IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 8, August 2025

DOI: 10.17148/IARJSET.2025.12846

Modern Cloud Security Threats and Vulnerabilities: A Comprehensive Review

Bhavana B R[1], Shashank R[2], Druva H P[3]

Assistant Professor, MCA, Surana College Autonomous, Bangalore, India[1]

Student, MCA, Surana College Autonomous, Bangalore, India[2]

Student, MCA, Surana College Autonomous, Bangalore, India[3]

Abstract: Cloud computing has revolutionized the provision of IT services via elastic models like Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). These models, though, come with an array of security threats that keep changing with technology. This review analyses and classifies widespread security attacks in the cloud service models—focusing on prevalent attacks like SQL injection in SaaS, unauthorized access in PaaS, and data breach in IaaS. It integrates current defence mechanisms, with a particular emphasis on machine learning methods and cryptographic mechanisms, and stresses the increasing importance of joint security efforts by cloud users and providers. Moreover, the paper summarizes actual cloud-based attack vectors in real life, categorizing them based on severity to facilitate risk prioritization. The assessment also discusses the specific challenges brought about by cloud integration into industrial SCADA systems, detailing their primary vulnerabilities and categorizing related threats into types such as hardware-level, protocol-based, and insider attacks. Lastly, it talks about changing trends and best practices and highlights the move from ad hoc security reactions to formal, risk-defined cloud security strategies.

Keywords: Cloud Security, Cloud Computing, Threats & Vulnerabilities (or "Cloud Threats"), Cloud Service Providers (CSPs), Cloud Deployment Models (SaaS, PaaS, IaaS), Zero Trust Architecture (ZTA)

I. INTRODUCTION

Cloud computing (CC) has evolved since the mid-1990s, with AWS and Alibaba being some of the prime movers shaping its trajectory [7]. In the view of NIST, it is an on-demand model of provision for network access to shared computer resources, CC offers economies on scalability and does not demand substantial investment in infrastructure. Its service models—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—are adaptable, but raise serious security and privacy of data concerns [7]. CC offers users access to computing power, storage, and applications via the internet, paying only for their use [8]. Cloud deployment models such as public, private, hybrid, and community clouds offer various levels of control and customization. With lower cost and dynamic scalability for organizations, maintaining data confidentiality, integrity, and availability are still pertinent concerns [8]. Over the last decade, adoption of CC has grown exponentially, especially with small and medium enterprises, due to its pay-per-use model [13]. Virtualized systems are under risk of data loss, unauthorized entry, and interruption of services. Anomaly detection, intrusion prevention, and system robustness have been offered by machine learning solutions [13].

Threats including distributed denial-of-service (DDoS) attacks and advanced malware continue to be major challenges [14]. Cyber attackers use cloud-connected networks to facilitate large attacks, often employing complex, mixed-malware strategies. Deep learning technologies enhance malware discovery by automatically recognizing unknown and evolving threats, enabling cloud providers to respond in a proactive way and strengthen overall security [14]. In addition, unsecured application programming interfaces (APIs) and misconfigurations continue to be leading causes of cloud breaches. As APIs are critical to linking services and applications together, bugs within their configuration or design can place sensitive information at the mercy of unauthorized actors. Studies highlight that insecurely protected . APIs, in conjunction with lax identity and access controls, open up account hijacking and privilege escalation attacks [10]. Equally, cloud misconfigurations like errant firewall configurations or lax access policies have been reported to cause most data exposures in recent years, necessitating serious compliance monitoring and auditing [11].

Insider threats and supply chain weaknesses also muddy the security waters. Legitimate insiders can misuse their access, either maliciously or inadvertently, causing drastic data leaks. This challenge is compounded in multi-tenant spaces where multiple users share infrastructure [12]. Meanwhile, breached third-party services that are incorporated in cloud workflows become supply chain attack vectors, affecting numerous organizations at once. To solve these challenges, experts recommend implementing Zero Trust models, micro-segmentation, and constant monitoring strategies that are in

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 8, August 2025

DOI: 10.17148/IARJSET.2025.12846

harmony with the distributed and dynamic nature of the cloud [4][9]. The authors intend to make particular attacks in each of the three models of cloud services: SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). For instance, they quote SQL injection in SaaS, unauthorized access in PaaS, and data breaches in IaaS. The paper offers cloud security threat solutions, such as machine learning and cryptographic-based solutions. It further recommends that collaboration between users and Cloud Service Providers (CSPs) is crucial to deal with the evolving threats and create normative cloud security practices. The study attempts to revisit real cloud-based attack vectors and rank them according to security severity score. This enables organizations to prioritize their defenses based on the impact and occurrence of various threats. The paper highlights security concerns in SCADA systems (Supervisory Control and Data Acquisition), especially their exposure when networked with cloud services. It classifies attacks on such systems and proposes targeted solutions to make them more secure against cloud-based cyber attacks

