Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

Cloud Security Architecture: A Comprehensive Guide to Zero Trust, Governance, and Operational Resilience

Dr.A.Shaji George[1], Dr.T.Baskar[2], Dr.M.M.Karthikeyan[3]

[1]Independent Researcher, Chennai, Tamil Nadu, India.
[2]Professor, Department of Physics, Shree Sathyam College of Engineering and Technology, Sankari Taluk, Tamil Nadu, India.
[3]Assistant Professor, Department of Computer Science, Karpagam Academy of Higher Education, (Deemed to be University), Coimbatore, Tamilnadu, India.

Abstract - Cloud computing has changed the design, deployment, and management of technology infrastructure among the organizations in a fundamental manner. With the movement of core workloads to cloud environments based on both Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) and Software as a Service (SaaS) models, the formerly understood security perimeter has become permeable. Instead, it has a dynamic, identity-driven attack surface which requires radically different approach to security governance. This paper is a technically based, full-scale guide to cloud security practitioners, architects, and organization decision-makers. It looks into the entire range of cloud security fields, starting with the basic threat landscape analysis and shared responsibility model, then moving on to Cloud Access Security Brokers, Identity and Access Management, identity federation protocols, data encryption practices, Cloud Security Posture Management, continuous compliance monitoring, and cloud security auditing. The paper ends with the discussion of design of integrated security architecture, best practices in operations in the DevSecOps models, and new technologies such as Cloud-Native Application Protection Platforms, confidential computing, and AI-based threat detection. The main thesis is that most of the major cloud security breaches can be avoided by exercising a disciplined operation, structural integrity, and unrelenting automation. This source is intended to generate real knowledge, rather than product catalog.

Keywords: Cloud Security, Zero Trust Architecture, Identity and Access Management, Shared Responsibility Model, CSPM, CASB, Encryption, Compliance, DevSecOps, CNAPP.

1. INTRODUCTION

1.1 The Perimeter That No Longer Exists

It was the time when a robust wall was built in order to ensure the safe environment of a corporation technologically. The firewalls were placed at the network periphery. Information was stored in servers within the building. The systems were accessed by users on desks within the same physical boundary. There was some logical clarity to the security model, although it was never flawless. The "inside" was trusted. The outward was not. Cloud computing has rendered such a model obsolete. Organizations today are running workloads of production on Amazon, Microsoft, or Google owned infrastructure. They have their employees using sensitive applications at their home networks, coffee shops, and airports internationally. Their information goes through information hubs of various continents. Their software is packaged together

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

using third-party modules, open-source libraries, and managed services which completely hide the actual hardware. The boundary has not changed. It is no longer a consistent notion.

This is not necessarily a harmful change, but it requires a radically new strategy of security. In cloud environment, attack surface is determined by identity, configuration and access policy rather than geography or topology of network. The attackers that the cloud environments are targeted by are not mostly the sophisticated state-sponsored hackers that utilize the zero-day vulnerabilities. More frequently, they are opportunistic members, who scan using automated scanning tools, and seek poorly configured storage buckets, unsecured API keys, and service accounts that are over-permitted. Exotic attacks have not been the most devastating breaches of a cloud in the recent history. They have included simple breakdowns to operation that could have been avoided by good teams which are armed with appropriate tools and processes.

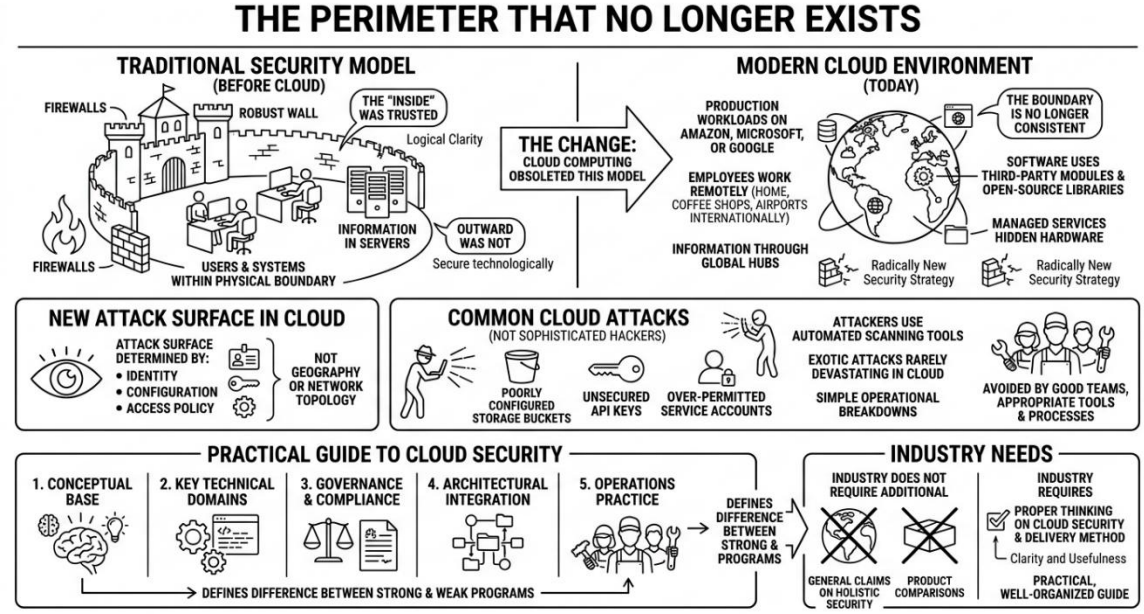

Fig -1: The Perimeter That No Longer Exists

This paper offers a well-organized, practical guide on the in-depth study of cloud security. It discusses the conceptual base, the key technical domains, the governance and compliance aspects, the architectural integration issue, and the operations practice that define the difference between the strong and the weak cloud security programs. There is a point of clarity and usefulness. The industry does not require additional product comparisons and general claims on holistic security. It requires proper thinking on what cloud security really entails and its delivery method.

2. OBJECTIVES

The main aims of this paper are the following. First, it will define a technical concept of the difference between cloud security and conventional on-premises security paradigms and why this difference is relevant to practice. Second, it attempts to clarify the shared responsibility model in finer details in the three key service models and where the provider roles finish and customer roles commence. Third, the article aims to offer an organised analysis of the fundamental disciplines of cloud security such as identity

management, data encryption, posture management and compliance monitoring in a manner that ties theory to operational reality. Fourth, it offers a combined architecture framework of how disparate security controls work better when intended to be employed together. Fifth, it determines the most significant emerging trends that transform cloud security such as artificial intelligence (AI)-based detection, confidential computing, and consolidation of cloud security tools into single platforms. Lastly, the paper provides practitioners and organizational leaders with practical advice that can be implemented at once to enhance cloud security programs at any maturity level.

3. THE THREAT LANDSCAPE

3.1 What Cloud Security Is Actually Defending Against

The threat landscape is the beginning of any security program. The threat landscape in cloud environments is highly defined that it has not significantly changed over the various years of reporting in the industry. The most common cause of cloud security attacks is misconfiguration. Misconfiguration has been continually listed in the Cloud Security Alliance, IBM Security, and various threat intelligence reports published by providers as the most common attack vector in IaaS, PaaS, and SaaS. The process is simple, cloud infrastructure can be provisioned via APIs and configuration files usually at high rate by teams that are being driven by delivery pressure. In case such configurations are not done correctly, then the resources that are supposed to be private are made public. Those services which are not supposed to be made available to everyone get in the hands of anyone on the internet. The Capital One breach of 2019 explains this point exactly. One of the attackers used a misconfigured Web Application Firewall in a AWS setup to attack it with a Server-Side Request Forgery attack to steal personal information of more than 100 million customers. It was not an advanced zero-day that would be the root cause of the vulnerability. It was a mistake in configuration.

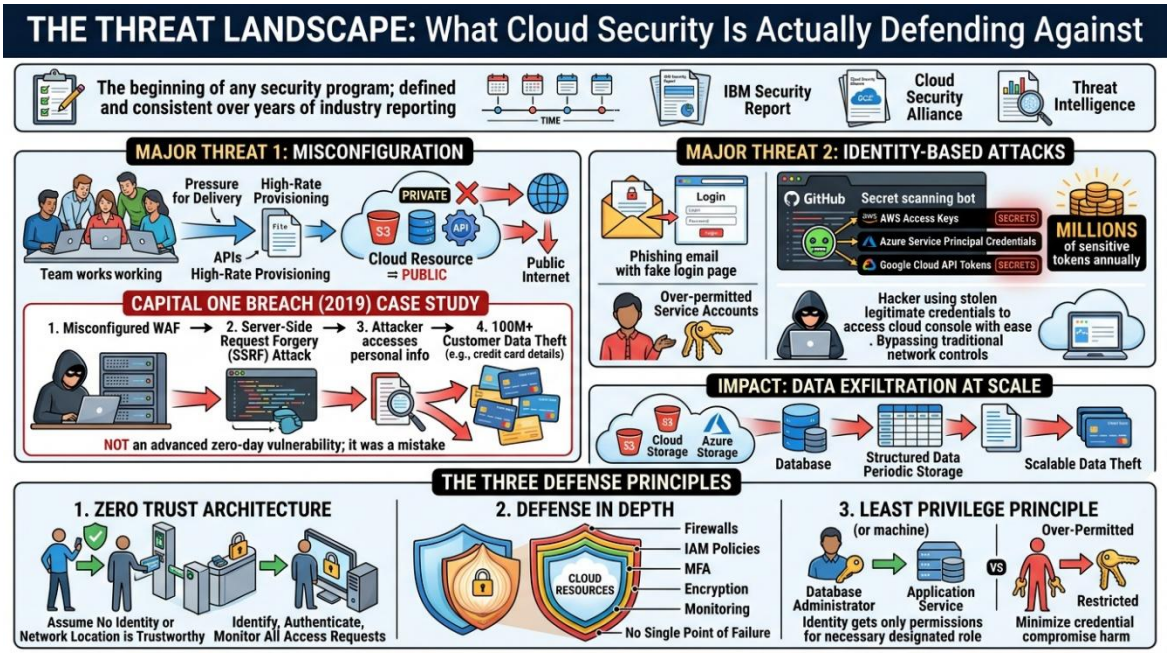

Fig -2: The Threat Landscape

The second type of dominating threat is Identity-based attacks. Hackers who gain legitimate cloud credentials are able to act within cloud environments with equivalent ability as the authorized users to whom those credentials are attributed. Phishing attacks on cloud users, secrets left in publicly accessible code repositories and over-permitted service accounts all are well documented attack vectors. The secret scanning service used by GitHub itself has been consistently identifying millions of sensitive tokens and credentials in public repositories every year, such as AWS access keys, Azure service principal credentials, and Google Cloud API tokens. After gaining access to a cloud environment and an authenticated user, an attacker will encounter minimal of the conventional barriers that a network-based security control would bring.

The impact of cloud security failures is data exfiltration at scale, which makes this security issue so expensive. Structured data is periodically stored in cloud storage systems and databases in volumes that would have been challenging to handle in-house. Failure of access controls means that cloud storage is fast and effective in data theft because of the same scalability. These threats are countered by the cloud security on three principles. Zero Trust Architecture does not consider any identity or network location as a trustworthy one. All access requests should be identified, authenticated and monitored irrespective of the source. In Defense in Depth, several overlapping controls are provided on both levels of the architecture, so that there will be a single point of failure that will not result in a total compromise. The Least Privilege principle provides that each identity, both human and machine, can only have the permissions necessary to accomplish its designated role, minimizing the harm that a credential compromise can cause.

4. THE SHARED RESPONSIBILITY MODEL

4.1 Understanding the Division of Obligation

There is no more significant concept in cloud security that is more misconceived than a shared responsibility model. All large cloud providers have it well defined. Amazon Web Services mentions that it takes care of the security of the physical data centers, hardware, the hypervisor and the global network infrastructure, the security of the cloud of. Security in the cloud is the responsibility of the customer, it includes operating systems, application code, data, and identity settings. Microsoft Azure and Google Cloud Platform have similar principles of operation, and slight variations in the description of the boundary of particular managed services.

This division varies dramatically with the three service models in terms of the practical meaning of the term. In IaaS designs, where the customer leases virtual computing, storage and networking capabilities, the customer is heavily burdened with security. The provider ensures that the physical structure and the hypervisor are safe. The customer is responsible for all the above the layer, the operating system, the runtime, the application, the network configuration, the access policy. Under PaaS, the provider controls the underlying OS and runtime and the customer is limited to application code, data and configuration. In SaaS settings, the vendor has control over virtually the whole technology stack. The key security levers to the customer are the access control policies, data classification and application configurations settings.

