Volume 2 No 6, 2026
Journal of Global Research in Multidisciplinary Studies (JGRMS)
Review Paper
Available online at https://saanvipublications.com/journals/index.php/jgrms/index

Security, Privacy, and Trust in Cloud Computing: An Integrated Survey of Techniques

Dr. Nilesh Jain
Associate Professor
Department of Computer Sciences and Applications
Mandsaur University, Mandsaur
nileshjainmca@gmail.com

***Abstract*—Cloud computing has emerged as a transformative model for delivering IT services, offering scalable, flexible, and cost-efficient access to computing resources over the internet. It is structured around three primary service models—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—which delineate varying levels of user control and provider responsibility. Deployment models, including public, private, hybrid, and community clouds, further define ownership, access, and operational scope. Key stakeholders in the cloud ecosystem include service providers, consumers, and intermediaries such as brokers. However, the adoption of cloud technologies introduces significant challenges, particularly in areas of security, privacy, and trust. Threats such as data breaches, insecure APIs, insider risks, and multi-tenancy vulnerabilities compromise cloud integrity, while issues like data ownership, cross-border data flow, and regulatory compliance raise privacy concerns. Trust in cloud environments hinges on transparency, robust service-level agreements (SLAs), auditability, and third-party certifications like ISO 27001 and SOC 2. Addressing these challenges is essential for ensuring secure, privacy-compliant, and trustworthy cloud services that can support mission-critical applications across sectors.**

***Keywords*—Cloud Computing, Security, Privacy, Trust Management, Data Protection, Access Control, Federated Learning, Risk Assessment, Regulatory Compliance, Trust Evaluation**

I. INTRODUCTION

Cloud computing has emerged as one of the most transformative paradigms in modern information technology, providing scalable, flexible, and cost-effective computing resources through the Internet. Organizations and individuals increasingly rely on cloud services for data storage, processing, and application deployment due to their advantages, including on-demand resource provisioning, virtualization, rapid elasticity, and reduced infrastructure management costs[1]. The widespread adoption of cloud computing has accelerated digital transformation across various sectors, including healthcare, finance, education, manufacturing, and government services. However, as critical data and services are increasingly outsourced to cloud environments, concerns regarding security, privacy, and trust have become significant challenges that must be addressed to ensure reliable and secure cloud operations.

The distributed and multi-tenant nature of cloud environments introduces numerous security risks, including unauthorized access, data breaches, insider threats, malware attacks, denial-of-service attacks, and vulnerabilities arising from shared infrastructures. Unlike traditional centralized systems, cloud platforms involve complex interactions among users, service providers, and third-party entities, thereby expanding the attack surface and increasing the difficulty of maintaining data confidentiality, integrity, and availability. Consequently, researchers and practitioners have proposed various security mechanisms, including encryption techniques, access control models, authentication protocols, intrusion detection systems, and AI-driven threat detection frameworks to strengthen cloud security and mitigate evolving cyber threats. Alongside security, privacy protection has become a critical concern due to the large volume of sensitive and personal information stored and processed in cloud infrastructures. Data often traverses multiple geographical regions and jurisdictions, creating challenges related to regulatory compliance, data sovereignty, and user consent management. Regulations such as the General Data Protection Regulation (GDPR) and other privacy frameworks have increased the need for privacy-preserving techniques, including anonymization, secure multi-party computation, differential privacy, federated learning, and privacy-aware data management strategies. These approaches aim to ensure that cloud services can effectively utilize data while protecting user privacy and maintaining compliance with legal and ethical requirements[2].

Trust represents another fundamental pillar of cloud computing and serves as a critical factor influencing user adoption and acceptance of cloud services[3]. Trust encompasses confidence in the cloud provider's ability to deliver secure, reliable, transparent, and accountable services while safeguarding user data and maintaining service availability. Establishing trust requires effective mechanisms for risk assessment, reputation management, service-level agreement enforcement, transparency, explainability, auditing, and compliance verification. As cloud ecosystems continue to expand and involve multiple stakeholders, trust management frameworks play an increasingly important role in fostering confidence among users and service providers[4]

Furthermore, the integration of emerging technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), big data analytics, edge computing, and fog computing has significantly enhanced the capabilities of cloud environments while simultaneously introducing new security, privacy, and trust challenges[5]. The massive volume of interconnected devices, real-time data processing

requirements, and intelligent decision-making systems demand advanced protection mechanisms capable of addressing sophisticated threats and ensuring trustworthy service delivery[6][7]. Recent research has therefore focused on developing intelligent, adaptive, and privacy-preserving solutions that strengthen the resilience and dependability of cloud-based systems. In light of these developments, a comprehensive understanding of security, privacy, and trust techniques is essential for the design and deployment of secure cloud infrastructures. This survey presents an integrated review of existing approaches, frameworks, and emerging solutions aimed at addressing these interconnected challenges. By examining current advancements, identifying research gaps, and highlighting future directions, this study provides a comprehensive perspective on the evolving landscape of security, privacy, and trust in cloud computing[8].