II. RELATED WORKS

Cloud computing provides elastic and cost-effective services through SaaS, PaaS, and IaaS models, but each has its own set of security challenges. In SaaS, application data can be compromised by SQL injection attacks, and in PaaS platforms, there can be unauthorized access through insecure APIs and misconfigured services. IaaS environments are most susceptible to data leakage through shared virtualized infrastructures [4]. In order to counter these threats, solutions that include machine learning-based intrusion detection and cryptographic protection have been suggested, highlighting that collaboration between Cloud Service Providers (CSPs) and customers is critical to ensure effective defence and security protocol standardization. Moreover, new attack vectors like ransomware-as-a-service and API exploitation have been recognized as emerging threats, necessitating periodic updates to prevention and detection measures [10]. Refer Table I

Prioritizing Threats Through Risk Scoring

Efficient cloud security involves not only the identification but also prioritization of vulnerabilities in terms of the likelihood and potential impact. Risk scoring models offer organizations a systematic means to distribute resources in an optimal manner by ordering threats like misconfigurations, data breaches, insider attacks, and insecure APIs on the basis of severity. For example, Gaikwad and Patil [21] are explicit that risks such as privileged access, lacking due diligence, and compliance gaps need to be ranked higher due to cascading impact throughout cloud ecosystems. Likewise, Shaffi et al. [22] point out that AI-powered analytics can boost risk scoring by identifying anomalies in real-time and updating threat levels continuously. This blend of adaptive intelligence and structured scoring makes it possible for cloud service providers (CSPs) and organizations to concentrate defence efforts on the most important vulnerabilities, instead of spreading resources uniformly across all threats.

Virtualization and Security Services

An important part of cloud infrastructure is virtualization, which supports multi-tenancy and effective resource sharing but also presents novel attack surfaces. To ensure availability, confidentiality, integrity, and authentication, CSPs employ a range of security services [9]. They include availability protection through redundancy and overload management, encryption mechanisms like SEAL, RC4, RC5, and IDEA, integrity checks utilizing MD5, SHA-1, and Tiger, and authentication schemes like HMAC-MD5 and CBC-MAC-AES. The deployment of these mechanisms varies with the sensitivity of user data and service-level agreements. Current literature also points to containerization-based threats like privilege escalation and insecure orchestration settings, recommending tighter isolation mechanisms for cloud-native deployments [10].

Obfuscation, Diversification, and Workflow Security

Paper [9] also addresses advanced confidentiality preservation techniques, such as data obfuscation (client-side encryption, partitioning, or noise injection), execution environment diversification (constantly switching between servers, hypervisors, and OS), logic obfuscation (dividing workflows into nodes that observe only partial processes), and information flow checking (auditing intra- and inter-service leakages). On the administrative end, secure cloud workflows are facilitated by modelling and execution tools, workflow management systems (centralized, distributed, or engine-less), and security-aware service selection with regard to confidentiality, reliability, and trust metrics. Embedding AI-based orchestration into these workflows can adapt configurations dynamically according to the threats identified [10].

Integration of AI in Cloud Security

Evolutionary studies emphasize the incorporation of Artificial Intelligence (AI) and Machine Learning (ML) into cloud security models [11]. AI-based systems can track, identify, and react to threats in real time, strongly enhancing defence against zero-day attacks and advanced persistent threats. AI also enables adaptive authentication, anomaly-based detection in user activity, and cognitive resource allocation that can proactively isolate suspicious behaviour without

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 8, August 2025

DOI: 10.17148/IARJSET.2025.12846

hindering legitimate services. Research also emphasizes that AI models need to be trained with diverse data sets so as not to include biases and ensure adversarial AI attack resilience [10].

Misconfiguration & Data Breaches

Cloud misconfiguration is still one of the most prevalent and perilous threats. Research identifies that improper security group configurations, poor identity settings, and overly permissive storage buckets frequently make sensitive data available to the public [5]. Misconfigurations in APIs or virtualization layers can enable attackers to escalate privilege and obtain unauthorized access to key systems [11]. Researchers believe that as cloud environments are extremely dynamic, ongoing auditing and automation are imperative to avoid misconfiguration-based breaches [13].Data breaches are the most serious threat since they compromise confidentiality, integrity, and trust. [6] explains that breaches are common as a result of poor access control and poor encryption in multi-tenancy environments. Paper [10] observes attackers targeting weaknesses in SaaS and PaaS applications to steal huge amounts of sensitive data, causing monetary and reputational losses. Precautionary steps like client-side encryption, diversification of storage, and obfuscation measures are advisable to minimize risks [9].

