Journal of Global Research in Electronics and Communication
Volume 1, No. 9, September 2025
Available Online at: www.jgrec.info
RESEARCH PAPER

Cloud Security and Privacy: A Systematic Review of Threats, Solutions, and Future Direction

Prof. (Dr.) Abid Hussain
Professor
School of Computer Application & Technology & Dean, Research
Career Point University
Kota
abid.hussain@cpur.edu.in, dean.research@cpur.edu.in

***Abstract*—The protection of data saved, transferred, and processed in cloud settings has become a significant concern as cloud computing becomes the foundation of today's digital infrastructure. Cloud systems' multi-tenant design can be complicated, and standard security models may not take these factors into account. The current state of cloud security and privacy is thoroughly examined in this assessment, with data breaches, unsafe APIs, and violations of regulatory compliance being the most important issues. Covered are the primary methods of mitigation, such as secure key management, data encryption while in transit and at rest, and intrusion detection systems for real-time threat monitoring. The paper also speaks on the use of the latest privacy-preserving technologies like homomorphic encryption and biometric cryptosystems to preserve confidentiality and not reporting functionality. The risks and consequences of multi-tenancy and compliance are also discussed to determine the effects of shared infrastructures on data isolation and governance. With more enterprises moving workloads to the cloud, it is crucial to safeguard the data of the enterprise which includes its confidentiality, integrity, and availability. This review will provide an in-depth insight into the current security issues, research gaps, and future research trends in terms of adaptive security frameworks, standardization of security protocols, and integration of privacy-enhancing technologies towards fostering trustworthy and resilient cloud adoption.**

Keywords—Cloud Security, Data Privacy, Multi-Tenancy, Encryption Techniques, Intrusion Detection Systems, Privacy-Preserving Technologies, Regulatory Compliance.

I. INTRODUCTION

Cloud computing has revolutionized the IT environment by allowing organizations to utilize shared computing facilities that deliver flexibility, cost and high scalability to the organization [1]. It is an enabling technology to a pay-as-you-go model, it uses resource sharing and storage virtualization so that it is appealing both to industry and academia [2]. Such characteristics as Fast elasticity, location-independent resource pooling, ubiquitous network connectivity, and on-demand self-service have enhanced the pace at which cloud has been adopted by people worldwide [3]. Mobile computing has also been developed, especially cloud computing and other forms of technology, which have enhanced productivity and service delivery.

The extension of conversations around security and privacy has also been facilitated by these advancements. Established data protection procedures are put to the test by the issue of cross-border data migration, the potential for data breaches, and unauthorized access [4]. The exposure of biometric data and other personal information introduces ethical and legal concerns regarding user privacy in the cloud [5]. Strong security standards are becoming more and more necessary as more businesses move vital services to the cloud [6].

The issues around cloud computing security and privacy [7]. It evaluates existing models, mechanisms, and frameworks designed to safeguard cloud infrastructure and user data [8]. Specifically, the review investigates key threats, surveys protection strategies, and highlights best practices used in the industry. It also seeks to uncover research gaps and propose future research directions to strengthen trust and resilience in cloud-based systems.

This review encompasses a wide range of scholarly and industry-based literature, focusing on the core issues of cloud security and privacy. It analyses widely used deployment methods (public, private, hybrid, and community) and service models (IaaS, PaaS, and SaaS), looking at how they affect data governance and security. Selection criteria were based on the technical depth, relevance, and clarity of contributions related to threat modeling, encryption techniques, access control, and regulatory compliance. Cloud security and privacy discuss important issues and predict which areas will be important in the future. Subsequent areas of the report look at essential models, key threats, protecting strategies and the latest innovations, giving a full picture for anyone interested in safe cloud adoption.

A. Structure of the Paper

This paper is organized in the following way: Section II covers the fundamentals of cloud security and privacy. Section III discusses key security threats and privacy challenges. Section VI reviews defense mechanisms and privacy-preserving techniques. Section V examines recent literature on advanced security models and emerging technologies. Section VI concludes with insights and future research directions.

II. CLOUD SECURITY AND PRIVACY FUNDAMENTALS

The integrated collection of frameworks, rules, and technologies known as "cloud security" is intended to defend cloud-based infrastructure, data, apps, and systems against a range of cyberthreats [9]. Privacy in cloud computing relates to ensuring that sensitive and personal data is gathered from users, stored, and processed in compliance with legal, ethical, and contractual requirements [10]. These privacy and security precautions are particularly important in multi-tenant settings since shared resources raise the possibility of data leakage and

illegal access. Effective cloud governance demands the implementation of robust controls to ensure confidentiality, integrity, availability, and accountability across all layers of the cloud stack.

