CLOUD-NATIVE SECURITY POSTURE MANAGEMENT IN AWS AND AZURE: AUDIT-DRIVEN APPROACHES TO RISK AND COMPLIANCE

Pavan Paidy [1], Krishna Chaganti [2]

[1] AppSec Lead At FINRA, USA
[2] Associate Director at S & P Global, USA

ABSTRACT

Strong security becomes very necessary in the fast-paced digital environment of today as businesses are switching to multi-cloud architectures for improved scalability and agility. Ensuring visibility, control, and compliance in dynamic environments such as AWS and Azure now primarily depends on Cloud-native Security Posture Management (CSPM). These systems provide freedom but also major risks: improperly set-up storage, too authorized identities, and unattended services can be readily overlooked. Constant monitoring offered by CSPM helps to find vulnerabilities before they become more critical by means of deviations from security baselines. This approach depends on audits, which enable teams to match present status of affairs with internal compliance requirements. Consistent audit trails assist quick issue resolution and informed decision-making by giving both responsibility and knowledge of system behavior. Along with this security is continuous compliance monitoring, carefully checking systems and instantly spotting changes. Beyond detection, good Cloud Security Posture Management (CSPM) interacts with DevOps pipelines to rapidly address problems and combines automated, prioritized risk mitigating technologies, therefore enhancing security protections early in the development process Cloud Security Posture Management (CSPM) products help to organize the anarchy and match security operations with corporate goals, so preserving the speed of innovation as safeguarding cloud environments gets more complicated becomes more difficult. Not only advised, but companies running both AWS and Azure systems absolutely have to put an audit-driven, policy-enforced Cloud Security Posture Management (CSPM) plan into action.

KEYWORDS

Cloud-Native Security, CSPM, AWS Security, Azure Compliance, Risk Assessment, Continuous Auditing, Multi-Cloud Strategy, Compliance Automation, DevSecOps, Security Monitoring, Cloud Compliance, Configuration Management, Policy Enforcement, Identity and Access Management, Cloud Risk Mitigation, Security Posture, Automated Remediation, Cloud Governance, Vulnerability Detection, Real-Time Monitoring, Security Best Practices, Regulatory Compliance, Cloud Workloads, Hybrid Cloud, Infrastructure as Code, Cloud Visibility, Security Baseline, Audit Trails, Misconfiguration Detection, Security Frameworks, Azure Governance, AWS Controls, Threat Detection, Compliance Reporting, Continuous Compliance, Risk Prioritization, DevOps Integration, Cloud Controls, Data Protection, Compliance Frameworks, Cloud Audit Tools, Security Automation, Azure Security Centre, AWS Security Hub, Cloud Security Tools, SOC 2 Compliance, HIPAA Cloud Security, NIST Compliance, CIS Benchmarks, Security Policy Enforcement.

David C. Wyld et al. (Eds): InWeS, NSEC, VLSIA, NLAIM, CSIP – 2025
pp. 61-71, 2025. CS & IT - CSCP 2025 DOI: 10.5121/csit.2025.151106

1. INTRODUCTION

Companies are quickly using multi-cloud solutions as digital transformation progressively changes the corporate environment to boost scalability, cut expenses, and improve performance. Leading the industry with their complete infrastructure capabilities and wide range of products are Microsoft Azure and Amazon Web Services (AWS). This shift to cloud-native architecture not only catches a significant change in the threat environment but also reflects Originally useful in fixed on-site environments, conventional perimeter-based security solutions are insufficient to control the dynamic and scattered components of cloud ecosystems. These days, proactive risk assessment, automated compliance enforcement throughout numerous cloud environments, and continuous visibility all depend on Cloud-native Security Posture Management (CSPM).

