The American Journal of Engineering and Technology
ISSN 2689-0984 Volume 08 - 2026

# Evaluation of Hybrid Cloud Computing Techniques to Enhance Data Security in Digital Enterprises

**Marwah Naeem Hassooni**
Ministry of Education, Directorate for Education in the Province of Maysan, Iraq

Received: 02 Mar 2026 | Received Revised Version: 19 Apr 2026 | Accepted: 23 May 2026 | Published: 04 June 2026

Volume 08 Issue 06 2026 | Crossref DOI: 10.37547/tajet/Volume08Issue06-03

## Abstract

*A large number of organizations have been increasingly adopting hybrid cloud computing models due to the significant acceleration of digital business transformations. These hybrid clouds offer organizations scalability and flexibility from public cloud platforms combined with control and compliance from their on-premises infrastructure. Hybrid cloud models also present organizations with several advantages such as greater operational agility; lower costs; and greater workload scalability. However, hybrid clouds create a variety of new and complex cybersecurity issues related to identity management; cross-cloud visibility; data governance; regulatory compliance; and distributed attack surfaces. The objective of this research is to analyze and compare several of the most recent data security methods used by hybrid cloud systems for digital businesses. In order to achieve the objective, the research will employ a multi-faceted approach consisting of literature synthesis; technical framework analysis; a metric based assessment model; and a simulated threat modeling process. Advanced security methods such as Zero Trust Architecture (ZTA); Cloud Security Posture Management (CSPM); Cloud Workload Protection Platforms (CWPP); Homomorphic Encryption; Secure Multi-Party Computation (SMPC); Trusted Execution Environments (TEEs) and AI-driven Security Operations (SecOps) were selected for examination. The proposed evaluation method examines each identified technique using a set of multiple operational and security metrics such as confidentiality; integrity; availability; scalability; compliance alignment; performance overhead and incident response efficiency. Evaluation results indicate that organizations can increase their hybrid cloud ecosystem's security resilience through the use of integrated security frameworks incorporating elements of ZTA; automated CSPM/CWPP components and hardware-enforced trust technologies. The proposed framework can assist decision makers at organizations in determining how best to implement their hybrid cloud security solutions in accordance with current cybersecurity regulations and standards.*

**Keywords:** Hybrid Cloud Security, Zero Trust Architecture, Cloud Security Evaluation, Data Protection, AI-Driven Threat Detection.



**Cite This Article:** Hassooni, M. N. (2026). Evaluation of Hybrid Cloud Computing Techniques to Enhance Data Security in Digital Enterprises. The American Journal of Engineering and Technology, 8(06), 64–78. https://doi.org/10.37547/tajet/Volume08Issue06-03

## 1. Introduction

The rapidly accelerating digital transformation of today's organizations has transformed how organizations manage their computing infrastructures and data management practices. Cloud computing is the dominant model for providing scalable, flexible, and cost-effective computing services in distributed environments [1], [2]. Hybrid cloud computing has been adopted at a significant level because it allows users to link private on-site (on premise) infrastructure to cloud based services while allowing users to maintain operational flexibility, workload scaleability and regulatory compliancy [3].. Industry and academic studies have reported that hybrid cloud configurations are the preferred configuration for large enterprise companies involved in highly sensitive data industries such as health care, financial services, governments and critical infrastructure [4], [5].

While there may be some benefits associated with hybrid cloud computing in terms of operational costs and business agility; hybrid cloud computing creates numerous and complex cybersecurity issues that arise from disparate systems, interdependent domain resource orchestration, and differing levels of trust among various domains [6]. In contrast to traditional centralized environment which are typically monitored by one or a few administrators within an organization; hybrid clouds represent a number of distinct administrative domains. These separate domains can include varying degrees of security policy inconsistency, different levels of monitoring visibility, increasing levels of workload migration and differences in cross-Cloud identity dependencies [7]. As a result of these characteristics, traditional perimeter defense models are becoming less effective against current cloud native attack vectors. This includes those types of attacks that involve micro-service applications, containerized workloads and integration of multiple cloud-based services [8].

The growing complexity of cyberattacks has increased the level of concern over security in Hybrid Cloud environments. Recent research has found that the most common causes for Hybrid Cloud security breaches are due to a variety of factors such as, Misconfiguration of resources; insecure Application Programming Interfaces (API's); vulnerabilities related to Identity Federation; Lateral Movement attacks; Compromise of the Supply Chain; and Data Exfiltration. Furthermore, the Shared Responsibility Model between Enterprise Administrators and Cloud Service Providers can lead to confusion regarding accountability which results in inconsistent security policy implementation and compliance gaps [10]. As a result, this creates an environment with many variables that make it difficult for Enterprises to ensure Confidentiality, Integrity, Availability, and Regulatory Compliance throughout their entire cloud-based infrastructure.

As a result, enterprises have implemented advanced Cybersecurity strategies to help reduce risk associated with utilizing Hybrid Clouds. Some of the strategies include Zero Trust Architecture (ZTA), Cloud Security Posture Management (CSPM), Cloud Workload Protection Platform (CWPP), Confidential Computing, Homomorphic Encryption, Secure Multi Party Computation (SMPC), and Artificial Intelligence driven Security Operations (SecOps).[11],[12] ZTA will improve identity-based security by continuously authenticating users and enforcing Least Privileged Access Enforcement [13]. Both CSPM and CWPP utilize automation to analyze both cloud configurations at rest and workload activity in real time to protect against threats [14]. Additionally, Confidential Computing utilizes hardware assistance to provide protection to sensitive data being processed,[15] and artificial intelligence powered SIEM Systems provide enhanced threat detection capabilities using behavior analytics and anomaly detection to enhance Incident Response capabilities [16].

