ISSN 2581 – 3781

AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

Available Online at www.ajcse.info
Asian Journal of Computer Science Engineering 2025;10(3)

REVIEW ARTICLE

Survey of Privacy-Preserving Mechanisms and Compliance Frameworks for Secure Cloud Adoption

Dr. Dinesh Yadav*
Associate Professor
CSE Department
St. Andrews Institute of Technology & Management, Gurugram, Haryana, India
Email: dinesh.yadav@saitm.ac.in

***Abstract*—Digital data and improved computing technologies have expanded exponentially, prompting an increased rate of adoption of up-and-coming IT resource delivery models. One of them has become prominent, cloud computing which comprises on-demand storage, application, and processing power of the virtualized environments. The cloud model is based on some fundamental characteristics like scalability, elasticity and pay-per-use and these characteristics save organizations a lot of money as well as provide high levels of flexibility in operations. Concerns about privacy, security, and regulatory compliance arise when critical data is stored in the cloud by unaffiliated third parties. Several privacy-preserving techniques (PPMs) have been suggested, including cryptography, anonymization, homomorphic encryption, and secure multi-party computations, to ensure long-term adoption and establish confidence. Consistent with this trend, data governance and regulatory compliance are receiving formal frameworks from international compliance models such as GDPR, HIPAA, and NIST standards. The foundations, mechanisms, and compliance frameworks that underpin the secure adoption of clouds are reviewed in this survey paper. It focuses on interconnection between privacy-protective technologies and regulatory needs, their effectiveness and drawbacks, and also outlines the upcoming issues. The debate seeks to point academia and industry the way to secure, privacy-sensitive and regulation-compliant cloud ecosystems.**

***Keywords*—Cloud Computing, Service Models, Deployment Models, Privacy-Preserving, Mechanisms. Compliance Frameworks, Secure Cloud, Cloud Adoption, Security, Privacy.**

INTRODUCTION

Cloud computing has become the revolutionary trend in both the academic and industrial world, which is the result of the development and adoption of different technologies and computational prototypes [1]. Storage, networks, servers, applications, and services may all be easily accessed on demand using shared clusters [2]. In the simplest definition, cloud computing refers to providing scalable IT-enabled services on a per-service basis as a service or resource provider over the Internet so that users can access resources dynamically without the demand to sustain costly infrastructure.

The speed of the transition toward cloud technologies has been catalysed by the meteoric increase in the volume of digitalized information, enhanced internet connection speeds, and the growing needs of flexible storage and computing resources [3]. The efficiency has also been enhanced by cloud databases, virtualization that allows organizations to develop, deliver and manage applications effortlessly [4]. Nonetheless, this ease of use poses serious issues in data privacy, security and regulatory compliance courses.

Security is a required underpinning to securing the cloud environments; however, this is not enough to instil trust in the users. Businesses and consumers alike are increasingly looking for assurances that their sensitive data will remain secure at all times, even when they aren't aware of certain threats [5]. Encryption, secure multi-party computation, differential privacy, and homomorphic encryption are examples of privacy-preserving mechanisms (PPMs) developed to safeguard sensitive data. These mechanisms, however, are susceptible to trade-offs in terms of the usefulness of data at the expense of their privacy levels; hence, their choice and setup are not easy. Since data gathered and processed in cloud settings is heterogeneous, automated tools have been suggested to aid in the configuration of PPMs and analysis results [6]. However, the problem of customization of PPMs to application-specific requirements is an open one.

In addition, there is also the concern of storage and processing of the data and managing data in a secure manner with so much data movement and volume [7]. Despite its scalable and cost-effective, the insidious nature of cloud computing is hampering its usage due to elaborate and tricky compliance guidelines [8]. The General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and the California Consumer Privacy Act (CCPA) are just a few examples of the new data protection and privacy rules that place stringent requirements on clouds and their users.

Cloud security frameworks have been presented to solve these risks. Such frameworks include rules, standards, policies, tools, and best practices that assist in assisting organizations in identifying vulnerabilities, controlling threats, and aligning their cloud operations to compliance requirements [9]. Cloud security frameworks also permit and provide a systematic way to address risk management, and therefore help enable cloud adoption and build trust.