The possibility of misconception of this model is direct and quantifiable. Take the example of an organization that is moving a relational database to Amazon RDS. AWS manages the patching of database engines, hardware, and default encryption of the storage. The customer will still be in charge of setting up the security group to only allow authoritative sources to access the database, administer database user privileges, enable and inspect audit logs, implement suitable data classification policies, and encrypt and

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

control database backups. The organizations that believe that the cloud implies that it will be the provider to take care of security usually bypass these steps. The gaps that are created are not hypothetical. They are regularly found in reports of breaches and audit results in all industries and geographies.

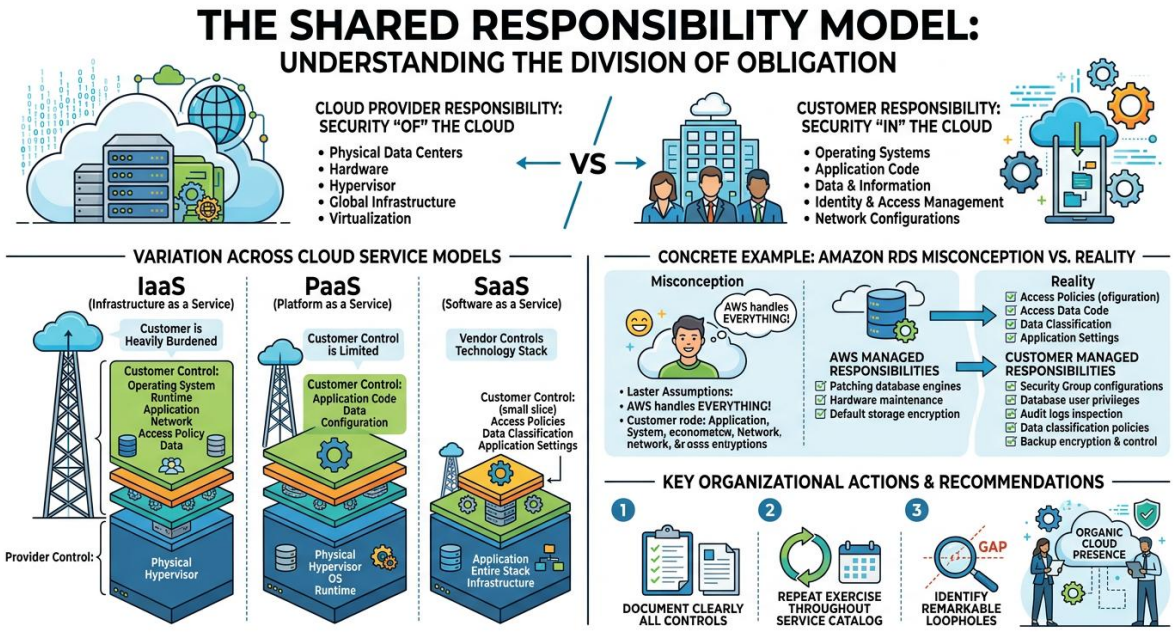

Fig -3: The Shared Responsibility Model Understanding the Division of Obligation

The implication to action is simple in case of any cloud service in use, security teams are supposed to document clearly what controls the provider is providing and what controls the customer is supposed to provide. This is a repeat exercise that is used throughout the service catalog and is likely to expose some remarkable loopholes in organizations that have expanded their cloud presence in an organic manner and lacked a formalized approach to security governance.

5. CLOUD ACCESS SECURITY BROKERS

5.1 Governing the Shadow and the Sanctioned

A Cloud Access Security Broker or a CASB can be described as a control entry point between the user and cloud services. It aims at creating visibility, data policing, threat detection, and compliance on cloud usage which would otherwise be hard to control or impossible to control using traditional network security measures. The motivation behind the creation of CASBs has been present since the time when employees started to use cloud services without IT knowledge and authorization, which the industry calls shadow IT. In cases where a sales team has a personal Dropbox account containing sensitive customer information, or an engineering department has one using a personal GitHub account where proprietary code is stored, then the organization has a data governance issue that cannot be addressed by a traditional firewall. The gap has been filled with the development of CASBs which offer visibility into the usage of clouds service, authorized and unauthorized, and application-layer policy enforcement.

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

CASBs have deployment models that have significant tradeoffs. A forward proxy will intercept outgoing user traffic to the cloud services and will give detailed visibility of the traffic even unsanctioned applications. It needs the deployment of the endpoint agents or the redirection of traffic and can face difficulties in handling encrypted traffic of the uncontrolled devices. A reverse proxy will capture the traffic between users and directly between them and particular sanctioned applications and is especially effective with browser-based cloud applications and does not need a specific endpoint agent. With API-based integration, APIs that are connected directly to the cloud service administrative APIs allow policy enforcement and data scanning of approved applications without any traffic flow modification. The API integration has the least difficulty to implement and can only work with applications, which provide the appropriate administrative interfaces, and lack the capability to monitor the traffic in real-time.

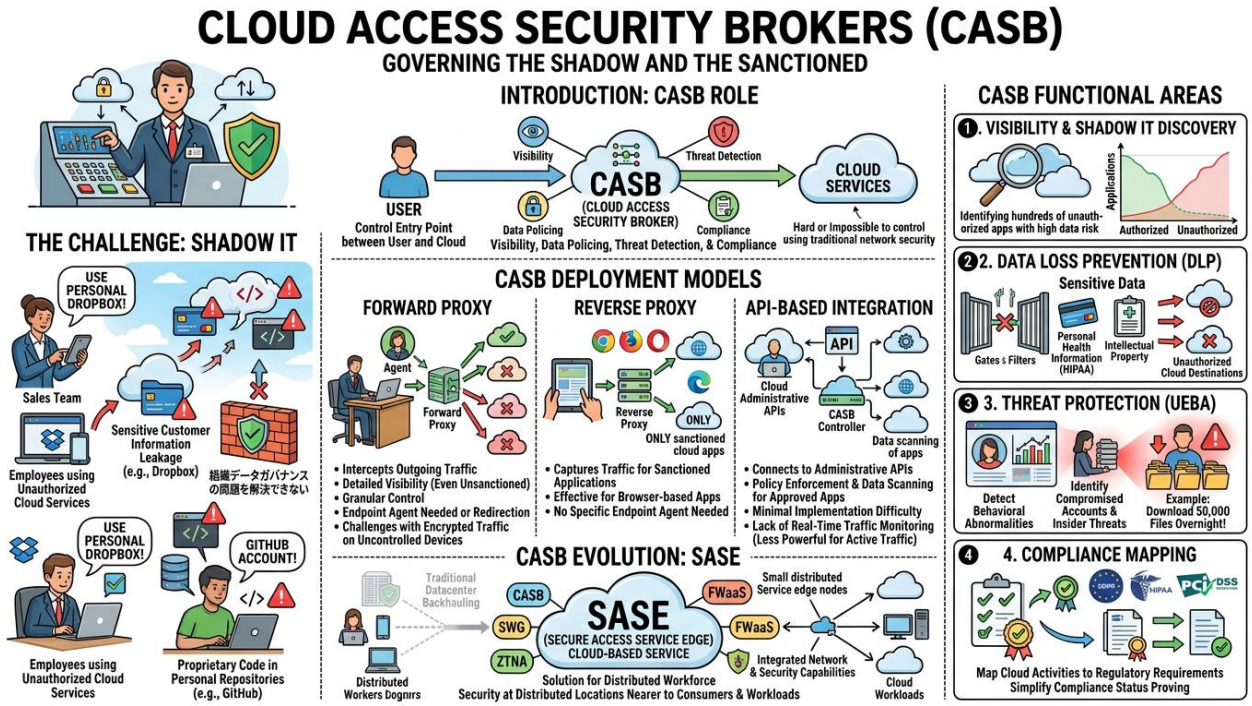

Fig -4: Cloud Access Security Brokers (CASB)

The functional areas on which the capabilities provided by CASB platforms are clustered are four. The visibility and shadow IT discovery provides the security teams with the full picture of how the cloud services are used in the organization. When an organization first uses a CASB, it is common to find out the presence of hundreds of different cloud applications that are currently in use. A large number of them have a high degree of data risk. Data Loss Prevention enforcement helps to be sure that the sensitive data, which may be the payment card data, personal health information, or intellectual property, does not pass to unauthorized cloud destinations. Threat protection based on UEBA detects behavioral abnormalities that can be used to identify compromised accounts or insider-threats. A customer that downloads 50,000 files in one session overnight is showing a behavior that does not reflect the historical background and should be investigated. The compliance mapping relates the data of cloud activities to the regulatory framework requirements and thus it is simpler to prove the compliance status under GDPR, HIPAA or PCI-DSS.

The development of CASB technology has been accelerated by the fact that it is built in the architecture of the Secure Access Service Edge. SASE integrates network security capabilities, such as the Secure Web Gateways, Zero Trust Network Access, and Firewall as a Service, with those of a CASB into a cloud-based service model. In distributed workforce and mostly cloud-based organizations SASE is a solution to a fundamental issue the traditional security architecture of supporting the user traffic with a back-end data center is ill-adapted to the operations based on the clouds. SASE provides security functions at distributed locations of presence, which are nearer to consumers and workloads.

6. IDENTITY AND ACCESS MANAGEMENT

6.1 The New Security Perimeter

The identity in a cloud environment has taken the role of a functional equivalent of the network perimeter. One cannot physically break into and tap network cables. When an attacker gets a valid identity credential with enough permissions, he or she will be able to work within a cloud environment with the same capability as the legitimate user. The correct approach to Identity and Access Management is thus not a security issue among others. It is the security discipline upon which the rest of the security disciplines rely.

IAM deals with three issues that are related to each other the issue of determining which identities exist in the system, the issue of determining whether an identity is who it says it is, and the issue of determining what identities that are verified are allowed to do. Identities in cloud environments are far beyond human beings. Service accounts to communicate with cloud APIs, workload identities to be example of containerized processes and machine credentials to be used in automated pipelines are all first-class identity subjects and need the same rigor of governance as human accounts. Service accounts are an especially high-risk commitment since they commonly have far-reaching authorization and are not as subject to the monitoring of human account activity as they often are.

Role-Based Access Control has continued to be the most popular authorization in AWS IAM, Azure RBAC, and GCP IAM. The RBAC model allocates roles to identities and assigns permissions to roles whereas it is good in a large environment because it allocates permissions on the role level and not on the individual user level. Permission drift is a major constraint to the practice of RBAC. With the increase of teams and changes of project requirements, roles gain authorizations gradually. The example of an engineer who required temporary access to a production database three years ago, might continue to have that access to the database under a role that has grown significantly bigger than it was originally. This permission drift is close to ubiquitous in mature cloud environments and a systemic and sustained exposure.

The attribute-based Access Control is more precise as it makes access decisions depending on contextual attributes of both the identity requesting access and the target resource, as well as the environmental conditions. One of the policies may only allow access to the database when the identity requesting access has an attribute of engineer, the resource requested is marked as part of the development environment and the requesting device is a device under corporate control and at specific working hours. ABAC minimises permission explosion created by RBAC at the cost of complexity in policy management that must be carefully managed.

Multi-Factor Authentication is an autonomous control that cannot be compromised under any environment even a cloud environment that deals with sensitive information or systems. The history of the industry of compromised credentials has been unambiguous and consistent: accounts with password-only protection are reliably compromised at scale due to phishing attacks, credential stuffing attacks, and

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

brute force attacks. MFA, and especially hardware-based tokens, or any authenticator application, removes most credential-based account takeover risk.

Privileged Access Management takes the control of IAM to the most vulnerable identity level. Routine operations should never be done with cloud organization administrators, root accounts and break-glass credentials. PAM solutions apply just-in-time access, i.e. privileged permissions are granted to perform specific tasks, and then automatically revoked, ensuring that the exposure period of any individual privilege credential compromise is limited.