Despite numerous advances made in the field of Cloud Security Research there are still many significant gaps that exist within the current literature. Firstly, nearly all previous investigations into Cloud Security Mechanisms were done as standalone investigations without investigating how these security mechanisms work together as an integrated hybrid Cloud Ecosystem [17]. Secondly, past investigations into Hybrid Clouds focused on conceptual or architectural level discussions with very little investigation at an empirical/operational level focusing on; performance, scalability, compliance alignment and overhead for enterprise scale implementations [18]. Lastly, past frameworks lacked standardized evaluation methodologies that could quantify Hybrid Cloud Security Strategies across multiple levels such as; Confidentiality, Integrity, Availability, Threat Mitigation Efficiency, Compliance Readiness and Operational Complexity [19]. Further, few investigations have looked at Cross-Cloud Interoperability Challenges, Dynamic Identity

Federation, Real-Time Compliance Orchestration and Automated Governance within Heterogeneous Multi-Cloud Environments [20].

As such, there is a large research gap in developing comprehensive and empirically validated evaluation frameworks for Hybrid Cloud Cybersecurity Architectures. Developing frameworks that fill this gap will enable organizations to evaluate security mechanisms objectively, develop optimized deployment strategies and enhance cyber-resiliency in increasingly complex Enterprise Cloud Infrastructures.

This research addresses these problems through a fully developed and metric-based Hybrid Cloud Cybersecurity Techniques Evaluation Framework. It goes beyond all prior evaluations of individual security methods by evaluating total enterprise-oriented security architecture and real-world threat models. It includes four major components to evaluate hybrid cloud cyber-security: Quantitative Performance Analysis; Threat Modeling; Compliance Assessment; and Operational Evaluation. The primary contributions of this work can be stated as follows:

1. A complete hybrid-cloud-cybersecurity-techniques evaluation method based on both quantitative and qualitative measures.
2. An evaluation of state-of-the-art hybrid cloud cybersecurity technologies (ZTA, CSPM, CWPP, Confidential Computing, Homomorphic Encryption, AI/ML driven SecOps) in an enterprise hybrid cloud environment.
3. Quantification of how well each security technique's combination in an overall architecture can mitigate the specific risks associated with hybrid clouds (misconfiguration, lateral movement attack, insider threat, ransomware propagation, and data exfiltration).
4. Investigation of the interplay among the various types of hybrid cloud cyber-enforcement mechanisms (e.g., network controls, process execution restrictions, etc.) and operational considerations (e.g., scalability, performance impact, compliance alignment, etc.).
5. Practical deployment guidance and implementation recommendations for supporting digital enterprises to improve their hybrid cloud security posture without sacrificing operational agility or regulatory compliance.

The rest of this document will proceed as follows. In section 2 we will present some relevant literature and recent developments in hybrid cloud security. In section 3 we will describe our theoretical background and outline the key challenges facing hybrid cloud cybersecurity. Section 4 will describe our research methodology and evaluation criteria. Section 5 will detail the comparison of current hybrid cloud security methodologies. In section 6 we will discuss the experimental results from the comparative evaluation of hybrid cloud security methodologies. Section 7 will provide examples of practical implementations to help digital enterprises to implement their own hybrid cloud cybersecurity strategy. Lastly in section 8 we will summarize our findings and suggest possible avenues for future research.

## 2. Literature Review

This part of the chapter is an overall review of the previously published literature on hybrid cloud security, and the different types of new cyber security solutions that will be used to secure data in enterprise organizations using hybrid clouds. The paper will discuss how hybrid cloud security has developed over time from a perimeter-based model to an Identity centric and Automated security model. The paper will also cover many different types of security technologies, which include; Zero Trust Architecture (ZTA), Cloud Security Posture Management (CSPM), Cloud Workload Protection Platforms (CWPP), Advanced Cryptographic Methods, Confidential Computing, and Artificial Intelligence Driven Security Operation Centers (SecOps).

In addition, this part of the paper will provide a current overview of the compliance and governance requirements associated with some of the most prominent regulatory frameworks (GDPR, HIPAA, NIS2, and ISO/IEC 27001). Overall, the majority of these studies point out the need for scalable and integrated security architectures to address the complexities of Hybrid Cloud Environments.

Finally, this portion of the paper identifies a number of previous areas of study that have identified gaps or shortcomings in hybrid cloud security research. These limitations include; the lack of standardization regarding evaluation methodologies, limited comparisons of interoperability, inadequate empirical support, and difficulties with assessing operational performance and managing Fmulti-cloud security.

### *2.1. Evolution of Hybrid Cloud Security Models*

The first hybrid cloud implementations used traditional firewalls and segmentation to separate public and private workloads. Studies with [2] have shown that perimeter controls are ineffective against lateral movement, insider threats, and API based attacks common to microservice based systems. This has led to the development of Identity-Centric Security models and ultimately the formalization of a Zero Trust Architecture (ZTA), as defined by NIST SP 800-207 in 2020. ZTA requires continuous validation of all users, minimal privilege access, and Micro-Segmentation which is very similar to Hybrid Cloud operations.
Further research conducted by [21] and [22] demonstrated that ZTA can decrease unauthorized access events in hybrid environments by 55-70%. However, there are still challenges with implementing ZTA. These include, integrating legacy systems into current architecture, synchronizing cross-cloud user identities, and decreasing latency with enforcing policies across clouds. Research performed by [23] identified that more than 40% of ZTA implementations experience configuration drift due to updated guidance policy, and therefore require automation and Infrastructure-as-Code (IaC).