A. Structure of the Paper

This paper organized in the following way: in the Section II, the principles of cloud computing presented along with the security issues related to cloud computing. Section III reviews privacy-preserving mechanisms, including cryptographic and anonymization techniques. Section IV discusses compliance frameworks such as GDPR, HIPAA, and NIST. Section V presents related literature, while Section VI concludes with insights and future research directions.

BASICS OF CLOUD COMPUTING AND SECURITY

Cloud computing is implemented using the centralization approach. Some argue that the advantages of modern security technologies—including data and process segregation, high availability, redundancy, and centralised security—make them the go-to for cloud computing providers. This leads providers to focus solely on protecting the cloud architecture [10]. However, a recent poll reveals that individuals are quite wary of moving their data and processes to the cloud due to privacy and security concerns. This is because customers do not always know where their data is stored or processed [11]. Some academics argue that privacy and security concerns with cloud computing are the biggest roadblocks to expanding the use of cloud services. Concerning the centralization concept and the anticipated expansion of cloud computing, security concerns would undoubtedly hinder its widespread adoption.

B. Cloud Computing Service Models

The different types of service models are briefly explained below. All of these models are used over the internet and have a pay-per-use strategy [12].

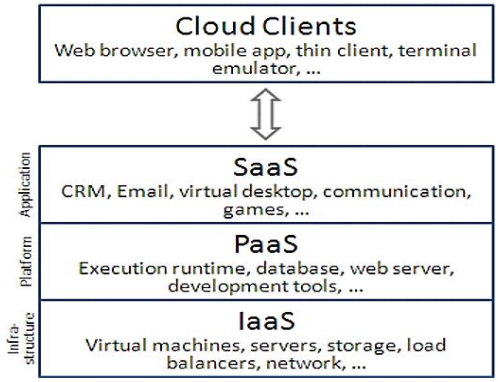

Fig. 1. The Layers of Cloud Service Models

Here are the cloud service models are as follows:

- **Software as a Service (SaaS):** Cloud computing's Infrastructure as a Service paradigm is one of three main ones. Figure 1 shows the infrastructure needs of a cloud computing platform with several layers. To execute their programs, users in this approach are given access to computer resources. Through a network of interconnected computers, the computing services are made available in a simulated setting, commonly known as the cloud.
- **Platform as a Service (PaaS):** Cloud-Based Platform is a subset of cloud computing that allows programmers to connect to a platform where they may create and access apps and services. Users can access PaaS services through web browsers because they are available in the cloud. The platform as a service (PaaS) concept relies on cloud providers to supply essential software components such as an OS, database, web server, and execution environment for programming languages.
- **Infrastructure as a Service (IaaS):** SaaS is the third approach; it makes software available to consumers over a cloud platform. Users of software as a service applications won't need to be concerned with the administration of the underlying cloud infrastructure or platform. The service providers are already responsible for software installation and operation with IaaS and PaaS. The applications are usually intended for end users and are made available through a network on an as-needed, pay-per-use basis.

C. Cloud Deployment Models

Cloud deployment tactics can be broadly categorised into four types: public, private, hybrid, and community [13]. See Figure 2 for an illustration of how each model caters to various organizational demands in terms of control, security, and scalability.

- **Public model:** Multiple users share the same storage hardware that their cloud provider supplies based on their subscription in this deployment architecture. Application development and testing, file-sharing, and non-mission-critical operations like email service make up the majority of public clouds' usage.
- **Private model:** This type of operation uses the cloud by a single company and has a cloud service provider, which can do the work on-site or off-site. The private cloud model requires more capital for acquisition and maintenance, making it more expensive than the public cloud model. Organizations' security and privacy issues are best handled by private clouds.

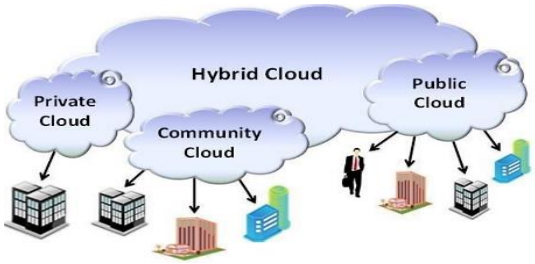

Fig. 2. Cloud Deployment Models

- Hybrid model: This deployment strategy is essentially a hybrid of the public and private cloud architectures, wherein an organization makes use of both types of cloud services. Businesses that experience cyclical storage needs often employ hybrid cloud solutions.
- Community model: Government agencies, financial institutions, businesses, etc., all work together under this approach.