A. Cloud Computing

Resource access and administration have been revolutionised by cloud computing, which offers scalable, on-demand services over the Internet. Across sectors, cloud systems have been adopted due to their scalability and adaptability. Cloud computing providers provide three primary models: Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and Software as a Service (SaaS). By providing varied degrees of concepts and services, these models satisfy certain economic and technological goals [11]. Figure 1 illustrates the deployment and service methodologies of two distinct forms of cloud computing:

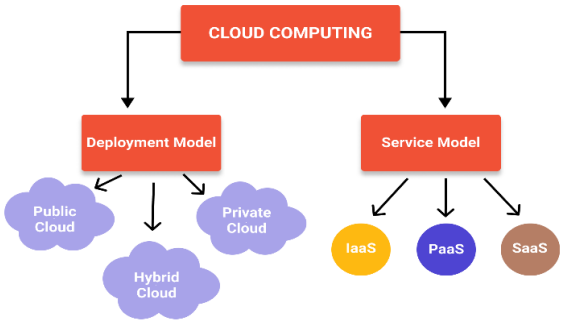

Fig. 1. Types of cloud computing models

- **Infrastructure as a Service (IaaS):** In only a few minutes, anyone may have a virtual server using the IaaS model, and they only have to pay for the services they use. Users may directly access infrastructure components under this paradigm that give them actual or virtual resources to satisfy their needs, including CPU, memory, operating system, and storage.
- **Platform as a Service (PaaS):** Customers that use Access to a platform or development environment that allows them to deploy their own code and apps are provided with PaaS. The customer is responsible for creating their own apps that run on the provider's infrastructure. To enable customers to administer applications, a product as a service provider provides a preconfigured operating system and application server configuration. LAMP (Linux, Apache, MySQL, and PHP), Ruby, J2EE, and others.
- **Software as a Service (SaaS):** A software supplier licenses a program to be used and paid for as required under the SaaS model. Applications may be accessed via a range of clients, such as mobile phones and web browsers, across a network. No client installation is required; all it need is a client device, such as a browser, and network connectivity [12].

Clouds can be classified as private, hybrid, or public. Public clouds, which offer shared resources via the internet, are managed by third-party businesses. Private clouds that are hosted or located on-site are dedicated to a particular business. Hybrid clouds integrate both, allowing for more flexibility through data and app exchange.

1) Key Security Principles in Cloud Environment

Effective cloud security governance requires clear accountability and a well-defined distribution of security responsibilities across the organization. Data protection remains a fundamental pillar of cloud security.

- Organizations must implement strong encryption methods, data masking, and access restrictions to safeguard private information processed and stored in the cloud.
- Encryption should be applied to guarantee that sensitive data cannot be accessed by unauthorized people while it is at rest or in motion. Additionally, the concepts of least-privilege and RBAC ought to be implemented.
- Cloud environments are dynamic and require continuous vigilance.
- Security teams must continuously monitor cloud environments for potential vulnerabilities, threats, and anomalies.
- An incident response strategy that is well stated is essential for handling security lapses or cyberattacks.

Effective cloud security demands strong encryption, stringent access restrictions, and ongoing observation. A proactive incident response plan ensures resilience against dynamic threats.

2) Privacy Concerns in Multi-Tenant Architectures

Cloud computing's core feature of multi-tenancy allows several tenants to share a single cloud infrastructure. The process of making Software that is available to multiple users in a single instance is referred to as "multitenancy." Figure 2 illustrates how a multi-tenancy cloud architecture operates.

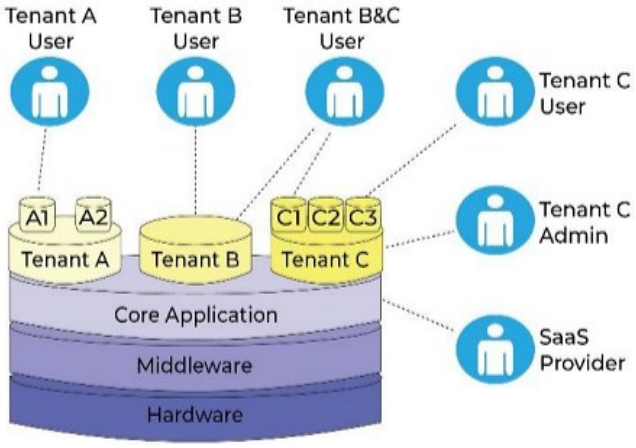

Fig. 2. Working of Multi-Tenancy Cloud Architecture

In a multi-tenant architecture, providers can use virtual machines to run several hardware versions on a single server. Because each version is distinct and encrypted, each tenant's data is safeguarded. Multi-tenancy enables easy access, maintenance, configuration, and modification of the information in a single database operating on the identical system [13].

3) Key Benefits of Cloud Security and Privacy Managed Services

There are several benefits of using managed services for cloud security, illustrated in Figure 3. Security is always on the agenda for providers of digital services, and constant monitoring 24/7 is no easy task. SECaaS (Security as a Service) adds an extra layer of protection to secure the data [16]. Security breaches are expensive, and managed services provide the proof and dependability that the data is safe [14].

It also removes the hassle of employing security professionals or being concerned with constant upgrades in hardware and software.