### *2.2. Cryptographic and Confidential Computing Techniques*

Encryption is still a fundamental security component within Hybrid Cloud Security. Although traditional methods such as TLS/SSL and AES-256 encryption protect data both while it is in motion and while it rests; managing keys and being agile in terms of cryptography can create operational hindrances. Newer encryption techniques including format preserving encryption (FPE), and tokenization are becoming increasingly popular for keeping sensitive information encoded on top of the same data, yet their compatibility issues and high overhead costs limit large scale adoption.

New generation cryptographic technologies such as homomorphic encryption (HE) and secure multi-party computation (SMPC) enable computations to be performed on encrypted data without decrypting that data. Research from [24], demonstrated real world examples of fully homomorphic encryption (FHE) used in financial analysis and sharing medical records. While there remains a significant amount of computational overhead associated with FHE, current research has shown that this overhead is approximately 30-50 times higher than if one were to perform the computations using unencrypted data. As recently as last year, new hardware accelerators (Intel's HE-Silk and NVIDIA's cuFHE) have reduced latency associated with performing these types of computations by 60-75% allowing for the use of HE in very specific, extremely high value applications.

Confidential computing enables data isolation during processing via trusted execution environments (TEEs). For example, Intel SGX, AMD SEV, and AWS Nitro Enclaves. The researchers discussed in [25] along with Microsoft Azure confidential computing white papers (2024), show that TEEs decrease an attacker's exposure floor to data by eliminating hypervisor level attacks and unauthorized access to memory. However, deploying TEEs will require application redesign/refactoring, mitigating issue channel vulnerabilities, and developing effective attestation mechanisms, which may hinder enterprise adoption.

### *2.3. Automated Security Posture Management and Threat Detection*

Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platforms (CWPP) are now a critical part of Hybrid Cloud Safety. CSPM is used to continuously monitor configurations to ensure they comply with industry standards and best practices (NIST, CIS, ISO). CWPP provides runtime protection to workloads such as Containers, Serverless Functions, and Virtual Machines. Research in [7] suggests that organizations implementing integrated CSPM/CWPP solutions will see a reduction in misconfigurations resulting in security breaches by 68%, as well as a reduction in Mean Time To Discover (MTTD) by 52% [26].
The use of Artificial Intelligence (AI) and Machine Learning (ML) has dramatically improved an organization's ability to detect cyber threats. Using Behavioral Analytics, Anomaly Detection and Threat Intelligence Feeds, AI-powered Security Information and Event Management (SIEM) systems can identify 0-day exploits and insider threats. The research conducted in [27], indicates that using AI powered SIEM systems results in a reduction of False Positive Rates from 40-60% while accelerating Incident Response times by 35-50%. As promising as AI/ML technology is there are many active areas of research including data drift, data poisoning, and explainability.

### *2.4. Compliance and Governance Frameworks*

Hybrid Cloud Security Investments are primarily driven by regulatory Compliance. The EU's GDPR, U.S. Healthcare Industry's HIPAA, Payment Card Industry Data Security Standard (PCI DSS), UK's National Cyber Security Centre's NIS2 and ISO/IEC 27001 require strict Data Protection requirements including transborder data protection and breach notification timeliness. The authors of [9] demonstrated how Automatic compliance mapping, Insurance as Code and Non-Preventative Audit Trails can significantly decrease compliance burden and exposure to penalties. Although some progress has been made there is still an ongoing issue with; (1) Lack of standardized evaluation metrics for hybrid cloud security techniques; (2) Inadequate empirical validation of the cryptography used within hybrid clouds in real-world deployment scenarios; (3) Limited Interoperability Research on go-between vendors; and (4) Inadequate Modeling of Multi-Cloud Risk Propagation. This project will address each of these gaps through developing a full, empirically based Evaluation Framework specifically designed to meet the Digital Enterprise Security Requirements.

## 3. Theoretical Framework and Security Challenges in Hybrid Cloud

### *3.1. Conceptual Architecture of Hybrid Cloud Security*

Hybrid Cloud Safety has to be viewed as being composed of layers that provide protection-in-depth throughout the Infrastructure, Platform, and Application levels. The three primary concepts on which this research is based are:

1. Continuous Verification: Rather than being configured once and then forgotten about, security is a continuous cycle of verification of authentication, authorization and monitoring of behavior.
2. Data-Centric Protection: No matter where data resides within a hybrid environment -- whether on-premises, in the public cloud or stored on various types of media -- security controls should be able to examine the data at some point.
3. Automated Governance: To keep pace with the speed of cloud-based services and operations, policy enforcement, compliance mapping and incident response must also be automated.

Both the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover) and the Zero Trust model, support these principles, providing a common theoretical foundation from which to evaluate hybrid-cloud safety strategies.

### *3.2. Threat Landscape in Hybrid Environments*

Hybrid Cloud Architectures increase the attack surface due to increased Complexity, Third-Party Integrations and Distributed Identity Management. The most significant Risk Training are:

1. Misconfigurations: Misconfigured IAM policies, Open Storage Buckets and Security Groups are the leading causes of Breaches.
2. Lateral Movement: An attacker who has compromised one workload can move laterally through Private and Public Environments if the workloads have been inadequately segmented.
3. Supply Chain Risks: A third-party API, Field Image or CI/CD Pipeline that is vulnerable represents a Backdoor for attackers to exploit within Hybrid Deployments.
4. Data Exfiltration: Transferring unencrypted Data, Inadequate Egress Filtering and Insider Threats allow unauthorized extraction of Data.
5. Compliance Failures: Failure to enforce consistent Data Residency, Insufficient Audit Trails and Fragmented Logging result in Regulatory Non-Compliance.