1.1. Challenges

Security administered in multi-cloud systems such as AWS and Azure presents various issues than in conventional systems. The fundamental problem is the complexity coming from the broad breadth and depth of offerings given by every provider Different security configurations, IAM models, data services, and compliance systems define every cloud platform, so coordinated management is rather challenging. Often leading to misconfiguration, this complexity is usually the main cause of cloud breaches. Usually arising from poor visibility and human error, various defects including too permissive IAM roles and exposed storage buckets reflect not from evil intent but from lack of knowledge.

Lack of real-time view is one of main concerns. Without centralized monitoring, security teams face blind spots that compromise their ability to uncover anomalies, evaluate posture, or react fast. Furthermore, manual compliance procedures cannot equal the rapid growth of cloud innovation. Conventional audits provide quick assessments free of regard for the ephemeral character of cloud computing. As settings increase, the demand for scalable and automated compliance solutions shifts from a wish to a need. Constant compliance and risk management needs to be introduced into this dynamic ecosystem right from the start.

1.2. Problem Statement

The basic problem is that conventional security instruments and methods are not sufficient to solve problems starting from clouds. Designed for stationary infrastructure, these essentially reactive techniques lack the agility required to guard very dynamic cloud assets. For containerized or serverless settings whereby assets may only endure minutes or even seconds, agent-based endpoint protection or network-based firewalls, for example, have limited efficacy.
The variations in compliance standards and enforcement strategies among cloud providers complicate the situation even more. AWS and Azure offer security solutions even if their setups, rules, and automation tools vary substantially. This disparity makes keeping a consistent security posture more challenging, especially in teams managing various dashboards, policy languages, and control sets.

Virtual machines, containers, databases, APIs—cloud resources—are naturally transient, typically instantiated and deleted automatically. Static audits become worthless in this process Weekly or monthly security checks are inadequate A posture management solution is required that suits the ephemeral, real-time character of cloud infrastructure so ensuring that compliance and risk awareness flow as naturally as the surrounds.

1.3. Motivation

In the cloud age, more intelligent and adaptable security solutions are badly needed and under growing demand. Usually, inadequate security posture management and careless misconfiguration explain rising rates of cloud breaches. Publically exposed data repositories, unpatched systems, and overly high permissions have received attention frequently, pointing rather than isolated posture problems.

Regulatory requirements are also speeding up. Frameworks as GDPR, HIPAA, SOC 2, PCI DSS reject point-in- time audits. Increasingly needed are real-time auditability, proactive incident response solutions, and verifiable standard compliance across all infrastructure layers. Businesses ensuring their environments are continuously checked upon and that security regulations are carefully implemented now carry more weight of proof.

Businesses aiming at these targets must adopt automated security intelligence with a platform approach. Working directly with cloud APIs, CSPM systems offer scalable, policy-driven security systems using native controls. These systems embed posture assessments into CI/CD pipelines, thereby integrating security measures early in the process, and help DevSecOps teams handle problems before they impact production. By means of CSPM, businesses can lower human error, improve visibility, and follow legal needs as well as business agility. One can establish robust cloud security by appreciating the ideas of the future and realizing the flaws of the past.

2. LITERATURE REVIEW

In the industrial as well as academic spheres, Cloud-Native Security Posture Management (CSPM) technologies have drawn a lot of interest. These products are meant to automatically find and fix risks in cloud systems by means of continuous configuration review, tracking for compliance violations, and provision of actionable security posture data. Professionals as well as researchers must understand the capabilities, constraints, and evolving trends in Cloud Security Posture Management (CSPM) since enterprises increasingly depend on multi-cloud architectures—particularly with AWS and Azure.

A) Evaluation of Contemporary CSPM Tools and Systems

Modern CSPM solutions have evolved into sophisticated, API-driven systems able of seamless interaction with the original products of cloud providers. Among significant commercial solutions are Trend Micro Cloud One, Lacework, Check Point CloudGuard, and Prisma Cloud from Palo Alto Networks. Features in misconfiguration detection, identity and access evaluation, workload security, and policy enforcement abound among these technologies. Targeting audits and automation capabilities for cloud settings, Prowler and Cloud Custodian open-source solutions help to democratize posture management.

