providers," in *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, ser. IMC '10, Melbourne, Australia: Association for Computing Machinery, 2010, pp. 1–14. DOI: 10.1145/1879141.1879143.

[10] M. Saraswat and R. Tripathi, "Cloud computing: Comparison and analysis of cloud service providers – AWS, Microsoft and Google," in *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, 2020, pp. 281–285. DOI: 10.1109/SMART50582.2020.9337100.

[11] V. V. Rajendran and S. Swamynathan, "Parameters for comparing cloud service providers: A comprehensive analysis," in *2016 International Conference on Communication and Electronics Systems (ICCES)*, 2016, pp. 1–5. DOI: 10.1109/CESYS.2016.7889826.

[12] G. Zhang and M. Ravishankar, "Exploring vendor capabilities in the cloud environment: A case study of Alibaba cloud computing," *Inf. Manage.*, vol. 56, no. 3, pp. 343–355, Apr. 2019. DOI: 10.1016/j.im.2018.07.008.

[13] J. Mulder, *Multi-Cloud Administration Guide: Manage and Optimize Cloud Resources Across Azure, AWS, GCP, and Alibaba Cloud*. De Gruyter, 2024, ISBN: 9781501519482.

[14] P. Rajendran, S. Maloo, R. Mitra, A. Chanchal, and R. Aburukba, "Comparison of cloud-computing providers for deployment of object-detection deep learning models," *Applied Sciences*, vol. 13, p. 12 577, Nov. 2023. DOI: 10.3390/app132312577.

[15] M. Hussain, "A comparative analysis of cloud migration strategies for enterprise systems architecture," *World Journal of Advanced Engineering Technology and Sciences*, vol. 15, pp. 747–756, May 2025. DOI: 10.30574/wjaets.2025.15.2.0622.

[16] R. Kyadasu, "Exploring infrastructure as code using Terraform in multi-cloud deployments," *SSRN Electronic Journal*, Jan. 2025. DOI: 10.2139/ssrn.5075647.

[17] S. Achar, "Enterprise SaaS workloads on new-generation Infrastructure-as-Code (IaC) on multi-cloud platforms," *Global Disclosure of Economics and Business*, vol. 10, pp. 55–74, Jul. 2021. DOI: 10.18034/gdeb.v10i2.652.

[18] H. Zhao, Z. Benomar, T. Pfandzelter, and N. Georgantas, "Supporting multi-cloud in serverless computing," in *2022 IEEE/ACM 15th International Conference on Utility and Cloud Computing (UCC)*, 2022, pp. 285–290. DOI: 10.1109/UCC56403.2022.00051.

[19] V. Yussupov, U. Breitenbücher, F. Leymann, and C. Müller, "Facing the unplanned migration of serverless applications: A study on portability problems, solutions, and dead ends," Dec. 2019, pp. 273–283. DOI: 10.1145/3344341.3368813.

[20] Amazon, "AWS Infrastructure," 2025, Accessed: 2025-05-08. [Online]. Available: https://aws.amazon.com/about-aws/global-infrastructure/regions_az/.

[21] Alibaba, "Alibaba Cloud Infrastructure," 2025, Accessed: 2025-05-08. [Online]. Available: https://www.alibabacloud.com/en/global-locations?_p_lc=1#J_5253092060.

[22] Amazon, "AWS China," 2025, Accessed: 2025-05-08. [Online]. Available: https://www.amazonaws.cn/en/about-aws/china/.

[23] Amazon, "AWS Documentation," 2025, Accessed: 2025-03-23. [Online]. Available: https://docs.aws.amazon.com/.

[24] Alibaba, "Alibaba Cloud documentation," 2025, Accessed: 2025-03-23. [Online]. Available: https://www.alibabacloud.com/help/en.

[25] Alibaba, "Alibaba Cloud Services Migration Guide Service Comparison," Accessed: 2025-08-04. [Online]. Available: https://www.alibabacloud.com/en/product/product-mapping.

[26] Amazon, "AWS S3 API Documentation," 2025, Accessed: 2025-05-05. [Online]. Available: https://docs.aws.amazon.com/AmazonS3/latest/API/API_ListObjectVersions.html.