**Table 1 categorizes hybrid cloud threats by attack vector, impact severity, and primary mitigation techniques.**

| Threat Category | Attack Vector | Impact Severity | Primary Mitigation Techniques |
|---|---|---|---|
| **Misconfiguration** | IAM policy errors, open S3 buckets | High | CSPM, Policy-as-Code, Automated Remediation |
| **Lateral Movement** | Compromised credentials, weak segmentation | Critical | Micro-segmentation, ZTA, Network Telemetry |

| | | | |
|---|---|---|---|
| **Supply Chain** | Malicious container images, API flaws | High | SBOM Verification, Image Scanning, Runtime CWPP |
| **Data Exfiltration** | Egress abuse, insider threats | Critical | DLP, Encryption, Behavioral Analytics, TEEs |
| **Compliance Violation** | Inconsistent logging, data residency gaps | Medium-High | Automated Audit, Compliance Mapping, Data Tagging |

### *3.3. Security Challenges Unique to Hybrid Cloud*

Hybrid environments present traumatic situations that are no longer defined by "unmarried-cloud" and on-premises deployments.

The hybrid environment has five challenges:

1. Federation of Identities Across Clouds: Strong federation protocols (SAML/OIDC) are needed for continuous identity synchronization with on-premises Active Directory, and Azure AD, and AWS IAM. Also required is a method to continuously monitor privilege access.
2. Data Residency and Sovereign Requirements: Many regulatory requirements mandate data be stored within an organization's own jurisdiction(s), which creates complexities in workload placement and replication strategies.
3. Fragmented Visibility: The use of disparate logging formats, proprietary monitoring tools, and varied methods for collecting telemetry data prevent uniform threat detection.
4. Complexity with Key Management: There is additional complexity when distributing encryption keys into all these different environments while also needing to integrate HSM and follow key management rotation guidelines to reduce operational overhead.
5. Latency Impact from Performance/Security Trade-offs: Because advanced cryptography strategies and continuous verification introduce latency, organizations need to carefully optimize their latency sensitive applications.

Therefore, there needs to be a methodical approach to evaluating safety technologies to meet both technical, operational, and compliance requirements.

## 4. Research Methodology

### *4.1. Research Design*

This observe employs a blended-strategies studies format combining quantitative overall performance assessment, qualitative framework analysis, and simulated hazard modeling. The technique is primarily based to make sure reproducibility, instructional rigor, and sensible relevance for organization IT choice-makers.

### *4.2. Evaluation Criteria and Metrics*

The following security characteristics can be measured against the 8 primary criteria (see below) that are used to evaluate security techniques.

1. Confidentiality: How strong is data encryption? What are the fine-grained access rights to manage the data? How effective is the data masking?
2. Integrity: How well does the system detect tampering? Is there an audit log for all changes made in the system? Does the system validate checksums?
3. Availability: What percentage of time is the system available? What is the amount of delay when a system fails over from one server to another? How well does it protect against Distributed Denial of Service attacks?
4. Performance Overhead: How much memory/CPU do you use as a result of using this technique? What additional delay will your users experience due to implementing this technique? Will their throughput be reduced?
5. Scalability: Can you add new servers horizontally or vertically? Can policies propagate quickly enough to keep up with demand? Do you have support to implement the technique at multiple locations?
6. Compliance Alignment: How accurate is the map of regulatory requirements to the technique implemented? Are you ready for audits? Are you able to automatically produce reports to demonstrate compliance?
7. Incident Response: How long until you discover there was an issue? How long after discovering an incident before you restore normal operations? How easily can you provide forensic evidence to

determine what happened during an incident? To what degree are events automated by systems versus manually processed?

8. Operational Complexity: The number of hours required to implement the technology. The type and quantity of technical expertise required to implement, maintain and preserve the technology.

### *4.3. Data Collection and Simulation Environment*

A controlled hybrid-cloud testbed was established using:

1. Public Cloud: AWS (us-east-1 & european-west-1) and Microsoft Azure (East US & West Europe).

2. Private Cloud: On-premises OpenStack cluster based totally totally at the same time as using sixteen nodes with each node having 256 GB RAM.

3. Network: With a SD-WAN that has symmetric one Gbps connectivity and Quality of Service (QoS) priority for the network traffic.

4. Workloads: Relational database workloads (PostgreSQL), Object Storage, Server-less functions, and Microservices architecture (Kubernetes)

The security techniques were applied in incremental steps while total performance metrics have been collected for ninety-day announcement duration. The threat simulation included testing to determine how well the system could prevent or detect attacks including: Credential Stuffing, API Abuse, Area Escape Attempts, Ransomware Deployment, Insider Data Exfiltration

### *4.4. Analytical Approach*

Evaluation of data employed:
1. Data descriptive to assess baseline statistics.

2. The comparison with the use of a two-way ANOVA and an analysis by Tukey's Honestly Significant Difference (HSD).

3. A Multi-Criteria Selection Evaluation (MCDE), specifically through the Analytical Hierarchy Process (AHP).

4. A threat model based on both the MITRE ATT&CK for Cloud and STRIDE frameworks.

5. Map compliance against NIST SP 800-53, ISO/IEC 27017, and GDPR.

All evaluations were performed for each simulation three times to be sure that there was statistical significance ($p < .05$). The results were normalized and then combined as a composite security rating.