Account Hijacking & Insider Threats

Account and service hijacking is on the rise, whereby attackers utilize stolen credentials, phishing, or malware to masquerade as bona fide users. Paper [11] emphasizes that privileged account abuse can hugely impact organizations because of escalated access rights. Poor authentication controls and session hijacking also leave cloud accounts vulnerable to compromise [7]. Multifactor authentication, stringent session monitoring, and AI-based anomaly detection are essential measures for preventing account hijacking [13].Insider attacks are particularly significant in cloud computing as administrators or employees usually possess privileged access to infrastructure. Malicious insiders can exfiltrate confidential data, compromise resources, or purposefully misconfigure systems [11]. Papers [6] and [13] point out that insider attacks are hard to identify because of their legitimate credentials. Solutions proposed are micro-segmentation, continuous monitoring, and least privilege enforcement [9].

Insecure APIs & Denial of Service (DoS) Attacks

Cloud platforms are dependent on APIs for integration and automation, but insecure APIs pose threats in the form of leakage of data, replay attacks, and unauthorized access. [11] is responsible for explaining how weak authentication tokens and inadequate logging make APIs an attractive target for attackers. Paper [9] describes how security-conscious workflows and obfuscation techniques can minimize exposure. In addition to this, API gateway security and strong policy enforcement are advised to keep risks at a minimum [6].Cloud platforms are extremely susceptible to Distributed Denial of Service (DDoS) attacks that flood resources and lead to outages in services. Paper [14] elaborates on the manner in which DDoS attacks critically impact availability within cloud-based systems. Conventional firewalls and static protections prove ineffective in many cases, necessitating AI-driven anomaly detection and automated traffic blocking. The use of redundancy and overload defence techniques has been found to enhance resilience to DoS attacks [9].

Malware Injection

Malware injection is an emerging threat, wherein attackers inject malicious code or virtual machine instances into cloud infrastructure. As detailed in [14], advanced malware uses strong obfuscation, polymorphism, and packing techniques in order to evade signature-based detection. Cloud environments are specially appealing to attackers because injected malware spreads easily over multi-tenant infrastructure. Use of deep learning and anomaly-based detection is stressed to address advanced malware [14].

TABLE I: RELATED WORKS

Paper	Title	Main Focus	Key Threats & Vulnerabilities	Proposed Solutions
paper-[1].pdf	A Comprehensive Survey on Security Threats and Challenges in Cloud Computing Models (SaaS, PaaS and IaaS)	Examines security challenges and attacks across SaaS, PaaS, and IaaS cloud models.	SQL injection, deceitful QR code attacks (SaaS), unauthorized access (PaaS), and data breaches (IaaS).	Proposes solutions such as the Multi-Perspective PaaS Security Model, and emphasizes shared responsibility.
paper-[2].pdf	Cloud Security and Security Challenges Revisited	Revisit attacks and attack vectors on cloud services and ranks them by severity.	Malicious insider, distributed denial-of-service (DDoS), data	Discusses successful and proposed solutions for security professionals to

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 8, August 2025

DOI: 10.17148/IARJSET.2025.12846

			leakage, and attacks on virtualization layers.	prioritize their efforts.
paper-[3].pdf	A Survey of Security Challenges in Cloud-Based SCADA Systems	Surveys cybersecurity vulnerabilities and attacks facing cloud-based Supervisory Control and Data Acquisition (SCADA) systems.	Connectivity with cloud services, shared infrastructure, malicious insiders, and security of SCADA protocols. Attacks are categorized into hardware, software,	Proposes security solutions and highlights the need for a comprehensive approach.
paper-[4].pdf	A Critical Analysis of Foundations, Challenges, and Directions for Zero Trust Security in Cloud Environments	Analyses the core principles, controversies, and barriers of Zero Trust Security (ZTS) in cloud computing.	Scalability issues, high cost, integration problems with existing systems, and compliance to legal requirements.	Highlights that ZTS can decrease security incidents by up to 40% but may decrease operational efficiency and require major upfront investment.
paper-[5].pdf	A Survey on Modern Cloud Computing Security over Smart City Networks: Threats, Vulnerabilities, Consequences, Countermeasures, and Challenges	Surveys cloud security over smart city networks.	Threats, vulnerabilities, and consequences related to cloud computing in a smart city context.	Presents countermeasures and addresses challenges.
paper-[6].pdf	An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions	Examines and compares cloud security frameworks, including COBIT5, NIST, ISO, CSA STAR, and AWS well-architected framework.	Identifies prevalent cloud security threats like data breaches, unauthorized access, and misconfigurations.	Discusses solutions and helps in selecting and implementing suitable security measures.
paper-[7].pdf	Data Security Challenges and Solutions in Cloud Computing: Critical Review	Provides a critical review of recent studies on data security in cloud computing.	Data leakage, data remoteness, privacy, and data segregation.	Proposes practical strategies like standards and models, and technologies.
paper-[8].pdf & paper-[16].pdf	A Review of Machine Learning-based Security in Cloud Computing	Explores the use of Machine Learning (ML) to address security risks in cloud computing.	Threats to availability, integrity, and confidentiality.	Examines the features and effectiveness of various ML algorithms for identifying and resolving security issues.
paper-[10].pdf	Security Challenges and Solutions in Cloud-Based Software Systems	Focuses on security threats and challenges in cloud-based software systems.	Data breaches, insecure APIs, shared technology vulnerabilities in a multi-tenant environment, insider threats, ransomware, container vulnerabilities, and supply chain attacks.	Recommends strong security practices like encryption, Identity and Access Management (IAM), and continuous monitoring.
paper-[11].pdf & paper-[19].pdf	Cloud computing threats and risks: uncertainty and uncontrollability in the risk society	Discusses cloud computing threats and risks	Uncertainty and un-controllability due to the complexity of the domain.	Aims to analyse the threats and risks in a constantly progressing digital environment.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 8, August 2025