A. Structure of the paper

This paper is organized as follows: Section II Overview of Cloud Computing. Section III Security challenges in cloud computing. Section IV. Privacy Concerns in the cloud computing. Section V Trust in Cloud Environments. Section VI literature of Review and Describe table. Section VII Conclusions.

II. Foundations of Cloud Computing: Architecture, Service Models, and Ecosystem

The rapid advancement of digital technologies has transformed cloud computing into a fundamental platform for delivering computing resources and services over the Internet. By providing on-demand access to shared resources such as computing power, storage, networking, and software applications, cloud computing enables organizations to improve operational efficiency while reducing infrastructure costs. Its ability to support scalability, flexibility, and ubiquitous access has encouraged widespread adoption across diverse sectors, including healthcare, education, finance, manufacturing, and government services[9].

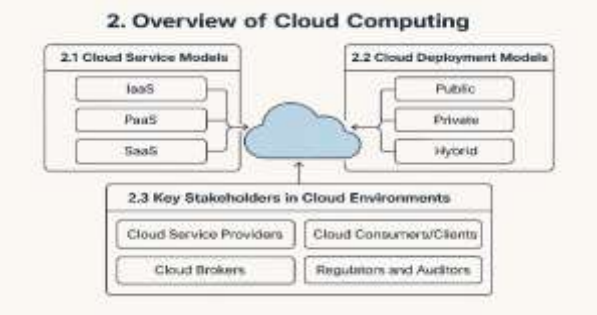

Fig. 1. Cloud Computing Services

As cloud environments continue to evolve, understanding their architectural foundations and operational ecosystems becomes essential for examining the security, privacy, and trust challenges associated with cloud-based services. Fig. 1 presents an overview of the cloud computing ecosystem.

A. Architectural Characteristics of Cloud Computing

Modern cloud platforms operate through a layered architecture that integrates physical infrastructure, virtualization technologies, resource management systems, and service delivery mechanisms. This architecture enables efficient utilization of computing resources by dynamically allocating workloads according to user demands. Several defining characteristics contribute to the effectiveness of cloud computing, including on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. While these characteristics provide significant operational advantages, they also introduce concerns related to data protection, access control, service reliability, and regulatory compliance, making security and trust critical considerations within cloud environments.

B. Service Delivery Paradigms

Different levels of abstraction are provided through cloud service models, allowing organizations to select services according to their technical and operational requirements. These models define the distribution of responsibilities between cloud service providers and cloud consumers. Fig. 2 illustrates the major cloud service models.

Fig. 2. Cloud Service

1) Infrastructure as a Service (IaaS)

IaaS provides fundamental computing resources such as virtual machines, storage, and networking. Users manage the operating systems, applications, and data, while the provider manages the underlying infrastructure[10]. Popular examples include Amazon EC2, Google Compute Engine, and Microsoft Azure VMs.

2) Platform as a Service (PaaS):

PaaS offers a development and deployment environment that abstracts the infrastructure layer. Developers can build, test, and deploy applications without worrying about server management or system updates. Examples include Google App Engine, Microsoft Azure App Service, and Heroku.

3) Software as a Service (SaaS):

SaaS delivers software applications over the internet, typically on a subscription basis. Users access these applications via a browser, while the provider handles everything from infrastructure to application logic and data management. Examples include Google Workspace, Microsoft 365, and Salesforce.

C. Cloud Deployment Models (Public, Private, Hybrid, Community)

Ownership, accessibility, and management responsibilities vary according to cloud deployment models. These deployment strategies enable organizations to balance performance, cost, security, and compliance requirements based on their operational objectives. Fig. 6 presents the primary cloud deployment models[11].

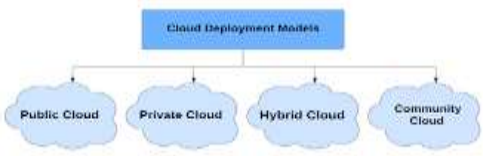

Fig. 3. Cloud Deployment Models

1) Public

Services are offered over the internet and available to the general public or large industry groups. These are owned and operated by third-party providers (e.g., AWS, Google Cloud). Public clouds are cost-effective but pose concerns over data residency, privacy, and multi-tenancy[12].

2) Private

Infrastructure is exclusively operated for a single organization, either internally or by a third party. It offers greater control and security, making it suitable for regulated industries or sensitive workloads, though it comes with higher costs.