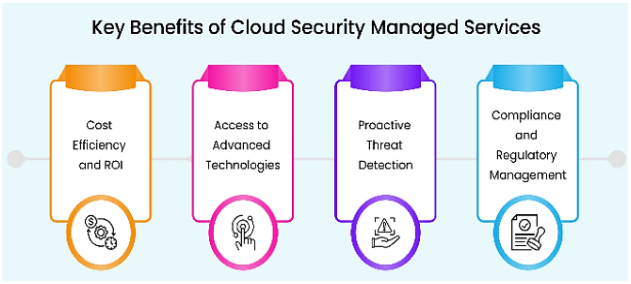

Fig. 3. Benefits of Cloud Security

MSPs are essential for improving a business's security posture since they proactively prevent the escalation of security incidents by offering real-time threat detection and response. They simplify compliance management, ensuring businesses adhere to industry regulations and standards. By outsourcing security, organizations can focus on their core operations while maintaining a strong safety stance, giving them a strategic advantage. Moreover, MSPs deliver ongoing security refinements, responsive solutions, and updates, which maintain business continuity and disaster recovery by enabling rapid recovery in case of possible security breaches.

- **Cost Efficiency and ROI:** Cloud security managed services minimize the requirement to have an in-house team which is quite expensive and the solution they provide is scalable such that the businesses only pay what they use hence more financial efficiency.
- **Access to Expertise and Advanced Technologies:** MSPs provide access to top-tier security experts and advanced technologies, ensuring businesses stay ahead of cyber threats.
- **Proactive Threat Detection and Incident Response:** MSPs detect threats early and respond quickly, preventing costly security breaches with effective incident management.
- **Compliance and Regulatory Management:** MSPs handle compliance challenges by ensuring businesses meet industry standards, avoiding penalties and reducing regulatory risk.

III. Classification of Security and Privacy Threats in Cloud

The security and privacy of cloud environments are commonly encountered with emerging threats that put organizational resilience and data protection at risk. The most significant risks that may have devastated financial and reputational consequences are data breaches and unauthorized access. Weak APIs and insecure interfaces also extend to the risk of misuse of cloud services due to their vulnerability, inter-application communication is also compromised [15]. Moreover, the requirements of regulatory and compliance are placing heavy restrictions on data confidentiality, integrity, and accountability, making adoption of cloud difficult. In this section, these essential threat vectors are explored in a systematic order, and this gives a basis upon which the available defense mechanisms can be analyzed and can be used to carry out future researches to enrich cloud security and privacy models.

A. Data Breaches and Unauthorized Access

Data breaches can be defined as the unauthorized access of sensitive information that has been stored in the cloud and can be mostly caused by the low access controls, poor encryption, or the vulnerability of cloud storage systems. This can result in huge financial losses, legal implications, as well as reputational damage that can be very difficult to overcome in the long term and hence, business survival [16]. To deal with these risks, cloud security frameworks present systematic guidelines that include policies, standards, tools, and best practices with a view of securing cloud infrastructure. These frameworks assist the organizations to understand their weakness and evaluate their threats and put measures in control to manage and reduce cloud security risks in a systematic manner.

B. Insider Threats

Insider threats are those insiders who have legitimate access to cloud systems with bad intentions of abusing them to the detriment of the organization. Such threats can either be evil where the attacker deliberately steals or sabotages information or accidental where the individual is untrained or careless [17]. Another factor that increases the risks in cloud environments is shared infrastructure and decentralized control [18]. The phrase refers to the current and former members of staff and the third-party partners whose legitimate credentials enable them to evade standard security measures. There are three types of insider threats in general.

- Malicious insiders who deliberately inflict harm:
- Insiders who are careless and inadvertently cause weaknesses.
- Compromised insiders who have had their credentials stolen by outside attacks.

To counter these dangers, stringent access control, ongoing observation, user training, and behavioral analytics are needed.

C. Denial of Service (DoS/DDoS) Attacks

The DoS and DDoS assaults in clouds differ from attacks on traditional networks due to vulnerabilities unique to the cloud [19]. Besides service interruption and resource exhaustion, Economic Denial of Sustainability (EDoS) attacks can affect cloud services [20]. where the attackers leave autoscaling being misused to drive up costs under consumption-based billing. Such attacks not only cause challenges on financial resources, but they may also impact on various tenants since the infrastructure is shared. The action to be taken in mitigation is filtering on the traffic, rate limiting, anomaly detection and intelligent scaling rules.

D. Insecure APIs and Interfaces

Cloud APIs (Application Programming Interfaces) are the most important tool to enable the interaction between cloud services and outsider applications. They play a critical role in promoting operability between clouds, as well as, user experience by promoting smooth integration between platforms. The growing dependence on APIs, however, creates a possible security hole, and, therefore, APIs are an essential part of cloud security evaluations.

The APIs that are provided by the clouds can be categorized into two broad categories, which are In-process APIs and Remote APIs.