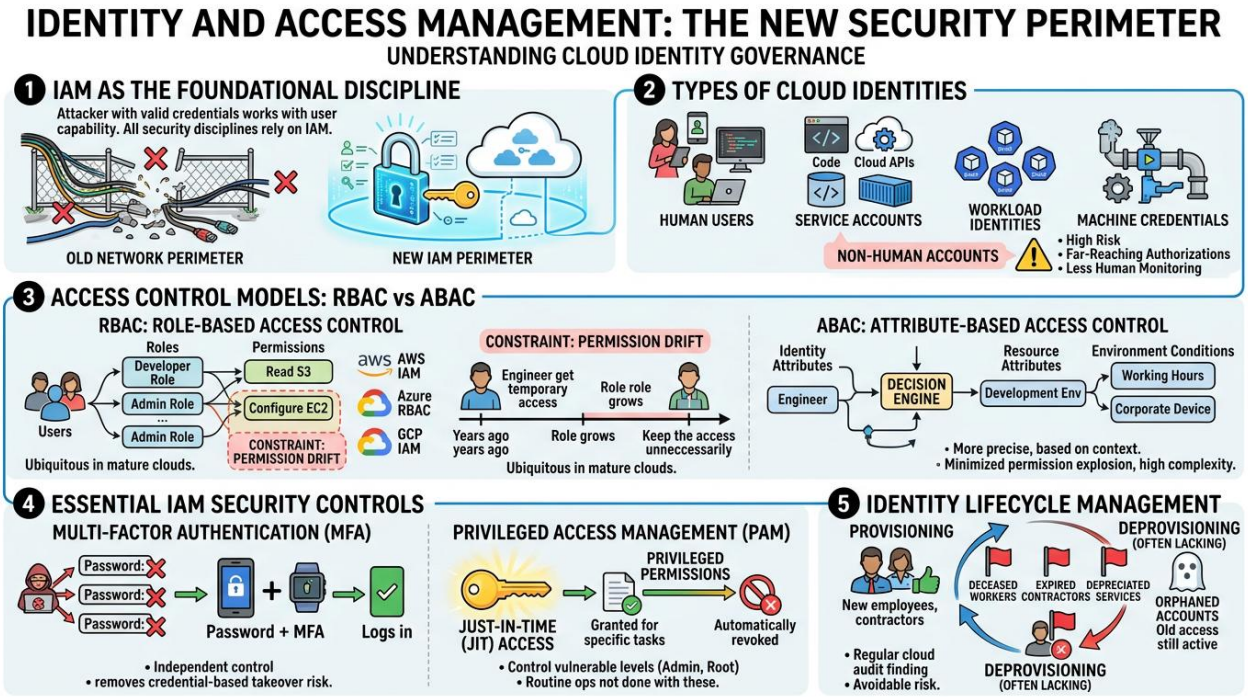

Fig -5: Identity And Access Management The New Security Perimeter

The areas that most organizations lack are in identity lifecycle management. Provisioning is usually under control since new workers have to have access to work. Discipline is often disintegrated in deprovisioning. The accounts of the deceased workers and the expired contractor arrangements as well as the depreciated services do not go to waste. One of the regular findings of cloud security audits is orphaned accounts, which have access permissions in the past, and are an avoidable risk that can be completely avoided.

7. CLOUD IDENTITY FEDERATION

7.1 Extending Enterprise Identity to Cloud Environments

The vast majority of organizations come to the cloud adoption with already developed identity infrastructure. Active Directory implementations with thousands of user accounts, LDAP directory implementations and existing single sign-on configurations are considered to be substantial institutional investment. Cloud identity federation enables the organizations to expand that current infrastructure to the cloud settings instead of having parallel identity systems.

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

Federation works through the defining of a relationship of trust between an Identity Provider which holds authoritative identity records and cloud services as Service Providers. The user logs in to the Identity Provider and is issued with a cryptographically signed assertion or a token. The cloud service authenticates that token with the configured trust and provides access without authenticating that token. The mechanism allows the Single Sign-On to scale to enterprise and centralize the identity governance in a manner that minimizes administrative overhead and enhances the consistency of security.

Enterprise cloud identity federation involves three protocols. The most developed standard is SAML 2.0 which is XML based which is widely used in enterprise applications and cloud providers. OAuth 2.0 is an authorization delegation protocol which allows users to provide applications with scoped access to resources without providing credentials. OpenID connect is a layer that is based on OAuth 2.0, which provides identity assertion in a JSON-based format that is appropriate to the new API-driven applications. OIDC is now the protocol of choice in cloud-native because it has a lighter implementation profile than SAML.

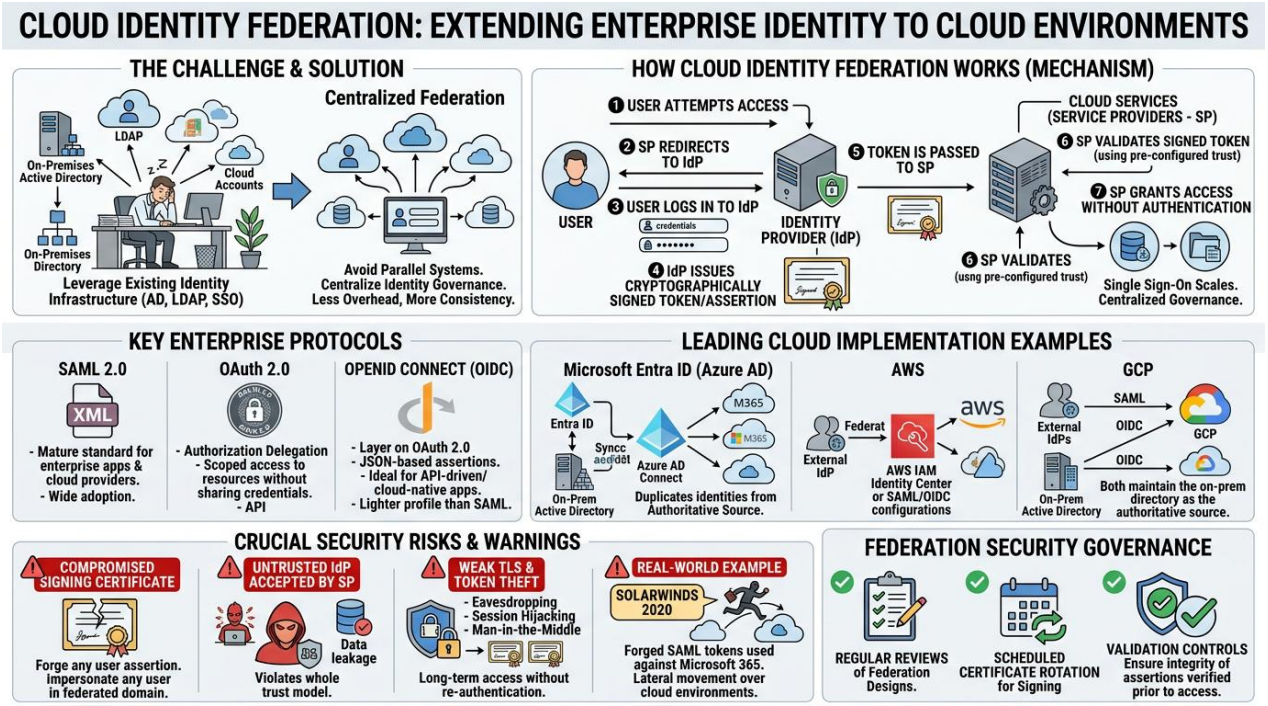

Fig -6: Cloud Identity Federation Extending Enterprise Identity to Cloud Environments

Combination of on-premises Active Directory and cloud platforms is frequently carried out with the help of synchronization software such as Azure AD connect which duplicates directory identities to Entra ID (previously Azure Active Directory). AWS and GCP have federation with external IdPs that are supported using AWS IAM Identity Center and SAML and OIDC configurations, respectively. Both solutions maintain the on-premises directory as the authoritative source of identity yet cloud service access is available without additional credential management.

One of the areas where the implementation errors have serious consequences is federation security. In the event that a SAML assertion signing certificate has been compromised, then the attacker will be able to forge assertions and impersonate any user in the federated domain. The configurations of Service Providers

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

that take in assertions by untrusted Identity Providers violate the whole trust model. The weakly configured TLS connections can be subjected to token theft by session hijacking or man in the middle attacks, which will provide long term access without re-authentication. Although it is indeed a complicated case, the SolarWinds case of 2020 has shown how trust relationships between identity systems, namely, the forged SAML tokens to authenticate against Microsoft 365 services, can facilitate lateral movement over cloud environments. Federation designs must be reviewed on a regular basis, signed certificates with scheduled rotation, and validation controls which ensure integrity of assertions is verified prior to access.

8. DATA ENCRYPTION

8.1 The Last Line of Defense

Encryption plays a particular and important role in cloud data security. The control is the one that works even when the rest of the controls do not work. When a storage bucket is exposed due to misconfiguration, when a database credential is obtained by an attacker, when a service account is compromised, encryption can be used to define whether the data accessed by the attacker is readable. Due to this reason, encryption is not a checkbox of compliance. It should be applied in a careful manner throughout the data life cycle.

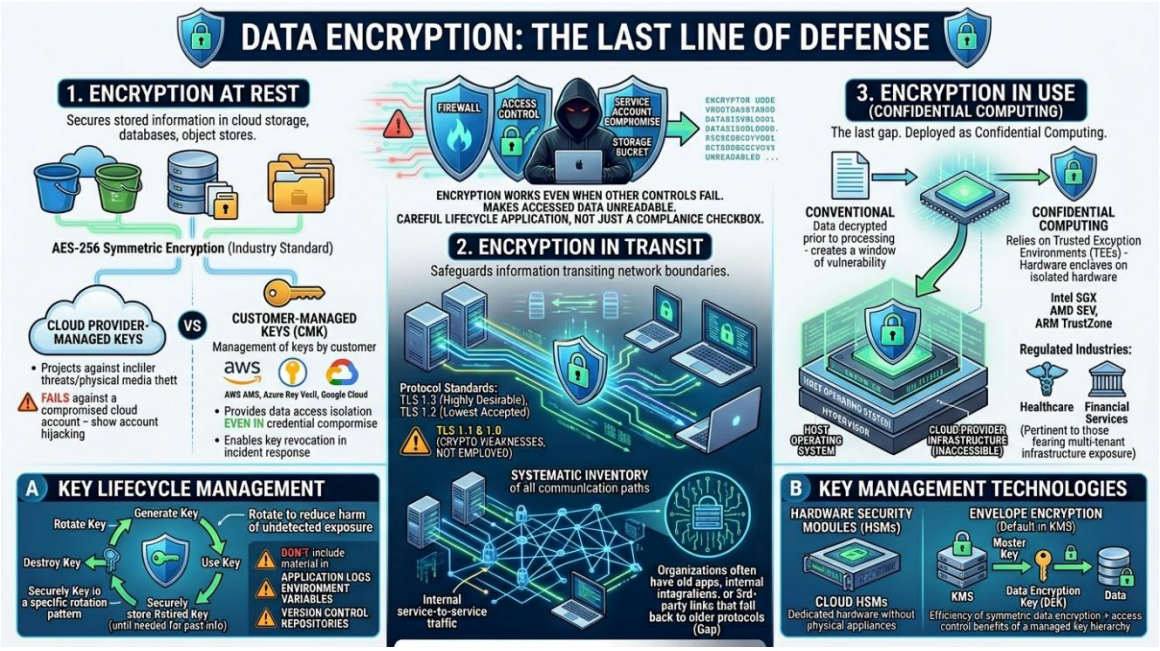

Fig -7: Data Encryption The Last Line of Defence

Rest encryption secures information that is stored in cloud storage, databases, and object stores. The three leading cloud providers use AES-256 encryption at rest, which is the default encryption for most storage services, as the current industry standard in symmetric encryption. Key management is the key variable. Encryption at rest offers the customer some reasonable protection against insider threats and physical media theft by the cloud provider when the cloud provider handles encryption keys on behalf of the customer. It fails to safeguard against a compromised cloud account, since the same authentication that allows access to the data usually allows access to the decryption keys, also. Customer-Managed Keys help solve this by leaving the management of keys to the customer, with services such as AWS KMS, Azure Key

Vault, or Google Cloud KMS. The data access isolation that CMK provides enables organizations to retain control over data accessibility even in the event that credentials to cloud accounts are compromised, and enables key revocation as a component of incident response.

The in transit encryption safeguards information that transits network boundaries. TLS 1.2 is the lowest standard that can be accepted, and TLS 1.3 is highly desirable when using a new implementation. TLS 1.0 and 1.1 are known to have cryptographic weaknesses, and should not be employed in a sensitive data environment. The reality issue is that most organizations have old application elements, internal service integrations, or third-party vendor links that fall back to older protocols. A mature cloud encryption program needs to include systematic inventory of transport encryption of all communication paths, including internal service-to-service traffic in cloud environments.