D. Security and Privacy Challenges in Cloud Adoption

Data breaches, unauthorized access, and insider threats that threaten confidentiality are some of the issues that come with using cloud computing [14]. Additionally, issues like data location, regulatory compliance, and lack of transparency create barriers to maintaining privacy and trust in cloud environments:

- **Immoral use and abuse of cloud computing:** Storage and bandwidth capacity are just two of the many functions made available to consumers by cloud computing infrastructure [15]. However, malicious users and attackers are quick to exploit these weaknesses because the cloud infrastructure has limited control over these resources.
- **Malicious insider attackers:** One of the most underrated types of assaults, attacks perpetrated by hostile insiders, has the potential to compromise every part of the cloud infrastructure.
- **Vulnerable programming interfaces:** One feature of cloud services that allows user engagement at all levels

is the publication of application programming interfaces (APIs) that make deployment or development easier. The cloud architecture becomes even more intricate with the addition of these APIs.

- **Data leakage and loss:** A significant concern with cloud computing is data leakage, which occurs as a result of the constant movement and transmission of data between unrelated networks. The largest problem in the IT industry right now is data theft, which happens when data is lost. This has terrible financial ramifications for companies and their consumers.
- **Distributed technology vulnerabilities:** Virtualization for shared on-demand services is a feature of the multi-tenant architecture. This means that several users with access to the same application can share it.

PRIVACY-PRESERVING MECHANISMS IN CLOUD COMPUTING

Protecting Personal Data sanitization processes like generalization, suppression, perturbation, anonymization, permutation, and slicing are frequently used by mechanisms. By erasing or altering data properties, sanitization aims to safeguard sensitive information. The substitution of a more generalized value for an existing one is the same as generalization [6]. For example, establishing a hierarchy for category attributes and substituting intervals for numerical data are two examples. One way to hide data is to remove part of its values from an attribute; this is called suppression [16]. In tables, this action is commonly used to remove an entire row of entries or all of the values of an attribute from a column. The process of perturbation entails substituting values with identical statistical information for the original data. Adding noise is a frequent way to accomplish this procedure. In order to avoid associating sensitive attributes (SAs) with quasi-identifiers (QIDs), anatomization involves de-associating the two in two different databases. Rearranging values after they have been partitioned into a set is what a permutation is all about. It is common practice to combine this procedure with slicing, even though it is insufficient for real-world data when used alone.

E. Cryptographic Approaches

The goal of cryptography is to make data unintelligible to anybody who doesn't have the proper key to decipher it. The primary goal of cryptography is to prevent unauthorized people from gaining access to sensitive data [17]. The three pillars of security are availability, integrity, and confidentiality. Protecting sensitive data stored in the cloud is the primary goal of cryptography [18]. Two types of algorithms exist: (i) those that rely on symmetric keys and (ii) those that rely on asymmetric keys and are also known as public-key sets of rules. The goal of data cryptography is to encrypt data in a way that makes it unintelligible, undecipherable, and invisible during storage and transmission, whether it be text or media. Encryption is the name given to this technique [19]. Decryption refers to the opposite process of obtaining the genuine records from encrypted ones. It is possible to encrypt records on cloud storage using either symmetric or asymmetric keys; but, as illustrated in Figure 3, a symmetric key-based technique is faster for the majority of databases and information stored in cloud storage.

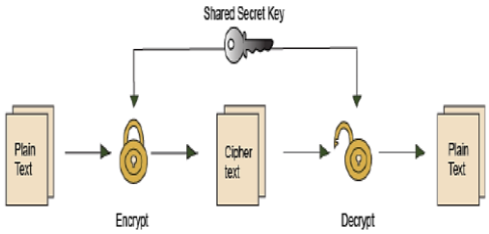

Fig. 3. Symmetric-key Cryptography

F. Data Anonymization Techniques

Data anonymization techniques are employed to safeguard sensitive information while enabling valuable research and analysis [20]. To avoid personal identification, these strategies use different types of data obfuscation or modification. Below are some of the most common types of data anonymization techniques:

- **Generalization:** The process of generalization entails substituting more general categories or ranges for more particular data values. This reduces the granularity of data, thus protecting individual privacy while maintaining some level of useful information.
- **Suppression:** Suppression refers to the complete removal of sensitive data fields or attributes from a dataset. This method is applicable in cases where some points of data information are felt to be too sensitive to save.
- **Data Masking:** Data masking is the practice of hiding sensitive information by using fake or encrypted values while keeping the underlying data's format and structure intact. Ensuring the security of sensitive data while preserving its usefulness for testing or analysis is the fundamental objective.
- **Perturbation:** The perturbation alters the original results by adding slight random deviations, which complicates the process of extracting specific knowledge but does not exclude the possibility of aggregate study
- **k-Anonymity:** k-Anonymity guarantees that no single dataset holding of a record can be distinguished by at least k other records on the attribute. This avoids re-identification such that a collection of records does not allow de-anonymization to one person.

G. Secure Multi-Party Computation (SMPC)

SMPC is a sophisticated system of mathematical constructs and cryptographic techniques that enable safe, collaborative computation over confidential information [21]. A number of people can enter values into a function, and the SMPC basically solves the problem of how to do it without letting each other in on the secret [22]. The section discusses the technical properties of SMPC, i.e. its mathematical background, its algorithmic description, and its cryptographic protocols:

1) Cryptographic Protocols in SMPC

SMPC relies on a multiplicity of cryptographic schemes so that the input of individual data is kept secret up to the execution of the computation. Such protocols are secret sharing, homomorphic encryption and oblivious transfer.

2) Mathematical Framework

SMPC is based on the principles of Number theory and complex algebra structures. The above classes of functions

that should be computed are often decomposed as circuits or as polynomials in order to simplify the computational procedures and to ensure secure executive process on encrypted data or shared data. SMPC security is normally analyzed in a computation model where adversary behavior and potential threats are considered to ensure that whatever the type of attack, the protocol is resilient to that attack.

3) Algorithmic Implementation

SMPC research aims to implement SMPC by reinterpreting the cryptographic protocols and mathematical models into computer-executable algorithms. This involves not only the design of efficient protocols to perform particular kinds of computation but also optimization of protocols in terms of speed and resource costs, and the provision of security against theoretical and practical attacks on the algorithms used. The practical concerns that should be addressed in the implementation include network communication among the parties, fault tolerance and the synchronization of the computation among the different participants.

COMPLIANCE FRAMEWORKS FOR SECURE CLOUD ADOPTION

Compliance frameworks offer assurance to organizations that the cloud is not disrupting industry, legal or regulatory laws compliance requirements but is rather a positive enabler [23]. More and more organizations are migrating sensitive workloads to the cloud, and compliance frameworks such as GDPR, HIPAA, ISO/IEC 27001, NIST Cybersecurity Framework and Cloud Security Alliance (CSA) guidance on data integrity and confidentiality accountability are becoming important sources of reference. By leveraging compliance frameworks to create a framework for compliance, organizations can reduce risks related to data privacy, cross-border data transfers, and regulatory obligations [24]. Compliance in cloud strategies is going to generate security weaknesses, risks that erode customer trust, and limit the availability of cloud technologies in specific industry, regulatory or legal sectors [25]. So, integrating compliance frameworks into cloud strategies enables a better measure of customer trust and the secure deployment of cloud technologies.

H. General Data Protection Regulation (GDPR) Compliance

The new rule for protecting personal data in the European Union (EU), called the General Data Protection Regulation (GDPR), came into effect on May 25, 2018. It affects all companies, regardless of location, that deal with personal data of EU residents. By definition, "any information relating to an identified or identifiable natural person" [26] is deemed personal data according to the General Data Protection Regulation (GDPR). Included in this category are both direct and indirect identifiers, such as names and government ID numbers, as well as, when applicable, online identifiers like IP addresses, cookies, and device IDs:

GDPR sets out some key principles relating to the processing of personal data.

- **Lawfulness, fairness and transparency:** Data should be processed in a lawful, fair, and transparent manner in such a way that individuals are informed as to what is being done with their data.
- **Purpose limitation:** Collection of personal data must have a specific, explicit and legitimate purpose and may not be used in other non-related actions.
- **Data minimization:** Personal data required to meet the explained purpose should be collected in only the necessary minimum amount.
- **Storage limitation:** Data must be retained as long as required by the purpose to which it was used and must be deleted securely when no longer needed any more.
- **Integrity and confidentiality:** Technical and organizational measures should be put in place to ensure the privacy of data from unauthorized access, adjustment or loss.

