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

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12604

Addressing the Shared Responsibility Model in Google Cloud: A Practical Guide to Data Security and Compliance

Neha Nikhath

Computer Science and Engineering. Vaagdevi College of Engineering, Warangal, India

Abstract: The Google Cloud Platform requires customers who want cloud security to fully understand the shared responsibility model, as their security obligations differ from the provider's duties. Through an in-depth analysis, the paper presents organizations with a practical approach to achieve data security along with compliance standards in Google Cloud. Google Cloud secures its underlying infrastructure, yet customers accept full accountability to protect their data applications along with configurations within the cloud system. This paper explains the security obligations between Google Cloud and its users by providing practical security implementation guidelines for robust safeguards. This document examines complete cloud security management through its key components of data protection, alongside access management and compliance guidelines, together with incident response systems. Organizations achieve risk reduction and improve security standing while meeting regulatory standards in Google Cloud through the proper use of the shared responsibility model.

Keywords: Shared Responsibility Model, Google Cloud Security, Cloud Compliance and Governance, Identity and Access Management (IAM), Data Protection in Cloud Computing, Incident Response in GCP.

I. INTRODUCTION

Cloud computing depends on the shared responsibility model, which establishes how security duties are divided between cloud providers and their customers [17]. Google Cloud maintains exclusive responsibility for the security of its physical data centres, along with networking infrastructure and fundamental services [1]. As cloud users maintain full accountability for cloud security through their responsibility to protect every element they store in the cloud, such as data, applications, and operating systems, and access controls [11]. A distinct definition of responsibilities between Google and customers requires a precise understanding of service limits because compliance failures and security flaws result when participants overlook their designated parts [7]. Organizations struggle to protect their cloud-based data and applications and their confidentiality, integrity, and availability [15]. The creation of an effective security approach needs to establish clear roles for both providers and customers to implement multi-layered defences against possible threats and security weaknesses. The shared responsibility model requires Google Cloud, along with its customers, to jointly work together for maintaining a secure environment because it establishes cloud security as a mutual responsibility [3]. Strong access control systems must be established to restrict resource access to authorized clients because cloud environments operate with constantly changing user access [4]. Organizations migrating to Google Cloud should develop a full comprehension of the shared responsibility model for building enhanced security postures and satisfying compliance needs [9]. Cloud computing trust is built through this model, which specifies what responsibilities belong to each participating organization [16]. Trust-building has become an essential goal for most stakeholders in public clouds due to its importance. Organizations that actively work together with Google Cloud achieve efficient security compliance standards through their motivated approach.

II. GOOGLE CLOUD SECURITY FUNDAMENTALS

The security architecture of Google Cloud operates to defend customer applications along with their related data. All security elements within Google Cloud infrastructure involve physical protection elements alongside network security protocols and encryption technology applications. Google devotes major capital to data center protection through extensive access control systems, surveillance methods, and environmental health standards, which deter unapproved physical incursions [18]. Network security stands as an essential framework for Google, as the company uses firewalls with advanced capabilities, together with intrusion detection systems and network segmentation approaches, to protect physical customer assets. Data encryption serves dual purposes: while data is moving across networks and stored in place, it is a way to keep information hidden from unauthorized access attempts [4]. The expansion of cloud computing framework usage has led to an unfortunate surge in cloud-based criminal activities [24]. The implementation of cloud

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

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12604

computing requires organizations to investigate the security aspects of cloud service platforms. The security services and tools at Google Cloud enable customers to boost their security profile through solutions like Cloud Identity and Access Management, Security Command Center, and Cloud Armor. Organizations can establish access control management capabilities, report security threats, and prevent Distributed Denial-of-Service attacks through this security software, as data holders and users stay in charge of ensuring data security along with data integrity during their time using cloud services [21]. Organizations can establish a multi-layered data protection system for Google Cloud through the implementation of its security features and services. The main reason why businesses should transition to cloud computing is its security risks [23]. NIST Special Publication 800-53 defines security measures as essential because data confidentiality, together with integrity and system availability, are crucial elements [5]. Figure 1 shows the Google Cloud Security Architecture which includes multiple layer of protection.