The last gap in the data lifecycle is filled with encryption in use, which is deployed as confidential computing. Conventional encryption secures data when at rest and in transit, but requires data to be decrypted prior to processing, which creates a window of vulnerability even in highly secured environments. Confidential computing relies on Trusted Execution Environments, hardware-based platforms, such as Intel SGX, AMD SEV, and ARM TrustZone, to compute on encrypted data on isolated hardware enclaves inaccessible to the host operating system, hypervisor, or cloud provider infrastructure. All of AWS, Azure, and GCP provide types of confidential computing instances. This feature is especially pertinent to regulated industries, including healthcare and financial services, which traditionally did not want to move sensitive workloads to the cloud because of the fear of being exposed to multi-tenant infrastructure.

Encryption programs most often fail in practice at key lifecycle management. The keys are required to be rotated in a specific rotation pattern to reduce the harm of exposure without detection. Retired keys should be stored in a secure place until the time needed to decrypt past information, and then destroyed. Important material should not be included in application logs, environment variable setup that can be accessed by any untrusted process, and version control repositories. Hardware Security Modules are tamper resistant hardware used to store keys and perform cryptographic functions. Cloud HSMs such as AWS CloudHSM and Azure Dedicated HSM, offer the security features of dedicated hardware, without requiring organizations to acquire and operate physical appliances. The default scheme in most cloud KMS systems, envelope encryption, is based on the efficiency of symmetric data encryption, and the access control benefits of a managed key hierarchy, by encrypting data encryption keys with a master key stored in the KMS.

9. CLOUD SECURITY POSTURE MANAGEMENT

9.1 Systematic Misconfiguration Detection

Cloud Security Posture Management solutions deal with the largest contributor to cloud security risk, statistically, misconfiguration. CSPM tools are used to conduct automatic, ongoing, evaluation of configurations of cloud environments, comparing actual deployed state with security best practice, compliance framework requirements, and organizational policy.

Misconfiguration detection at scale is the basic capability of CSPM. Manual review of configurations is not viable and cannot be trusted in large cloud environments with hundreds of accounts, thousands of resources, and dozens of services being used. CSPM platforms will scan configurations that are violating security principles S3 buckets with open access, RDS instances with open internet access, security groups with open inbound traffic, IAM roles with wildcard permissions, storage services with server-side encryption

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

disabled, and virtual machines without endpoint protection. These results are actual exploitable vulnerabilities. Misconfiguration and exposed credentials have continued to be among the leading root causes of cloud-related incidents in both the IBM Cost of a Data Breach Report and the Verizon Data Breach Investigations Report.

Successful CSPM systems use contextual scoring of risk, as opposed to equal treatment of findings. A storage bucket with encrypted, publicly accessible marketing data has a different risk profile to an internet-accessible database instance with customer financial data. Remediation effort can be prioritized to where it is most needed by risk scoring that considers resource sensitivity, exposure level and likelihood of exploitation. Compliance mapping extrapolates CSPM results to regulatory and framework requirements. Cloud platform CIS Benchmarks, NIST 800-53, ISO 27001, SOC 2, and PCI-DSS controls each contain configuration requirements that can be mapped findings to using CSPM tools. This ability converts technical results into compliance language which can be acted upon by organizational stakeholders, legal teams and auditors.

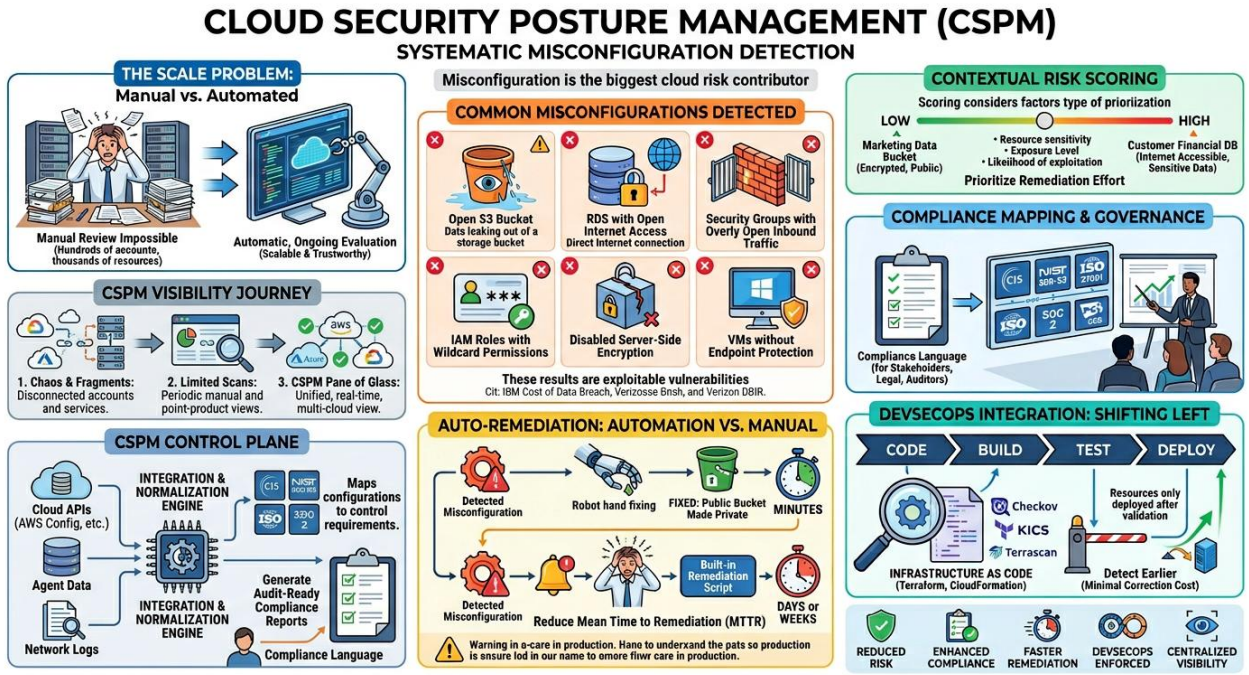

Fig -8: Cloud Security Posture management (CSPM)

Auto-remediation is one of the most valuable features of scaling CSPM to scale. In case of a misconfiguration, an automated workflow can take action to fix the situation automatically. A publicly accessible storage bucket can be configured to be private. A security group that has a too liberal inbound rule can issue an automated notification containing a built-in remediation script. Auto-remediation needs to be handled with care, especially in the context of production environments, but when finding categories are well-defined and low-risk, automation can reduce the mean time to remediation by days or weeks to minutes. CSPM is integrated with DevSecOps pipelines to detect CSPM earlier in the development lifecycle when the cost of correction is minimal. Infrastructure as Code (like Terraform, CloudFormation, etc.), can be scanned against security vulnerabilities prior to deployment with services such as Checkov, KICS, and Terrascan as part of CI/CD pipelines and enforced as quality gates as needed. A resource that cannot be

deployed due to a misconfiguration is always better than a resource that is misconfigured and was identified in production three months after deployment.

10. CONTINUOUS COMPLIANCE MONITORING AND CLOUD SECURITY AUDITS

The old fashioned compliance testing was conducted on annual or semi-annual basis. A sample of configurations and controls were audited at a single point in time by an auditor who produced a findings report and returned the next year. This model has been structurally inadequate in cloud environments. Clouds can be altered within a couple of minutes. A Monday audit-passing environment might have materially changed by Friday as a result of automated deployments or new service provisioning, or configuration changes under operational pressure.

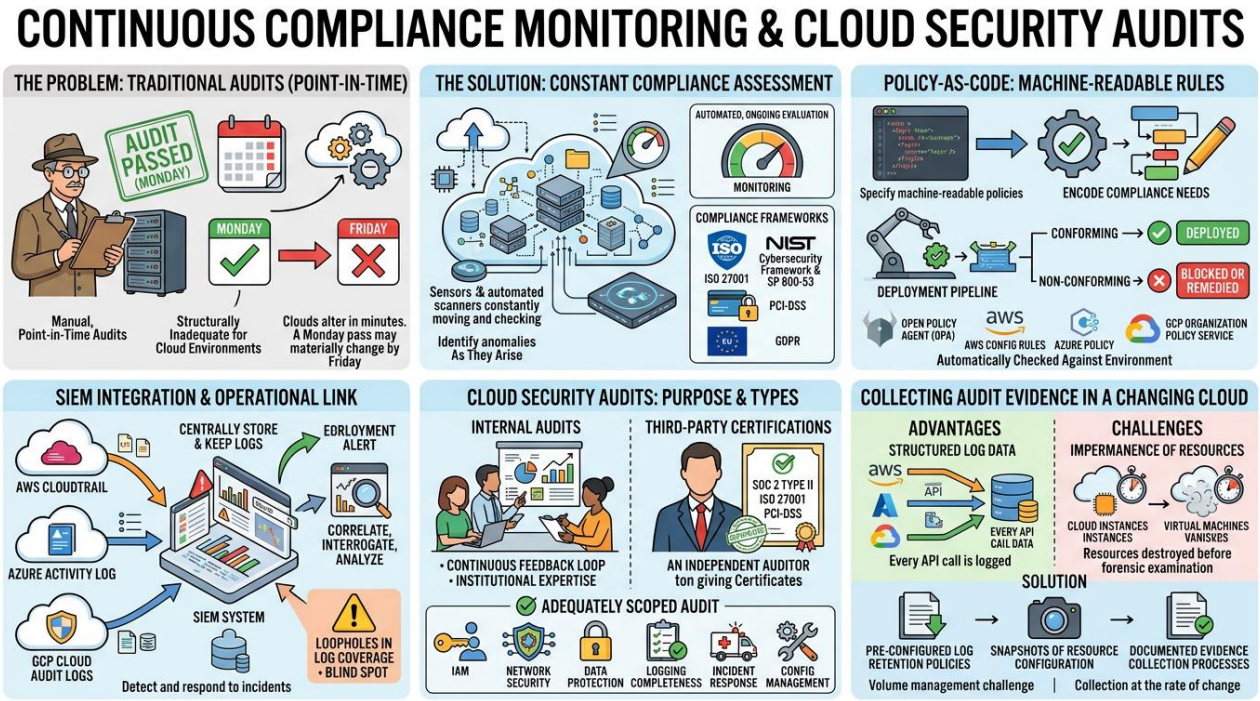

Fig -9: Continuous Compliance Monitoring & Cloud Security Audits

Constant compliance assessment is an alternative to the periodical snapshot as it is an automated, ongoing evaluation process. The compliance status of the environment is monitored and anomalies identified and brought to the fore as they arise and not at the next scheduled review. The most widely discussed compliance frameworks in cloud security programs are ISO 27001, the NIST Cybersecurity Framework and SP 800-53, the PCI-DSS in the context of an environment that works with payment card data, and the GDPR in the context of organizations that work with personal data of EU residents.

Policy-as-Code is an innovative change in the way compliance requirements are handled and implemented. Instead of specifying requirements in a set of static documents that need to be manually checked, requirements are specified as machine-readable policies that are automatically checked against the environment. Open Policy Agent, AWS Config Rules, Azure Policy and GCP Organization Policy Service allow organizations to encode their compliance needs in policy definitions that trigger on each

resource deployment and configuration change. Non-conforming resources may be blocked or marked to be remedied on the spot. This model eradicates the disconnect between what is recorded and what is happening in the field that characterises traditional compliance management.

SIEM integration links continuous compliance monitoring with the rest of the security operations capability. AWS CloudTrail, Azure Activity Log and GCP Cloud Audit Logs are cloud-native audit logs that contain detailed records of all actions undertaken on a management plane within a cloud environment. These logs have to be centrally stored, and kept over time periods as mandated by the relevant frameworks, and fed into SIEM systems where they can be correlated, interrogated and analyzed. Loopholes in log coverage are a compliance shortcoming as well as an operational blind spot that restricts the ability to detect and respond to incidents.

Cloud security audits are used to control risks internally as well as to comply with regulatory requirements. Internal audits, where the security or compliance team of the organization conducts them, give the organization a continuous feedback loop and build institutional expertise. Certifications such as SOC 2 Type II, ISO 27001 and PCI-DSS require third-party audits, which are performed by independent assessors. An adequately scoped audit includes identity and access control, network security settings, data protection, completeness of logging, ability to respond to incidents, and configuration management.

The structured comprehensive log data that cloud platforms produce by default is advantageous in the collection of evidence to support cloud audits. Every API call is logged with AWS CloudTrail. Azure Activity Log logs every management activity. GCP Cloud Audit Logs offer a similar coverage. Volume management and the impermanence of cloud resources are the challenge, and a cloud resource can be destroyed before it can be forensically examined. Cloud environments need pre-configured log retention policies, snapshots of resource configuration, and documented evidence collection processes that can work at the rate of change of cloud infrastructure.