Data subjects are entitled to a variety of rights under it, including the following: access, rectification, erasure ("right to be forgotten"), restriction of processing, data portability, objecting, and rights pertaining to automated decision-making and profiling.

I. Health Insurance Portability and Accountability Act (HIPAA) Compliance

"HIPAA" stands for the Health Insurance Portability and Accountability Act. Administrative simplification (AM), a provision of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), places an emphasis on the need to secure health information in order to improve the efficiency and effectiveness of the healthcare system. The security, efficiency, and efficacy of the country's healthcare system are meant to be enhanced by the standard. Under specific conditions, HIPAA mandates the acquisition of consent prior to the disclosure of personally identifiable health information [27]. After de-identification, sharing health information without agreement is no longer restricted by the Privacy Rule. "Covered entities" [28] refer to businesses that must follow HIPAA rules. Health insurance companies, healthcare aggregators, medical facilities, home health agencies, nursing homes, pharmacies, labs, doctors, physical therapists, and primary care physicians are all examples of covered entities.

J. NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) was created in reaction to Executive Order (EO) 13636 of 2013 to strengthen the cybersecurity of America's vital infrastructure. It provides a voluntary, risk-based approach that organizations can adopt to strengthen their cybersecurity posture [29]. Identify, Protect, Detect, Respond, and Recover are the five pillars upon which the framework rests, and they encompass the whole range of cybersecurity operations that a company may undertake. These features are useful for handling important things like system recovery, incident response, monitoring, access control, and asset management. The framework can help businesses with a variety of tasks, including assessing the efficacy of vulnerability scanning procedures and how they fit into a larger risk management plan. Figure 4 depicts the five core functions of the NIST Cybersecurity Framework: Identify risks through assessment, protect systems with proactive safeguards, detect threats via continuous monitoring, respond with incident containment, and recover through resilience planning, ensuring comprehensive cybersecurity management.

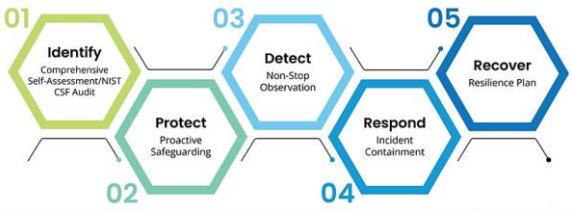

Fig. 4. The NIST Cybersecurity Framework

LITERATURE REVIEW

This literature Summary highlights diverse advancements in cloud security, encompassing risk assessment, privacy-preserving encryption, distributed learning, audience-based authorization, fog-based access control, and SDN-enabled architectures, while emphasizing persistent challenges and outlining future research directions for secure cloud adoption.

Drissi et al. (2025) offered the newest solutions to evaluating risks on cloud, thus, adding in the progress of an integrated RA as well as taking up the peculiarities of the cloud and the complexity of the system into consideration. Also, it is used to discuss the procedure of further research work that should contribute to the improvement of RA in terms of various criteria. This industrial revolution is based on key aspects of Cloud Computing, AI, Big data, the IoT. Cloud Computing is a service that provides organizations with a variety of possibilities which include; flexibility, scalability and cost effectiveness [30].

Mohamoud et al. (2024) examine the problem of image privacy in cloud computing ecosystems and suggest a new paradigm of privacy-enhanced image security based on the combined use of intelligent encryption mechanisms. The main research topic here is to prevent the security of sensitive visual information when the information is stored and processed within cloud platforms, in which conventional encryption cannot be sufficiently used to maintain confidentiality and utility. The proposed resolution utilizes smart encryption function that morphs according to the image to be encrypted, providing a high level of protection that doesn t compromise the needs of image processing within the clouds to be efficient. The results of this study are useful in continued conversation on privacy-preserving methods in cloud computing and can provide a fruitful direction in the creation of secure efficient image protection interventions [31].

Afzal et al. (2023) developed the paradigms emerging in distributed learning. The next section will provide a high-level review of distributed learning-related privacy and security concerns, and then it will offer solutions to those concerns. Also, highlight key areas of opportunity and challenge for future research on distributed systems strengthening. A number of approaches have recently emerged that can support ubiquitous IoT systems with distributed learning and pervasive computing. To address the drawbacks of centralised learning, such as privacy concerns and delay caused by sharing local data, several decentralised solutions have been put forward, with distributed computations being seen as a potential replacement for centralised learning [32].