- The APIs used in in-process APIs share the same memory space with the application. They are usually functional, methods, objects or procedures that hide low-level resources of the system, like allocation of memory, data structures or code that can be executed. The in-process APIs are often employed by developers when they need low-latency communication, intra-application tight coupling and require high efficiency because they provide direct access to internal system resources [21].
- Remote APIs, however, are meant to communicate between different systems or networked worlds. Such APIs make distributed parts communicate, and in many cases, they are published on the internet, thus widening their attack surface. The typical examples of remote APIs are:
  - **Web Services APIs:** based on protocols that enable communication over HTTP, such as REST and SOAP).
  - **Remote Procedure Calls:** Technologies like Sun RPC, Java RMI, and AME enable invoking procedures on remote servers as if they were local.
  - **Message Passing Protocols:** Simple Text Orientated Messaging Protocol (STOMP) and AMQP are two examples of protocols that provide asynchronous message-based communication between services.
  - **Application-Specific Protocols:** These include the Simple Network Management Protocol (SNMP) and FTP, which address certain application-level interactions.

These interfaces offer powerful integration capabilities, it also poses significant security risks if not properly secured. Common vulnerabilities include weak authentication mechanisms, insufficient access control, lack of encryption, and improper input validation. As cloud environments grow increasingly interconnected, securing APIs becomes imperative to prevent unauthorized access, data breaches, and service disruptions.

E. Regulatory and Compliance-Related Risks

There are many challenges when a company moves to the cloud, including privacy, security, and compliance, despite the growing popularity and demand. Although there are several studies that examine security and privacy in cloud computing [22]. only compliance-related elements are covered; in fact, there aren't many studies that focus only on compliance-related issues.

Regulations are sets of rules that govern the usage of confidential corporate data. Through the enforcement of qualities like confidentiality, integrity, availability, and accountability (CIAA), these regulations' primary objectives are to safeguard the privacy and security of customers. Compliance is defined as upholding the rules that implement the policies specified in the regulations [23]. Legal compliance is seen to be the most crucial Non-Functional Requirement (NFR) for many software systems.

IV. Security and Privacy Solutions and Mitigation Strategies

Effective mitigation strategies are critical to addressing the intricate privacy and security concerns with cloud computing. Data confidentiality and integrity are achieved using encryption techniques such as data-at-rest security and strict key management [24]. IDS and Prevention Systems are used as an adjunct to network defense to continually monitor and respond to malicious activity. Additionally, increasingly sophisticated privacy-preserving technologies allow for safe computation on encrypted data without revealing personal information, such as biometric cryptosystems and homomorphic encryption [25]. This part critically assesses these solutions, and they include their contribution to Future research on secure cloud environments and strengthening cloud security designs.

A. Security and Privacy Solutions in Cloud

The foundation of robust cloud security is intrusion detection, access control, encryption, and secure APIs, which secure data. It is private due to homomorphic encryption, anonymization, and adherence to data protection laws, which include:

1) Cloud Encryption Methods and Key Management

The importance of data availability is growing as more data is processed and stored in cloud settings, and confidentiality and integrity are crucial. Encryption as a security control is the major security technique that secures sensitive information against unauthorized access and monetary loss. Data encryption is a security measure that reduces risks by making information unintelligible and requiring a decryption key:

- **Data-at-Rest Encryption:** Data held on physical media, such hard drives or cloud storage systems, is protected by data-at-rest encryption, from unauthorized access.
- **Key Management in the Cloud:** In cloud security, key management is a crucial element, as it ensures that encryption keys used to protect sensitive data are generated, stored, and handled securely [26].

2) Secure Cloud Storage Solutions and Zero Trust Architecture (ZTA)

Secure cloud storage solutions use methods like end-to-end Data availability, confidentiality, and integrity are protected via encryption, access control, and redundancy. These technologies shield private information from unwanted access, both at rest and in transit [27]. Zero Trust Architecture (ZTA) has been used because dynamic cloud environments have made traditional perimeter-based security techniques insufficient. ZTA, which follows the tenet of "never trust, always verify," employs robust access controls, continuous authentication, and micro-segmentation strategies. For each access request, ZTA demands identity verification and policy-based authorization rather than relying on implicit trust inside the network. When integrated with secure storage mechanisms, ZTA offers a strong foundation for contemporary cloud security, significantly reducing the likelihood of insider threats and data breaches.

3) Intrusion Detection and Prevention Systems (IDPS)

Network security has risen to prominence as a critical concern in the last few years. An IDPS is a software that monitors computer networks for malicious activities, such as censorship, protocol breaches, and data theft. IDSs are frequently employed by both internal and external attackers to detect known and unexpected network threats. Most intrusion detection systems on the market today are unable to manage the complex and dynamic nature of computer network threats [28].

An IDS detects network intrusion via monitoring of network activities. These days, there are two primary forms of IDS: either network-based or host-based. In contrast to HIDSs, which are intended to identify network intrusions in particular hosts, NIDSs are intended to identify intrusions by monitoring various network activity.