3) Hybrid

Combines public and private clouds, enabling data and application portability. This model allows organizations to use public clouds for less-sensitive tasks while keeping critical functions on private infrastructure.

4) Community

Shared by several organizations with common interests or requirements (e.g., regulatory compliance). It supports collaborative efforts in specific sectors such as healthcare, finance, or government.

D. Key Stakeholders in Cloud Environments

Effective cloud operations depend on collaboration among several entities that collectively contribute to service delivery, governance, and security management[13]. Each participant plays a distinct role in maintaining the functionality and trustworthiness of cloud environments. Fig. 7 presents the major stakeholders involved in the cloud ecosystem.

Fig. 4. Stakeholders in Cloud Environment

1) Cloud Service Providers (CSPs):

Entities that offer cloud-based services, infrastructure, or platforms. They are responsible for physical security, network infrastructure, and often parts of data management depending on the service model.

2) Cloud Consumers/Clients:

Individuals or organizations that use cloud services. They are responsible for application-level security, data integrity, and access management—especially in IaaS and PaaS contexts.

3) Cloud Brokers

Intermediaries that enhance service delivery by managing relationships between providers and consumers. They may offer value-added services such as integration, customization, or compliance support.

4) Cloud Auditors

Independent assessment of cloud services, security controls, and regulatory compliance is conducted by cloud auditors. Their evaluations enhance transparency, accountability, and confidence among stakeholders, thereby contributing to trust establishment within cloud environments.

5) Cloud Carriers

Communication networks and connectivity services are supplied by cloud carriers, enabling reliable access to cloud resources. Service quality, network performance, and secure data transmission largely depend on the effectiveness of carrier operations.

III. Security Challenges in Cloud Computing

Cloud computing has revolutionized how organizations manage and deploy their IT resources, offering scalability, flexibility, and cost efficiency. However, alongside these advantages come significant security challenges that must be addressed to protect sensitive data and maintain trust. This section outlines key security challenges that are pervasive in cloud environments.Fig.8

Fig. 5. Cloud Security challenges

A. Threat Landscape

The cloud threat landscape is broad and continuously evolving, encompassing a variety of actors and attack vectors. Threats range from opportunistic attacks by individual hackers to highly organized campaigns by nation-states. Attackers exploit vulnerabilities in cloud infrastructure[14], software, and human factors to gain unauthorized access or disrupt services. The dynamic, multi-tenant nature of cloud environments expands the attack surface, requiring constant vigilance and adaptive security measures.

B. Data Breaches and Insider Threats:

Data breaches remain one of the most critical risks in cloud computing. Unauthorized access to sensitive data can result from external attacks or negligent configurations. Insider threats, whether malicious or accidental, pose an equally serious concern[15]. Employees, contractors, or cloud service providers with elevated access privileges can intentionally or unintentionally expose or misuse data. The lack of direct control over cloud infrastructure complicates detection and response to these incidents[16].

C. Vulnerabilities in APIs and Management Interfaces:

Cloud services rely heavily on Application Programming Interfaces (APIs) to enable integration, automation, and user interaction[17]. These APIs and web interfaces become prime targets for attackers[18]. Vulnerabilities such as insufficient authentication, improper access controls, and

lack of encryption can be exploited to compromise cloud services. Securing APIs through rigorous design, testing[19], and continuous monitoring is crucial to maintaining the integrity and confidentiality of cloud resources.

D. Risks Associated with Virtualization and Multi-Tenancy:

Virtualization is the foundation of cloud infrastructure, allowing multiple tenants to share physical resources. However, this multi-tenancy introduces unique security risks[20]. Vulnerabilities in hypervisors or virtual machines can lead to cross-tenant attacks, where a malicious tenant gains access to other tenants' data or resources. Ensuring strong isolation between virtual machines and implementing robust access controls are essential to mitigate these risks.

E. Denial of Service (DoS) and Distributed DoS Attacks:

Denial of Service (DoS) attacks aim to disrupt cloud service availability by overwhelming resources with excessive requests. Distributed Denial of Service (DDoS) attacks, leveraging a network of compromised devices, amplify this threat significantly[21][22]. Cloud services, especially public-facing ones, are attractive targets for these attacks due to their broad accessibility and critical roles. Implementing scalable mitigation strategies, such as traffic filtering, rate limiting, and leveraging cloud provider DDoS protection services, is vital for maintaining service continuity.

F. Cloud Misconfiguration and Access Control Weaknesses

Improper configuration of cloud resources remains a major cause of security incidents and data exposure. Misconfigured storage services, overly permissive access policies, unsecured databases, and incorrect network settings can unintentionally expose sensitive information to unauthorized users. The complexity of cloud environments often increases the likelihood of configuration errors, highlighting the importance of automated security assessments, configuration management tools, and regular auditing procedures to identify and remediate vulnerabilities.

