A Review on Challenges & Solutions of Cloud Security and Data Privacy

Anirudh BS, Sharan S, Rohith R, Neha Singh

Department of Computer Science and IT, JAIN (Deemed-to-be University), Bengaluru, Karnataka, India,

neha.singh@jainuniversity.ac.in

ABSTRACT

The worldwide adoption of cloud computing has transformed how businesses and individuals store and manage data, offering greater flexibility and scalability. But this shift in patterns poses significant challenges to cloud security and data privacy. This paper explores key issues in these two domains, highlighting the vulnerabilities and threats that may affect them. We explore key security threats, such as data breaches, unauthorised access, and DDoS attacks, while investigating the problem to ensure data privacy across jurisdictions and diverse cloud models. Our analysis also covers the role of various security controls, including encryption, access controls, and multi-factor authentication, in mitigating these risks. Furthermore, we cover widely adopted data protection regulations such as the GDPR and the CCPA. This paper aims to provide a broad overview of the current state of cloud security and data privacy and, hence, examines best practices and technological solutions for protecting sensitive information in the cloud. The paper concludes with a discussion of future research directions and a call for collaboration among stakeholders to build a stronger, more trustworthy cloud ecosystem.

Keywords: Cloud Security, Data Privacy, Data Protection, Encryption, Access Control, Multi-Factor Authentication, GDPR Compliance, Cloud Computing

1. INTRODUCTION

Cloud Computing has largely driven the digital transformation in the 21st century. Cloud Computing is a technology that provides access to a shared pool of scalable computing resources. It has become the cornerstone of modern IT infrastructure for organisations, whether small or big. From small startups to huge multinational corporations, the benefits of the cloud, which help in reducing costs, improving efficiency, and fostering better collaboration, are undeniable. However, moving data and applications from local, on-premises servers to external cloud environments introduces a new set of serious concerns. Cloud security and data privacy: These are no longer secondary considerations but are fundamental to the success and sustainability of any cloud-based operation. Cloud security is a multi-layered discipline that encompasses policies, controls, and technologies to protect data, applications, and infrastructure. Unlike the defined network perimeter of traditional IT security, cloud security operates under a complex shared responsibility model between the cloud service provider (CSP) and the user. The cloud's dynamic and distributed nature introduces new vulnerabilities and attack vectors for malicious actors.

Data privacy mainly focuses on the proper management and guarding of personal information. Its main goal is to ensure that data collection, storage, and utilisation respect individual expectations and rights. A significant difficulty in the cloud environment is the potential for data to be distributed across multiple locations, which complicates compliance due to differing, sometimes contradictory, legal requirements. This paper aims to give a proper exploration of the relationship between cloud security and data privacy. We will first examine the main security threats cloud environments face, ranging from sophisticated cyberattacks to insider threats. Then we will look into the technical and organisational measures that can be used to reduce these risks. We will then look into data privacy, discussing the regulatory landscape and the challenges of

Proceedings of ICICCS-2026 (Poster Papers), DMPedia Lecture Notes in Computer Science & Engineering.
ISBN: 978-81-993813-1-5

achieving compliance in a globalised cloud ecosystem. By shedding light on the current state of these issues, this paper highlights the importance of a proactive and comprehensive approach to protecting data in the cloud. Our goal is to serve as a valuable resource for researchers, professionals, and students seeking to understand and navigate the complexities of securing data in an increasingly cloud-centric world, as shown in Figure 1.