DOI: 10.17148/IARJSET.2025.12846

paper-[12].pdf	Emerging Challenges in Cloud Computing Security: A Comprehensive Review	A comprehensive review exploring emerging security challenges in cloud computing.	Data breaches, insider attacks, insecure APIs, and shared vulnerabilities.	Provides insights into mitigation strategies to safeguard sensitive information.
paper-[13].pdf	Cloud Security Challenges and Solutions: A Review of Current Best Practices	Provides an overview of challenges and solutions in cloud security.	Data breaches, unauthorized access, compliance issues, and the dynamic nature of cloud environments.	Explores current best practices to mitigate risks.
paper-[14].pdf	Enhancing cloud security through the integration of deep learning and data mining techniques: A comprehensive review	Reviews cloud-based malware detection technologies.	The rise of sophisticated malware that uses complex jamming and packing methods.	Proposes integrating deep learning and data mining techniques for malware detection in the cloud.
paper-[17].pdf & paper-[22].pdf	Al-Driven Security in Cloud Computing: Enhancing Threat Detection, Automated Response, and Cyber Resilience	Discusses the use of AI to enhance cloud security.	Complex threats that traditional solutions cannot handle in real-time.	Recommends using AI-powered solutions for threat detection.

III. CLOUD SECURITY &CHALLENGES

IAM Complexity & Lack of Visibility

Identity and Access Management (IAM) is the foundation of cloud security, where access to sensitive resources is only granted to authorized users. IAM management across hybrid and distributed cloud environments introduces complexity. Role and permission misconfigurations tend to result in privilege escalation risk or unauthorized access [10]. Papers point out that the implementation of Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) aids principle-of-least-privilege enforcement in principle, yet enterprises continue to struggle with scalability and management of dynamic user roles in large businesses [11]. Refer Fig. 1. This poses operational overhead and renders IAM one of the most frequently mentioned cloud adoption pain points. Cloud users do not have constant, direct access to the underlying infrastructure, and thus visibility into data flows, configurations, and monitoring is lessened. This "blind spot" hinders the ability to find malicious actions, unauthorized modifications, or even compliance violations [12]. With multi-tenant environments noted in the literature as additionally making monitoring more complicated because logs and telemetry are spread among a variety of services [13]. Advanced logging tools and Security Information and Event Management (SIEM) products are suggested, but research indicates they need major customization to work in rapidly changing cloud environments [10].

Multi-Cloud Environments & Compliance Challenges

Increased adoption of multi-cloud strategies, by which organizations spread workloads across AWS, Azure, Google Cloud, and on-premises infrastructures, offers flexibility but creates fragmentation in security controls. Each provider has distinctive security tools, so standard monitoring and enforcement are challenging [9]. Papers point out that this fragmentation tends to cause configuration inconsistencies and redundant security efforts, raising the likelihood of misconfigurations and breaches [11]. Researchers posit that centralized policy orchestration and cloud-agnostic security frameworks are critical to mitigate these issues [13].Cloud adoption necessitates compliance with global compliance frameworks like GDPR, HIPAA, and ISO standards. A significant problem is that cloud hosts can host data across borders, introducing legal ambiguity for buyers [12]. Numerous reports discuss how challenging it is to audit cloud workflow, particularly when hosts only provide limited insight into their internal controls [9]. Organizations tend to rely on third-party certifications, but literature is cautious that over-reliance on such certifications might create a mirage of security [10]. Ongoing compliance monitoring with the help of cloud-native tools is proposed as a long-term solution.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 8, August 2025