4) Privacy-Preserving Technologies (e.g., Differential Privacy, Homomorphic Encryption)

Privacy-preserving technologies are essential in protecting sensitive data in cloud environments, especially when handling personally identifiable information such as biometric data. The measuring of human physiological and behavioral traits to identify and characterize people is known as biometrics [29]. The term "biometric attribute" may refer to both physical characteristics (like a fingerprint, face, or iris) and mental ones (like a signature, keystroke, or voice). As seen in Figure 4, the choice of protection method is contingent upon particular applications and the required degree of security, since each category has unique characteristics, benefits, and drawbacks that are detailed below:

- **Biometric Cryptosystems:** The advantages of cryptography and biometrics are combined in bio-cryptosystems. Secret keys in bio-cryptosystems are either generated directly from biometric data or are technically linked to it.
- **Homomorphic Encryption (HE):** Data privacy concerns are addressed by homomorphic encryption, which performs many actions on the encrypted data without requiring decryption. Because the HE computation's output is encrypted and only the data owners may decode it [30].

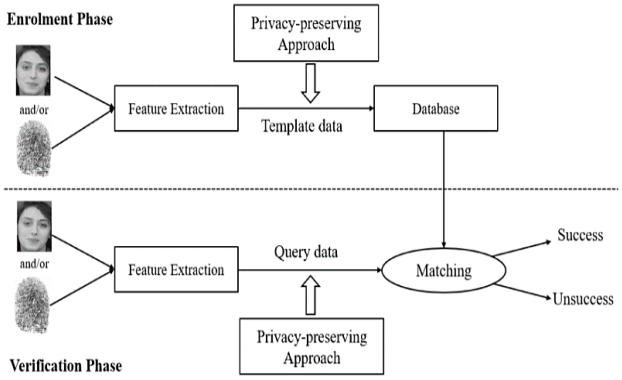

Fig. 4. A privacy-preserving functionality (e.g., homomorphic encryption).

5) Emerging Trends and Future Directions

Cloud computing is advancing with key trends reshaping its landscape. The ability of edge computing to analyze data near the source is advantageous for IoT and real-time applications, which lowers latency. The combination of AI and ML enables chatbots, fraud detection, intelligent automation, and predictive analytics. Serverless computing (FaaS) allows code execution without server management, with auto-scaling and cost efficiency. Quantum cloud services, such as Google Quantum AI and IBM Quantum, offer access to powerful computation for complex problem-solving [31]. These trends enhance performance, scalability, and innovation across sectors.

Here are some Future directions in cloud are as follows:

- **Hybrid and Multi-Cloud Evolution:** Hybrid and multi-cloud strategies will continue to evolve, offering greater flexibility and resilience. Advances in cloud orchestration and automation will enable seamless integration across multiple cloud environments, reducing complexity and improving security.
- **AI-Driven Cloud Automation:** AI will play a more significant role in automating cloud management, optimizing resource allocation, and enhancing security. AI-driven cloud platforms will provide self-healing infrastructure, predictive analytics, and automated threat detection, lowering operational expenses and human involvement.
- **The Impact of 5G on Cloud Computing:** The 5G networks will improve cloud computing capabilities by offering low latency and incredibly fast connectivity. This will drive innovations in cloud gaming, remote work solutions, and IoT applications, enabling real-time data processing and seamless cloud interactions.
- **Enhanced Security and Zero-Trust Architecture:** As cyber threats evolve, cloud security will focus on implementing zero-trust architectures [32]. The model supposes that no system or user is trusted and that any access privileges are required to be verified at all time. Cloud providers will improve security standards to reduce the dangers of ransomware, insider attacks, and data breaches.
- **Cloud-Native Development and Kubernetes Adoption:** Cloud-native development, driven by containerization and microservices architecture, will become the standard for application deployment. In hybrid and multi-cloud contexts, Kubernetes, an open-source container orchestration technology, will be essential for managing cloud-native applications.

V. Literature Review

This section presents a literature review on cloud security and privacy, emphasizing threat classifications, security models, AI-driven defense mechanisms, privacy-preserving techniques, and workflow protection strategies. Table I summarizes key studies, their approaches, findings, challenges, and future directions, offering a thorough analysis of the changing field and unmet research needs in cloud security.

Liang and Xu (2025) analyze the security situation in the cloud nowadays. The four types of artefacts into which findings are separated are constructs, models, techniques, and instantiations; the study greatly expands the technological understanding of the topic. At different levels of cloud architecture, the following areas are assessed: Identity and access, data management, host and virtualization, application and software, privacy, trust, and compliance. In order to better understand the difficulties businesses have in protecting their cloud-based systems from dangers like data breaches, unauthorized access, and cyberattacks, the suggested study approach is used. To improve cloud security, the evaluation also looks at how advanced technologies like blockchain, zero trust, multi-cloud architecture, ML, and AI may be integrated into a variety of industries, including healthcare, the IoT, and smart cities [33].

