IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

Enhancing Data Security in Google Cloud Platform: A Comprehensive Analysis

Shreya Gupta, Nikita Shekhar, Ms. Palvi Gupta
Department of Computer Science and Applications
School of Engineering and Technology, Sharda University, Greater Noida, UP, India

Abstract: *For almost a decade, the cloud computing concept has completely changed the computing industry. When compared to traditional benefits, cloud computing offers many advantages such as lower costs, quicker speeds, less setup time, pay per use, resilient service, round-the-clock availability, service availability on the go, and many more. Notwithstanding all these benefits, cloud computing is not without its problems and difficulties. the shared data or information in a cloud-based virtual environment. Since virtual computers, which offer a virtual environment, are the foundation of the cloud concept. Data security is not always at the same level. Instead, it varies depending on the kind of data and occasionally the owner's request. As a result, a basis for classifying data that will be shared on the cloud must be determined to implement an appropriate encryption technique dynamically and provide the best possible data encryption at the lowest possible cost.*

Keywords: data security, cloud, encryption, key management, security.

I. INTRODUCTION

Cloud computing has fundamentally transformed the commercial and information technology industries in the last few years. Large scale, fast elasticity, robust computing, 24/7 service availability at a low cost, and ubiquity are some of its unmatched features. When using a cloud service, renting is more common than buying. The virtual world provides the service in the cloud environment. A portion of the cloud computing services are managed and controlled by a third party.[3]

The users that Cloud users who share their data have no control over how it is transmitted or stored. Because of this, the cloud is an open, diverse environment that is susceptible to issues with data security. Building cloud users' confidence that their data is safe and secure in the cloud also becomes crucial. Research is now being done on an efficient and successful cloud security paradigm that addresses security at different levels, including network, host, application, and data security. Out of all these cloud security considerations, data security in the cloud becomes increasingly crucial and significant. A flexible and optimal data security model is necessary for cloud computing.[7]

It is acknowledged that there is no one fixed level of data security; rather, it varies depending on the circumstances and requirements. Certain types of data, such as multimedia elements, do not need to be secured during storage or transmission. Certain types of data, such as those relating to orders, proposals, MOUs, and Uusinesses, require low or medium level protection. High levels of security are needed for some of the most important and sensitive data, including information on financial transactions, military activities, covert operations, and data utilized by intelligence agencies, among other things. As a result, data security standards might range from minimal to high. Therefore, the goal of cloud data security cannot be achieved by a single or static type of security system.[2]

When it comes to crucial factors like speed, efficiency, effectiveness, and cost, the security mechanism's level counts. If low-level security measures are used, they might be more affordable. UUT will be open to hackers and susceptible to important data breaches. However, if high-level security measures are implemented, they will be beneficial and useful for important data. UUT won't be worthwhile if there is little to no security.[4]

DOI: 10.48175/568

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

Data Security in Google Cloud

A significant component of an organization's security posture is data security. One of the most important data security controls is encryption, and Google Cloud provides a variety of encryption choices for data that is in use, in transit, and at rest. Now let's clarify each.[6]

By default, encryption while at rest

Google encrypts data while it is in storage to help safeguard your information. This means that only roles and services that are permitted may access the data, and the encryption keys are audited. Before data is written to disk, it is encrypted. This is the method:

1. First, the data is "chunked," or divided into smaller portions, and each chunk is encrypted using a unique data encryption key.
2. A key encryption key is used to encrypt each data key. Google's storage infrastructure then receives the encrypted chunks and wrapped encryption-keys.
3. When a piece of data is modified, a new key is used to encrypt it instead of utilizing the old one.

When data needs to be retrieved, the process repeats in reverse. As a result, if an attacker were to compromise an individual key or gain physical access to storage, they would still be unable to read customer data - as they need to identify all the data chunks in an object, retrieve them, and retrieve the associated encryption keys.[6]

By default, encryption while in transit

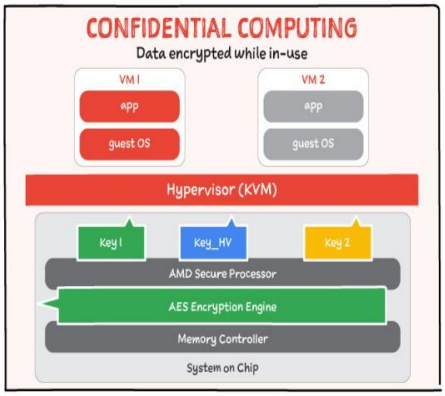
TLS connections that have been correctly ended are necessary for any Internet-based communications with Google Cloud. When data travels between your website and the cloud provider or between two services, encryption in transit guards your information if communications are intercepted.[6] The data is encrypted prior to transmission, endpoints are authenticated, and the data is decrypted and verified upon arrival to accomplish this protection. For instance, Secure/Multipurpose Internet Mail Extensions (S/MIME) are frequently used for email message security, while Transport Layer Security (TLS) is frequently used to encrypt data in transit for transport security.[5]