These all-around solutions support DevSecOps workflow integration, notification, and compliance mapping. Their fundamental ability is in the real-time or near-real-time assessment of cloud setups against established security and compliance criteria. Since Cloud Security Posture Management (CSPM) solutions are scalable and usually offer multi-cloud compatibility, companies employing different platforms find them interesting. Usually the degree of integration and detail of discoveries depends on how closely the tool interacts with the native APIs of any cloud service provider.

B) Natural security elements of Azure and AWS

AWS and Azure have built strong native CSPM-like capabilities to help security operations on their platforms run more effectively. AWS Security Hub aggregates Guard Duty, Inspector, and Macie data from AWS services onto a single dashboard to increase visibility. It also allows policy-driven repair using AWS Lambda via automated response systems An essential tool, AWS Config enables businesses to enforce compliance guidelines and continuously monitor configural changes.

Conversely, Microsoft Azure Defender now included within Microsoft Defender for Cloud offers threat prevention for Azure and hybrid settings. It provides SIEM capabilities compatible with Microsoft Sentinel together with security rating and suggestions. Azure highlights its Security Benchmark and Azure Policy, which allow businesses to evaluate and implement governance generally.

Comparative studies reveal that whereas Azure Defender displays improved unified security management inside Microsoft's large ecosystem, AWS Security Hub provides wide integrations and service maturity since AWS's earlier efforts in CSPM enable this. Companies running both environments have to make use of outside Cloud Security Posture Management (CSPM) solutions since both systems fail to offer full multi-cloud visibility.

Compliance Guidelines and CSPM Coordination Security compliance still greatly affects the choice of CSPM Prominent systems of control and best-practice consist in: CIS Benchmarks released by Center for Internet Security: Usually applied as basic policy models, these offer complete setup instructions for cloud services. They are frequently used by CSPMs.

- Regarding constant monitoring and correction, NIST's risk management strategy fits Cloud Security Posture Management.
- Globally approved for information security management, ISO/IEC 27001 is frequently utilized as a compliance goal for corporate Cloud Security Posture Management processes.
- HIPAA, PCI DSS, and GDPR—industry-specific compliance requirements—call for cloud-native controls, data encryption, and increasingly frequent audits.

CSPM systems enable businesses to satisfy these standards by automatically matching configurations with controls, generating audit-ready data, and routinely identifying noncompliance. Advanced platforms either directly into cloud environments or via pull requests in infrastructure-as- code (IaC) pipelines, therefore providing remediation-as- code.

C) Shortcomings in Academic and Current Industrial Solutions

- Notwithstanding their promise, both scholarly publications and commercial solutions highlight many continuous shortcomings in the present CSPM system.
- **Integration Failure:** Many CSPM systems find it difficult to completely interface with unique resources or tailored DevOps tools Security assessments neglecting Infrastructure as Code (IaC) pipelines, container orchestration (such as Kubernetes), or Continuous Integration/Continuous Deployment (CI/CD) triggers produce inadequate coverage.
- On many systems, real-time repair is still unattainable even with evolving detection capabilities. Although most CSPM systems notify users of misconfigurations, they must

be fixed using hand involvement or scripting. This delay could cause tremendous risk for companies.

Consumption and Productivity Trade-offs: Enterprise CSPM systems could be too costly for smaller companies specifically. Academic prototypes sometimes indicate limited scalability while open-source solutions typically demand substantial tweaking. Not always implemented consistently are full CSPM solutions; cost and complexity can present difficulties.

Lack of context-sensitive risk ranking is one major drawback of contextual risk assessment. Usually produced in great numbers, warnings hamper security teams' ability to triage and react properly Absence of an IAM policy on a test server could award the same severity score as one on a production database, therefore generating alert fatigue and possibly overlooking.
Multi-cloud CSPM systems notwithstanding their deployment still reveal a gap in uniform compliance enforcement across cloud platforms. Every provider utilizes a different security language, which influences the defining and measuring of controls. Still a technological difficulty for which CSPM providers are only starting to handle is cross-cloud correlation.