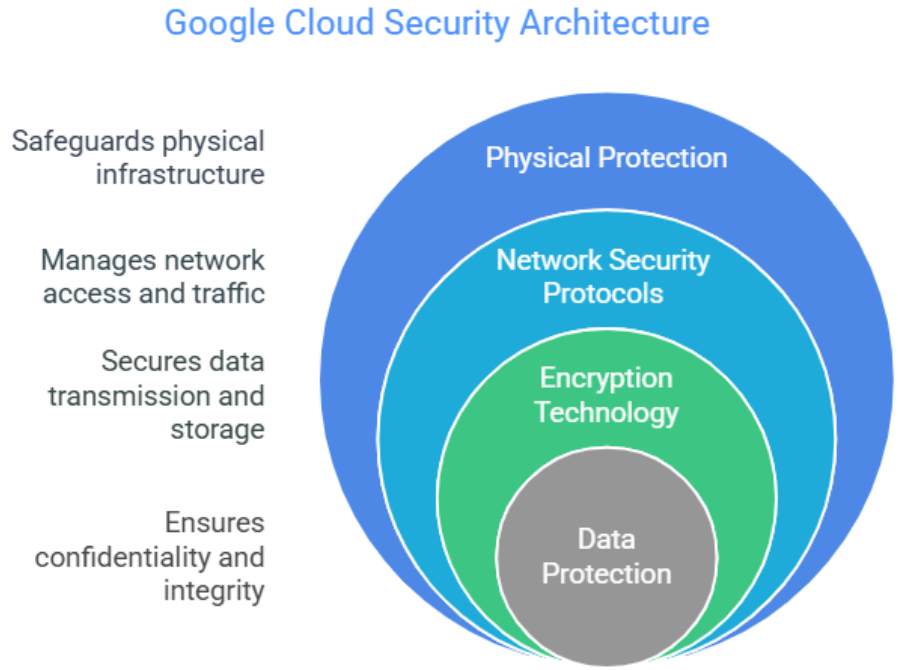

Figure 1: Google Cloud Security Architect

III. THE IMPLEMENTATION OF DATA REGULATIONS TAKES PRIORITY AS AN ESSENTIAL REQUIREMENT WITHIN THE GOOGLE CLOUD ENVIRONMENT

Organizations must carefully follow data regulatory standards when doing business in Google Cloud [27]. Business operations need to comprehend the multiple data protection frameworks fully to comply with GDPR, HIPA, 28A, and PCI DSS standards based on the stored and processed data specifics [5]. Organizations must follow regulations that establish firm rules for managing cloud-based data security and privacy, as well as governance protocols [14]. Organizations guarantee compliance through the deployment of suitable security measures that should consist of data encryption combined with access controls and audit log tracking systems. Organizations need to maintain active compliance monitoring and security breach detection of their cloud environments to swiftly handle all identified problems [20]. Organizations must perform constant observation together with regular compliance audits to find weaknesses while maintaining regulatory standards [25, 29]. Organizations can use Google Cloud tools to fulfill their compliance requirements through features that include data residency options alongside compliance reports and security assessment capabilities. The need to maintain compliance emerges as a critical business mandate since security breaches attract major penalties, together with potential legal repercussions and damage to corporate reputation. The research results in this study apply to all governing areas, including financial services, since cloud-related innovations heavily affect business-critical operational services [15]. Organizations must set precise data governance methods along with rules to specify exact roles that handle data security and management tasks. Cloud computing security statements require log files, together with backups and metadata, because these elements serve regulatory incident management [2]. Through an extensive compliance program, organizations show their dedication to data security protection, thus maintaining customer faith and stakeholder confidence. Legal problems surface during the data storage process, along with its processing across multiple nations [13].