Use of encryption: private computer

By encrypting data while it is processed, Confidential Computing creates a "third pillar" that guards against compromise or exfiltration of your data stored in memory. Confidential GKE Nodes and Confidential VMs allow you to encrypt your data while it's being used. The defenses Shielded VMs provide against rootkits and bootkits are strengthened by this.[3]

On-die memory controllers have specialized circuitry that handles main memory encryption. Every controller has an efficient AES engine. When data is written to DRAM or shared between sockets, the AES engine encrypts it; when data is read, it decrypts.

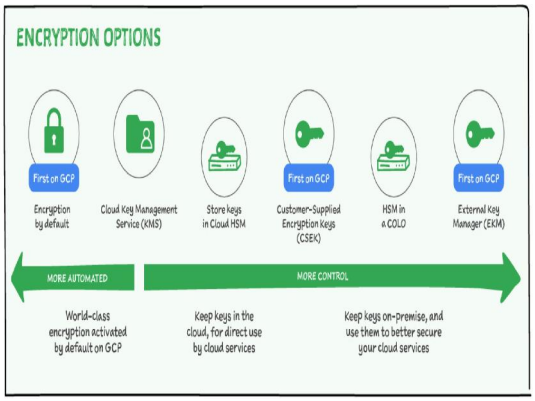
Google isn't in possession of the encryption key



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

At-rest Encryption options

Depending on your business needs and degree of trust, Google Cloud offers additional encryption options, while in certain circumstances the default encryption may be sufficient.[8]



Customer Supplied Encryption Keys

The consumer Provided Security Secrets (CSEK) allows company to preserve oneself autonomous source of confidence while pushing data through the Google Internet through an application programming interface when required, so they're a great choice should you need to function using a minimum level of trust. These data stay in Memory during the length of the process.

Whenever use ,it is important to maintain your private information confidential. When you accidentally delete or forget your passwords, the internet will be impossible to recover your information. It is actually easy to perform that improperly. To move data through Google as the same time as they are used in your programs, you have to spend in a separate sharing keys network and apply Case with much care.[5]

Key Management Service

These Clouds Key Services Solutions enables you to use our worldwide accessible involved management platform with full oversight of important operations, includes full review reporting of each of your rights. This solution allows you to keep responsibility for the public view of each of your secrets while avoiding the need to construct a new circulation mechanism.

Whenever via The Knowledge Management System (Google is normal key-encryption data are substituted by those developed and stored via cloud-based KMS.[7]

Hardware security modules

Users even have the choice of storing keys in a security module that is installed in the cloud. The service allows you to perform secure operations on a set of FIPS 140-2 three-level certified HSMs and host keys for encryption. You will not have to stress around the case of clustering scaling, and patching if Google handles HSM cluster management. Cloud HSM uses Cloud the Knowledge Management System (as its user interface, allowing customers to take benefit of all of Cloud KMS's features and benefits.[8]

Cloud External Key Manager

Cloud EKM allows you to safeguard information in Google Cloud Platform with keys that are encrypted which you hold via an allowed independent control of keys partner. Here's how it works:

In an accepted internal authentication collaborate The system you start by creating an entirely new key or using an existing one. Each key has a separate URI. [2]

Next, you approve the key's use in the external administration of keys partnership system used by your Google Cloud computing project.

In your Google Cloud project, you create a Cloud EKM key using the URI of the externally managed key.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

Your data is safeguarded by an assortment of the externally encryption partnership very important and a cloud-based EKM in order key. the Google never has access to the exterior key.[9]

Other data security services

In addition to data encryption, the following other Google Cloud services are useful for data security:

VPC Service Controls that isolate multi-tenant services to reduce the risk of data exfiltration

Data loss prevention aids in identifying, categorizing, and safeguarding sensitive information. I'll talk about this in the upcoming blog.

For a more thorough examination of how encryption functions both in transit and at rest across all of our services look over the whitepapers.[1]

CIA TRIAD

Three requirements must be met in order to secure any information system, including cloud computing, software, and computer networks: confidentiality, integrity, and availability. then it is possible to guarantee the security of data or information within the system. The acronym CIA stands for Confidentiality, Integrity, and Availability, and it is known as the "CIA Triad."[8]

A. Confidentiality

Information access must be protected from unauthorized users to maintain confidentiality. If the material is confidential, only those who are intended to access it may do so.