Shaffi (2025) study looked at how AI may improve cloud security through AI-stirring encryption, predictive analytics, and behavior-based security threat detection. Additionally, it describes the issues with earlier security models and how AI fixes them. Similar justifications underlie the coverage of

topics like data privacy, AI model biases, and regulatory compliance. Therefore, artificial intelligence (AI) enhances cloud computing security; nevertheless, further work is required in the following stages to expand the reliability, modularity, and ethical aspects of the technology. This implies that blockchain and other cutting-edge computing technologies may be used with AI to further enhance security frameworks. The study addresses future research and application possibilities while discussing current trends in cloud data architecture security utilizing AI [34].

Dhinakaran et al. (2024) panorama of privacy concerns at the dynamic nexus of cloud and IoT systems was carefully examined in this article. The thorough literature analysis summarizes the body of research, highlighting important issues and identifying new developments in privacy-preserving strategies. The classification of various methods reveals a sophisticated comprehension of access control systems, encryption methods, anonymization tactics, and the increasing incorporation of artificial intelligence. The implementation of AI-powered access control systems, homomorphic encryption for secure computing, and ML for dynamic anonymization are some significant advancements. This survey's conclusion offers a comprehensive perspective and establishes the foundation for comprehending the many approaches used to protect sensitive data in IoT-based cloud systems. For academics, professionals, and policymakers navigating the difficult terrain of privacy protection in the quickly evolving IoT and cloud computing landscape, the survey's insights offer a useful resource [35].

Chauhan and Shiaeles (2023) analyze cloud security frameworks, discussing problems related to the cloud and offering remedies. By increasing understanding of the different frameworks, their research helps people make informed choices about the security measures to implement for cloud-based systems. The article begins with a summary of cloud computing before delving into its drawbacks and infrastructure security standards. It next looks at several cloud security frameworks that are available on the market. The framework's emphasis, breadth, approach, strengths, limits, implementation procedures, and tools are all evaluated through a thorough comparison. The focus of this study is on well-designed frameworks such as STAR, Cloud Security Alliance, International Organization for Standardization (ISO), COBIT5, AWS, and the NIST. Afterwards, the research delves into determining and examining common cloud security problems [36].

Soveizi, Turkmen and Karastoyanova (2023) recognised the gaps and limits in reviewing the most recent advancements in tackling privacy and security concerns with cloud-based research and commercial processes, as well as the body of existing research in this field. They begin by classifying the most advanced security solutions in this comprehensive literature study according to the workflow life cycle stages that they are meant to handle. They provide a comprehensive evaluation and grouping of the best available research on the phases of workflow implementation, monitoring, and adaptation, based on their findings. Lastly, a list of unresolved research questions on cloud-based process security was explored and presented. Because cloud computing can provide a substantial quantity of computer resources when needed, its use has grown in tandem with the expansion of data-intensive and compute-intensive applications, including business and scientific endeavors [37].

Sarkar et al. (2022) review contrasts Modern research models for zero-trust cloud networks include special features that are tailored to requirements. When completely implemented, ZTNA enables network managers to handle critical challenges as preventing external and internal cyberattacks, improving network visibility, coordinating user security, and automating trust calculations for network entities. In the context of contemporary cloud computing networks, it prioritizes domain-specific challenges via intelligent security orchestration, automation, and response in addition to selecting and implementing the necessary features. The main goal of this study is to examine the innovative features used by state-of-the-art research models for zero-trust cloud networks that are created to address certain requirements. The article also covers the criteria for creating zero-trust architecture and the difficulties with cloud platforms[38].

Table I summarizes key studies on cloud security and privacy, highlighting focus areas, approaches, main findings, challenges, and future research directions.

TABLE I. COMPARATIVE ANALYSIS OF RECENT STUDIES ADDRESSING SECURITY THREATS, PRIVACY CONCERNS IN CLOUD ENVIRONMENTS

Reference	Study On	Approach	Key Findings	Challenges	Future Direction
Liang & Xu (2025)	Multi-layered cloud security frameworks	Systematic categorization and framework analysis	Identified constructs, models, methods, and instantiations across cloud layers	Managing security in diverse domains; compliance	Integration of ML, blockchain, and zero-trust across smart ecosystems
Shaffi (2025)	AI in cloud security	Review of AI-enhanced techniques	AI enables behavior-based detection, predictive analytics, and intelligent encryption	Bias in AI models, regulatory compliance, ethical concerns	Combine AI with blockchain and modular architectures
Dhinakaran et al. (2024)	IoT-cloud privacy	Comparative review of ML algorithms in healthcare (cancer, diabetes, brain tumor)	Trends in anonymization, AI-driven access control, homomorphic encryption	Real-time dynamic threats in IoT-cloud environments	AI integration in privacy automation, scalable encryption
Chauhan et.al. (2023)	Analysis of cloud security frameworks, including AWS Well-Architected, CSA STAR, NIST, ISO, and COBIT5	Comparative analysis of existing frameworks; assesses their implementation tools, scope, strengths, and limits	Provides a comprehensive understanding of cloud security governance models; helps organizations choose suitable frameworks	Complexity in framework integration, lack of standardization across sectors, and implementation difficulties	Suggests the need for a unified, adaptive security framework tailored for dynamic cloud environments
Soveizi et al. (2023)	Workflow security in cloud	Workflow life cycle-based classification	Analyzed security strategies by workflow phase	Fragmented solutions across workflow phases	Unified models for secure cloud-based workflow orchestration