G. Advanced Persistent Threats and Emerging Cyber Risks

Sophisticated attackers increasingly employ Advanced Persistent Threats (APTs) to infiltrate cloud environments and maintain long-term unauthorized access. These attacks typically involve multiple stages, including reconnaissance, initial compromise, lateral movement, and data exfiltration. Furthermore, emerging technologies and increasingly complex cloud ecosystems continue to introduce new attack vectors and security challenges[23]. Detecting and mitigating such threats requires advanced monitoring systems, threat intelligence integration, and proactive incident response strategies.

H. Security Challenges under the Shared Responsibility Model

Cloud security operates under a shared responsibility model in which security obligations are divided between cloud service providers and cloud consumers. While providers are generally responsible for securing the underlying infrastructure, customers remain accountable for protecting applications, user identities, configurations, and data. Misunderstandings regarding these responsibilities can create security gaps and increase organizational risk. Establishing clear security policies, governance frameworks, and compliance procedures is therefore essential for ensuring comprehensive protection across cloud environments.

1) Privacy Concerns in the Cloud

The increasing adoption of cloud computing has introduced significant privacy concerns due to third-party data management, shared infrastructures, and geographically distributed storage systems. Unlike traditional environments, cloud platforms involve multiple stakeholders and complex data processing activities, making privacy protection a critical requirement. Ensuring proper data governance, regulatory compliance, and user control over personal information is essential for maintaining confidence in cloud services.

I. Data Ownership and User Consent:

Control over cloud-hosted information remains a significant privacy concern because data is stored and processed by third-party cloud service providers (CSPs). Although users and organizations retain ownership of their data, CSPs often manage storage, processing, and maintenance activities. This separation may create uncertainty regarding data access, usage rights, and accountability.

- **Data Ownership:** Determining ownership rights over cloud-stored data can be challenging due to the involvement of multiple stakeholders. Service-level agreements (SLAs) must clearly define responsibilities related to data access, processing, sharing, and protection to avoid disputes and ensure accountability.
- **User Consent:** Privacy protection requires organizations to obtain informed and explicit consent from users before collecting, processing, or sharing personal information. Transparent consent mechanisms help users understand how their data will be utilized and support compliance with privacy regulations such as GDPR.

J. Data Localization and Jurisdictional Issues:

Cloud data is frequently distributed across multiple data centres located in different countries and regions. As a result, information may become subject to diverse legal and regulatory frameworks, creating challenges related to data sovereignty and cross-border data transfers. Many governments require sensitive or critical information to remain within national boundaries, making compliance with localization requirements an important consideration for cloud service adoption.

K. Anonymization and Data Minimization:

Organizations employ privacy-preserving techniques to reduce the exposure of sensitive information and strengthen regulatory compliance.

- **Anonymization:** Removing or modifying personally identifiable information (PII) so that individuals cannot be identified.
- **Data minimization:** Collecting and storing only the minimum amount of data necessary for the intended purpose.

L. GDPR, HIPAA, and Other Compliance Challenges:

- **GDPR (EU):** Emphasizes data subject rights, consent, breach notification, and cross-border transfer restrictions.

- **HIPAA (US)**: Applies to healthcare data, requiring safeguards like encryption and access controls.
- **CCPA (California)**, **PDPA (Singapore):** and others impose varying degrees of control over data use and retention.

IV. Trust in Cloud Environments

Trust is a fundamental factor influencing the adoption and continued use of cloud computing services. Since cloud users entrust their data, applications, and business operations to third-party providers, confidence in the reliability, security, and integrity of cloud services becomes essential. Unlike traditional computing environments, cloud systems operate through shared infrastructures and remote management, making trust a multidimensional concept that encompasses technical, organizational, and regulatory aspects.

A. Defining Trust in Cloud Context:

Trust in cloud computing refers to the user's confidence that the cloud provider will behave as expected in terms of data security, service availability, compliance, and ethical responsibility.[24]. Unlike traditional IT systems, the cloud environment introduces abstraction and shared control, making trust more complex and multi-dimensional. Trust is both **subjective** (based on perception and experience) and **objective** (measurable through evidence like certifications and service guarantees).

B. Factors Affecting Trust (Transparency, SLA, Auditability):

Several factors contribute to establishing and maintaining trust within cloud environments. Table I summarizes the major factors affecting trust.