Yi et al. (2022) a unique method for protecting personal data, wherein the effect of each audience on the data owner's privacy problem is assessed. More specifically, in order to satisfy the information owner's subjective needs, it is recommended to apply prospect theory in order to align the audience's impact with the owner's criteria. Access to the information should only be allowed to audiences that fit these matching parameters. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is also employed by the proposed method, which can likewise prevent service providers from obtaining private data. Thus, mechanism grants the data owner the ability to fulfil its unique needs while minimizing risk posed by individuals and service providers [33].

Gai et al. (2022) A fog-based access filter (FAF) is a concept for multi-layer access filtering that is specifically intended for fog computing environments that prioritize privacy. The three primary algorithms that comprise FAF are tuple reduction, optimal privacy-energy-time, and access filter initialization. To further differentiate the security goals, a hierarchical classification is employed. The experimental evaluation results demonstrate that FAF successfully strikes a balance between privacy protection and computing costs. Even among conservative and delicate spheres like the military and governments, fog computing is gaining traction [34].

Liang et al. (2021) a safe cloud using cloud computing, add security agents to the business cloud, link the two clouds using software defined networking, and use the security agents to dynamically partition the business cloud into logically separate areas. Consequently, security is considered independently of the business cloud's implementation technology and deployment scheme. To improve the security of network information, a protection scheme for information security in a cloud computing environment is suggested, taking into account certain factors' characteristics [35].

Table I provides a synopsis of current research on privacy-preserving methods and compliance frameworks for safe cloud adoption, comparing different studies and highlighting methodologies, important results, difficulties, and potential future research directions.

TABLE I. SUMMARY OF A STUDY ON PRIVACY-PRESERVING CLOUD ADOPTION FRAMEWORKS

Author	Study On	Approach	Key Findings	Challenges	Future Directions
Drissi et al (2025)	Risk assessment (RA) in cloud computing	Integration of AI, Big Data, IoT with Cloud Computing	Proposed solutions for comprehensive RA addressing cloud complexities	Handling multi-criteria risk factors in dynamic cloud environments	Develop adaptive RA frameworks considering evolving cloud risks
Mohamoud et al (2024)	Image privacy in cloud	Intelligent encryption techniques	Preserves confidentiality and utility of cloud-based image processing	Traditional encryption fails in maintaining both privacy and usability	Advance adaptive encryption for real-time cloud image security
Afzal et al. (2023)	Protecting personal information during remote education	Survey of decentralized learning approaches in IoT	Distributed systems mitigate privacy risks of centralized learning	Privacy leakage, latency, and system robustness	Explore robust privacy-preserving distributed learning frameworks
Yi et al. (2022)	Audience-based privacy-preserving mechanism	CP-ABE + Prospect theory	Selective authorization ensures owner-controlled privacy	Balancing subjective privacy requirements with system efficiency	Extend CP-ABE for scalable, user-centric privacy in cloud

Gai et al. (2022)	Fog-based access control	Fog-based Access Filter (FAF) with multi-layer filtering	Achieves balance between privacy protection and computational costs	High complexity in fog environments	Enhance scalability and efficiency in fog-cloud integration
Liang et al. (2021)	Protecting data in the cloud	security agents in an SDN-enabled cloud	Proposes logically isolated business cloud areas for enhanced security	Integration overhead and management of distributed agents	Design lightweight, adaptive cloud–SDN security architectures

CONCLUSION AND FUTURE WORK

Cloud computing has transformed the digital world by providing scalability, flexibility, and cost-effective solutions that allow organizations to utilize storage, processing, and applications efficiently. Through its deployment models, it reduces infrastructure costs while offering accessibility and performance benefits across industries. However, this paradigm shift is accompanied by persistent challenges in security, privacy, and compliance, which continue to hinder universal adoption. Cyberattacks, insider threats, and the complex demands of regulatory frameworks highlight the need for strong and consistent solutions. Privacy-preserving technologies, including cryptographic protocols, anonymization, and secure multi-party computation, along with internationally recognized guidelines such as GDPR, HIPAA, and NIST, are crucial in building trust and accountability. Despite its enormous potential as a driver of digital transformation, a critical concern remains in balancing usability and efficiency with stringent security controls. High implementation costs, compliance complexity, and performance overhead also limit widespread adoption.