[27] Alibaba, "Alibaba OSS API Cloud Documentation," 2025, Accessed: 2025-05-05. [Online]. Available: https://www.alibabacloud.com/help/en/oss/developer-reference/listobjectversions?spm=a2c63.p38356.0.i2#reference-n2s-xy3-fhb.

[28] Thingsboard, "Thingsboard Documentation," Accessed: 2025-08-04. [Online]. Available: https://thingsboard.io/docs.

[29] M. Zizler, "Global Multi-Cloud Strategies: Efficient Utilization of AWS and Alibaba Cloud for Scalable Cloud Applications," Master's Thesis, Ostbayerische Technische Hochschule Amberg-Weiden, Sep. 2025. DOI: 10.5281/zenodo.17400896.

[30] European Union, "General Data Protection Regulation (GDPR), Regulation (EU) 2016/679," 2016, Official Journal of the European Union, L 119, 4 May 2016.

[31] National People's Congress of the People's Republic of China, "Data Security Law of the People's Republic of China (DSL)," 2021, adopted on 10 June 2021, effective from 1 September 2021, translation by DigiChina (Stanford University).

[32] National People's Congress of the People's Republic of China, "Cybersecurity Law of the People's Republic of China (CSL)," 2017, adopted on 7 November 2016, effective from 1 June 2017, translation by DigiChina (Stanford University).

[33] Ministry of Public Security of the People's Republic of China, "Multi-Level Protection Scheme 2.0 (MLPS 2.0) – Classified Protection of Cybersecurity," 2019, adopted on 13 May 2019, effective 1 December 2019, translation not publicly available.

[34] Federal Ministry of Finance, "Principles for the proper management and storage of books, records and documents in electronic form and for data access," 2019, translation, notice dated 28 November 2019, valid from 1 January 2020.

[35] United States Congress, "Sarbanes–Oxley Act (SOX)," 2002, Public Law 107–204, enacted July 30, 2002.

[36] U.S. Department of Health and Human Services, "Health Insurance Portability and Accountability Act (HIPAA) of 1996, Security Rule – 45 CFR §164.308(a)(4) Information Access Management," 1996, codified in Title 45 of the Code of Federal Regulations (CFR), Subpart C – Security Standards for the Protection of Electronic Protected Health Information.

[37] Federal Office for Information Security (BSI), "Cloud Computing Compliance Controls Catalogue (C5:2020)," 2020.

[38] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection – Security techniques – Information security management systems – Requirements," 2022.

[39] European Parliament and Council of the European Union, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)," 2022, Official Journal of the European Union, L 333, 27 December 2022, pp. 80–152.

[40] Federal Republic of Germany, "Act on the Federal Office for Information Security (BSI Act – BSIG)," 2021, translation, as amended by the IT Security Act 2.0 of 28 May 2021.

[41] Federal Republic of Germany, "Second Act on increasing the Security of IT Systems (German IT Security Act 2.0)," 2021, translated, promulgated in the Federal Law Gazette I, No. 25, 27 May 2021, pp. 1086–1103.

[42] United States Congress, "Clarifying Lawful Overseas Use of Data Act (CLOUD Act), H.R. 4943," 2018, enacted March 23, 2018, as Division V of the Consolidated Appropriations Act, 2018 (Public Law 115–141).

[43] Gaia-X European Association for Data and Cloud, "Gaia-x policy rules document," 2022, Version 22.04, April 2022.

[44] Gaia-X European Association for Data and Cloud, "Gaia-x trust framework," 2022, Version 22.10, October 2022.

[45] National People's Congress Standing Committee, "Personal Information Protection Law of the People's Republic of China (PIPL)," 2021, adopted on 20 August 2021, effective 1 November 2021, translation by DigiChina (Stanford University).

[46] Cyberspace Administration of China, "Questions and Answers on Data Outbound Security Management Policy," Apr. 2025, Accessed: 2025-07-21. [Online]. Available: https://www.cac.gov.cn/2025-04/09/c_1745906286623776.htm.