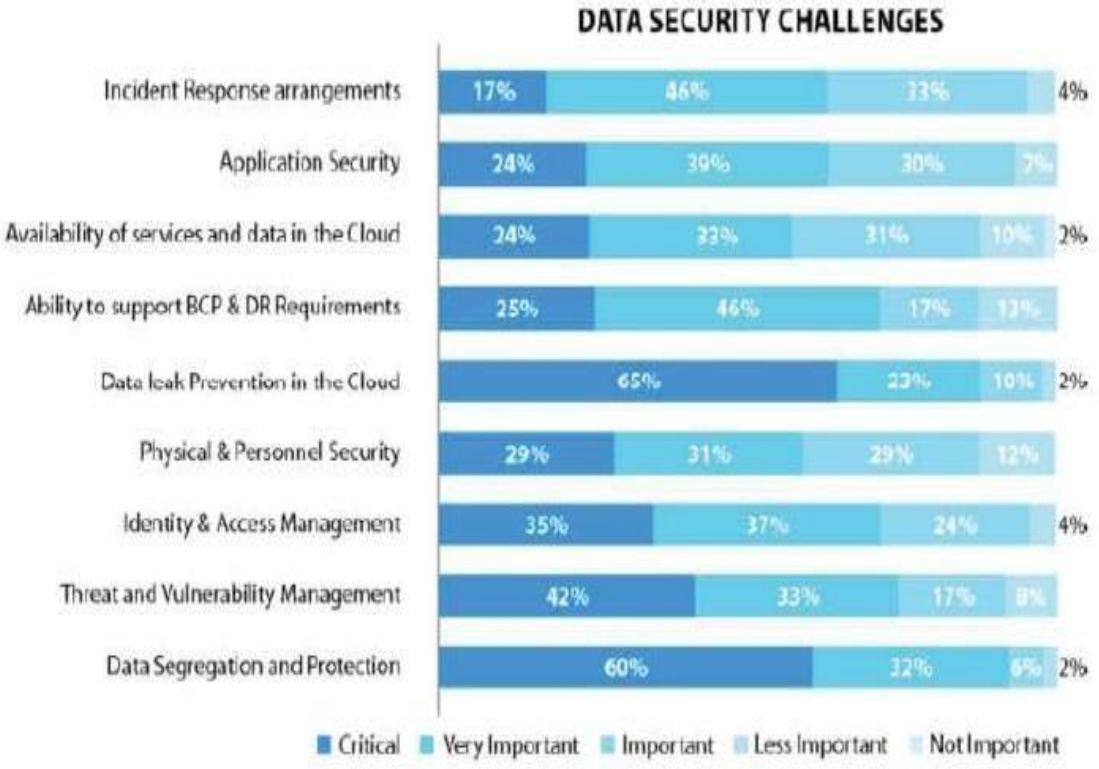

Figure 1: Different data security challenges.

Cloud computing originated with foundational concepts such as time-sharing in the 1960s, progressing from environments where security was primarily focused on safeguarding a physical perimeter. However, an important shift occurred with the introduction of the Internet and new technologies.

A. EARLY SECURITY MEASURES:

When cloud computing first came out, the big worry was keeping sensitive data safe when it wasn't physically on your own turf anymore. Early services like Salesforce.com (1999) and Amazon Web Services (AWS) (2002) showed how much money could be saved, but security was a major sticking point for people actually to use them. Seriously, back in 2009, an IDC survey said security was the number one reason companies hesitated to move to the cloud.

B. INITIAL SETUP:

The initial security setup wasn't great. They basically just used the same old security tools from the office and a basic shared responsibility model. The provider handled the infrastructure security, and the customer was totally on their own for their data and applications. This weak approach led to several well-known data breaches and privacy slip-ups, as per FIGURES 2 and 3.

.

FIGURE 2 RDFI feedback loop - an adaptation of the MAPE-K framework to support security fault injection campaigns and transfer of information to security mechanisms