DOI: 10.17148/IARJSET.2025.12846

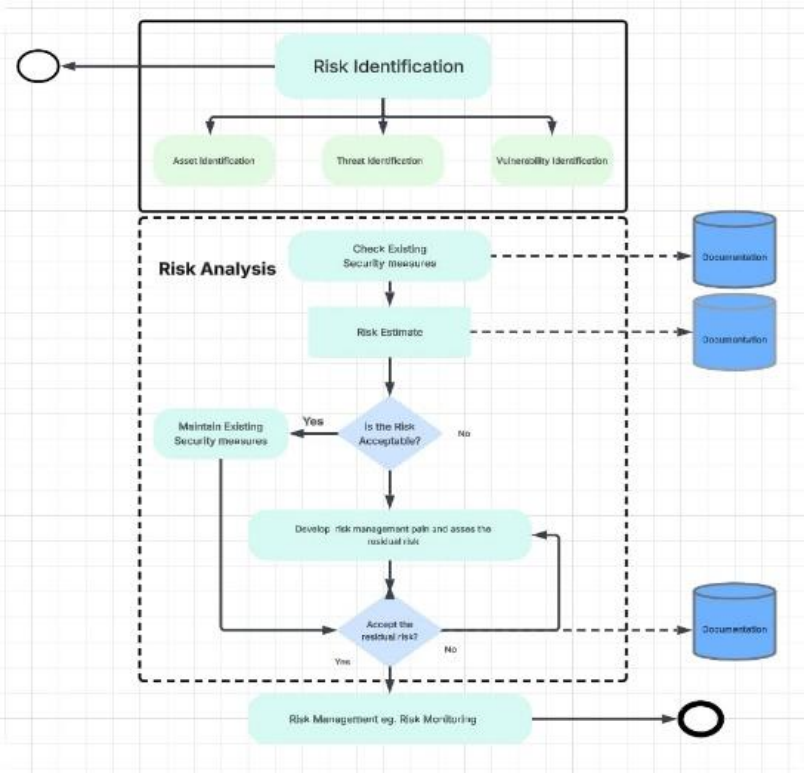

Fig. 1

Security Challenges and Mitigation in Cloud Computing

The swift development of cloud computing, fuelled by the progress in the Fourth Industrial Revolution, has brought with it a plethora of intricate security issues [19]. Studies identify common vulnerabilities such as cloud misconfigurations, data exposure, and insider threats, with the economic cost of data breaches in cloud computing being comparatively high [15]. The shared responsibility model of security is a very important but usually complicated feature of cloud platforms, with need for precise definitions between users and vendors of cloud [15, 17]. In response to such issues, artificial intelligence (AI) and machine learning (ML) are being used more and more to improve the detection of threats, automate response, and make systems more cyber resilient, providing a means of processing large volumes of data and generating high-accuracy predictions with limited human interaction [22, 16]. Although cloud services have much to offer in terms of benefits such as scalability and affordability for most ML applications, real-time applications like autonomous driving require the use of fog computing to reduce latency and to safeguard sensitive information from public network transmissions [17].

Data Residency Concerns

Residency and sovereignty of data are key concerns given the trend of organizations operating in various regions. Cloud vendors replicate and transfer data for redundancy, at times crossing borders without clear user perception [12]. Research identifies that this presents risks of non-compliance with data protection legislation, particularly in sensitive industries such as health and finance [9]. Researchers suggest that customers secure explicit data locality terms in Service-Level Agreements (SLAs) and use encryption with locally controlled keys to have control [11].

IV. DISCUSSION & FUTURE TRENDS

Changing threat landscape (AI-based threats, quantum age readiness)

Cloud security is reaching a point where attackers more and more weaponize AI to automate reconnaissance, create highly sophisticated phishing, bypass anomaly detectors, and test multi-tenant boundaries at scale. Meanwhile, defenders are implementing AI/ML for behaviour analytics, adaptive authentication, and real-time threat hunting—yet these systems themselves become attack targets for data poisoning, model evasion, and API abuse. Existing work in your community has already established AI as a force multiplier for real-time monitoring and response in cloud environments, looking forward to increasingly autonomous control loops that minimize detection and containment times; continuing that arc, the near-term research imperative is sound ML governance (data lineage, drift detection, red-teaming of models) and "secure-by-design" telemetry pipes to stop biased or spoofed inputs from spilling over into access decisions.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 8, August 2025

DOI: 10.17148/IARJSET.2025.12846

Concurrently, quantum advancements put pressure on today's cryptography lifecycles: notwithstanding the absence of large-scale cryptanalytic capability, wise cloud programs must initiate crypto-agility planning (algorithm/key inventory, phased conversion to NIST-post-quantum contenders, hybrid key exchange) so that data with long confidentiality time horizons stay secure if reaped today and decrypted tomorrow. These paths are consistent with your sources' focus on AI-enabled detection and standards-enforced controls but require overtly stated adversarial-ML and crypto-agility roadmaps as future action. [11], [6].