11. INTEGRATED CLOUD SECURITY ARCHITECTURE

11.1 Building a Coherent System

Individual security controls can be far more effective when they are created to be part of an integrated architecture and not standalone. An identity context, which does not share identity with the IAM system, cannot allow risk-aware access decisions to be made by the CASB. A CSPM tool that does not feed its results to the SIEM cannot be used to provide contributions to the threat detection picture. Architectural integration is not a feature to have. It is what differentiates security programs that identify and take action against actual incidences and programs that produce reports.

An effective cloud security architecture lays out the controls in four functional layers. The identity layer is the most important and the most outer layer and it includes the IAM system, federation settings, MFA implementation, and privileged access control. Any access attempt is controlled by the identity layer first and then by any other control. The network layer manages the traffic between resources of a cloud, between users and cloud services, and between cloud environment and outside systems. Security groups, network ACLs, private endpoints, VPN configurations, and cloud-native firewall services are all considered network controls. The data layer includes encryption of data at rest and data in transit, key management infrastructure, data classification, and DLP policy enforcement. Application layer deals with security of API gateways, web application firewalls, container security controls, and enforcement of application level authentication.

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

CASB, IAM, CSPM, and SIEM are operational components of a mature cloud security program, which combines them into a single detection/response capability. CASB offers insights into the use of cloud services and imposes data policy at the user-to-cloud traffic edge. IAM controls access in a cloud environment and provides identity context to SIEM. CSPM continuously tracks configuration state and produces findings which are sent to the SIEM and to the ticketing system to track remediation. The SIEM matches signals of all three with threat intelligence, user behavior analytics and network telemetry. A CSPM finding that a publicly exposed service is present, an IAM event that some unusual permission grant has occurred, and a CASB alert that an unusual amount of downloads have been made are correlated detection signals that would be much more important than individual alerts.

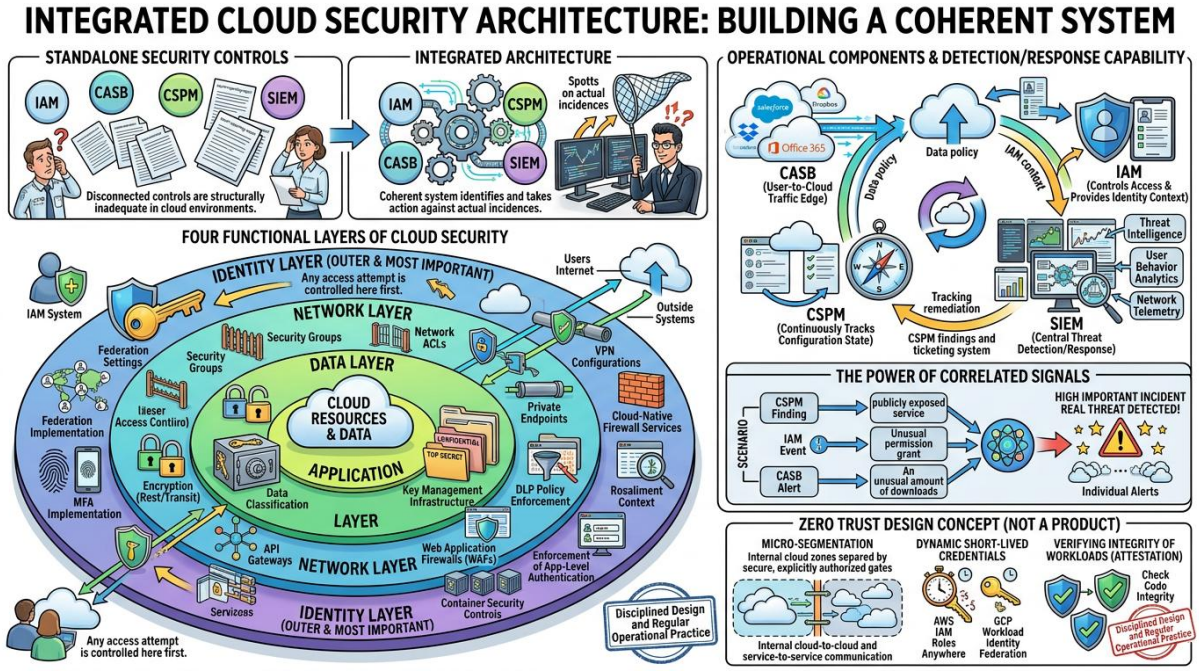

Fig -10: Integrated Cloud Security Architecture Building A Coherent System

Zero Trust in the cloud is a design concept rather than a product. It is achieved by micro-segmentation that must explicitly authorize all internal cloud-to-cloud communication, service-to-service communication dynamically issued short-lived credentials, by mechanisms such as AWS IAM Roles Anywhere and GCP Workload Identity Federation, and by verifying the integrity of workloads through attestation instead of assumption. Contemporary cloud platforms have the components of true Zero Trust implementation built into them, but it takes disciplined design and regular operational practice to make the architecture a reality.

12. OPERATIONAL BEST PRACTICES

12.1 Security at Cloud Velocity

Cloud environments are so fast that the conventional change management processes are no longer sufficient. Infrastructure, code deployment and configuration iterations are all done in hours, rather than weeks, by development teams. Manual review gates at all stages of security practices introduce friction to

teams that motivates them to bypass security controls instead of working through them. The best cloud security programs address this issue by integrating security into the development and operations process to such a degree that it becomes the course of least resistance.

The organization practice that enables this embedding is called DevSecOps. CI/CD pipelines include security checks that identify vulnerabilities before they get to production. Statics on Infrastructure as Code settings, scanning of container images within the build pipeline, scanning of software dependencies within the software build pipeline, and detection of secrets within a code commit are all executed in code without human involvement at the rate of automated delivery pipelines. Security teams are no longer gatekeepers, who are reviewed on deployments, but platform engineers, who autogenerate the security tooling on which development teams deploy.

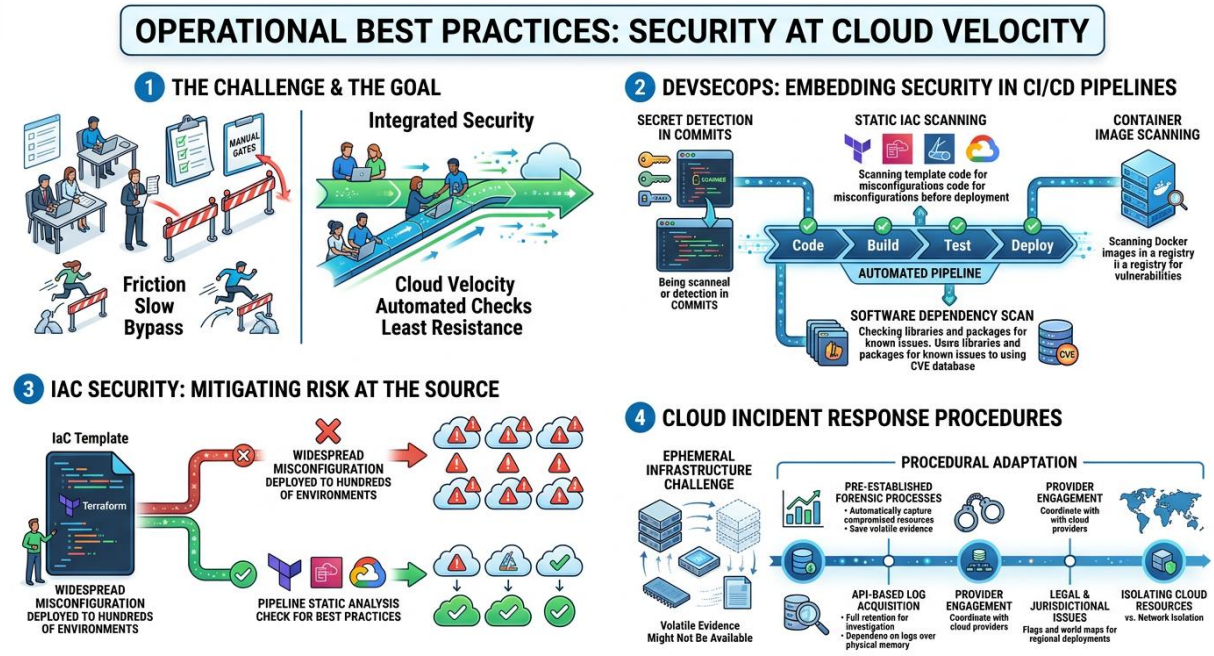

Fig -11: Operational Best Practices Security At Cloud Velocity

The discipline of IaC security is now a pressing one as Terraform, AWS CloudFormation, Azure Bicep, and Google Cloud Deployment Manager have become the main tools to provision cloud infrastructure. Consistency, repeatability, and version control are the same qualities that make IaC valuable, so that a misconfiguration in an IaC template can be deployed to hundreds of environments before anyone ever notices. This risk is mitigated at the source by the use of static analysis tools as part of a pipeline check.

Response to an incident in the cloud environment will need procedural adaptation. The fact that cloud infrastructure is temporary implies that any forensic evidence that would otherwise be found on a physical server, memory contents, disk images, network interface captures, etc. might not be available when an incident is detected. Components of a cloud incident response plan include pre-established forensic processes that automatically capture compromised resources and save volatile evidence at the time an incident is declared. Most cloud investigations rely on API-based log data instead of on physical memory acquisition; therefore, full retention of logs is not just a compliance requirement but an operational one. Cloud incident response plans should also cover provider engagement processes, legal and jurisdictional

issues during regional deployments, and the difference between isolating compromised cloud resources and the physical network isolation processes that are used in traditional set ups.

13. CURRENT TRENDS

13.1 The Technologies Reshaping Cloud Security

The cloud security market is shifting at a fast pace, as the threat to cloud environments is becoming more and more sophisticated, the security capabilities built into the clouds are becoming more mature, and the previously disjointed tooling segments are being integrated into a single platform.

Cloud-Native Application Protection Platforms are the biggest trend in cloud security tooling architecture. A CNAPP is a platform that integrates Cloud Security Posture Management, Cloud Workload Protection of virtual machines and containers, Kubernetes Security Posture Management, and container image scanning into one platform that uses a single data model. The key value of this consolidation is the ability of the tools to analyze risk contextually which is impossible when using siloed tools. A critical vulnerability in a deployed container image that exposes itself to the public internet and uses overly liberal service account bindings is of a categorically higher priority than the same vulnerability in an image deployed in a development environment that does not go to production. CNAPP platforms compute this context automatically, and rank findings based on the aggregate evaluation of vulnerability severity, exposure level, and permission scope. Vendor platforms such as Wiz, Palo Alto Prisma Cloud, and Orca Security have been quickly adopted by enterprises who are looking to simplify the management of multiple specialized cloud security platforms.

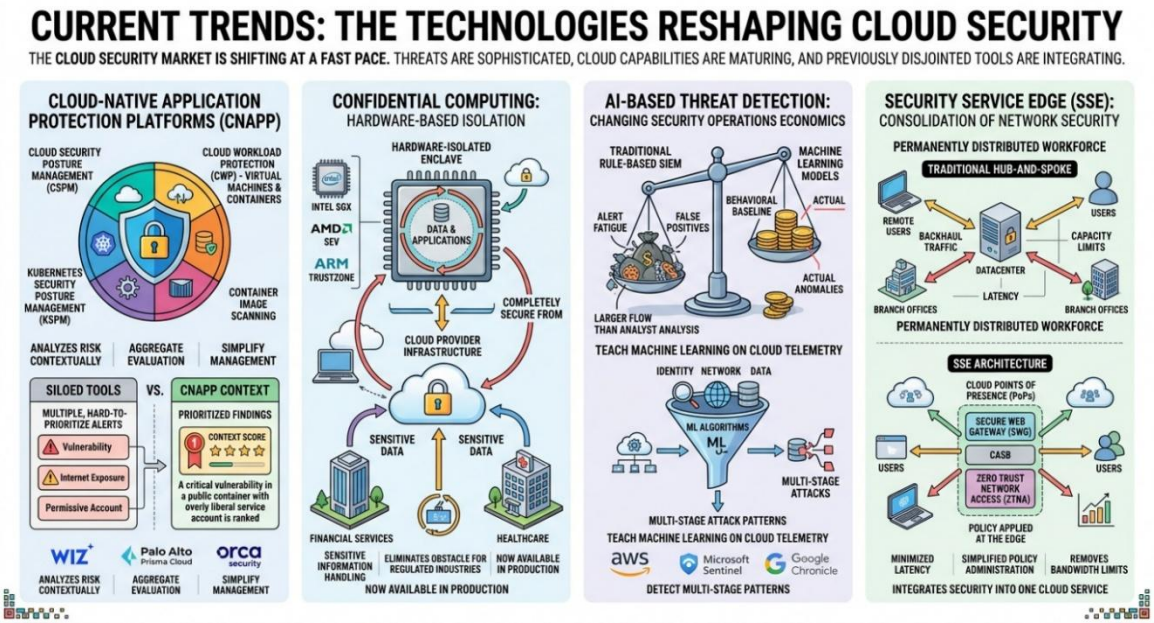

Fig -12: The Technologies Reshaping Cloud Security

Confidential computing is now no longer a research novelty, but is a service available in production. General availability instances of confidential computing based on Intel SGX, AMD SEV or ARM TrustZone hardware are now available on all three major cloud providers. The capability to handle sensitive information in hardware-isolated enclaves that the cloud provider infrastructure cannot access eliminates a major obstacle to cloud migration of highly regulated industries. Financial services companies and

healthcare organizations that have been keeping their most sensitive workloads on-premises in part due to the multi-tenant isolation considerations now have a technically plausible cloud option.