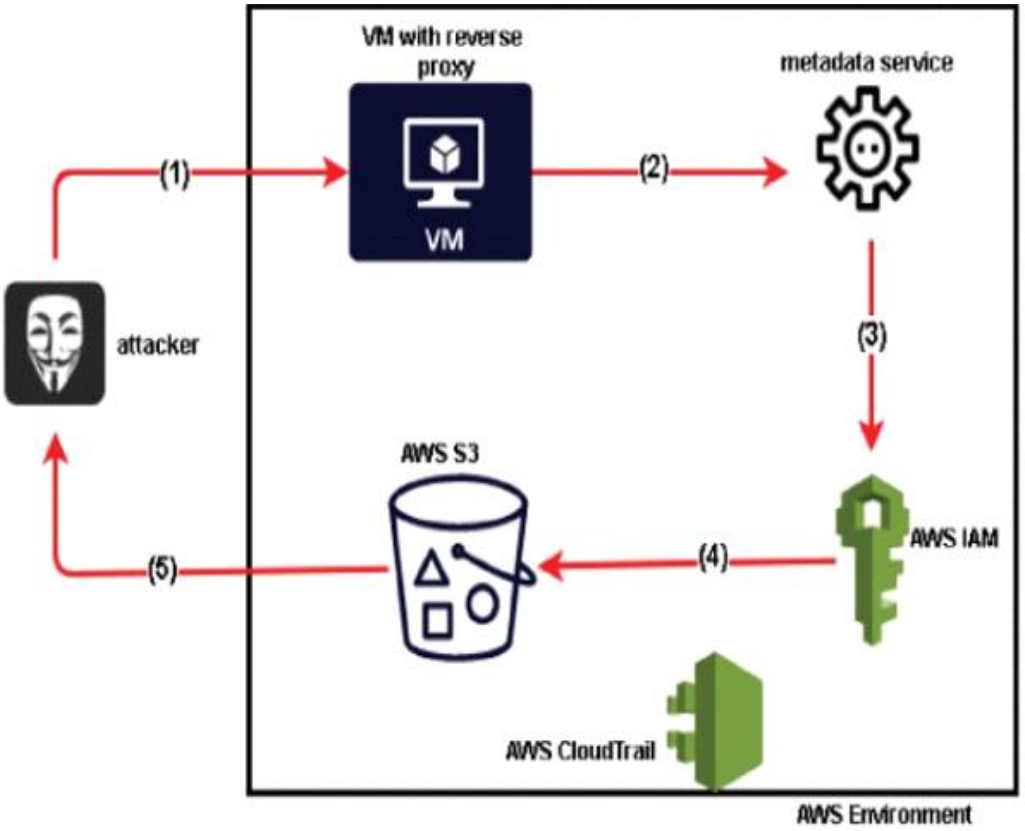

Figure 3: Running example- an illustration of the Capital One data breach.

2. DEVELOPMENT

PAST	PRESENT	FUTURE
1. From the years From 2010 to 2020, cloud security has mainly focused on encryption methods such as Attribute-Based Encryption (ABE), Identity-Based Encryption (IBE) and Provable Data Possession (PDP) to maintain Data Integrity.	1. Organisations have shifted from perimeter-based security to Zero Trust architectures, integrating identity, context, and device posture verification for every access request. SASE frameworks combine network security and connectivity (SD-WAN, CASB, ZTNA) to secure distributed users and workloads.	1. Explore emerging technological solutions that have the potential to change the cloud's security and data privacy landscape, with a special focus on homomorphic encryption, confidential computing, and post-quantum cryptography.
2. Searchable encryption and Key-Aggregate Encryption (KASE) allow users to make keyword searches and share encrypted data efficiently in cloud environments.	2. Cloud providers like Microsoft Azure, Google Cloud, and AWS have rolled out confidential computing offerings that protect data in use by isolating sensitive computations within secure enclaves, mitigating insider threats and side-channel attacks.	2. Assess the future of significant global data protection laws and regulations, such as GDPR, CCPA, and regional regimes, and their expected influence on the compliance and data management practices of cloud services.
3. Blockchain-based systems like ProvChain and AuthPrivacyChain were made to create tamper-proof audit trails	3. While still computationally expensive, partially homomorphic encryption and secure multiparty computation (MPC) have started to appear in privacy-preserving analytics and federated learning, especially in healthcare and finance sectors	3. Research the development of advanced and sophisticated cyber threats targeting cloud environments, including supply chain vulnerabilities, the exploitation of API security, and the misuse of AI/ML.
4. Smart Contracts turned access rules into self-running code: drop the right key, get in; every step gets stamped and stored, no human intermediary needed.	4. Security Information and Event Management (SIEM) systems are being augmented by AI and ML for predictive analytics, anomaly detection, and automated incident response—enabling faster detection of complex attacks and misconfigurations.	4. Review the role of Artificial Intelligence and Machine Learning in defending against, and contributing to, new threats in cloud security. Assess future applications for automated threat detection and response
5. Tools like Netflix's Chaos Monkey and CloudStrike deliberately broke pieces of the Cloud, yanking servers offline or scrambling settings to prove the system could shrug off mistakes and attacks without crashing.	5. Security has become embedded in CI/CD pipelines, with Infrastructure as Code (IaC) scanning, container image signing, and automated compliance checks to ensure "shift-left" security from the development phase onward.	5. Understand the security and privacy implications of emerging cloud architectures, including the increased adoption of serverless computing, edge computing, and complex multi-cloud deployments.