Zero-Trust Architecture (ZTA)

Zero Trust redefines cloud defense in terms of continuous verification authenticating and authorizing each user, device, and workload for each request, enforcing least privilege, and segmenting laterally to limit blast radius. Your references emphasize micro-segmentation, adaptive access, and continuous monitoring as foundation capabilities, what that translates to as proactive practice is the convergence of identity signals (user, service, workload identities), enforcing Just-In-Time and Just-Enough-Access on privileged operations, and moving policy evaluation alongside the resource (sidecars, service mesh) so access is context-aware and revocable in real time. Future directions consist of risk-adaptive policies that combine device posture, behavioural baselines, data sensitivity, and runtime workload attestation, along with automated validation to maintain ZTA guardrails in place with rapid moving pipelines. [4], [10], [11]. Refer Table II

SASE (Secure Access Service Edge

SASE unites networking and security in the cloud—integrating SD-WAN, secure web gateway, CASB, ZTNA, and firewall-as-a-service—so users, devices, and workloads are policy-consistent in protection wherever they are. For cloud applications, SASE brings Zero Trust to life at the edge: identities become the perimeter, traffic is examined within the provider fabric, and access is brokered through points of presence in the cloud to minimize attack surface and gain visibility. In the future, the most effective thread is closer integration of SASE with identity/attribute stores, data classification engines, and runtime workload identities, so policies follow data and services from SaaS, PaaS, to IaaS. More posture-aware access (device, app, and workload signals), deterministic routing to in-region PoPs to align for data residency, and ongoing checks of third-party SaaS through CASB controls. These guidelines complete your sources' focus on identity-based controls and standardized frameworks that regulate access and data protection. [4], [6], [10]

Automation for cloud security

The speed at which cloud deployments scale and happen renders manual security strategies infeasible. The long-term solution is automation, under which proactive and reactive security defend continuously in a closed-loop cycle. Among these preventive measures are codifying guardrails as policy-as-code and enacting pre-merge or pre-deployment checks on infrastructure, identity, and data policies [10]. Detection is reinforced by normalizing telemetry from APIs, control planes, workloads, and user identities and then using AI-powered analytics to create behavioural baselines for every tenant or cluster [9]. Such baselines enable quick recognition of deviations like insider abuse, insecure API calls, or misconfigurations [22]. During the response phase, remediation mechanisms in automation can quarantine infected accounts or instances, revoke tokens, rotate keys, and reconfigure networks with minimal downtime. Research emphasizes preserving human control for high-impact decisions, and low-risk processes can be automated fully to speed recovery and keep operational burden low [11] [18]. Recovery continues into proactive resilience testing, where chaos-engineering and failure-injection ensure that incident response playbooks still function under real-world stress [21].

In the future, research highlights intent-based security orchestration, with organizations specifying desired secure states and automated mechanisms that monitor continuously for drift from those baselines [19]. Inherent cloud controls like Guard Duty, IAM scanners, and policy engines embedded within are predicted to integrate into DevOps and platform engineering pipelines, so new environments are automatically provisioned with encryption defaults, identity segmentation, and monitoring hooks [20]. This intersection of automation, orchestration, and AI-driven analytics is an indicator toward cloud ecosystems that are not merely secured, but self-repairing and resilient to changing threats [21] [22].

Global security standards

Non-uniform provider controls and fragmented regulations are still points of friction, especially in multi-cloud and cross-border data flows. Your sources list prominent frameworks (NIST, ISO/IEC 27017, CIS, CSA STAR, FedRAMP) and their complementary functions; future development depends on harmonization (mappings and mutual recognition) and implementation (control libraries as reusable building blocks in code). Two tangible steps to take: (1) standardized schemas of evidence and automated attest ability. (collect-once, attest-many) to lower audit drudgery among providers; (2) express inclusion of post-quantum cryptography, software supply-chain assurance (SBOMs, provenance attestation), and AI system verifiability (data governance, model transparency, adversarial testing) in baseline control sets. A single, machine-readable control ontology that maps to provider-native policy would allow organizations to state one policy and

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 8, August 2025

DOI: 10.17148/IARJSET.2025.12846

compile it to enforcement primitives for each cloud—translating standards from PDFs to executable guardrails. [6], [11], [13], [14]

TABLE II: DISCUSSION & FUTURE TRENDS

Approach	Description	Benefits	Challenges	Refs.
Zero Trust Architecture (ZTA)	Continuous verification with least privilege access	Reduces lateral movement, context-aware access	Complex IAM, policy sprawl	*[4], [10], [11*
SASE (Secure Access Service Edge)	Converges networking & security (ZTNA, CASB, SWG) in cloud PoPs	Uniform global access control, stronger data protection	Vendor lock-in, latency in global deployments	*6], [10]*
Automation & SOAR	Policy-as-code, auto-remediation, closed-loop response	Faster incident response, scalable governance	False positives, trust in automation	*[9], [11]*
Global Standards & Compliance	SO, NIST, CSA STAR, FedRAMP harmonization	Simplifies audits, unified security posture	Regulatory frag-mentation, adoption costs	*[6], [13], [14]*

V. FUTURE RESEARCH & DIRECTIONS

Cloud security is changing fast, but there are some research gaps that need serious exploration. One of the strongest areas is the use of Artificial Intelligence and Machine Learning (AI/ML) for predictive threat detection and incident response. While current studies stress anomaly-based detection and adaptive authentication through AI [11], more work needs to be done to enhance explainability and trustworthiness of these models. False positives and scalability issues in real-time multi-cloud scenarios underscore the necessity for stronger and interpretable AI-driven frameworks that can augment human decision-making.