TABLE I. Describe the Factors Affecting Trust

Factor	Description	Impact on Trust	Example
Transparency	The clarity with which cloud providers disclose policies, procedures, and events	Builds user confidence by reducing uncertainty	Public incident reports, data handling policies
SLA (Service Level Agreement)	A formal agreement defining performance and uptime guarantees	Ensures accountability and measurable expectations	99.9% uptime SLA for cloud storage
Auditability	The ability to verify and inspect system operations and data handling	Provides evidence of compliance and operational integrity	Logs, third-party audits, SOC 2 or ISO 27001 certification reports

C. Trust Models and Evaluation Metrics:

Trust assessment in cloud environments is commonly performed through various trust models and evaluation mechanisms. These approaches help users and organizations determine the reliability and trustworthiness of cloud services.

- **Reputation-Based Trust:** Evaluates trust using historical performance records, customer feedback, and service reputation.
- **Behaviour-Based Trust:** Assesses trust based on observed provider behaviour, policy compliance, and service reliability over time.
- **Risk-Based Trust:** Considers security risks, vulnerabilities, and potential threats associated with cloud services.
- **Multi-Criteria Trust Models:** Combine multiple factors such as security, privacy, availability, compliance, and reputation to generate comprehensive trust scores.

D. Role of Certification and Third-Party Assurance:

Formal certifications and third-party assessments play a vital role in establishing trust by demonstrating compliance with recognized standards and best practices:

- **ISO/IEC 27001:** Validates the implementation of information security management systems.
- **SOC Reports:** Provide independent assessments of security, availability, processing integrity, confidentiality, and privacy controls.
- **CSA STAR Certification:** Evaluates cloud-specific security and transparency practices.
- **Regulatory Compliance Audits:** Verify adherence to legal and industry-specific requirements.

E. Relationship Between Trust, Security, and Privacy

Trust in cloud computing is closely connected to security and privacy. Effective security mechanisms protect data and services from threats, while privacy-preserving practices ensure responsible handling of sensitive information. Together, these measures enhance transparency, accountability, and user confidence. Consequently, trust can be viewed as an outcome of robust security controls, strong privacy protections, regulatory compliance, and reliable service delivery within cloud environments.

V. Literature Review

The reviewed literature highlights the growing importance of security, privacy, and trust in cloud computing. Existing studies focus on cloud security frameworks, risk assessment models, privacy-preserving techniques such as federated learning and differential privacy, and trust-enhancing mechanisms. However, challenges including evolving cyber threats, data protection, regulatory compliance, and adaptive trust management remain significant research concerns.

Ali, Al-Khalidi and Al-Zaidi (2026) Cloud computing faces more security threats, requiring better security measures. This paper examines the various classification and categorization schemes for cloud computing security issues, including the widely known CIA trinity (confidentiality, integrity, and availability), by considering critical aspects of the cloud, such as service models, deployment models, and involved parties. A comprehensive comparison of cloud security classifications constructs an exhaustive taxonomy. ISO27005, NIST SP 800–30, CRAMM, CORAS, OCTAVE Allegro, and COBIT 5 are rigorously compared based on their applicability, adaptability, and suitability within a cloud-based hosting methodology. The findings of this research recommend OCTAVE Allegro as the preferred cloud hosting paradigm [25].

Rahdar et al. (2025) The increasing need to process large, high-dimensional datasets and the substantial computational power required have made the use of distributed cloud servers essential. These servers provide cost-effective solutions that make storage and computing accessible to ordinary users. However, they might face significant vulnerabilities,

including data leakage, metadata spoofing, insecure programming interfaces, malicious insiders, and denial of service. To gain public trust in distributed computing, addressing concerns related to privacy and security while ensuring high performance and efficiency is crucial. Multiparty computation, differential privacy, trusted execution environments, and federated learning are the four major approaches developed to address these issues. This survey paper reviews and compares these four approaches based on a structured framework, by highlighting recent top-tier research papers published in prestigious journals and conferences. Particular attention is given to progress in federated learning, which trains a model across multiple devices without sharing the actual data, keeping data private and secure [26].

Kawalkar and Bhoyar (2024) gain public trust in distributed computing, addressing concerns related to privacy and security while ensuring high performance and efficiency is crucial. Multiparty computation, differential privacy, trusted execution environments, and federated learning are the four major approaches developed to address these issues. This survey paper reviews and compares these four approaches based on a structured framework, by highlighting recent top-tier research papers published in prestigious journals and conferences. Particular attention is given to progress in federated learning, which trains a model across multiple devices without sharing the actual data, keeping data private and secure. The survey also highlights federated learning techniques, including secure federated learning, by detecting malicious updates and privacy-preserving federated learning via data encryption, data perturbation, and anonymization, as new paradigms for building responsible computing systems [27]