B. Integrity

The integrity of data refers to how reliable the information is while it is kept or transferred between locations. If content is changed or destroyed by an unauthorized party, data integrity is lost. As a result, the sender's original material will not reach the receiver.

C. Availability

Information availability refers to the ability of the authorized individual, organization, or device to access it when needed. Depending on how important a piece of knowledge is, its absence might have different effects. There is typically a trade-off between the availability and criticality of data.[9]

II. LITERATURE REVIEW

The foundation of cloud computing is built upon several essential ideas and innovations. The foundation for distributed computing models was laid in the 1960s by eminent computer scientist J.C.R. Licklider, who imagined a "Intergalactic Computer Network" that would enable remote access to data and applications. Grid computing first appeared in the 1990s as a means of utilizing geographically distributed resources for computationally demanding tasks. Ian Foster and Carl Kesselman created the Globus Toolkit, a software platform for controlling computing grids. During this period, utility computing also began to emerge, providing computer resources as a pay-per-use service. Utility computing models were established by Sun Microsystems and Amazon, showcasing the advantages of renting resources on demand. When the term "cloud computing" first surfaced in the middle of the 2000s, it completely changed how computer resources are allocated and used. Infrastructure as a Service (IaaS) was founded by Amazon Web Services (AWS) in 2006 and offers virtualized servers, storage, and networking through the Internet. This introduced cloud-based infrastructure that is both scalable and adaptive, completely changing the concept of traditional hosting.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

Reference	Topic	Key Points	Methodology	Findings/Conclusions
Rayaprolu, A. (2023)	Adoption of Cloud Computing	Overview of cloud computing adoption in companies, market trends, and usage statistics	Data analysis from tech industry surveys	Cloud computing is widely adopted with significant market growth; key sectors include IT, finance, and healthcare
Marston, S.; Li, Z.; Bandyopadhyay, S.; Zhang, J.; Ghalsasi, A. (2011)	Business Perspective on Cloud Computing	Focus on cloud computing benefits, drawbacks, and cost efficiencies in business contexts	Analytical review	Cloud computing enhances business flexibility and scalability but poses integration and security challenges
Weinhardt, C.; Anandasivam, A.; Blau, B.; Borissov, N.; Meinl, T. (2009)	Classification and Business Models of Cloud Computing	Categorizes cloud services and explores various business models	Literature review and classification	Identifies SaaS, PaaS, and IaaS models, highlights their respective advantages and business applications
Bhushan, K.; Gupta, B.B. (2017)	Security Challenges in Cloud Computing	Discusses major security issues in cloud environments, including data breaches and privacy concerns	State-of-the-art review of security risks	Recommends advanced encryption, regular audits, and compliance standards for improved security in cloud computing

Cloud computing was defined by the National Institute of Standards and Technology (NIST) in 2011 as a concept that permits on-demand network access to a shared pool of programmable computer resources. NIST played a significant role in standardizing cloud computing. NIST highlighted the universality and simplicity of use of the model. Numerous perspectives on cloud computing have been thoroughly studied, providing insight into its potential and repercussions.[8]

2.1 Cloud Security Frameworks

A. Ability of Framework

The purpose of cloud security frameworks is to guarantee the availability, confidentiality, and integrity of an organization's data in a cloud environment [3]. conducted a careful analysis to see whether new security frameworks would be beneficial in boosting cloud security. The study's objective is to examine and compare several cloud security frameworks and standards to determine their advantages, disadvantages, and overall impact on enhancing cloud security posture. The Cloud Security Alliance (CSA) Security Guidance, the NIST Cloud Computing Security Reference Architecture, and the ISO/IEC 27017:2015 Cloud Security Controls are just a few of the well-known cloud security frameworks that the writers have examined. The evaluation of these frameworks was conducted on the basis of their capacity to address significant issues related to cloud security, including encryption, data protection, access control, and incident response. The study used a comparison to highlight the advantages and disadvantages of each framework. Through its insights into the specific security measures and suggestions offered by these standards, it helped readers understand their significance and use in a variety of cloud deployment types. The study also examined how new security frameworks performed in comparison to previous standards. Di Giulio's study paper completes the comparison of cloud security frameworks and standards, contributing to the body of knowledge currently available. It is an

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

excellent tool for academics and practitioners who wish to make informed judgments on cloud security adoption and grasp the advantages and disadvantages of different security frameworks. Gartner lists security/privacy, cloud environment selection, and governance as the three main challenges in cloud computing. The board of directors should oversee cloud investments to reduce risk, control costs, and turn a profit