Sarkar et al. (2022)	Cloud computing's Zero Trust Architecture (ZTA)	Comparative survey of ZTA approaches	Emphasized security orchestration, automation, and intelligent access	Difficulty in ZTA deployment, lack of real-time adaptability	Research into AI-integrated ZTA for dynamic enterprise cloud systems

VI. Conclusion and Future Work

Cloud computing's broad use has drastically changed how digital services are delivered by providing increased scalability, flexibility, and cost-effectiveness. But, particularly in multi-tenant and virtualized systems, this transformation has also exacerbated significant security and privacy concerns. This study has carefully investigated the risks connected to cloud computing, such as data breaches and dangerous APIs, as well as the intricacies of regulations, while assessing how well the present defenses are working. Service models like IaaS, PaaS, and SaaS, though beneficial, demand rigorous implementation of intrusion detection systems, access control methods, and encryption protocols. Examples of privacy-preserving technologies that are now necessary for secure computing without jeopardizing user confidentiality are biometric cryptosystems and homomorphic encryption. Ensuring data protection, regulatory compliance, and operational resilience in such dynamic environments requires adaptive governance and multi-layered security strategies.

Future studies should concentrate on creating scalable and intelligent cloud security frameworks that can automatically adjust to attacks in real time. The development of privacy-enhancing technology like federated learning and differential privacy should be prioritized, while also exploring quantum-resistant encryption to prepare for next-generation security challenges. Establishing standardized, globally harmonized compliance protocols will be crucial in addressing cross-border data governance issues. Additionally, integrating AI/ML for automated threat detection and leveraging collaborative efforts across academia, industry, and policy domains will be essential in constructing a secure, privacy-centric, and future-ready cloud ecosystem.

References

[1] V. Shah, "Managing Security and Privacy in Cloud Frameworks: A Risk with Compliance Perspective for Enterprises," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 06, pp. 1–13, 2022, doi: 10.14741/ijcet/v.12.6.16.

[2] Y. S. Abdulsalam and M. Hedabou, "Security and Privacy in Cloud Computing: Technical Review," *Futur. Internet*, vol. 14, no. 1, Dec. 2021, doi: 10.3390/fi14010011.

[3] P. K. P, S. K. P, and A. P.J.A., "Attribute based encryption in cloud computing: A survey, gap analysis, and future directions," *J. Netw. Comput. Appl.*, vol. 108, pp. 37–52, Apr. 2018, doi: 10.1016/j.jnca.2018.02.009.

[4] L. A. Tawalbeh and G. Saldamli, "Reconsidering big data security and privacy in cloud and mobile cloud systems," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 33, no. 7, pp. 810–819, Sep. 2021, doi: 10.1016/j.jksuci.2019.05.007.

[5] A. R. Ladole, K. K. Chhajed, and F. M. Shelke, "A Survey on Privacy Preserving Techniques in Cloud Environments," in *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, IEEE, Mar. 2018, pp. 1–5. doi: 10.1109/ICCTCT.2018.8551019.

[6] A. R. Duggasani, "Scalable and Optimized Load Balancing in Cloud Systems: Intelligent Nature-Inspired Evolutionary Approach," *Int. J. Innov. Sci. Res. Technol.*, vol. 10, no. 5, pp. 2153–2160, May 2025, doi: 10.38124/ijisrt/25may1290.

[7] S. Kabade and A. Sharma, "Cloud-Native AI Solutions for Sustainable Pension Investment Strategies," *Int. J. All Res. Educ. Sci. Methods*, vol. 13, no. 3, pp. 3930–3939, 2025.

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

[9] A. Mishra, "AI-Powered Cyber Threat Intelligence System for Predicting and Preventing Cyber Attacks," *Int. J. Adv. Eng. Manag.*, vol. 7, no. 02, pp. 873–892, 2025.

[10] V. Singh, "Lessons Learned from Large-Scale Oracle Fusion Cloud Data Migrations," *Int. J. Sci. Res.*, vol. 10, no. 10, pp. 1662–1666, 2021.

[11] 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 Trend," in *2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE)*, IEEE, Oct. 2024, pp. 1–6. doi: 10.1109/ICECCE63537.2024.10823401.

[12] D. Rani and R. K. Ranjan, "A Comparative Study of SaaS , PaaS and IaaS in Cloud Computing," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 6, pp. 458–461, 2014.

[13] S. Chippagiri, "A Study of Cloud Security Frameworks for Safeguarding Multi-Tenant Cloud Architectures," *Int. J. Comput. Appl.*, vol. 186, no. 60, pp. 50–57, Jan. 2025, doi: 10.5120/ijca2025924369.