Chauhan and Shiaeles (2023) rapidly growing use of cloud computing raises security concerns. This study paper seeks to examine cloud security frameworks, addressing cloud-associated issues and suggesting solutions. This research provides greater knowledge of the various frameworks, assisting in making educated decisions about selecting and implementing suitable security measures for cloud-based systems. The study begins with introducing cloud technology, its issues and frameworks to secure infrastructure, and an examination of the various cloud security frameworks available in the industry. A full comparison is performed to assess the framework's focus, scope, approach, strength, limitations, implementation steps and tools required in the implementation process. The frameworks focused on in the paper are COBIT5, NIST (National Institute of Standards and Technology), ISO (International Organization for Standardization), CSA (Cloud Security) Later, the study digs into identifying and analyzing prevalent cloud security issues. This contains attack vectors that are inherent in cloud environments [28]

Soveizi, Turkmen and Karastoyanova (2023) the number of data-intensive and compute-intensive applications like business and scientific workflows has dramatically increased, which made cloud computing more popular because of its ability to deliver a large number of computing resources on demand. Security is a critical issue affecting the wide adoption of cloud technologies, especially for workflows that deal mostly with sensitive data and tasks. In this paper, we carry out a review of the state-of-the-art on how security and privacy concerns in scientific and business workflows in cloud environments are being addressed and identify the limitations and gaps in the current body of knowledge in this area. In this extensive literature review, we first present the state-of-the-art security solutions organized according to the phases of the workflow life cycle they target for both business and scientific workflows. The analysis shows that most of the existing literature focuses on the modelling and execution phases, while the monitoring and adaptation phases are not covered adequately by a scarce amount of publications thus leaving a huge gap in the body of knowledge relevant to detection, prevention of and reaction to security violations in cloud-based workflows. [29]

Janet Julia Ang'udi (2023) The security issues surrounding cloud computing, a quickly developing technology that is now essential to both personal and business computing, are thoroughly examined in this study. Cloud computing presents serious security risks that require careful attention, despite its many advantages such as scalability, cost-effectiveness, and flexibility. In-depth discussions of a number of important security topics are covered in this paper, including network security, access control, data breaches, legal and regulatory framework compliance, and new threats and vulnerabilities. The paper illuminates the complexities of data and application security in the cloud environment by thoroughly examining these subjects. The study intends to offer insightful analyses of security challenges with practical implications by examining these cases and providing lessons learned from incidents that have happened in various cloud computing scenarios. Our comprehension of the complex nature of security threats and the tactics used to counter and mitigate them is improved by looking closely at these cases. Cloud environments may be able to improve their security posture against new and sophisticated threats by utilizing the powers of AI and machine learning [30]

Table II presents a comparative analysis of recent cloud computing research, highlighting advances in security frameworks, privacy-preserving techniques, trust management, and risk assessment. The studies collectively address evolving cyber threats, data protection challenges, regulatory compliance, and the need for secure and trustworthy cloud environments.

TABLE 2 COMPARATIVE ANALYSIS OF CLOUD SECURITY RESEARCH ON LITERATURE REVIEW

Reference	Focus Area	Key Findings	Challenges	Key Contribution
[25]	Cloud Security Classification and Risk Assessment	Developed a comprehensive taxonomy of cloud security issues and compared major risk assessment frameworks.	Selecting suitable security frameworks for dynamic cloud environments.	Recommended OCTAVE Allegro as an effective risk assessment model for cloud hosting.
[26]	Privacy-Preserving Distributed Cloud Computing	Reviewed multiparty computation, differential privacy, trusted execution environments, and federated learning.	Balancing privacy, security, trust, and computational efficiency.	Provided a structured comparison of privacy-preserving techniques and highlighted federated learning advancements.

[27]	Privacy and Trust in Distributed Computing	Examined secure federated learning, encryption, anonymization, and privacy-preserving mechanisms.	Detecting malicious updates while maintaining privacy and model performance.	Identified federated learning as a promising approach for trustworthy cloud-based systems.
[28]	Cloud Security Frameworks	Compared COBIT5, NIST, ISO, and CSA security frameworks for cloud environments.	Addressing evolving cloud threats and selecting appropriate security controls.	Offered a detailed evaluation of major cloud security frameworks and mitigation strategies.
[29]	Security and Privacy in Cloud Workflows	Analyzed security solutions across workflow life-cycle phases in cloud environments.	Limited research on monitoring, adaptation, and response to security violations.	Identified research gaps in workflow security and privacy management.
[30]	Cloud Security Challenges and Emerging Threats	Discussed network security, access control, compliance, data breaches, and AI-driven protection.	Managing sophisticated and evolving cloud security threats.	Provided a comprehensive overview of cloud security issues and future AI-based security solutions.