The future of cloud security lies in the advancement of cryptographic algorithms, AI-based threat detection, and blockchain-enabled trust models. Optimized privacy-preserving strategies, integrated compliance monitoring, and harmonized international regulations will support secure scalability. Furthermore, energy-efficient practices, combined with seamless integration of IoT and edge environments, will shape sustainable, trusted, and globally adopted cloud solutions.

REFERENCES

[1] V. Verma, "Big Data and Cloud Databases Revolutionizing Business Intelligence," *TIJER*, vol. 9, no. 1, pp. 48–58, 2022.

[2] A. Reley, A. Jain, and M. S. Sabri, "A Literature Survey on Privacy-Preserving in Cloud Storage," *Researchgate.Net*, no. 7, pp. 7–14, 2018.

[3] V. Shah, "Securing the Cloud of Things : A Comprehensive Analytics of Architecture , Use Cases , and Privacy Risks," *ESP J. Eng. Technol. Adv.*, vol. 3, no. 4, pp. 158–165, 2023, doi: 10.56472/25832646/JETA-V3I8P118.

[4] J. Neethu, E. Daniel, and N. A. Vasanthi, "Survey on Privacy-Preserving Methods for Storage in Cloud Computing," *Researchgate.Net*, no. January 2013, pp. 1–4, 2013.

[5] V. Shah, "Managing Security and Privacy in Cloud Frameworks : A Risk with Compliance Perspective for Enterprises," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 6, pp. 606–618, 2022.

[6] M. Cunha, R. Mendes, and J. P. Vilela, "A survey of privacy-preserving mechanisms for heterogeneous data types," *Comput. Sci. Rev.*, vol. 41, p. 100403, Aug. 2021, doi: 10.1016/j.cosrev.2021.100403.

[7] M. Najana and P. Ranjan, "Compliance and Regulatory Challenges in Cloud Computing: A Sector-Wise Analysis," *Int. J. Glob. Innov. Solut.*, no. July, Jun. 2024, doi: 10.21428/e90189c8.68b5dea5.

[8] G. Maddali and S. J. Wawge, *Site Reliability Engineering*. 2025.

[9] 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.

[10] T. Alashoor, "Cloud computing: a review of security issues and solutions," *Int. J. Cloud Comput.*, vol. 3, p. 228, 2014, doi: 10.1504/IJCC.2014.064760.

[11] A. Sharma and S. Kabade, "Serverless Cloud Computing for Efficient Retirement Benefit Calculations," *Int. J. Curr. Sci.*, vol. 12, no. 4, 2022.

[12] S. B. Dash, H. Saini, T. C. Panda, and A. Mishra, "A Theoretical Aspect of Cloud Computing Service Models and Its Security Issues: A Paradigm," *J. Eng. Res. Appl. www.ijera.com ISSN*, vol. 4, no. 1, pp. 248–254, 2014.

[13] U. Patkar, P. Singh, H. Panse, S. Bhavsar, and C. Pandey, "Cloud Computing and Security Fundamentals," *Int. J. Comput. Sci. Mob. Comput.*, vol. 11, no. 4, pp. 18–24, 2022, doi: 10.47760/ijcsmc.2022.v11i04.004.

[14] Y. S. Abdulsalam and M. Hedabou, "Security and Privacy in Cloud Computing: Technical Review," *Futur. Internet*, vol. 14, no. 1, 2022, doi: 10.3390/fi14010011.

[15] S. P. Bheri and G. Modalavalasa, "Advancements in Cloud Computing for Scalable Web Development: Security Challenges and Performance Optimization," *J. Comput. Technol. Int. J.*, vol. 13, no. 12, 2024.

[16] N. K. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[17] A. J. S. Bhargav and A. Manhar, "A Review on Cryptography in Cloud Computing," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, 2020, doi: 10.32628/cseit206639.

[18] D. Patel and R. Tandon, "Cryptographic Trust Models and Zero-Knowledge Proofs for Secure Cloud Access Control and Authentication," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 2, no. 1, pp. 749–758, Dec. 2022, doi: 10.48175/IJARSCT-7744D.

[19] N. K. Prajapati, "Review of Quantum Computing Advances and their Impact on Modern Cryptographic Security," *Int. J. Innov. Sci. Res. Technol.*, pp. 2023–2035, May 2025, doi: 10.38124/ijisrt/25may501.