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

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12604

IV. PROTECTION MEASURES FOR CUSTOMER DATA STORED IN GOOGLE CLOUD SYSTEMS NEED IMPLEMENTATION

Protecting customer data at Google Cloud requires organizations to establish multiple security strategies that will ensure confidentiality and integrity, as well as data availability. Data protection during transfers and storage depends on encryption as an essential security control [10,18]. AES-256 encryption serves as a strong method to secure sensitive information by making it incomprehensible to unauthorized users. Data protection requires the establishment of powerful access control systems that restrict users according to their minimum required privileges. Organizations should use multi-factor authentication methods that mandate users to utilize different forms of verification to secure access to sensitive data systems. The organization can block its sensitive data from unauthorized exit through data loss prevention tools. Organizations must establish data loss prevention systems that stop the intentional and unintended release of sensitive information. Security incidents become detectable when organizations maintain a system for monitoring activities and logging all events. Regular security examinations and penetration tests must be scheduled to discover weaknesses in the cloud system so appropriate corrections can be made [26, 30]. The protection of patient data processed through cloud workflows remains essential, while proper data security measures need implementation for secure information exchange between parties [19]. Organizations need to develop specific incident response plans that enable effective security breach response and incident impact reduction. Users forfeit their data control after cloud uploading because data theft becomes a risk [6]. User data protection in Google Cloud must continue as a constant operation that needs sustained surveillance, together with performance assessments for continuous development.

Organizations require genuine attention to data security because Information Technology usage presents various security threats, including hacker intrusions, natural disasters, and separation failures, among other risks [22]. Data privacy and security protection matter greatly since people use cloud services for an increasing number of tasks [12]. Figure 2 shows the cloud security life cycle, which includes data monitoring, audit of security practices, detection of security risks, etc.

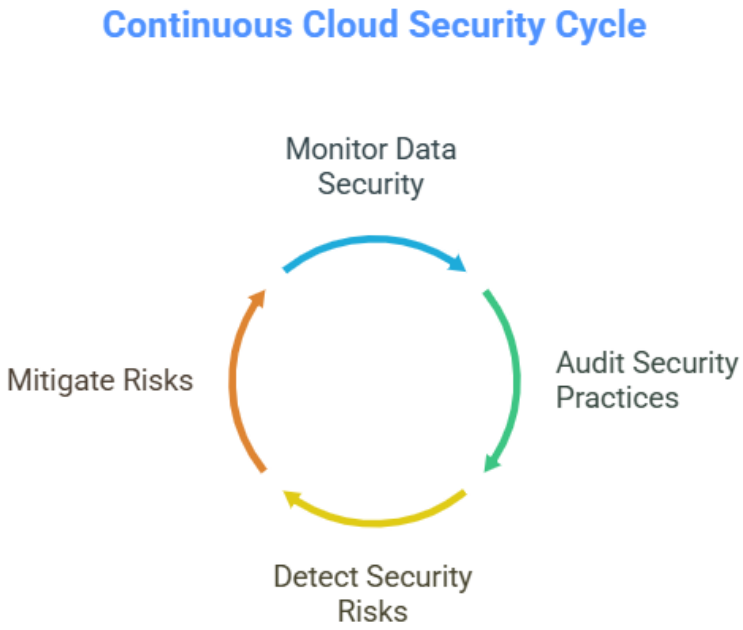

Figure 2: Cloud security cycle

V. MONITORING AND AUDITING DATA SECURITY

Keeping track of data security requirements through Google Cloud monitoring and auditing reveals a vital security enforcement approach that fulfills industry standards. Agencies must deploy extensive tracking and recordkeeping methods that enable users to monitor system events alongside security incidents, along with their activity streams. Companies can use Security Information and Event Management systems to combine security logs from different sources, so they gain immediate insight into potential security attacks [10, 32]. Organizations need to establish intrusion detection systems with prevention features to both detect and stop malicious activities. Security systems monitor irregular patterns through their detection process to notify security personnel about possible security threats. Security audits need to run regularly to determine the success of implemented security controls while spotting potential enhancement opportunities. The auditing of cloud systems consists of a continuous process that generates a record of security-related cloud events.