VI. Conclusion And Future Work

Cloud computing is an integral part of the technology that helps provide scalable, flexible and affordable computing resources over a wide range of application areas. However, cloud environments still have many security, privacy, and trust-related issues. This survey covered the architectural underpinning of cloud computing, service and deployment models, key security issues, privacy issues, and trust establishment. A literature review found that significant advances have been made with the use of security frameworks, privacy-preserving techniques, risk assessment models, federated learning, and compliance-based methods. But a number of problems have not yet been solved, such as data breaches, insider threats, insecure interfaces, multi-tenancy risks, compliance problems, and the building of trustworthy cloud services. The analysis also shows that security, privacy, and trust are closely coupled and cannot be solved by stand-alone solutions, but by integrated ones.

Future research is needed to build a single framework that can meet the security and privacy needs and trust in a cloud environment. There are a number of areas of interest that require more attention, such as AI-driven threat detection, explainable and trustworthy AI, adaptive trust management systems, and privacy-preserving machine learning techniques. Moreover, new concepts like edge computing, Internet of Things (IoT), trust mechanisms based on blockchain technology, and zero-trust architectures have shown potential to improve the resilience, transparency, and reliability of future cloud computing networks.

References

[1] S. Stoykova and N. Shakev, "Artificial Intelligence for Management Information Systems: Opportunities, Challenges, and Future Directions," *Algorithms*, vol. 16, no. 8, p. 357, Jul. 2023, doi: 10.3390/a16080357.

[2] M. L. Hernandez-Jaimes, A. Martinez-Cruz, K. A. Ramírez-Gutiérrez, and C. Feregrino-Uribe, "Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures," *Internet of Things*, vol. 23, p. 100887, Oct. 2023, doi: 10.1016/j.iot.2023.100887.

[3] P. C. Jakku, P. Sundaramoorthy, S. C. Kondaparthy, T. Desai, R. Jarubula, and A. Nerella, "Enhancing Cloud Security Via Quantum Computing," in *Proceedings of Data Analytics and Management*, A. Swaroop, B. Virdee, S. Correia, and Z. Polkowski, Eds., Cham: Springer Nature Switzerland, 2025, pp. 377-386,November.

[4] V. R. Iyer, K. Babu, and V. R. Guruswamy, "Cyber Security Frameworks through the Lens of Foreign Direct Investment (FDI): A Systematic Literature Review," *Int. J. Intell. Syst. Appl. Eng.*, 2024.

[5] R. Palwe, "Onboarding for AI features: Reducing friction at the first use," *Int. J. Comput. Artif. Intell.*, vol. 6, no. 2, pp. 393–400, Jul. 2025, doi: 10.33545/27076571.2025.v6.i2e.227.

[6] H. Makina, A. B. E. N. Letaifa, and A. Rachedi, "Leveraging Edge Computing, Blockchain and IPFS for Addressing eHealth Records Challenges," in *Proceedings of the 2022 15th IEEE International Conference on Security of Information and Networks, SIN 2022*, 2022. doi: 10.1109/SIN56466.2022.9970495.

[7] R. Lingam, S. Nagi, M. Chigurupati, and B. T. Myneni, "Resilient DevSecOps: Self-Healing Cloud-Native Systems via SRE-Driven AI Threat Detection and Response," in *2026 International Conference on Smart Futuristic Technology*, IEEE, Jan. 2026, pp. 1–6. doi: 10.1109/ICSFT66733.2026.11508049.

[8] O. C. Obi, S. O. Dawodu, A. I. Daraojimba, and S. Onwusinkwue, "Review Of Evolving Cloud Computing Paradigms: Security, Efficiency, And Innovations," *Comput. Sci. IT Res. J.*, vol. 5, no. 2, pp. 270–292, Feb. 2024, doi: 10.51594/csitrj.v5i2.757.

[9] A. Atadoga, U. J. Umoga, O. A. Lottu, and E. O. Sodiya, "Evaluating the impact of cloud computing on accounting firms: A review of efficiency, scalability, and data security," *Glob. J. Eng. Technol. Adv.*, vol. 18, no. 2, pp. 065–075, Feb. 2024, doi: 10.30574/gjeta.2024.18.2.0027.

[10] R. Younis, M. Iqbal, K. Munir, M. A. Javed, M. Haris, and S. Alahmari, "A Comprehensive Analysis of Cloud Service Models: IaaS, PaaS, and SaaS in the Context of Emerging Technologies and Trends," in *2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE)*, IEEE, Oct. 2024, pp. 1–6. doi: 10.1109/ICECCE63537.2024.10823401.

[11] M. Alshinwan, A. Y. Shdefat, N. Mostafa, A. A. M. Alsokkar, T. Alsarhan, and D. Almajali, "Integrated cloud computing and blockchain systems: A review," *Int. J. Data Netw. Sci.*, 2023, doi: 10.5267/j.ijdns.2022.12.016.

[12] T. Shah, "Cloud-Based Data Warehousing for Marketing Agility: Lessons from FinTech Migrations to Snowflake and AWS," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 4, March, pp. 642–652, 2024, doi: 10.48175/IJARSCT-16000B.