**Table 2: The outline of the evaluation matrix structure.**

| Evaluation Dimension | Metric | Measurement Method | Weight (%) |
|---|---|---|---|
| **Confidentiality** | Encryption strength, access control depth | Cryptographic audit, IAM policy review | 20 |
| **Integrity** | Tamper detection rate, audit completeness | Log analysis, checksum validation | 15 |
| **Availability** | Uptime %, failover latency | Load testing, chaos engineering | 15 |
| **Performance Overhead** | Latency increase, CPU/memory usage | Benchmarking, APM tools | 15 |
| **Scalability** | Policy propagation time, multi-region sync | Stress testing, orchestration logs | 10 |
| **Compliance Alignment** | Regulatory coverage, audit readiness | Framework mapping, compliance scans | 10 |
| **Incident Response** | MTTD, MTTR, automation level | SOC simulation, IR playbook testing | 10 |

| | | | |
|---|---|---|---|
| **Operational Complexity** | Implementation hours, skill requirements | IT team surveys, deployment logs | 5 |

### *4.5. Ethical and Validation Considerations*

All simulated attacks were performed in isolated environments with special authorization. Privacy was ensured through data anonymization and the creation of synthetic datasets. A systematic review was also conducted by three independent cloud security researchers to minimize bias.

## 5. Evaluation of Hybrid Cloud Security Techniques

This section provides a comprehensive assessment of modern hybrid cloud computing security strategies, which were analyzed at some point in the installation evaluation criteria. Each approach is examined in terms of technical effectiveness, operational feasibility, and applicability within commercial organizations.

### *5.1. Zero Trust Architecture (ZTA)*

ZTA substitutes for explicit take delivery of that is true by means of non-stop verification. The main elements consist of identity aware proxies, micro segmentation, a dynamic risk engine, and continual threat rating. During our test bed, we determined ZTA decreased unauthorized access attempts by using seventy-four% when compared to traditional VLAN based mostly segmentation. We also found out that it took us over 320 hours to configure and continue to synch IAM on all devices.

The overall performance hit changed based totally upon the type of workload: Latency sensitive applications experienced an average of 8 – 12% overhead, whilst batch processing had virtually no affect. Compliant alignment was high (ninety percent) according to NIST 800 fifty-three insurance requirements; however, we still have increased operational complexity as a result of having to integrate legacy equipment.

### *5.2. Cloud Security Posture Management (CSPM)*

Continuous testing of cloud configuration against compliance benchmarks by CSPM system. Average number of misconfigured items found across three top CSPM solutions (Microsoft Defender for Cloud, Wiz, Prisma Cloud) was 142. Continuous automated remediation reduced average time it took to correct issues from seventy-two hours to four hours and twenty minutes.

Compliance (alignment to ISO 27017), as well as operational aspects were where CSPM performed best. Human intervention validated false excessive costs on an average basis at eighteen percent. Drift through integration with IaC pipeline dropped eighty-nine percent in ninety days.

### *5.3. Cloud Workload Protection Platforms (CWPP)*

CWPP provides run-time security to containers, Virtual Machines (VMs) and Serverless features. The above assessment evaluated File Integrity Monitoring, Run-Time Risk Detection and Network Insurance Enforcement. CWPP reduced subject breakout success rates by 81% while reducing malware execution by 76%. The average performance overhead was 6.3% for containers and 9.1% for Virtual Machines. CWPP provided high scalability with policy propagation being completed in under fifteen seconds over 500+ nodes. However, CWPP's use of agents in deploying increased operational complexity as it required a consistent baseline image.

### *5.4. Advanced Cryptographic Techniques*

Tokenization, homomorphic encryption, and layout-preserving encryption were compared to assess record security while retaining the data encrypted. FHE provided a completely confidential system but was associated with a large increase in computational overhead (35 – 48X). Tokenization limited the amount of overhead to 12 percent but also had a major impact on the software refactor. Private Computing using TEE achieved 89 percent protection of data during processing with an average decrease in performance of 14 percent. The attestation process added a delay of 100 – 350 ms for verification. Key management integration with AWS KMS and Azure Key Vault significantly reduced administrative overhead by as much as 67 percent.

**Table 3 compares cryptographic techniques across key metrics.**

| Technique | Confidentiality | Performance Overhead | Implementation Complexity | Compliance Support | Use Case Suitability |
|---|---|---|---|---|---|
| **AES-256 (At Rest/Transit)** | High | 3–5% | Low | High | General data storage |
| **Format-Preserving Enc.** | Medium-High | 8–12% | Medium | Medium | Database fields, PII masking |
| **Tokenization** | High | 10–14% | High | High | Payment processing, PCI-DSS |
| **Homomorphic Encryption** | Very High | 35–48% | Very High | Medium | Secure analytics, ML training |
| **TEE/Confidential Comp.** | Very High | 12–16% | High | High | Multi-tenant processing |

### *5.5. AI-Driven Security Operations (SecOps)*

AI-enhanced SIEM and SOAR systems have been used to test the ability of both threat detection and response automation. Hybrid Cloud Telemetry based machine learning models had a true positive rate of 94.2%, as well as an average false positive rate of 5.8%. As automated "playbooks" were introduced, the Mean Time To Response (MTTR) was significantly decreased by 66.7% or 3.3 hours (from 4.5 hours to 1.2 hours). The time it took to train new model drifts that occur approximately every quarter consumed between 40-60 hours of Data Science Resources. The primary issue with explainability is still a problem for regulatory audits although some advancements in using SHAP and LIME have increased transparency. AI driven Sec Ops scored best in Incident Response (88/100), Compliance Alignment (91/100)

### *5.6. Integrated Security Framework Evaluation*

No one approach is effective by itself. Our evaluation in this research shows a combination of all four of these (ZTA; CSPM/CWPP; Cryptographic Controls and AI-based SecOps) produce the best results. A composite security score of 87.4 / 100 was found with an Integrated Deployment as opposed to a baseline configuration which produced a score of 52.1.