[20] B. Raghunathan, "- Data Anonymization Techniques," in *The Complete Book of Data Anonymization*, no. April 2023, Auerbach Publications, 2013, pp. 192–217. doi: 10.1201/b13097-20.

[21] U. H. Patel, "Secure Multi-Party Computation (SMPC) For Privacy-Preserving Data Analysis," vol. 12, no. 4, pp. 2320–2882, 2024.

[22] G. Modalavalasa and S. Pillai, "Exploring Azure Security Center : A Review of Challenges and Opportunities in Cloud Security," *ESP J. Eng. Technol. Adv.*, vol. 2, no. 2, 2022, doi: 10.56472/25832646/JETA-V2I2P120.

[23] V. M. L. G. Nerella, "Architecting Secure, Automated Multi-Cloud Database Platforms Strategies for Scalable Compliance.," *Int. J. Intell. Syst. Appl. Eng.*, vol. 9, pp. 128–138, 2021.

[24] A. Folorunso, O. Babalola, C. E. Nwatu, and and U. Ukonne, "Compliance and Governance issues in Cloud Computing and AI: USA and Africa," *Glob. J. Eng. Technol. Adv.*, vol. 21, no. 2, pp. 127–138, Nov. 2024, doi: 10.30574/gjeta.2024.21.2.0213.

[25] S. Narang and A. Gogineni, "Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment," *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, 2025, doi: 10.38124/ijsrmt.v4i5.542.

[26] S. Kanungo, "Data Privacy and Compliance Issues in Cloud Computing: Legal and Regulatory Perspectives," *Int. J. ofINTELLIGENT Syst. Appl. Eng.*, pp. 1721–1734, 2024.

[27] B. K. R. Janumpally, "A Review on Data Security and Privacy in Serverless Computing: Key Strategies, Emerging Challenges," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 3, p. 9, 2025.

[28] P. Tyagi, N. Aggarwal, B. P. Dubey, and E. S. Pilli, "HIPAA Compliance and Cloud Computing," *Int. J. Comput. Appl.*, vol. 70, no. 24, pp. 29–32, 2013, doi: 10.5120/12215-8356.

[29] J. Edwards and G. Weaver, " NIST Cybersecurity Framework ,"

Cybersecurity Guid. to Governance, Risk, Compliance, vol. 10, no. 8, pp. 191–207, 2024, doi: 10.1002/9781394250226.ch11.

[30] S. Drissi, M. Chergui, and Z. Khatar, "A Systematic Literature Review on Risk Assessment in Cloud Computing: Recent Research Advancements," *IEEE Access*, vol. 13, no. May, pp. 76289–76307, 2025, doi: 10.1109/ACCESS.2025.3561123.

[31] A. H. Mohamoud, G. Gupta, and A. Kumar, "Privacy-Preserving Image Protection in Cloud Computing Using Intelligent Encryption," in *2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0*, 2024, pp. 1–5. doi: 10.1109/OTCON60325.2024.10688284.

[32] M. U. Afzal, A. A. Abdellatif, M. Zubair, M. Q. Mehmood, and Y. Massoud, "Privacy and Security in Daistributed Learning: A Review of Challenges, Solutions, and Open Research Issues," *IEEE Access*, vol. 11, no. September 2023, pp. 114562–114581, 2023, doi: 10.1109/ACCESS.2023.3323932.

[33] Y. Yi, J. He, N. Zhu, X. Ma, and Y. Luo, "A Privacy-Preserving Mechanism Based on Privacy Situation Awareness for Information Sharing in OSNs," in *2022 3rd International Conference on Electronics, Communications and Information Technology (CECIT)*, 2022, pp. 285–290. doi: 10.1109/CECIT58139.2022.00057.

[34] K. Gai, L. Zhu, M. Qiu, K. Xu, and K.-K. R. Choo, "Multi-Access Filtering for Privacy-Preserving Fog Computing," *IEEE Trans. Cloud Comput.*, vol. 10, no. 1, pp. 539–552, 2022, doi: 10.1109/TCC.2019.2942293.

[35] H. Liang, H. Liu, F. Dang, L. Yan, and D. Li, "Information System Security Protection Based on SDN Technology in Cloud Computing Environment," in *2021 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA)*, 2021, pp. 432–435. doi: 10.1109/AEECA52519.2021.9574276.