Another exciting field is the advent of quantum computing, which can pose huge threats to existing cryptographic schemes. Research based on conventional methods like AES, DES, and RSA [9][10] could become susceptible in the near future. Hence, post-quantum cryptography is becoming increasingly relevant, and future research will be focused on incorporating quantum-resistant schemes into cloud services without reducing the performance or usability. This transition will necessitate intensive cooperation among academia, industry, and standardization organizations.

In addition, the adoption of Zero-Trust architectures and automation in security enforcement represents a growing research trend. Current approaches to IAM, access control, and SIEM [10][12] are often complex and error-prone in multi-tenant cloud systems. Future studies should focus on combining Zero-Trust principles with policy automation, federated identity management, and self-healing security systems. This will enable dynamic and adaptive security, ensuring resilience against insider threats, account hijacking, and misconfigurations. Lastly, the increasing dependence on multi-cloud and hybrid deployment raises open issues on compliance, governance, and data residency. Reports [4], [6], and [9] identify the dilemma of risk management and SLA enforcement with heterogeneous platforms, calling for single frameworks that strike a balance between flexibility and regulation compliance. Future work should also consider ethical and legal issues, creating world-class cloud security standards to alleviate fragmentation and ensure trust across borders. Through filling these gaps, the future of cloud security research can construct more robust, scalable, and interoperable globally defence mechanisms.

Summary

The future of near-cloud security is identity- and data-centric, continually validated (ZTA/SASE), and more autonomous—instrumented by AI but secured against AI-powered attackers, and grounded in converging worldwide standards. In practice, that involves designing crypto-agile architectures today, bringing identity for people and workloads up to first-class protected assets, moving controls left into platform and pipeline code, and checking readiness against evidence that meets multiple frameworks simultaneously. Organizations that see security as an engineered platform ability—rather than a bolt-on—will evolve quickest to the changing environment your references outline. [4], [6], [9], [10], [11], [13], [14]

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 8, August 2025

DOI: 10.17148/IARJSET.2025.12846

VI. CONCLUSION

Cloud computing is now the foundation of contemporary IT infrastructures, but its increasing usage has also grown the attack surface for cyber attackers. The literature reviewed in this paper identifies that attacks like misconfiguration, data breaches, hijacking of accounts, insider attacks, insecure APIs, DoS attacks, malware injection, and supply chain compromises are ongoing in all service models [5][9][10]. Misconfigurations of cloud configurations are still the top reason for security breaches, usually by human factor or lack of adequate access control policies [10]. Data breaches by either outside attackers or inside negligence are still draining faith in cloud usage and causing immense reputational and monetary damage [11]. Moreover, insider threats and account hijacking reveal fundamental vulnerabilities in identity management and monitoring processes, further increasing danger in shared cloud infrastructures [9].

The need for implementing proactive security tactics is underscored in various studies. Reactive tactics are insufficient in the face of cloud threats' magnitude and complexity [6]. Active defense measures like constant monitoring, zero-trust design, micro-segmentation, and multi-factor authentication immensely lower exposure by implementing security at all levels [4][11]. Likewise, AI-based anomaly detection and automation have been suggested as a crucial set of enablers for active defenses that assist organizations in identifying unusual activity even before it grows into an active breach [11]. Articles also highlight the importance of incorporating security into DevSecOps pipelines to ensure vulnerabilities are fixed early in software development and not as an afterthought [10].

According to these findings, authors suggest a mix of technical, administrative, and policy-based actions for future organizations. Organizations, first, need to enforce rigorous identity and access management (IAM) practices backed by zero-trust philosophy and least-privilege access models [4][10]. Second, adherence to global standards like GDPR, ISO 27001, and NIST protocols must be prioritized to make sure cloud implementations are consistent with legal and regulatory requirements [12]. Third, using strong encryption, tokenization, and multi-factor authentication methodologies can protect sensitive data even in cases of partial breaches [10]. Lastly, cooperation among Cloud Service Providers (CSPs), users, and regulatory authorities is needed to develop harmonized frameworks addressing shared responsibility and facilitating secure cloud environments [6][11].