3. PROPOSED METHODOLOGY

Designed especially for seamless integration with AWS and Azure ecosystems, this strategy offers a Cloud-Native Security Posture Management (CSPM) architecture to manage the security and compliance concerns inherent in modern multi-cloud deployments. Operating at scale, providing real-time security posture data, and enabling proactive risk correction, the architecture first priority is audit-driven, automated, policy-enforced, architecture.

AWS CSPM System Blueprint for Integration Azure Architectural Notes
The architecture is based on a modular, cloud-native design closely related with AWS and Azure capabilities. The system comprises in the following fundamental parts:

- **Cloud Connectors**: Designed as API-driven modules linking with AWS and Azure services, Cloud Connectors include AWS Security Hub, Azure Security Centre, AWS Config, Azure Resource Graph. These modules are set for continuous consumption of configuration, identification, and workload statistics.

- **Policy Engine**A single policy interpreter enables policy-as-code be implemented using open standards like OPA (Open Policy Agent) or proprietary formats fit for cloud-native apps. Policies lay out allowed layouts, security policies, and compliance checks.

- **Compliance Mapping Layer** This module connects controls from frameworks including CIS Benchmarks, NIST 800-53, ISO/IEC 27001, and customized company rules with cloud configurations.

- **Risk Scoring and Prioritization Module** Combining machine learning techniques with rules-based logic, hierarchization and risk evaluation module distributes dynamic risk ratings based on asset relevance, effect, and exposure.

- **Automation and Remediation Engine**Using cloud-native capabilities—e.g., AWS Lambda, Azure Functions— Infrastructure-as- Code (IaC) pull requests, or ticket generation in ITSM systems—automation and remedial engine supports automatic corrective action.

- **Unified Dashboard**:Consolidating risk and compliance statuses across cloud platforms, unified dashboards—a centralized interface—offer visualization, drill-down capability, and reporting for many levels of stakeholders.

Audit-Driven Security Model

Basically based on an audit-driven one, the strategy helps businesses to ensure continuous compliance by spotting and fixing configuration drift.

Differentiation in Compliance: Instant Alert System

Constant real-time monitoring of designated security baselines enables the system to detect changes. Resources are quickly assessed in line with security policies either in update or development. For instance, the difference is obvious right away when an Azure storage account lacks encryption or S3 bucket enabled for public access on AWS. Real-time alarms are enabled by membership to cloud event streams including AWS CloudTrail, AWS Config Rules, Azure Activity Logs, and Azure Policy Events.

Policy as recommended. Systems of Code Enforcement:

Policy-as- code makes it practical in part reusable, tested, version-controlled security guidelines. CI/CD integration comes first before their implementation and then via continuous monitoring follows these rules. Tools included in the layer of enforcement include tailored JSON/YAML policy templates connected with Terraform Sentinel, AWS Config Rules, and Azure Policy as OPA Gatekeeper for Kubernetes. This allows constant security oversight apart from the selected delivery approach.

Automation Workflow

Automaton helps to establish security while preserving agility. This structure takes use of automation at several points of contact:

- **Continuous Surveillance of Security Integrating CI/CD:**

  Included within the CI/CD process, security checks operate as guardrails rather than barriers. A Terraform plan is looked at for security misconfigurations—that is, exposed security groups, unencrypted volumes—before usage. The pipeline could fail the build depending on degree of severity or generate a ticket for hand review.

  Pre-commit hooks and Gitops tools look over codes during development and verify that only policy-compliant infrastructure is used, therefore improving this process. Complementing GitHub Actions, GitLab CI, or Azure DevOps Pipelines are tools Checkov, TFSec, and Bridge crew.