[14] Abhishek and P. Khare, "Cloud Security Challenges: Implementing Best Practices for Secure SaaS Application Development," *Int. J. Curr. Eng. Technol.*, vol. 11, no. 06, pp. 669–676, Nov. 2021, doi: 10.14741/ijcet/v.11.6.11.

[15] B. Chaudhari, S. C. G. Verma, and S. R. Somu, "Next-Generation Authentication and Authorization Models for Secure Financial Microservices APIs: Challenges, Innovations, and Best Practices," *Int. J. Curr. Sci.*, vol. 14, no. 1, 2024, doi: 10.56975/ijcsp.v14i1.303089.

[16] D. Molitor, A. Saharia, V. Raghupathi, and W. Raghupathi, "Exploring the Characteristics of Data Breaches: A Descriptive Analytic Study," *J. Inf. Secur.*, vol. 15, no. 02, pp. 168–195, 2024, doi: 10.4236/jis.2024.152011.

[17] V. S. Thokala, "Improving Data Security and Privacy in Web Applications : A Study of Serverless Architecture," *Tech. Int. J. Eng. Res.*, vol. 11, no. 12, pp. 74–82, 2024.

[18] E. R. Sophie, "Insider Threats in Cloud Computing: Detection and Mitigation Strategies," 2025.

[19] H. Kali, "The Future of HR Cybersecurity: AI-Enabled Anomaly Detection in Workday Security," *Int. J. Recent Technol. Sci. Manag.*, vol. 8, no. 6, pp. 80–88, 2023.

[20] A. Bhardwaj, V. Mangat, R. Vig, S. Halder, and M. Conti, "Distributed denial of service attacks in cloud: State-of-the-art of scientific and commercial solutions," *Comput. Sci. Rev.*, vol. 39, p. 100332, Feb. 2021, doi: 10.1016/j.cosrev.2020.100332.

[21] I. Odun-Ayo, C. Okereke, and O. Evwieroghene, "Cloud and Application Programming Interface," in *he World Congress on Engineering 2018*, 2018.

[22] G. Maddali, "An Efficient Bio-Inspired Optimization Framework for Scalable Task Scheduling in Cloud Computing Environments," *Int. J. Curr. Eng. Technol.*, vol. 15, no. 3, pp. 229–238, 2025.

[23] S. Balasubramaniam and V. Kavitha, "A survey on data encryption tecniques in cloud computing," *Asian J. Inf. Technol.*, vol. 13, no. 9, pp. 494–505, 2014, doi: 10.3923/ajit.2014.494.505.

[24] 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.

[25] R. P. Sola, N. Malali, and P. Madugula, *Cloud Database Security: Integrating Deep Learning and Machine Learning for Threat Detection and Prevention*. Notion Press, 2025.

[26] M. Blessing, "Cloud Encryption Strategies and Key Management," 2024.

[27] D. Patel, "Zero Trust and DevSecOps in Cloud-Native Environments with Security Frameworks and Best Practices," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, 2023.

[28] M. Ozkan-Okay, R. Samet, Ö. Aslan, and D. Gupta, "A Comprehensive Systematic Literature Review on Intrusion Detection Systems," *IEEE Access*, vol. 9, pp. 157727–157760, 2021, doi: 10.1109/ACCESS.2021.3129336.

[29] Vikas Prajapati, "Role of Identity and Access Management in Zero Trust Architecture for Cloud Security: Challenges and Solutions," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 3, pp. 6–18, Mar. 2025, doi: 10.48175/IJARSCT-23902.

[30] W. Yang, S. Wang, H. Cui, Z. Tang, and Y. Li, "A Review of Homomorphic Encryption for Privacy-Preserving Biometrics," *Sensors*, vol. 23, no. 7, 2023, doi: 10.3390/s23073566.

[31] J. Dolejsova, "The Evolution of mHealth Apps: Current Trends and Future Directions," *EJBI*, vol. 20, no. 3, pp. 258–259, 2025, doi: 10.24105/ejbi.2024.20.4.258-259.

[32] 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.*, pp. 749–758, Dec. 2022, doi: 10.48175/IJARSCT-7744D.

[33] X. Liang and Y. Xu, "A novel framework to identify cybersecurity challenges and opportunities for organizational digital transformation in the cloud," *Comput. Secur.*, vol. 151, Apr. 2025, doi: 10.1016/j.cose.2025.104339.

[34] 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. doi: 10.2139/ssrn.5212904.

[35] D. Dhinakaran, S. M. U. Sankar, D. Selvaraj, and S. E. Raja, "Privacy-Preserving Data in IoT-based Cloud Systems: A Comprehensive Survey with AI Integration," 2024.

[36] 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.

[37] 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.

[38] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, "Security of Zero Trust Networks in Cloud Computing: A Comparative Review," *Sustainability*, vol. 14, no. 18, Sep. 2022, doi: 10.3390/su141811213.