In summary, the dynamic cloud environment requires multi-layered, adaptive, and visionary strategies to successfully address impending threats. Organizations need to recognize that cloud security is more than a technical matter but also concerns governance, compliance, and culture. By investing in proactive security frameworks, embracing automation, and following global best practices, organizations can not only reduce risks but also unlock the full power of cloud computing securely and sustainably [4][6][9][10][11][12].

REFERENCES

[1]. E. Fatima, I. A. Sumra, and R. Naveed, “A comprehensive survey on security threats and challenges in cloud computing models (saas, paas and iaas),” Journal of Computing & Biomedical Informatics, vol. 7, no. 01, pp. 537–544, 2024.

[2]. F. S¨uß, M. Freimuth, A. Aßmuth, G. R. Weir, and B. Duncan, “Cloud security and security challenges revisited,” arXiv preprint arXiv:2405.11350, 2024.

[3]. . Wali and F. Alshehry, “A survey of security challenges in cloud-based scada systems,” Computers, vol. 13, no. 4, p. 97, 2024.

[4]. G. Oladimeji, “A critical analysis of foundations, challenges and directions for zero trust security in cloud environments,” arXiv preprint arXiv:2411.06139, 2024.

[5]. A. I. Tahirkheli, M. Shiraz, B. Hayat, M. Idrees, A. Sajid, R. Ullah, and K. I. Kim, “A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures, and challenges,” Electronics, vol. 10, no. 15, p. 1811, 2021.

[6]. M. Chauhan and S. Shiaeles, “An analysis of cloud security frameworks, problems and proposed solutions,” Network, vol. 3, no. 3, pp. 422–450, 2023.

[7]. S. Z. Al-Otaibi, “Data security challenges and solutions in cloud computing: Critical review,” Communications in Mathematics and Applications, vol. 13, no. 2, p. 795, 2022.

[8]. A. Babaei, P. M. Kebria, M. M. Dalvand, and S. Nahavandi, “A review of machine learning-based security in cloud computing,” arXiv preprint arXiv:2309.04911, 2023.

[9]. N. Soveizi, F. Turkmen, and D. Karastoyanova, “Security and privacy concerns in cloud-based scientific and business workflows: A systematic review,” Future Generation Computer Systems, vol. 148, pp.184–200, 2023.

[10]. Z. J. Alibadi, “Security challenges and solutions in cloud-based software systems.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 8, August 2025

DOI: 10.17148/IARJSET.2025.12846

[11]. I. M. Khalil, A. Khreishah, and M. Azeem, "Cloud computing security: A survey," Computers, vol. 3, no. 1, pp. 1–35, 2014.
[12]. A. K. Y. Yanamala, "Emerging challenges in cloud computing security: A comprehensive review," International Journal of Advanced Engineering Technologies and Innovations, vol. 1, no. 4, pp. 448 – 479, 2024.
[13]. A. O. Akinade, P. A. Adepoju, A. B. Ige, and A. I. Afolabi, "Cloud security challenges and solutions: A review of current best practices," International Journal of Multidisciplinary Research Growth and Evaluation, vol. 6, no. 1, pp. 26–35, 2025.
[14]. I. E. Salem, "Enhancing cloud security through the integration of deep learning and data mining techniques: A comprehensive review," Periodicals of Engineering and Natural Sciences, vol. 11, no. 3, pp. 176–192, 2023.
[15]. A. Alquwayzani, R. Aldossri, and M. Frikha, "Prominent security vulnerabilities in cloud computing," International Journal of Advanced Computer Science & Applications, vol. 15, no. 2, 2024.
[16]. A. Babaei, P. M. Kebria, M. M. Dalvand, and S. Nahavandi, "A review of machine learning-based security in cloud computing," arXiv preprint arXiv:2309.04911, 2023.
[17]. S. Bhadra and S. Mohammed, "Cloud computing threats and risks: uncertainty and uncontrollability in the risk society," Electronic Journal, vol. 7, no. 2, pp. 1047–1071, 2020.
[18]. A. Pakmehr, A. Aßmuth, C. P. Neumann, and G. Pirkl, "Security challenges for cloud or fog computing-based ai applications," arXiv preprint arXiv:2310.19459, 2023.
[19]. T. S. Chou, "Security threats on cloud computing vulnerabilities," International Journal of Computer Science Information Technology, vol. 5, no. 3, p. 79, 2013.
[20]. S. M. Makoshi, "In-depth analysis of cloud security: Significance, service providers, and nist standards," arXiv preprint arXiv:2505.03945, 2025.
[21]. P. Gaikwad and D. Patil, "A semantic study on emerging risk and security management in cloud computing."
[22]. S. M. Shaffi, S. Vengathattil, J. N. Sidhick, and R. Vijayan, "Ai-driven security in cloud computing: Enhancing threat detection, automated response, and cyber resilience," 2025.