- **Infrastructure-as-Code (IaC) Scanning**:

  Early misconfiguration diagnostics are driven by Infrastructure-as- Code (IaC) scanning Using tools assessing Terraform, Cloud Formation, ARM templates, and Kubernetes YAML files, the CSPM system discovers vulnerabilities before to production release. Source code repositories let one rapidly integrate these ready-to-fix contextual solutions.

- **Automated Remediation**:

  Once a policy breach surfaces during execution, the automatic remedial engine can respond utilizing pre-approved playbooks. It might demand encryption-at-rest, separate off public access from a bucket, or rotate compromised credentials Starting these initiatives could call for outside orchestration technologies like PagerDuty or ServiceNow or cloud-native services like AWS Systems Manager Automation.

Risk Prioritization Strategy

Given the projected signal flooding for a security team, priority is really critical. This methodology uses a context-sensitive, machine learning-enhanced method to assign problems top attention.

Leveraging Native Services for Context:

The system taps into **AWS Config** and **Azure Policy Insights** to understand the full context of violations. Metadata such as region, service type, associated identity, and resource tags are used to infer the operational criticality of an asset.

Machine-Learning-Based Prioritization:

To further refine alerting, machine learning models are trained on historical remediation data, asset behavior, and attack surface exposure. For example, the system may learn that publicly accessible resources with write permissions are typically remediated faster, and thus elevate similar alerts in future incidents. ML also aids in suppressing false positives by correlating with threat intelligence feeds and log telemetry.

Risk Buckets and SLA-Driven Triage:

Alerts are grouped into buckets (e.g., critical, high, medium, low) based on impact and exploitability. These buckets are tied to SLAs—critical alerts may require remediation within 24 hours, while low-priority items may be deferred or automated.

Unified Dashboard for Cross-Cloud Visibility

To unify insights from disparate cloud environments, the methodology includes a **cross-cloud dashboard** accessible via web interface or API. This dashboard includes:

- **Compliance Overview**: Scorecards for CIS, NIST, and custom benchmarks across both AWS and Azure.
- **Drift Detection Feed**: Real-time stream of configuration changes and their impact.
- **Risk Heatmaps**: Visual indicators of hotspots across accounts, regions, and services.
- **Remediation Tracker**: Status of manual and automated remediation actions.
- **Audit Reports**: Exportable artifacts for SOC 2, HIPAA, and ISO compliance.

This dashboard supports role-based access control (RBAC), allowing different teams—security, operations, auditors, and executives—to access relevant views.

4. RESULTS AND DISCUSSION

The suggested Cloud-Native Security Posture Management (CSPM) approach is practically implemented and evaluated in this part inside a simulated hybrid cloud environment including AWS and AZURE. Maintaining cross-platform visibility, the goal was to confirm architectural defects, guarantee compliance, and let the architecture to automatically fix misconfigurations. Benchmark testing helped to assess system performance; findings were linked with existing systems to highlight areas of business value, strength, and weakness.

Implementation Details

Hybrid Environment Setup

A controlled lab environment was set up to simulate enterprise-level infrastructure deployed across both **AWS and Azure**. This environment included a mix of services such as:

- **AWS**: EC2 instances, S3 buckets, IAM roles, RDS databases, CloudTrail logs, and AWS Config.
- **Azure**: Virtual Machines, Blob Storage, Azure Active Directory, Azure SQL, Defender for Cloud, and Azure Policy.

The environment was intentionally seeded with known misconfigurations such as:

- Publicly accessible storage (S3 and Blob)
- Unencrypted data volumes
- Overly permissive IAM roles
- Disabled logging for critical service.