**Table 4: displays the results of our evaluation of the Integrated Framework.**

| Framework Component | Confidentiality | Integrity | Availability | Perf. Overhead | Scalability | Compliance | IR Efficiency | Complexity | Composite Score |
|---|---|---|---|---|---|---|---|---|---|
| Baseline (Perimeter + Manual) | 48 | 51 | 62 | 5% | 55 | 42 | 38 | High | 52.1 |
| ZTA + IAM Federation | 78 | 72 | 74 | 10% | 68 | 81 | 65 | High | 71.4 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| CSPM + CWPP | 74 | 81 | 79 | 8% | 85 | 92 | 72 | Medium | 79.8 |
| Cryptographic + TEEs | 91 | 85 | 71 | 15% | 62 | 84 | 58 | High | 76.2 |
| AI-Driven SecOps | 68 | 76 | 83 | 6% | 88 | 91 | 88 | Medium | 78.5 |
| Integrated Framework | **89** | **87** | **85** | **14%** | **91** | **94** | **92** | **High** | **87.4** |

## 6. Results and Discussion

### *6.1. Comparative Performance Analysis*

1. The assessments show that there are some very distinct performance levels when it comes to how well you perform a technique of protection. All integrated models performed better than stand-alone model's on all measurements of performance. ZTA was able to provide the best access control, but it is an expensive solution to begin with. Both CSPM and CWPP were able to produce a quick Return On Investment through automated computer-based misconfigurations corrections at runtime.

2. Cryptography has shown great success in protecting confidential data, but has also resulted in large amounts of unnecessary computation time. Private computing using TEE technology shows the greatest security for sensitive data, especially where multiple tenants are involved in accessing the same data, such as cross border data processing. SecOps using AI technology provides great ability in responding to incidents, but requires a mature data governance structure and constant version validation.

3. Statistical analysis (ANOVA, $p < .01$) indicated that there were significant differences in performance between baseline and integrated models regarding confidentiality ($F = 42.7$), integrity ($F = 38.1$), and compliance ($F = 51.3$). There were not statistically significant differences in performance overhead ($p = .12$) if the solutions are optimized; this indicates that modern security solutions can be used without causing unacceptable delay.

### *6.2. Threat Mitigation Efficacy*

Simulated Danger Modeling Identified Wonderful Mitigation Strategies for Each of the Following Attack Types:

1. Credential Stuffing & Brute Force Attack: Success rates were decreased by 94% with use of ZTA + MFA.

2. Container Escape (Evasion): The CWPP Runtime Protection Mechanism Blocked 87% of attempts to escape from containers.

3. Data Exfiltration: DLP, Encryption, Egress Filtering Averted 91% of Unauthorized Transfers

4. Ransomware Deployment: Immune Backups + CWPP + AI Detection Reduced Impact Scope by 78%.

5. Insider Threats: Use of Least Privilege IAM + Behavioral Analytics Reduced Unauthorized Access Attempts Through 82%.

**Table 5 summarizes threat mitigation efficacy.**

| Threat Type | Baseline Mitigation | ZTA Efficacy | CSPM/CWPP Efficacy | Integrated Framework Efficacy |
|---|---|---|---|---|
| Credential Compromise | 32% | 94% | 61% | 96% |
| Misconfiguration Exploit | 18% | 45% | 89% | 93% |
| Container/VM Escape | 21% | 38% | 87% | 91% |
| Data Exfiltration | 25% | 67% | 74% | 91% |
| Ransomware Deployment | 15% | 42% | 79% | 88% |
| Insider Threat Activity | 28% | 71% | 58% | 82% |

### *6.3. Compliance and Governance Outcomes*

Automated compliance mapping has greatly helped reduce audit practice time from 450 hours to 65 hours as part of the overall Framework. The company is at 96% for GDPR alignment; we have completed 94% of our NIS2 compliance work; and we have a 98% passing rate on our ISO/IEC 27017 insurance. We are now achieving non-stop compliance versus validating at the point in time (factor-in-time). We have also automated regulatory reporting and it has resulted in an 82% reduction in attempts to find correct guidance and an improvement in accuracy by 91%. Although automating cross-border statistics will be a challenge that requires the ability to dynamically enforce residency requirements, as well as aligning with criminal frameworks.

### *6.4. Operational and Economic Implications*

Analysis by the total cost of ownership (TCO) for the protection framework has shown a better initial investment in terms of dollars for an average of thirty-five percent to forty percent; however, it is expected that they will save companies an estimated sixty-eight percent to seventy-five percent of their breach-related costs over the course of the next three years. In addition to saving money, organizations have seen operational efficiencies due to the automated processes involved with the remediation process, reduced frequency of audit guides, and faster incident responses. The skills required to operate these systems are now focused on the engineering of networks rather than protecting clouds; engineering automation; and managing artificial intelligence models. The training provided for each protection engineer included an average of 120 hours per year; however, the engineers were able to use the same certification program as a means of providing standardization for skill development.

## 7. Practical Implications for Digital Enterprises

### *7.1. Strategic Implementation Roadmap*

\Businesses have to employ a step-by-step strategy in deploying Hybrid Cloud Security:

Step 1: Assessment & Baseline (months 1 – 2):

1. Inventory applications, data categories, and compliance requirements.
2. Implement CSPM for both configuration insight as well as risk rating of configurations.
3. Implement centralized logging and telemetry.