Security operations economics is being changed by AI-based threat detection. The inherent problem with the traditional rule-based SIEM is that it creates a flow of alerts that is larger than can be analyzed by human analysts, and the false positive rates are so high that real threats are lost in the noise. Machine learning models that have been trained on telemetry in the cloud environment can provide a behavioral baseline and detect actual anomalies with accuracy that cannot be matched by rule sets. ML-based detection models have become part of AWS GuardDuty, Microsoft Sentinel, and Google Chronicle as well. The most advanced implementations map signals on identity, network and data plane telemetry to identify multi-stage attack patterns that would not have been signaled by any single alert rule.

The development of Security Service Edge is the network security version of CNAPP consolidation. SSE integrates Secure Web Gateway, CASB and Zero Trust Network Access into one cloud-based service. Organizations with permanently distributed workforces, and whose infrastructure is largely cloud-based, use SSE instead of a hub-and-spoke network security architecture, where all traffic backhauled to a central data center, with a model that applies security policy at cloud points of presence near users and workloads. This architectural change minimizes latency, simplifies policy administration and removes the bandwidth capacity limits that cause traditional network security architectures to become less and less feasible at scale.

14. CONTAINER AND KUBERNETES SECURITY

14.1 Securing the Cloud-Native Deployment Model

Container technology has been adopted as the default unit of deployment of cloud-native applications. The most popular container orchestration system is Kubernetes, which is used to handle containerized workloads on a large scale in nearly all enterprise clouds. The security implications are significant and they are not similar to virtual machine based security as they need to be treated as a separate entity and not as a footnote in the larger discussion of CSPM or CNAPP.

14.2 The Container Attack Surface

Containers imply a different threat model. Containers do not have the host kernel that virtual machines do as they are fully isolated with the hypervisor. A vulnerability in the kernel that enables a process to break out of its container namespace may expose the host and all of the other containers operating on the same node. The security of a container environment is consequently directly related to the patch currency of the host kernel and security configuration of the container runtime.

Another attack surface layer is the container image per se. Base images are used to create images, and very often they contain unpatched OS packages and vulnerabilities in the application libraries. Hackers that breach a container registry, or who add malicious code to a public base image, can release modified workloads at scale. This danger was made a reality in 2018 when the official Docker Hub library images were compromised and a cryptocurrency mining image was found with more than five million pulls.

14.3 Kubernetes-Specific Security Controls

Kubernetes has a number of security configuration areas, which need to be explicitly addressed. Role-Based Access Control in Kubernetes controls who may do what operations on the Kubernetes API, as well as who can do them. The over-permissioned service accounts, which is a common occurrence in cloud

Partners Universal International Innovation Journal (PUIIJ)
Volume: 04 Issue: 02 | March-April 2026 | ISSN: 2583-9675 | www.puiij.com

security evaluations, are especially harmful in Kubernetes since a service account that is attached to a pod with the permissions of a cluster-admin can list, alter, or delete any resource in the cluster. The least privilege principle of Kubernetes RBAC implies that the permissions of service accounts are defined at the namespace level and have an explicit resource and verb scope instead of defaulted or inherited permissions.

The Pod Security Standards, originally named PodSecurityPolicy, the resource that supersedes the decommissioned PodSecurityPolicy resource in Kubernetes 1.25, impose security restrictions on a pod. They specify three levels of policy: Privileged, offering no restrictions; Baseline, offering known privilege escalation vectors; and Restricted, offering the current hardening best practices such as privilege escalation prevention, host namespace access restriction and non-root execution. Majority of production workloads must run under Baseline or Restricted policy and workloads that must be run with Privileged access must be clearly justified, narrowly defined and closely monitored.

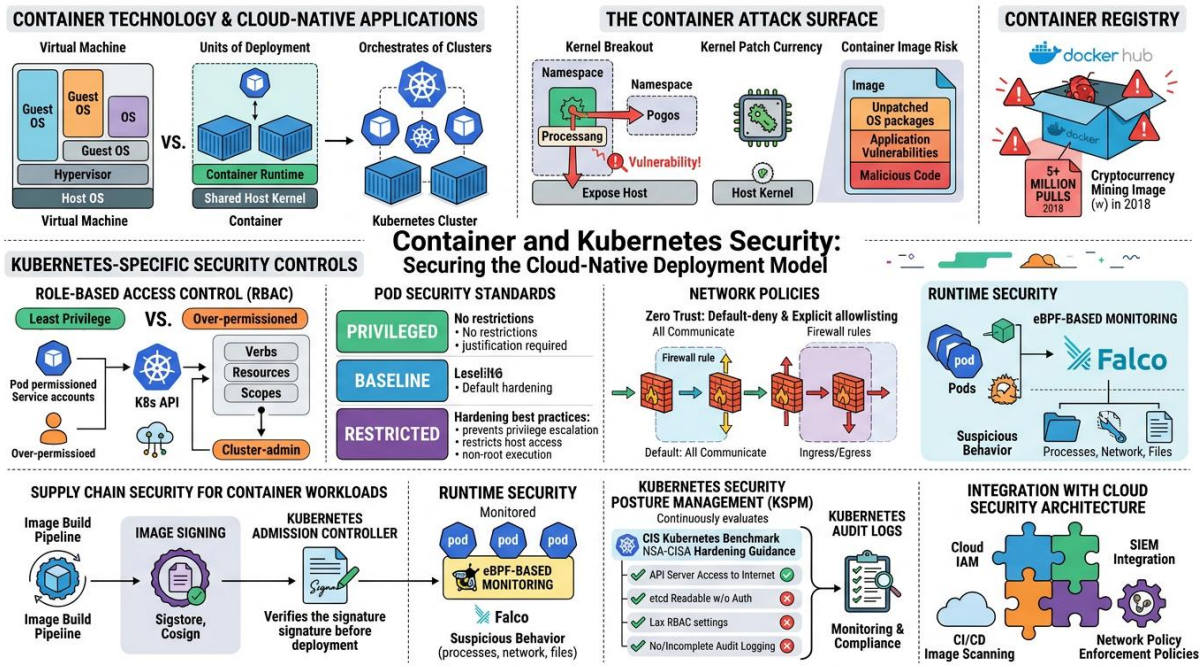

Fig -13: Securing The Cloud-Native Deployment Model

Kubernetes network policies are firewall rules of pod-to-pod communication. A cluster of pods can by default communicate with all other pods. A hacked workload has the potential to reach any other service within the cluster without any explicit network policies that define what ingress and egress flows are allowed. Use of default-deny network policies and explicit allowlisting of communication paths that are required is an application of Zero Trust micro-segmentation principles at the workload layer.

14.4 Supply Chain Security for Container Workloads

The image integrity of containers has become a major control after several high profile incidents in the supply chain. Container image signing with Sigstore and Cosign and enforcing signature verification at admission time with Kubernetes admission controllers will ensure that only images that are signed as being

built by trusted build pipelines can be deployed. This control deals with the risk of the compromised registry credentials or tampered images directly.

14.5 Runtime Security

The configuration controls that are set in the static configuration should be supplemented by the behavioral monitoring during the runtime. Tools that can be used to identify suspicious container usage at the eBPF (Extended Berkeley Packet Filter) level, such as Falco, can identify threats that cannot be detected by image scanning and configuration hardening. eBPF-based monitoring is associated with a low performance cost and offers insight into the activity of containers with no changes to container images or processes.

14.6 Kubernetes Security Posture Management

KSPM, which is currently commonly provided as part of CNAPP platforms, can continuously evaluate the configuration of Kubernetes clusters against standards such as the CIS Kubernetes Benchmark and NSA-CISA Kubernetes Hardening Guidance (last updated in August 2022). Such typical results are API server access to the internet, etcd readable without authentication, lax RBAC settings, and no or incomplete audit logging in the Kubernetes control plane. Kubernetes audit logs document all the interactions with the API server and are an essential source of evidence in security monitoring as well as compliance evaluation. The security of containers and Kubernetes needs to be integrated with the rest of cloud security architecture. The policies of IAM controlling access to the Kubernetes API, SIEM integration to analyze Kubernetes audit logs, image scanning built into CI/CD pipelines, and network policy enforcement policies cannot be maintained in isolation of each other, in case Kubernetes security posture is to be taken seriously at scale.

15. CONCLUSION

15.1 Building a Cloud Security Program That Endures

The main conclusion of this discussion is obvious and practical. The vast majority of the severe cloud security breaches are based on avoidable factors. The vast majority of cloud-related incidents are explained by misconfiguration, over-permitted identities, lack of and/or incomplete encryption, poor logging, and mis-understanding of the shared responsibility model. They are not the issues that demand the use of some exotic technology and unlimited security budgets. They are discipline issues, the failures of operations that can be avoided by efficient teams, operating in a properly designed process and being provided with the right tooling.

The sustainability of a cloud security program is based on a number of commitments that cannot be compromised. Identity should be considered as the main security control, MFA should be implemented everywhere, service accounts should be managed with the same strictness as human ones, and least privilege should be used everywhere. Every repeatable security function should be automated, including misconfiguration detection and remediation as well as compliance policy enforcement and IaC security scanning. The logging should be extensive, centralized and stored over durations that are adequate to respond to the operational incidents as well as comply with the regulations. The model of shared responsibility should be written down specifically on each service being used, and controls should be clearly stated to take care of the share of the responsibility on the part of the customer. The security controls and incident response process are supposed to be tested frequently, since unproven controls are not defences, but guesses.

The future of cloud security is towards being more automated, more integrated with AI, consolidated tooling architecture, and hardware-based data protection with confidential computing. Companies that establish their programs on viable principles in the present, identity-first security, unremitting automated observing, policy-as-code compliance, and integrated architecture design, will be well-positioned to embrace and enjoy these developments as they grow up. Cloud security is a challenging one, but it can be attained. The ones that get it right do not necessarily have to be the biggest or the most resource endowed organizations. They are those who take cloud security seriously and understand what they are securing, strictness on how they are securing it, and the discipline to keep on advancing as their environments and threats facing them keep changing.