Toolchain Integration

The CSPM system was composed of both **native services** and **third-party tools**:

- **Open Policy Agent (OPA)**: Used for policy-as-code enforcement in Kubernetes and CI/CD pipelines.
- **Cloud Custodian**: Deployed to scan cloud resources, enforce policies, and automate remediation
- **Terraform**: Used to provision and manage infrastructure in both AWS and Azure.
- **Checkov**: Integrated into GitHub Actions for IaC scanning.
- **AWS Config and Azure Policy**: Used for real-time drift detection and remediation evaluation.
- **Prometheus + Grafana**: Monitored alerting metrics and compliance scores.
- **Unified Dashboard**: Built using a Python-based Flask backend with React frontend for visualization.

Benchmarking Metrics

Three core metrics were selected to evaluate the CSPM system:

1. **Time to Detect Misconfigurations**

- Pre-implementation baseline: Average detection time was **6 hours**, often dependent on scheduled audits or manual inspection.
- Post-implementation: With real-time cloud event ingestion, the average detection time dropped to **<3 minutes**.
- Most critical violations (e.g., public storage buckets or exposed SSH) were flagged in under **60 seconds** after deployment or change.

2. Compliance Adherence Improvement

Compliance was measured against CIS Benchmarks and custom enterprise controls across five resource types: compute, storage, networking, IAM, and logging.

- Baseline adherence (before CSPM): **67%**
- Post-implementation adherence: **92%**
- Most significant gains were seen in IAM policy enforcement and storage encryption, largely due to policy-as-code and auto-remediation workflows.

3. Remediation Speed and SLA Compliance

- Manual remediation took **24–72 hours**, depending on severity.
- Automated remediation actions (via Lambda and Azure Functions) reduced this to **under 10 minutes** for high-priority issues.
- SLA targets for high-severity issues (remediation within 24 hours) were met **98%** of the time after implementing automation.

Comparative Analysis

Effectiveness vs. Existing Solutions

The proposed CSPM model was benchmarked against existing native and third-party tools operating independently.

Feature/Metric	Native Tools Only	Third-Party Only	Proposed CSPM
Real-Time Detection	Moderate	High	Very High
Multi-Cloud Visibility	Low	Moderate	High
Auto-Remediation Coverage	Limited	Partial	Extensive
Policy-as-code support	Minimal	Moderate	Comprehensive
CI/CD Integration	weak	Strong	Seamless
Alert Triage Intelligence	None	Moderate	ML-Enhanced

The **proposed architecture outperformed existing configurations** due to its unified integration approach, combining native controls with customizable third-party extensions.

Capability	AWS	Azure
Real-Time Drift Detection	AWS Config + Lambda (Fast)	Azure Policy (Moderate)
Policy Flexibility	High (Custom Rules via Lambda)	Moderate (Preset Definitions)
Auto-Remediation Ease	High (Step Functions, Lambda)	Moderate (Logic Apps, Functions)
CI/CD Integration	Robust (Code Pipeline)	Good (Azure DevOps, GitHub)
Compliance Reporting	Integrated with Security Hub	Integrated with Defender for Cloud

Azure excelled in integrated security suggestions and centralized compliance views; AWS showed better in modularity and developer autonomy for instantaneous correction. Both systems benefited considerably by including outside solutions like OPA and Cloud Custodian.

Discussion

Trade-offs Between Native and Third-Party Tools

Although native solutions like Azure Defender and AWS Config offer necessary functionality, they are sometimes restricted by ecosystem constraints and lack of significant customizing. Third-party solutions provide policy-as-ide support, further flexibility, and multi-cloud compatibility while lacking complete integration without much tweaking. Simple, integrated compliance models, devoid of outside deployment responsibilities characterize native advantage. Improved extensibility, more total integrations, and non-standard configuration compatibility characterize third-party benefits. Trade-off: The complexity and cost of integration; third-party products usually need specific security engineering skills for correct operationalizing.