Step 2: Access & Identity Hardening (months 3 – 4):

1. Implement ZTA standards utilizing identity aware proxies.

2. Enforce multi-factor authentication (MFA), least privilege IAM policies, and just-in-time access.

3. Implement micro segmentation on critical applications.

Step 3: Runtime & Cryptographic Protection (months 5 – 6):

1. Integrate CWPP to protect containers/ VM's.

2. Implement TEEs or FHE for high sensitivity application processing.

3. Automate key rotation and integrate HSM.

Step 4: AI-Driven Operations & Continuous Compliance (months 7 – 12):

1. Deploy AI-enhanced SIEM / SOAR systems that can automatically execute playbooks.

2. Implement code-based coverage and compliance automation.

3. Develop continuous risk modeling and red team exercises.

### *7.2. Organizational and Cultural Shifts*

Transformation to security requires an organizational and cultural shift as well as the implementation of new technologies. Therefore, enterprises will need to:

1. Establish practical cloud security centers of excellence (CoEs).

2. Merge safety into their devops pipeline (devsecops).

3. Promote a culture of safety across all departments in development, operation and enterprise wide.

4. Support with metrics driven safety governance (KPIs, KRIs, OKRs).

5.

### *7.3. Vendor Selection and Interoperability*

Transforming to security also requires the ability to select vendors and operate across multiple vendor environments. Therefore, enterprises will need to focus on selecting products that support:

**1.** Cnfc safety standards

**2.** The use of Open Policy Agent (OPA)

**3.** Intercloud identity federation using scim or oidc

**4.** Automated compliance mapping

**Table 6. The criteria of vendor evaluation**.

| Selection Criteria | Weight | Assessment Method | Minimum Threshold |
|---|---|---|---|
| **API Interoperability** | 20% | Integration testing, API docs review | 85% |
| **Compliance Coverage** | 20% | Framework mapping, audit reports | 90% |
| **Automation Capability** | 20% | Playbook testing, CI/CD integration | 80% |
| **Performance Impact** | 15% | Benchmarking, APM monitoring | <12% overhead |
| **Vendor Support & Roadmap** | 15% | SLA review, customer references | Tier 1 |
| **Total Cost of Ownership** | 10% | 3-year TCO projection | Within budget |

## 8. Limitations and Future Research Directions

### *A. Research Limitations*

Although the evaluation framework for a hybrid cloud that was evaluated in this research study offers an extensive framework for evaluating the hybrid cloud as

well as its respective security architecture; it has some limitations. The first limitation is that while the simulated hybrid cloud can evaluate many aspects of a hybrid cloud's ability to scale and integrate multiple systems and legacy systems into one large hybrid cloud; the simulated environment is limited from being able to simulate all the complexities and nuances of the real-world hybrid cloud deployment. A second limitation is that the performance of more sophisticated methods of cryptography such as Confidential Computing and Homomorphic Encryption are heavily reliant upon how much the computing platform has been optimized or accelerated using specialized hardware accelerators and specific configurations to the underlying infrastructure. A third limitation is that the overall effectiveness of AI-based Security Analytics can be influenced by the quality of the training data used to train the models, the ability of those models to generalize beyond what they have been trained on, and the amount of bias present in the results of detecting threats. Lastly, due to changing regulatory requirements and changing compliance regulations, which are continually evolving, it may also be necessary to periodically update the proposed evaluation model in order to ensure that it continues to meet these regulatory requirements.

### *B. Future Research Directions*

There are a number of avenues that could be pursued as part of furthering our current work. For instance, researchers can explore how to integrate post-quantum cryptography into hybrid cloud deployments in order to mitigate potential future risks associated with quantum computing. Researchers should also pursue developing standardized cross-cloud attestation protocols to validate the integrity of Trust execution Environments (TEEs) on multiple different cloud systems. As well, autonomous security orchestration solutions utilizing both Artificial Intelligence and Reinforcement Learning may provide an even better method for dynamically enforcing policies and adapting to new threats through autonomous means. Data Sovereignty and Compliance Automation by using AI may also allow for better decision making regarding real time placement of workloads and alignment to regulations across many distributed environments. Last but certainly not least; there will likely be continued interest in providing scalable supply chain security methods in the hybrid cloud model such as SBOMs (Software Bills of Material), provenance tracing and automated tracking of vulnerabilities.

## 9. Conclusion

Hybrid cloud is an architectural model used by most organizations today due to the scalable resources and flexible operations it provides. However, one of the largest challenges facing hybrid cloud is cyber threats such as data breaches due to identity management issues, cross-cloud interoperability, regulatory compliance, data governance and distributed threat exposure. Conventional perimeter-based security models are not able to be effective due to these challenges; therefore, the need for integrated and adaptive security frameworks have arisen.

In this paper we have completed an extensive review of advanced cybersecurity solutions developed to improve data security in hybrid clouds. Our proposed framework examined all aspects of zero trust architecture, cloud security posture management, cloud workload protection platforms, confidential computing, advanced encryption techniques, and artificial intelligence driven security operations utilizing both technical and operational metrics. These metrics included confidentiality, integrity, availability, scalability, compliance alignment, operational overhead, and efficiency of incident response.

Our results showed that integrated security architectures were significantly better at providing protection against threats compared to isolation. Specifically, our findings indicated that when ZTA was combined with automated CSPM/CWPP mechanisms and hardware-assisted trusted technology there were improved effectiveness in mitigating threats and improving incident responses with minimal additional operational overhead. Additionally, our research found several ongoing problems including cross-cloud identity federations, forensic tracing, automating compliance with regulations, and ensuring heterogeneous cloud interoperability.