REFERENCES

[1] A roadmap to Auditing Cloud Security | Global Best Practice | The IIA. (n.d.). https://www.theiia.org/en/content/articles/global-best-practices/2025/a-roadmap-to-auditing-cloud-security/
[2] Bayona, N., Epstein, H., Glaesser, D., Rosario, A., Vaez-Zadeh, R., Van Zant, E., B, Babu, A., Brezina, M., Chuenniran, A., Sattaburuth, A., Chow, P., De Montjoye, Y., Radaelli, L., Singh, V., Pentland, A., Wood, M. E., Milstein, M., Ahamed-Broadhurst, K., . . . Yee, Y. (2021). Big Data for Better Tourism Policy, Management, and Sustainable Recovery from COVID-19. https://doi.org/10.22617/spr210438-2
[3] CIS Google Cloud Computing Platform Benchmarks. (n.d.). CIS. https://www.cisecurity.org/benchmark/google_cloud_computing_platform
[4] George, A. S. (2025). Digital Watermarking in Cloud Environments for Copyright Protection: A Comprehensive Review. Partners Universal Multidisciplinary Research Journal (PUMRJ), 02(06), 54–74. https://doi.org/10.5281/zenodo.17726895
[5] Cloud Controls Matrix | CSA. (n.d.). CSA. https://cloudsecurityalliance.org/research/cloud-controls-matrix
[6] George. (2024). The Cloud Comedown: Understanding the Emerging Trend of Cloud Exit Strategies. Partners Universal International Innovation Journal, 2(5), 1–32. https://doi.org/10.5281/zenodo.13993933
[7] Cost of a data breach 2025 | IBM. (n.d.). https://www.ibm.com/reports/data-breach
[8] Enterprise foundations blueprint. (2025, May 15). Google Cloud Documentation. https://cloud.google.com/architecture/security-foundations
[9] George, D. A. S., Sagayarajan, S., AlMatroudi, Y., & George, A. S. H. (2023). The Impact of Cloud Hosting Solutions on IT Jobs: Winners and Losers in the Cloud Era. Partners Universal International Research Journal, 2(3), 1–19. https://doi.org/10.5281/zenodo.8329790
[10] Farooq, M. S., Riaz, S., & Alvi, A. (2023). Security and Privacy issues in Software-Defined Networking (SDN): A systematic literature review. Electronics, 12(14), 3077. https://doi.org/10.3390/electronics12143077
[11] George, D., George, A., Dr.T.Baskar, & Dr.V.Sujatha. (2023). The rise of hyperautomation: a new frontier for business process automation. Zenodo (CERN European Organization for Nuclear Research). https://doi.org/10.5281/zenodo.10403036
[12] Gopstein, A., Nguyen, C., O'Fallon, C., Hastings, N., & Wollman, D. (2021). NIST framework and roadmap for smart grid interoperability standards, release 4.0. https://doi.org/10.6028/nist.sp.1108r4
[13] George, Dr. A. Shaji., & Dr.T.Baskar. (2025). Securing the Future: A Review of Cutting-Edge Advances for Cloud and IoT Cybersecurity. Zenodo, 03(02). https://doi.org/10.5281/zenodo.15288362
[14] Katal, A., Dahiya, S., & Choudhury, T. (2022). Energy efficiency in cloud computing data centers: a survey on software technologies. Cluster Computing, 26(3), 1845–1875. https://doi.org/10.1007/s10586-022-03713-0
[15] George, D. A. S. (2024). Consequences of Enterprise Cloud Migration on Institutional Information Technology Knowledge. Partners Universal Innovative Research Publication, 2(2), 38–55.
[16] Msmbaldwin. (n.d.). Microsoft cloud security benchmark. Microsoft Learn. https://learn.microsoft.com/en-us/security/benchmark/azure

[17] George, A. Shaji., George, A. S. Hovan., & Baskar, T. (2023). Edge Computing and the Future of Cloud Computing: A Survey of Industry Perspectives and Predictions. Zenodo (CERN European Organization for Nuclear Research), 2(2). https://doi.org/10.5281/zenodo.8020101

[18] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. https://doi.org/10.6028/nist.sp.800-207

[19] Dr. A.SHAJI GEORGE, & A.S.HOVAN GEORGE. (2022). Potential Risk: Hosting Cloud Services Outside the Country. International Journal of Advanced Research in Computer and Communication Engineering, 11(4), 5–11. https://doi.org/10.5281/zenodo.6548114

[20] Security Pillar - AWS Well-Architected Framework - Security Pillar. (n.d.). https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/welcome.html

[21] George, Dr. A. Shaji. (2026). Real-Time IoT-Enabled Smart Water Quality Monitoring System Using Embedded Multi-Parameter Sensor Analytics and Attention-Based Predictive Modeling for Environmental Protection. Zenodo, 04(01). https://doi.org/10.5281/zenodo.18791197

[22] Team, C. R. (n.d.). Security Logging and Monitoring Failures: Risk and defenses. Radware. https://www.radware.com/cyberpedia/application-security/security-logging-and-monitoring-failures/

[23] George, A. S., & Sagayarajan, S. (2023). Securing Cloud Application Infrastructure: Understanding the Penetration Testing Challenges of IaaS, PaaS, and SaaS Environments. Partners Universal International Research Journal, 2(1), 24–34. https://doi.org/10.5281/zenodo.7723187

[24] Verizon Business. (n.d.). Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

[25] Dr. A.SHAJI GEORGE, & A.S.HOVAN GEORGE. (2021). Serverless Computing: the Next Stage in Cloud Computing's Evolution and an Empowerment of a New Generation of Developers. International Journal of All Research Education and Scientific Methods (IJARESM), 9(4), 21–35. https://doi.org/10.5281/zenodo.7027409

[26] What is a Cloud Security Audit? (2025, May 16). wiz.io. https://www.wiz.io/academy/cloud-security/cloud-security-audits

[27] George, Baskar, D. T., & Balaji, P. (2025). Bridging the Security Skills Gap: A Comprehensive Framework for Developing Application Security Competencies in Modern Software Engineering. Partners Universal Innovative Research Publication, 3(3), 96–123.

[28] CISA. (2023). Cloud Security Technical Reference Architecture, Version 2. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/resources-tools/resources/cloud-security-technical-reference-architecture

[29] Abdulla, S. (2026). IAM (identity and access management) is the core security control in cloud environments. International Journal of Science and Research (IJSR), 1747-1752. https://doi.org/10.21275/sr26129224021

[30] Chang, V., Walters, R. J., & Wills, G. B. (2015). Cloud computing and frameworks for organisational cloud adoption. Advances in Systems Analysis, Software Engineering, and High Performance Computing. https://doi.org/10.4018/978-1-4666-8210-8.ch001

[31] Chenkang Tang, Kumar, V., & Chaisiri, S. (2017). Understanding software-defined perimeter. Data Security in Cloud Computing. https://doi.org/10.1049/pbse007e_ch7

[32] Khan, N., & Al-Yasiri, A. (2018). Cloud security threats and techniques to strengthen cloud computing adoption framework. Cyber Security and Threats. https://doi.org/10.4018/978-1-5225-5634-3.ch016

[33] Smith, C. B. (2023). The semantic attack surface: A systems-dynamic model of narrative in cyberspace. IEEE Transactions on Technology and Society, 4(2), 146-157. https://doi.org/10.1109/tts.2022.3210782

[34] Tatineni, S. (2023). Ai-infused threat detection and incident response in cloud security. International Journal of Science and Research (IJSR), 12(11), 998-1004. https://doi.org/10.21275/sr231113063646

[35] Yousif, M. (2015). In pursuit of disciplined execution. IEEE Cloud Computing, 2(5), 4-5. https://doi.org/10.1109/mcc.2015.94

[36] (2021). CHAPTER 9 CLOUD SECURITY AND PRIVACY: FLAWS, ATTACKS, AND IMPACT ASSESSMENTS. Empirical Cloud Security. https://doi.org/10.1515/9781683926849-012

[37] (2023). DISINFORMATION SUPPORTED BY ARTIFICIAL INTELLIGENCE FROM DYNAMIC RESEARCH TO HOLISTIC SOLUTIONS. PUBLIC SECURITY AND PUBLIC ORDER, 35(2024). https://doi.org/10.13165/pspo-24-35-02

[38] (2024). Cloud adoption. Conference of European Statisticians Statistical Standards and Studies. https://doi.org/10.18356/9789213587256c006

[39] Al-Karaki, J. N. (2025). Defense in depth: A multilayered approach. Defense in Depth, 51-72. https://doi.org/10.1002/9781394340750.ch3

[40] Daswani, N., & Elbayadi, M. (2021). The capital one breach. Big Breaches. https://doi.org/10.1007/978-1-4842-6655-7_2
[41] Kudrati, A., & Pillai, B. (2022). Zero trust architecture components. Zero Trust Journey Across the Digital Estate. https://doi.org/10.1201/9781003225096-8
[42] Meli, M., McNiece, M. R., & Reaves, B. (2019). How bad can it git? characterizing secret leakage in public github repositories. Proceedings 2019 Network and Distributed System Security Symposium. https://doi.org/10.14722/ndss.2019.23418
[43] Samani, R., Honan, B., & Reavis, J. (2015). The cloud threat landscape. CSA Guide to Cloud Computing. https://doi.org/10.1016/b978-0-12-420125-5.00003-0
[44] Shackelford, A. (2015). Getting started with amazon web services. Beginning Amazon Web Services with Node.js. https://doi.org/10.1007/978-1-4842-0653-9_1
[45] Weik, M. H. (2000). Least privilege principle. Computer Science and Communications Dictionary. https://doi.org/10.1007/1-4020-0613-6_10052
[46] (2019). Overview of google cloud platform. Google Cloud Certified Associate Cloud Engineer Study Guide. https://doi.org/10.1002/9781119564409.ch1
[47] (2021). IBM: 2021 x-force threat intelligence index. Network Security, 2021(3), 4-4. https://doi.org/10.1016/s1353-4858(21)00026-x
[48] Abdulla, S. (2026). IAM (identity and access management) is the core security control in cloud environments. International Journal of Science and Research (IJSR), 1747-1752. https://doi.org/10.21275/sr26129224021
[49] Ahmad, S., Mehfuz, S., & Beg, J. (2021). Enhancing security of cloud platform with cloud access security broker. Lecture Notes in Networks and Systems. https://doi.org/10.1007/978-981-16-0882-7_27
[50] Bhoyar, N. (2025). Introduction to identity and access management. Identity Analytics. https://doi.org/10.1007/979-8-8688-1745-8_1
[51] Ganachari, G. (2023). Secure authentication and authorization frameworks for aws cloud services: Evaluating iam, cognito, and third-party solutions. Journal of Artificial Intelligence & Cloud Computing, 1-3. https://doi.org/10.47363/jaicc/2023(2)e140
[52] Gudhka, V. (2025). The evolution of secure access service edge in the digital landscape: Comprehensive literature review. 2025 IEEE International Carnahan Conference on Security Technology (ICCST). https://doi.org/10.1109/iccst63435.2025.11295250
[53] Gunnam, V., & Kilaru, N. B. (2024). Securing pci data: Cloud security best practices and innovations. Securing Pci Data: Cloud Security Best Practices And Innovations. https://doi.org/10.53555/nveo.v8i3.5760
[54] Hu, V. C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R., & Scarfone, K. (2014). Guide to attribute based access control (ABAC) definition and considerations. https://doi.org/10.6028/nist.sp.800-162
[55] Islam, M. N., Colomo-Palacios, R., & Chockalingam, S. (2021). Secure access service edge: A multivocal literature review. 2021 21st International Conference on Computational Science and Its Applications (ICCSA). https://doi.org/10.1109/iccsa54496.2021.00034
[56] Kesavulu, M., Helfert, M., & Bezbradica, M. (2017). A usage-based data extraction framework for cloud-based application - an human-computer interaction approach. Proceedings of the International Conference on Computer-Human Interaction Research and Applications. https://doi.org/10.5220/0006512700850092
[57] Khalil, I., Dou, Z., & Khreishah, A. (2016). Your credentials are compromised, do not panic. Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. https://doi.org/10.1145/2897845.2897925
[58] Kiviharju, M. (2014). RBAC with ABS - implementation practicalities for RBAC integrity policies. Proceedings of the 11th International Conference on Security and Cryptography. https://doi.org/10.5220/0005122105000509
[59] Mallmann, G., Pinto, A. D. V., & Maçada, A. C. (2019). Shedding light on shadow IT: Definition, related concepts, and consequences. Lecture Notes in Information Systems and Organisation. https://doi.org/10.1007/978-3-030-14850-8_5
[60] Mastrogiacomo, R. (2025). Security controls and countermeasures for AI identities. AI Identities. https://doi.org/10.1007/979-8-8688-2034-2_22
[61] Mistri, P. (2022). Cloud security audit: A necessity in the cloud computing environment. The Management Accountant Journal, 64-67. https://doi.org/10.33516/maj.v57i7.64-67p