6. CVSS, CCSS, and CIS Benchmarks gave everyone the same yardstick: one score for how bad a flaw is, one checklist for staying legal, and one playbook for locking down servers properly.	6. Tools now automatically map workloads to regional compliance frameworks like GDPR, CCPA, and APAC privacy laws. Cloud providers offer region-specific data sovereignty guarantees and audit dashboards for transparency.	6. Find and synthesise reports and white papers from major industry analysts and cloud platform providers that outline their predictions and strategic roadmaps related to the future of cloud security and data governance.
7. Defenders upgraded from basic alarms to attack graphs (blueprints of every possible hack path), kill-chain breakdowns, and nonstop scans that hunted weak spots before intruders did.	7. In response to attacks like SolarWinds and dependency hijacking, organisations are strengthening software supply chain security with SBOMs (Software Bills of Materials), API gateways, and continuous dependency monitoring.	7. Elaborate on the future adoption of advanced security models, particularly on how the concept of Zero Trust architecture will evolve and be applied across hybrid and distributed cloud environments.
8. EC-ACS lets entire teams sign documents with a single compact proof, no certificate mess, while Fine-grained access meant “read this file, but don’t touch that one,” keeping enterprise and medical data both shared and safe.	8. Standardisation efforts led by NIST are preparing cloud vendors and enterprises for the post-quantum era, with pilot deployments of lattice-based and code-based cryptographic schemes for secure key exchange and digital signatures.	8. Future trends in data access control and governance will include automated policy enforcement, decentralised identity management, and the use of technologies like blockchain for the creation of data provenance.
9. Logging in now required multiple proofs (phone + password), role-based locks kept rookies away from critical buttons, and every action was automatically recorded for later review.	9. The proliferation of edge computing and serverless architectures has driven demand for fine-grained identity, event-driven policy enforcement, and runtime security controls that protect ephemeral workloads.	
10. By the end of the 2010s, four bedrock ideas ruled: ironclad encryption, complete activity logs, self-fixing systems, and toughness under fire, the DNA of every secure cloud today.	10. Modern security platforms unify CSPM, CIEM (Cloud Infrastructure Entitlement Management, CWPP (Cloud Workload Protection Platform), and CNAPP (Cloud-Native Application Protection Platform) capabilities for continuous risk visibility and automated remediation	

3. CONCLUSION

The development of cloud computing has transformed the technology landscape, providing unprecedented scalability and efficiency. But as this shift changes, it gives an increasingly complex challenge to cloud security and data privacy. This review has covered the different nature of these challenges, analysing critical vulnerabilities such as tenancy risks associated with shared tenancy, insider threats, and a lack of standard security protocols. We have also emphasised the importance of a multilayered defence model, including strong encryption,

robust access controls, and regular monitoring. In conclusion, this review proves that while the cloud offers immense potential, its promise can only be fully realised by addressing the main issues of security and privacy. The current environment requires a strategic approach to security. Looking ahead, the combination of cutting-edge technologies such as zero-trust architecture and AI-driven threat detection will be essential. Hence, building a truly trustworthy cloud system will require a collaborative effort among cloud service providers and end-users to ensure that innovation does not come at the expense of data integrity and privacy.