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

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 6, June 2025

DOI: 10.17148/IARJSET.2025.12604

Organizations need to perform frequent scanning of vulnerabilities alongside operational penetration tests to locate and fix security flaws that exist in their cloud infrastructure. Audits establish the necessary requirements for verifying that systems operate by established guidelines and ensuring hazard control and data protection [31]. Audit processes must be automated because this practice ensures faster reporting and documentation while verifying regulatory compliance. Organizational data safety remains intact because a thoroughly developed monitoring and auditing system allows for rapid security incident detection and response while containing the security breach impact [8, 33].

The assessment of security posture must occur frequently, with concurrently updated policies, while staff members receive security awareness training. A reliable cloud security approach requires constant data security monitoring, together with auditing for the purpose of detecting security risks before they escalate. Organizations must activate continuous environmental audits of Google Cloud platforms through tools that detect vulnerabilities while providing incident response capabilities to achieve data security and compliance requirements [34].

VI. CONCLUSION

Organizations that want to achieve cloud computing benefits through robust security need to optimize their shared responsibility model in Google Cloud. The clear definition of responsibilities between Google Cloud and the customer helps organizations efficiently use their resources to implement correct security procedures. Organizations must apply both encryption to sensitive data along with strong access controls, yet they need to conduct active monitoring and audit their cloud environments to detect and respond to security incidents. Cloud-based systems provide unmatched flexible scalability, together with cost-efficient services, yet these add new security complexities that need active collaboration between customers and cloud service operators. The secure infrastructure of Google Cloud includes security tools that help businesses protect their own applications and data, but customers need to maintain primary accountability for these assets. Organizations need to execute periodic security posture assessments while updating their security policies plus delivering employee security training to decrease security risks. Security procedures need regular evaluation to identify modern security threats, followed by necessary updates and deployments. Organizations that skillfully handle their duties under the Shared Responsibility Model will gain improved security postures that let them fully utilize Google Cloud power. Intrusion detection systems operate to protect cloud networks, while anomaly detection methods strengthen their overall security measures. Cloud computing provides a shared environment that attackers can target.

Organizations build effective security postures for using Google Cloud's features when they accept their collaborative security obligations and implement protective measures. All entities should negotiate agreements before starting cloud service operations. Security protocols must be implemented in cloud computing operations that handle user data. Cloud computing faces three primary security threats: physical theft, combined with malicious internal users, and shared environmental risks. Cloud computing serves as a principal technology platform for users linked to networking systems.

REFERENCES

[1]. B. Konda et al., "Enhancing Traceability and Security in mHealth Systems: A Proximal Policy Optimization-Based Multi-Authority Attribute-Based Encryption Approach," *2025 29th International Conference on Information Technology (IT)*, Zabljak, Montenegro, 2025, pp. 1-6, doi: 10.1109/IT64745.2025.10930307.

[2]. Pawar, P. P., Kumar, D., Ananthan, B., Christopher, S. B., & Surya, R. (2024, May). An advanced Wasserstein-enabled generative adversarial network enabled attack detection for blockchain-Assisted Intelligent Transportation System. In 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT) (pp. 1-6). IEEE.