5. CONCLUSION & FUTURE SCOPE

Conclusion

Keeping the integrity and resilience of cloud systems largely depends on audit-driven Cloud Security Posture Management (CSPM), on platforms like AWS & Azure. By means of frequent monitoring of configuration deviations, security protocol implementation, & alignment of resource situation with compliance requirements, audit-driven Cloud Security Posture Management (CSPM) helps companies to maintain a strong cloud posture. These solutions enable proactive correction by providing useful knowledge about misconfigurations, permission deviations, and compliance problems.

Audit tracks & customisable documentation support responsible, exactly traceable, control of security. Reducing human errors and policy deviations dramatically lowers the attack surface and increases industry standards including CIS, NIST, and ISO conformance. Driven by audits, Cloud Security Posture Management in AWS and Azure actively lowers risk exposure and raises corporate security maturity.

Future Scope

Audit-driven Cloud Security Posture Management (CSPM) will define advancement towards platform-agnostic and AI-augmented security orchestration going forward. Gradually adopting multi-cloud strategies including Google Cloud Platform (GCP), Alibaba Cloud, and Oracle Cloud, companies more and more rely on CSPM capabilities outside of AWS and Azure. In many different settings, this change will provide uniform risk control and policy execution.

Moreover, incorporating artificial intelligence driven anomaly detection can help CSPM to perform even better. Machine learning systems provide fast identification of developing hazards and insider threats by learning to detect postural deviations from behavioural baselines.

Perfect integration between Security Information & Event Management (SIEM) and Security Orchestration, Automation, & Response (SOAR) systems with the Cloud Security Posture Management (CSPM) ecosystems defines a future way. This convergence will allow integration of cloud posture monitoring with the primary corporate security goals by means of automated incident response systems, prioritized alerting, & closed-loop remedial action.

REFERENCES

[1] Jimmy, F. N. U. "Cloud security posture management: tools and techniques." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.3 (2023).

[2] Leaua, M. S., Chiş, A., Bălan, T. C., & Ilca, L. F. (2024, September). Assesment of Cloud Security Posture Management Scenarios. In *2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet)* (pp. 1-6). IEEE.

[3] John, Johnathan. "EXPLORING TOOLS FOR EFFECTIVE CLOUD SECURITY POSTURE MANAGEMENT." (2023).

[4] Bolarinwa, Amos, John Posi, and Daniel Daniel. "Cloud Security Posture Management: Tools and Best Practices."

[5] Arif, Tuba, Byunghyun Jo, and Jong Hyuk Park. "A Comprehensive Survey of Privacy-Enhancing and Trust-Centric Cloud-Native Security Techniques Against Cyber Threats." *Sensors* 25.8 (2025): 2350.

[6] Talwar, Sanat. "Unified Framework for Securing Cloud-Native Storage: Approach for Detecting and Mitigating Multi-Cloud Bucket Misconfigurations."

[7] Sabir, Asim, and Ahtsham Shahid. *Effective Management of Hybrid Workloads in Public and Private Cloud Platforms*. MS thesis. uis, 2023.

[8] Gebregergis, Robel Michael, and Lothar Fritsch. *Supply chain risks from Cloud Security Posture Management*. MS thesis. Oslomet-storbyuniversitetet, 2023.

[9] Kodakandla, Naveen. "Securing Cloud-Native Infrastructure with Zero Trust Architecture." *Journal of Current Science and Research Review* 2.02 (2024): 18-28.

[10] Yadav, G. Sreenivasa, G. Karthick, and C. H. Mukundha. "ENHANCING CLOUD SECURITY POSTURE MANAGEMENT-A COMPREHENSIVE ANALYSIS AND EXPERIMENTAL VALIDATION OF CSPM STRATEGIES." *International Journal of Communication Networks and Information Security* 16.3 (2024): 237-253.

[11] Colotti, Manuel Enrique. *Enhancing Multi-cloud Security with Policy as Code and a Cloud Native Application Protection Platform*. Diss. Polytechnic di Torino, 2023.

[12] Odeh, Ammar, et al. "Navigating Cloud Computing Security: Strategies, Risks, and Best Practices." statistics 6: 8.