[62] Sumathi, K., & Aruljothi, D. A. (2025). Enhanced privileged access management with identity access management to improve the user's safety measures in online circumstances. Communications on Applied Nonlinear Analysis. https://doi.org/10.52783/cana.v32.3628
[63] Wang, H., Ding, W., & Xia, Z. (2012). A cloud-pattern based network traffic analysis platform for passive measurement. 2012 International Conference on Cloud and Service Computing. https://doi.org/10.1109/csc.2012.8
[64] (2017). Risk assessment process. Risk Thinking for Cloud-Based Application Services. https://doi.org/10.1201/9781315268835-29
[65] Ambiel, S. (2024). The case for confidential computing: Delivering business value through protected, confidential data processing. https://doi.org/10.70828/iynl6589
[66] Bertocci, V., & Campbell, B. (2023). Oauth 2.0 step up authentication challenge protocol. https://doi.org/10.17487/rfc9470
[67] Campbell, B., Mortimore, C., Jones, M., & Goland, Y. (2015). Assertion framework for oauth 2.0 client authentication and authorization grants. https://doi.org/10.17487/rfc7521
[68] Cholkar, P., & Patel, M. (2023). Introduction: Cloud storage security and homomorphic encryption in cloud computing. International Journal of Science and Research (IJSR), 12(10), 1816-1822. https://doi.org/10.21275/sr231017115439
[69] Johansson, L., & Cantor, S. (2018). The entity category security assertion markup language (SAML) attribute types. https://doi.org/10.17487/rfc8409
[70] Katz, J. (2026). Key management and the public-key revolution – solutions. Introduction to Modern Cryptography, Revised Third Edition. https://doi.org/10.1201/9781003776994-11
[71] Martínez, J., & Durán, J. M. (2021). Software supply chain attacks, a threat to global cybersecurity: Solarwinds' case study. International Journal of Safety and Security Engineering, 11(5), 537-545. https://doi.org/10.18280/ijsse.110505
[72] Moriarty, K., & Farrell, S. (2021). Deprecating TLS 1.0 and TLS 1.1. https://doi.org/10.17487/rfc8996
[73] Nikhil Sagar Miriyala (2025). Comparative review of AWS and azure confidential computing systems. Journal of Information Systems Engineering and Management, 10(12s), 257-268. https://doi.org/10.52783/jisem.v10i12s.1805
[74] Ramos Brandão, P. (2018). The importance of authentication and encryption in cloud computing framework security. International Journal on Data Science and Technology, 4(1), 1. https://doi.org/10.11648/j.ijdst.20180401.11
[75] Ravikumar, S. (2025). SSO protocols: SAML vs. oauth2 vs. openid connect - comparative security analysis. International Scientific Journal of Engineering and Management, 04(06), 1-8. https://doi.org/10.55041/isjem04627
[76] Rosenberg, M., White, J., Garman, C., & Miers, I. (2023). Zk-creds: Flexible anonymous credentials from zksnarks and existing identity infrastructure. 2023 IEEE Symposium on Security and Privacy (SP). https://doi.org/10.1109/sp46215.2023.10179430
[77] Ryu, H. J., & Lee, S. (2023). Design and implementation of a document encryption convergence program selecting encryption methods, and integrating the program into the existing office system. Proceedings of the 12th International Conference on Data Science, Technology and Applications. https://doi.org/10.5220/0012124000003541
[78] Wilson, Y., & Hingnikar, A. (2019). SAML 2.0. Solving Identity Management in Modern Applications. https://doi.org/10.1007/978-1-4842-5095-2_7
[79] (2017). Federation, presence, identity, and privacy in the cloud. Cloud Computing. https://doi.org/10.1201/9781439806814-6
[80] Ćurguz, J. (2016). Vulnerabilities of the SSL/TLS protocol. Computer Science & Information Technology (CS & IT). https://doi.org/10.5121/csit.2016.60620
[81] Basu, S., Sengupta, A., & Mazumdar, C. (2017). A quantitative methodology for cloud security risk assessment. Proceedings of the 7th International Conference on Cloud Computing and Services Science. https://doi.org/10.5220/0006294401200131
[82] Chowdhary, A., & Sabur, A. (2025). Security automation: AI and ML in cloud security. Cloud Security. https://doi.org/10.1201/9781003384496-7
[83] Fuehne, D., & Lattin, R. (2021). Annual performance testing of tracer gas and tracer aerosol detectors for use in radionuclide NESHAP compliance testing. https://doi.org/10.2172/1766953
[84] Garg, P. (2025). Cloud security posture management: Tools and techniques. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5357921

[85] Ojo, A. O., & Benmubarak, M. (2025). Investigating advanced persistent threat tactics in cloud environments: A forensic study of AWS cloudtrail log data. International Journal of Innovative Science and Research Technology. https://doi.org/10.38124/ijisrt/25jul1786

[86] Patel, A. (2025). Infrastructure as code (iac) for advanced security automation. Implementing Security with AI in GCP. https://doi.org/10.1007/979-8-8688-2213-1_9

[87] Ramya Deevi, S. (2022). Devsecops in the hybrid cloud: Best practices for end-to-end security integration. International Journal of Science and Research (IJSR), 1303-1307. https://doi.org/10.21275/sr220911050851

[88] Ruebsamen, T., Pulls, T., & Reich, C. (2015). Secure evidence collection and storage for cloud accountability audits. Proceedings of the 5th International Conference on Cloud Computing and Services Science. https://doi.org/10.5220/0005408403210330

[89] Sabbani, G. (2025). Enhancing cloud security and compliance through integrated GRC and IAM frameworks. Journal of Artificial Intelligence & Cloud Computing, 4(3), 4. https://doi.org/10.47363/jaicc/icaicc/2025(4)4

[90] Singh, H. (2025). Leveraging cloud security audits for identifying gaps and ensuring compliance with industry regulations. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5267898

[91] Somi, V. (2025). Automated resource management in AWS: A review of tagging strategies and config rules. International Journal For Multidisciplinary Research, 7(2). https://doi.org/10.36948/ijfmr.2025.v07i02.40639

[92] Sridharan, A., & Kanchana, V. (2022). SIEM integration with SOAR. 2022 International Conference on Futuristic Technologies (INCOFT). https://doi.org/10.1109/incoft55651.2022.10094537

[93] Wang, W., Sadjadi, S. M., & Rishe, N. (2024). A survey of major cybersecurity compliance frameworks. 2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity). https://doi.org/10.1109/bigdatasecurity62737.2024.00013

[94] Williams, J. (2019). Compliance with code and data policy. https://doi.org/10.5194/gmd-2019-195-ec1

[95] (2006). RELIABILITY IN AUTOMATED EVALUATION TOOLS FOR WEB ACCESSIBILITY STANDARDS COMPLIANCE. Issues In Information Systems. https://doi.org/10.48009/2_iis_2006_218-223

[96] (2021). IBM: Cost of a data breach report. Computer Fraud & Security, 2021(8), 4-4. https://doi.org/10.1016/s1361-3723(21)00082-8

[97] (2023). ISO 27001 REQUIREMENTS. ISO 27001/ISO 27002. https://doi.org/10.2307/jj.9039966.8

[98] D'Onofrio, D., Fusco, M., & Zhong, H. (2023). CI/CD pipeline and devsecops integration for security and load testing. https://doi.org/10.2172/2430395

[99] Madsen, T. (2023). Cloud and zero-trust. Zero-trust – An Introduction. https://doi.org/10.1201/9781003464587-5

[100] Noviyarto, H., Samopa, F., & Setiawan, B. (2025). Security audit process design based on SIEM and CSPM integration with design science research methodology approach. 2025 International Conference on Data Science and Its Applications (ICoDSA). https://doi.org/10.1109/icodsa67155.2025.11157488

[101] Ramesh Bishukarma (2023). Scalable zero-trust architectures for enhancing security in multi-cloud saas platforms. International Journal of Advanced Research in Science, Communication and Technology, 1308-1319. https://doi.org/10.48175/ijarsct-14000s

[102] Ramya Deevi, S. (2022). Devsecops in the hybrid cloud: Best practices for end-to-end security integration. International Journal of Science and Research (IJSR), 1303-1307. https://doi.org/10.21275/sr220911050851

[103] Reza Febriana, & Ahmad Luthfi (2023). Comparative study of cloud forensic investigation using ADAM and NIST 800-86 methods in private cloud computing. Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 7(5), 1097-1110. https://doi.org/10.29207/resti.v7i5.5279

[104] Soma, V. (2021). Threat detection and incident response in the cloud. International Journal of Science and Research (IJSR), 10(11), 1578-1581. https://doi.org/10.21275/sr24822145029

[105] Sullivan, C. (2015). Protecting digital identity in the cloud. The Cloud Security Ecosystem. https://doi.org/10.1016/b978-0-12-801595-7.00007-0

[106] Wilson, F., & Smith, B. (2006). Hall thruster system qualification provides major satellite benefits. 57th International Astronautical Congress. https://doi.org/10.2514/6.iac-06-c4.4.09

[107] (2012). - cloud security architecture (CSA). Cloud Enterprise Architecture. https://doi.org/10.1201/b13088-16

[108] (2022). Chapter 11 cloud-driven change management and learning. Cloud Governance. https://doi.org/10.1515/9783110755374-011

[109](2026). IAC systems security methodologies and approaches. Industrial Automation and Control System Security Principles, 147-215. https://doi.org/10.1002/9781394438273.ch6

[110]-, A. G. (2025). Application protection platforms (CNAPP) for healthcare: Safeguarding patient data in cloud infrastructure. International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences, 13(5). https://doi.org/10.37082/ijirmps.v13.i5.232622

[111]Ambiel, S. (2024). The case for confidential computing: Delivering business value through protected, confidential data processing. https://doi.org/10.70828/iynl6589

[112]Baba, S., & Kitazono, Y. (2025). Improving anomaly detection system accuracy using tadgan with flexhyperband. The Proceedings of The 13th IIAE International Conference on Industrial Application Engineering 2025. https://doi.org/10.12792/iciae2025.063

[113]Cesarano, C., & Natella, R. (2025). Kubefence: Security hardening of the kubernetes attack surface. 2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). https://doi.org/10.1109/dsn64029.2025.00054

[114]Janiszewska, A. (2013). Małżeństwa vs związki nieformalne w opiniach młodych mieszkańców łodzi. Space – Society – Economy, 185-211. https://doi.org/10.18778/1733-3180.12.11

[115]Jordan, S. (2026). Certified kubernetes security specialist (CKS) guide. https://doi.org/10.55277/researchhub.wktrc913

[116]Kaur, M., & Kaimal, A. B. (2023). Analysis of cloud computing security challenges and threats for resolving data breach issues. 2023 International Conference on Computer Communication and Informatics (ICCCI). https://doi.org/10.1109/iccci56745.2023.10128329

[117]Kim, H., & Yoo, S. (2018). Vulnerability analysis on kernel code and memory protection in nested kernel. Journal of KIISE, 45(9), 873-880. https://doi.org/10.5626/jok.2018.45.9.873

[118]McKay, M. (2012). Best practices in automation security. 2012 IEEE-IAS/PCA 54th Cement Industry Technical Conference. https://doi.org/10.1109/citcon.2012.6215678

[119]Michel, J., & Parren, P. (2025). Graph-based intelligent cyber threat detection system. Handbook of AI-Driven Threat Detection and Prevention. https://doi.org/10.1201/9781003521020-13

[120]Mohan, A., Ye, M., Franke, H., Srivatsa, M., Liu, Z., & Gonzalez, N. M. (2024). Securing AI inference in the cloud: Is CPU-GPU confidential computing ready?. 2024 IEEE 17th International Conference on Cloud Computing (CLOUD), 164-175. https://doi.org/10.1109/CLOUD62652.2024.00028

[121]Mulpuri, G. (2021). Container orchestration: Experiences with container orchestration platforms like docker swarm, kubernetes, and nomad, focusing on scalability and security improvements. International Journal of Science and Research (IJSR), 10(3), 1976-1978. https://doi.org/10.21275/sr24402110309

[122]Patra, M. K., Kumari, A., Sahoo, B., & Turuk, A. K. (2022). Docker security: Threat model and best practices to secure a docker container. 2022 IEEE 2nd International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC). https://doi.org/10.1109/isssc56467.2022.10051481

[123]T, P. P., & Kumar, C. (2021). Building cloud native application — analysis for multi-component application deployment. 2021 International Conference on Computer Communication and Informatics (ICCCI). https://doi.org/10.1109/iccci50826.2021.9402422

[124]Tambolkar, K., wavhal, P., & Sawant, K. (2025). Trends and challenges in cloud computing security — literature-based study. International Journal of Scientific Research in Engineering and Management. https://doi.org/10.55041/ijsrem54369

[125]Torrey, K. (2026). Cloudsec-pro: Palo alto networks cloud security professional certification. https://doi.org/10.55277/researchhub.dlclyu81

[126]Ul Haq, M. N., & Sharma, M. K. (2023). MASTERING CLOUD SECURITY: TECHNIQUES AND BEST PRACTICES. EMERGING TRENDS IN CLOUD SECURITY AND INTELLIGENT AGENTS. https://doi.org/10.52458/9788196869434.2023.eb.grf.ch-07

[127]You, M., Kim, J., & Shin, S. (2022). Revisiting security landscape of docker hub container images. The Journal of Korean Institute of Communications and Information Sciences, 47(8), 1231-1243. https://doi.org/10.7840/kics.2022.47.8.1231

[128](2025). Protecting your accounts with strong passwords and mfa. Cyber Defense, 51-66. https://doi.org/10.1002/9781394337040.ch04