[13] E. Irmak, E. Kabalci, and Y. Kabalci, "Digital Transformation of Microgrids: A Review of Design, Operation, Optimization, and Cybersecurity," 2023. doi: 10.3390/en16124590.

[14] S. Reema, "Cloud Computing as a Solution for Security and Privacy Concerns," *Int. J. Res. Appl. Sci. Eng. Technol.*, 2023, doi: 10.22214/ijraset. 2023.49375.

[15] T. Esho, O. Ayeni, O. Lasisi, and O. Peter, "The Role of Cloud Computing in Personalized Medicine: A Systematic Review," *Curr. J. Appl. Sci. Technol.*, 2024, doi: 10.9734/cjast/2024/v43i34355.

[16] M. R. C. Mukkolakkal, "InfraLLM: A Generic Large Language Model Framework for Production-Grade Microservice Auto-Scaling in Cloud Infrastructure," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 11, pp. 113–123, 2025, doi: 10.38124/ijsrmt.v4i11.1023.

[17] F. Mohd Ali, N. A. Md Yunus, N. N. Mohamed, M. Mat Daud, and E. A. Sundararajan, "A Systematic Mapping: Exploring Internet of Everything Technologies and Innovations," 2023. doi: 10.3390/sym15111964.

[18] R. Palwe, "Three Layers of Trust in AI Interfaces: Interface, Behaviour, and Organization," *Int. J. Sci. Res.*, vol. 15, no. 1, pp. 1152–1160, Jan. 2026, doi: 10.21275/SR26112072531.

[19] J. B. Mehta, "AI-Driven Test Engineering for Cloud-Native Systems," *Int. J. Data Sci. IoT Manag. Syst.*, vol. 5, no. 1, 2026, doi: 10.64751/ijdim. 2026. v5i1.297.

[20] A. Nag *et al.*, "Exploring the applications and security threats of Internet of Things in the cloud computing paradigm: A comprehensive study on the cloud of things," *Trans. Emerg. Telecommun. Technol.*, 2024, doi: 10.1002/ett.4897.

[21] L. Liu, J. Li, J. Lv, J. Wang, S. Zhao, and Q. Lu, "Privacy-

Preserving and Secure Industrial Big Data Analytics: A Survey and the Research Framework," *IEEE Internet Things J.*, 2024, doi: 10.1109/JIOT.2024.3353727.

[22] A. Katangoori, "The Role of Big Data in Advancing Artificial Intelligence: Methods and Case Studies," *Int. J. Artif. Intell. Mach. Learn.*, vol. 6, no. 1, pp. 37–54, Jan. 2026, doi: 10.51483/IJAIML.6.1.2026.37-54.

[23] S. K. Chintagunta and S. Amrale, "Enhancing Cloud Database Security Through Intelligent Threat Detection and Risk Mitigation," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, pp. 756–768, 2022.

[24] S. Ahmad, S. Mehfuz, and J. Beg, "Assessment on potential security threats and introducing novel data security model in cloud environment," in *Materials Today: Proceedings*, 2022. doi: 10.1016/j.matpr.2022.03.536.

[25] T. Ali, M. Al-Khalidi, and R. Al-Zaidi, "Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review," *J. Comput. Inf. Syst.*, vol. 66, no. 1, pp. 123–150, Jan. 2026, doi: 10.1080/08874417.2024.2329985.

[26] A. Rahdari *et al.*, "A Survey on Privacy and Security in Distributed Cloud Computing: Exploring Federated Learning and Beyond," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 3710–3744, 2025, doi: 10.1109/OJCOMS.2025.3560034.

[27] S. A. Kawalkar and D. B. Bhoyar, "Design of an Efficient Cloud Security Model through Federated Learning, Blockchain, AI-Driven Policies, and Zero Trust Frameworks," *Int. J. Intell. Syst. Appl. Eng.*, 2024.

[28] M. Chauhan and S. Shiaeles, "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions," *Network*, vol. 3, no. 3, pp. 422–450, 2023, doi: 10.3390/network3030018.

[29] N. Soveizi, F. Turkmen, and D. Karastoyanova, "Security and privacy concerns in cloud-based scientific and business workflows: A systematic review," *Futur. Gener. Comput. Syst.*, vol. 148, pp. 184–200, Nov. 2023, doi: 10.1016/j.future.2023.05.015.

[30] J. J. Ang'udi and S. Awour, "Security challenges in cloud computing: A comprehensive analysis," *World J. Adv. Eng. Technol. Sci.*, vol. 10, no. 2, pp. 155–181, Dec. 2023, doi: 10.30574/wjaets. 2023.10.2.0304.