## References

1. Dalal, Aryendra. "Leveraging Cloud Computing to Accelerate Digital Transformation Across Diverse Business Ecosystems." *Available at SSRN 5268112* (2025).
2. Zerbini, Filippo. "The cloud revolution in the ERP industry: business model transformation and organizational impacts." (2024).
3. Oladosu, Sunday Adeola, et al. "Advancing cloud networking security models: Conceptualizing a unified framework for hybrid cloud and on-premises

integrations." *Magna Scientia Advanced Research and Reviews* 2.1 (2021): 1-10.

4. Arul, Kishore. "Data Engineering Challenges in Multi-cloud Environments: Strategies for Efficient Big Data Integration and Analytics." *International Journal of Scientific Research and Management (IJSRM)* 10.06 (2022).
5. Taha, Mustafa Sabah, et al. "Information hiding: a tools for securing biometric information." *Technology Reports of Kansai University* 62.04 (2020): 1383-1394.
6. Ismael, Bahaa Muneer, et al. "Non-dominated sorting genetic algorithm for channel assignment in multiple radio interfaces with multiple channels." *AIP Conference Proceedings*. Vol. 3393. No. 1. AIP Publishing LLC, 2026.
7. Bitkuri, Varun, et al. "A Survey on Hybrid and Multi-Cloud Environments: Integration Strategies, Challenges, and Future Directions." *International Journal of Computer Technology and Electronics Communication* 4.1 (2021): 3219-3229.
8. Sideek, Shirin Muataz Mohammed, et al. "An Improved Anomaly-based Intrusion Detection System for IoT Applications using Machine Learning Methods." *Pertanika Journal of Science & Technology* 34.1 (2026).
9. Khokhar, Rashid Hussain, et al. "A survey on supply chain management: Exploring physical and cyber security challenges, threats, critical applications, and innovative technologies." *International Journal of Supply and Operations Management* 11.3 (2024): 250-283.
10. Singh, Umesh Kumar, and Abhishek Sharma. "Cloud computing security framework based on shared responsibility models: Cloud computing." *Cyber-Physical, IoT, and Autonomous Systems in Industry 4.0*. CRC Press, 2021. 39-55.
11. Arshad, Nayab. "A comprehensive review of emerging challenges in cloud computing security." *Journal of Engineering and Computational Intelligence Review* 2.1 (2024): 27-37.
12. Abiola, Olumide Bashiru, and M. O. Ijiga. "Implementing dynamic confidential computing for continuous cloud security posture monitoring to develop a zero trust-based threat mitigation model." *International Journal of Innovative Science and Research Technology (IJISRT) IJISRT25MAY587* (2025): 69-83.
13. Prithviraj, R., R. Saminathan, and R. Manishankar. "Securing Cloud Workloads: An In-Depth Study Of Cloud Workload Protection Platforms And Their Impact." *Architecture Image Studies* 6.4 (2025): 947-962.
14. Anasuri, Sunil. "Confidential Computing Using Trusted Execution Environments." *International Journal of AI, BigData, Computational and Management Studies* 4.2 (2023): 97-110.
15. Ali, Gauhar, Sajid Shah, and Mohammed ElAffendi. "Enhancing cybersecurity incident response: AI-driven optimization for strengthened advanced persistent threat detection." *Results in Engineering* 25 (2025): 104078.
16. Asraa, Safaa Ahmed, et al. "An Accurate Model for Text Document Classification Using Machine Learning Techniques." *Ingenierie des Systemes d'Information* 30.4 (2025): 913.
17. Ismael, Bahaa Muneer, et al. "Multi-Agent Reinforcement Learning for User-Router Assignment in Multi-Radio Multi-Channel Wireless Mesh Networks." *International Journal of Intelligent Engineering & Systems* 18.8 (2025).
18. Julakanti, Sivananda Reddy, Naga Satya Kiranmayee Sattiraju, and Rajeswari Julakanti. "Multi-cloud security: strategies for managing hybrid environments." *NeuroQuantology* 20.11 (2022): 10063-10074.
19. Obaid, Abbas Luaibi, Nabeel Mahdy Haddad, and Mustafa Sabah Taha. "DL-SCDDS: Accurate Skin Cancer Detection and Diagnosis Scheme Based on an Improved Convolutional Neural Networks Model." *International Human-Centered Technology Conference*. Cham: Springer Nature Switzerland, 2024.
20. Emmanni, Phani Sekhar. "Implementing a zero trust architecture in hybrid cloud environments." *International Journal of Computer Trends and Technology* 72.5 (2024): 33-39.
21. Shukla, P. R., and V. M. Patil. "A comprehensive review of frameworks for achieving interoperability in multi-cloud environments." *2023 Second International Conference on Informatics (ICI)*. IEEE, 2023.
22. Liu, Yizhong, et al. "Secure and scalable cross-domain data sharing in zero-trust cloud-edge-end environment based on sharding blockchain." *IEEE Transactions on Dependable and Secure Computing* 21.4 (2023): 2603-2618.

**23.** Su, Yang, et al. "FPGA-based hardware accelerator for leveled ring-LWE fully homomorphic encryption." *IEEE Access* 8 (2020): 168008-168025.

**24.** Zobaed, S. M., and Mohsen Amini Salehi. "Confidential Computing Across Edge-To-Cloud for Machine Learning: A Survey Study." *Software: Practice and Experience* 55.5 (2025): 896-924.

**25.** Manne, Tirumala Ashish Kumar. "Enhancing Hybrid Cloud Security: Strategies for Managing Threats and Vulnerabilities." *Journal of Scientific and Engineering Research* 7.9 (2020): 258-265.

**26.** Irion, Kristina. "Government cloud computing and national data sovereignty." *Policy & Internet* 4.3-4 (2012): 40-71.