[3]. Kasula, V. K. (2024). Cryptocurrency: An Opportunity for Traditional Banking? International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), 4(1): 596-598

[4]. Almorsy, M., Grundy, J., & Müller, I. (2016). An Analysis of the Cloud Computing Security Problem. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.1609.01107

[5]. Addula, S. R., Tyagi, A. K., Naithani, K., & Kumari, S. (2024). Blockchain-Empowered Internet of Things (IoTs) Platforms for Automation in Various Sectors. Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing, 443-477

[6]. Anilkumar, C., & Sumathy, S. (2018). Security strategies for cloud identity management - a study. International Journal of Engineering & Technology, 7(2), 732. https://doi.org/10.14419/ijet.v7i2.10410

[7]. A. R. Yadulla et al., "Lightweight Neural Networks for Adversarial Defense: A Novel NTK-Guided Pruning Approach," 2025 37th Conference of Open Innovations Association (FRUCT), Narvik, Norway, 2025, pp. 331-337, doi: 10.23919/FRUCT65909.2025.11008002.

DOI: 10.17148/IARJSET.2025.12604

[8]. B.G, S. S., & Phulre, S. (2021). Detailed Study of Cloud Infrastructure Attacks and Security Techniques. International Journal of Innovative Research in Computer Science & Technology, 9(2), 22. https://doi.org/10.21276/ijircst.2021.9.2.4

[9]. Brandis, K., Dzombeta, S., Colomo‐Palacios, R., & Stantchev, V. (2019). Governance, Risk, and Compliance in Cloud Scenarios. In Applied Sciences (Vol. 9, Issue 2, p. 320). Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/app9020320

[10]. A. R. Yadulla et al., "Enhanced Cybersecurity Entity Recognition Using DeBERTa, Transformer-CNN Hybrids, and BiLSTM-Softmax," 2025 37th Conference of Open Innovations Association (FRUCT), Narvik, Norway, 2025, pp. 323-330, doi: 10.23919/FRUCT65909.2025.11008057.

[11]. A. Chahal et al., "Systematic analysis based on Conflux of machine learning and internet of things using bibliometric analysis," Journal of Intelligent Systems and Internet of Things, vol. 13, no. 1, pp. 196–224, 2024. doi:10.54216/jisiot.130115

[12]. Daniel, V. A. A., Vijayalakshmi, K., Pawar, P. P., Kumar, D., Bhuvanesh, A., & Christilda, A. J. (2024). Enhanced affinity propagation clustering with a modified extreme learning machine for segmentation and classification of hyperspectral imaging. e-Prime-Advances in Electrical Engineering, Electronics and Energy, 9, 100704.

[13]. Konda, B. (2024). Explore Data Mining (DM) Techniques That Data Scientists Adopt in IT.

[14]. Yadulla, A. R. (2024). A qualitative approach to data breaches in mobile devices.

[15]. Commey, D., Griffith, S., & Dzisi, J. (2020). Performance comparison of 3DES, AES, Blowfish and RSA for Dataset Classification and Encryption in Cloud Data Storage. In International Journal of Computer Applications (Vol. 177, Issue 40, p. 17). https://doi.org/10.5120/ijca2020919897

[16]. V. K. Kasula et al., "Enhancing Hyperledger Fabric Security with Lightweight Post-Quantum Cryptography and National Cryptographic Algorithms," 2025 37th Conference of Open Innovations Association (FRUCT), Narvik, Norway, 2025, pp. 93-99, doi: 10.23919/FRUCT65909.2025.11008110.

[17]. Dawson, J. K., Twum, F., Acquah, J. B. H., & Missah, Y. M. (2023). Ensuring privacy and confidentiality of cloud data: A comparative analysis of diverse cryptographic solutions based on run time trend. In PLoS ONE (Vol. 18, Issue 9). Public Library of Science. https://doi.org/10.1371/journal.pone.0290831

[18]. S. Almotairi et al., "Personal data protection model in IOMT-blockchain on secured bit-count transmutation data encryption approach," Fusion: Practice and Applications, vol. 16, no. 1, pp. 152–170, 2024. doi:10.54216/fpa.160111

[19]. V. K. Kasula et al., "Federated Learning with Secure Aggregation for Privacy-Preserving Deep Learning in IoT Environments," 2025 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 2025, pp. 1-7, doi: 10.1109/ICCA65395.2025.11011120.