REFERENCE

[1] Asaad, R. R., & Zeebaree, S. R. M. (2024). Enhancing Security and Privacy in Distributed Cloud Environments: A Review of Protocols and Mechanisms. Academic Journal of Nawroz University, 13(1), 476-488. DOI:10.25007/ajnu.v13n1a2010

[2] Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. IEEE Access, 7, 82721–82743. DOI:10.1109/ACCESS.2019.2924045

[3] Greavu-Șerban, V., Pavaloaia, V. D., & Esanu, C. (2024). Analysis of cloud technology adoption in Romanian public institutions: Implications for security and confidentiality. Journal of Public Administration, Finance and Law, 32, 493–498. DOI:10.47743/jopafl-2024-32-38.

[4] Hamid, I., & Frikha, M. (2024). Blockchain-Enhanced Cybersecurity and Privacy in Cloud Computing: A Systematic Literature Review. Journal of Theoretical and Applied Information Technology, 102(2), 514-532.

[5] Torkura, K. A., Sukmana, M. I. H., Cheng, F., & Meinel, C. (2020). CloudStrike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure. IEEE Access, 8, 123044-123060. DOI:10.1109/ACCESS.2020.3007338

[6] Andrea Fieschi, Pascal Hirmer, Sachin Agrawal, Christoph Stach, Bernhard Mitschang, "HySAAD – A Hybrid Selection Approach for Anonymization by Design in the Automotive Domain", 2024 25th IEEE International Conference on Mobile Data Management (MDM), pp.203-210, 2024.

[7] Mohsen Hatami, Lhamo Dorje, Xiaohua Li, Yu Chen, "Electric Network Frequency as Environmental Fingerprint for Metaverse Security: A Comprehensive Survey", Computers, vol.14, no.8, pp.321, 2025.

[8] Parast, F. K., Khodadadi, S., & Ganjali, Y. (2022). Cloud computing security: A survey of service-based models. Computers & Security

[9] Ammar Almomani, Ahmad Al-Qerem, Mohammad Alauthman, Amjad Aldweesh, Samer Aoudi, Said A. Salloum, "Ethical Foundations of AI-Driven Avatars in the Metaverse for Innovation and User Privacy", IEEE Access, vol.13, pp.130610-130628, 2025.

[10] Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. IEEE Access, 8, 131723–131741.

[11] Morol M, Das SS, Mahmood S. Data Security and privacy in cloud computing platforms: a comprehensive review. Int. J. Curr. Sci. Res. Rev. 2022 May;5(05).

[12] Sun Y, Zhang J, Xiong Y, Zhu G. Data Security and Privacy in Cloud Computing.

International Journal of Distributed Sensor Networks. 2014;10(7). doi:10.1155/2014/190903

[13] Mohamad, Nur Hidayah, Norsuhaida Binti Saidin, and Muhammad Izwan Haikal Bin Zaidi. "Data security and privacy issues in cloud computing: challenges and solutions review." Authorea Preprints (2023).

[14] Lianghao Li, Haibo Mi, Kun Wang, Bo Ding, Huaimin Wang, "A Review of Multi-Objective Optimization for Cloud Environment Storage Optimization", 2025 IEEE International Conference on Joint Cloud Computing (JCC), pp.91-100, 2025.

[15] J. Zhang, B. Chen, Y. Zhao, X. Cheng and F. Hu, "Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues," in IEEE Access, vol. 6, pp. 18209-18237, 2018, doi: 10.1109/ACCESS.2018.2820162.

[16] Asaad, Renas Rajab, and Subhi RM Zeebaree. "Enhancing Security and Privacy in Distributed Cloud Environments: A Review of Protocols and Mechanisms." Academic Journal of Nawroz University 13, no. 1 (2024): 476-488.

Torkura, K. A., Sukmana, M. I. H., Cheng, F., & Meinel, C. (2020). CloudStrike: Chaos

[17] Engineering for Security and Resiliency in Cloud Infrastructure. IEEE Access, 8, 123044-123060. DOI:10.1109/ACCESS.2020.3007338.

[18] Khan, Shakir & Alajmi, Mohamed. (2019). A Review on Security Concerns in Cloud Computing and their Solutions. 9.