[20]. Meesala, M. K. (2024). Security Policy Compliance Among Remote Workers Using BYOD Policies.

[21]. Pawar, P. P., Kumar, D., Meesala, M. K., Pareek, P. K., Addula, S. R., & KS, S. (2024, November). Securing Digital Governance: A Deep Learning and Blockchain Framework for Malware Detection in IoT Networks. In 2024 International Conference on Integrated Intelligence and Communication Systems (ICIICS) (pp. 1-8). IEEE.

[22]. M. Yenugula et al., "A Graph Neural Diffusion Network for Sophisticated Persistent Threat Hunting in IoT Environments," 2025 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 2025, pp. 1-6, doi: 10.1109/ICCA65395.2025.11011108.

[23]. Vadakkethil, S. E., Polimetla, K., Alsalami, Z., Pareek, P. K., & Kumar, D. (2024, April). Mayfly Optimization Algorithm with Bidirectional Long-Short Term Memory for Intrusion Detection System in Internet of Things. In 2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1-4). IEEE.

[24]. Kumar, N., et al. (2025). Advanced banking solutions for Industry 5.0: From industry's perspective. In Creating AI synergy through business technology transformation (pp. 1–24). IGI Global.

[25]. Thumma, B. Y. R., Ayyamgari, S., Azmeera, R., & Tumma, C. (2022). Cloud Security Challenges and Future Research Directions. International Research Journal of Modernization in Engineering Technology and Science, 4(12), 2157-2162.

[26]. Ahmadi, S. (2024). Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. Journal of Information Security, 15(2), 148. https://doi.org/10.4236/jis.2024.152010

[27]. Gonaygunta, H., Nadella, G. S., Meduri, K., Pawar, P. P., & Kumar, D. (2024). The Detection and Prevention of Cloud Computing Attacks Using Artificial Intelligence Technologies. International Journal of Multidisciplinary Research and Publications (IJMRAP), 6(8), 191-193.

[28]. Yadulla, A. R., Konda, B., & Kasula, V. K. (2025). Blockchain for Secure Communication. In S. Alangari (Ed.), Blockchain Applications for the Energy and Utilities Industry (pp. 103-140). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-2439-5.ch006.

DOI: 10.17148/IARJSET.2025.12604

[29]. Sajja, G. S., & Meesala, M. K. (2024). Integrating AI in Sustainable Supply Chain Practices: Comparative Analysis Between the USA and Europe. International Journal of Computer Applications, 186(58), 55–62. https://doi.org/10.5120/ijca2024924342

[30]. P. Pawar et al., "Exploring Blockchain-Enabled Secure Storage and Trusted Data Sharing Mechanisms in IoT Systems," 2025 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Gwalior, India, 2025, pp. 1-6, doi: 10.1109/IATMSI64286.2025.10984499.

[31]. M. H. Maturi et al., "Optimizing energy efficiency in edge-computing environments with dynamic resource allocation," Environments, vol. 13, no. 07, pp. 1–8, 2024.

[32]. Tumma, C., Azmeera, R., Ayyamgari, S., & Thumma, B. Y. R. (2022). Data Security and Privacy Protection in Artificial Intelligence Models: Challenges and Defense Mechanisms. International Journal of Scientific Research in Engineering and Management, 7(12), 1-11.

[33]. Yenugula, M. (2022). Google Cloud Monitoring: A Comprehensive Guide. Journal of Recent Trends in Computer Science and Engineering (JRT26CSE), vol. 10, no. 2, pp. 40-50.

[34]. Meesala, M. K., Vallabhaneni, R., Mathapati, M., Pareek, P. K., & Metan, J. (2024, September). Arithmetic Optimized Bi-GRU: A Swift Approach to Combat Fake News in the Digital Sphere. In 2024 International Conference on Distributed Systems, Computer Networks and Cybersecurity (ICDSCNC) (pp. 1-6). IEEE.