B. Use of Framework

It discussed how these frameworks addressed emerging security issues like threat information sharing, DevOps security, and container security. The study's conclusions shed light on how cloud security frameworks are evolving and how that is affecting cloud security. It underlined how important it is to keep these frameworks updated and evaluated in order to keep up with the ever-changing nature of cloud threats. To oversee and manage cloud investments, ISACA advises using the COBIT 5 framework, which ensures consistency and helps to optimize value and reduce risk. Generally, cloud computing relies heavily on goal achievement and strategy alignment, which makes cloud governance an essential component. Several essential elements are combined in this framework: governance, risk management, compliance, incident response, and continuous monitoring. It emphasizes how important it is to have a thorough and proactive strategy in place to guarantee cybersecurity in cloud environments. It is impossible to overstate the importance of SLA management in the governance framework. A scorecard prototype for cloud service level agreements (SLAs) was developed using NIST, ISACA, and CSA principles (ISACA, 2012), (CSA, 2011), and (NIST, 2011). According to Naseer's conference paper, availability, security, and data privacy concerns must be addressed as essential components of cloud risk management.

C. Implementation Challenges

Because cloud ecosystems are complex and threat scenarios are always changing, implementing cloud security frameworks can be challenging.

Integration Complexity: Interoperability problems and redundant controls arise when organizations are unable to smoothly integrate cloud security frameworks into their current IT infrastructures.

Allocation of Resources: Inadequate financial and human resources might make implementation difficult. recommend that companies spend their resources wisely to handle important security measures.

Shared Responsibility Model: Users and cloud providers are both accountable for security. Roles and responsibilities should be clearly defined to avoid confusion and implementation gaps. rules and Compliance: Ensuring adherence to data protection laws and industry rules complicates implementation and emphasizes the necessity of modifying frameworks to satisfy certain regulatory requirements. Dynamic Environment: Because cloud environments are scalable and dynamic, it might be difficult to maintain constant management and monitoring. For security to be maintained, automation and real-time threat detection are essential.

Although there is a wealth of literature on cloud security frameworks, previous studies have pointed up several drawbacks. These holes show places in which more investigation and advancement are needed to raise the effectiveness of cloud security measures.[9]

Cloud Security Problems

Cloud computing has completely changed how businesses handle, store, and use apps and data. To guarantee the privacy, availability, and integrity of data in the cloud, several security issues have been brought about by this paradigm change, which must be resolved.[4]

- Data Privacy and Leakage
- Data Location and Jurisdiction
- Multi-tenancy Risks
- Inadequate Access Control

Cloud Security Solution

Numerous approaches have been proposed and used to address the problems and mitigate the risks associated with cloud security. Here are a few illustrations.[7]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

- Encryption and Key Management
- Identity and Access Management
- Virtualization Security
- Cloud-specific Security Tools
- Security Monitoring and Incident Reaction
- Standards and Certifications for Cloud Security

III. CONCLUSION

Due to its inherent benefits above normal computing and its numerous purposes, the use of cloud technology has fundamentally changed the computing economy. Among the many benefits of cloud computing, one of the most significant challenges is data security. Several encryption algorithms are used to safeguard data in the cloud. Each type of encryption varies on several important ways, like expense, rapidity, effectiveness, and optimality. In a cloud context, the degree of protection for shared data also varies. As a result, using a uniform or random encryption strategy does not provide the best and most efficient protection for cloud data. Research is needed to create a dynamic data security solution that is both ideal and efficient. The research is broken down into multiple stages, such as using the appropriate encryption approach in accordance with the SR, analyzing the security mechanisms currently in place in the cloud, and classifying data based on sensitivity rating (SR). The CIA trio—confidentiality, integrity, and availability—are the three fundamental security factors that have been used to classify data in this article.

REFERENCES

[1]. Rayaprolu, A. How-Many-Companies-Use-Cloud-Computi ng/#gref, Techjury, February 2023. Available online: https://techjury.net/blog (accessed on 2 April 2023).

[2]. Marston, S.; Li, Z.; Bandyopadhyay, S.; Zhang, J.; Ghalsasi, A. Cloud computing—The business perspective. Decis. Support Syst. 2011, 51, 176–189. [Google Scholar]

[3]. Weinhardt, C.; Anandasivam, A.; Blau, B.; Borissov, N.; Meinl, T. Cloud Computing—A Classification, Business Models, and Research Directions. Bus. Inf. Syst. Eng. 2009, 1, 391–399. [Google Scholar]

[4]. Bhushan, K.; Gupta, B.B. Security challenges in cloud computing: State-of-art. Int. J. Big Data Intell. 2017, 4, 81–107. [Google Scholar]

[5]. Dinh, H. T., Lee, C., Niyato, D., & Wang, P. (2013). A survey of mobile cloud computing: Architecture, applications, and approaches. *Wireless Communications and Mobile Computing, 13*(18), 1587-1611. https://doi.org/10.1002/wcm.1203

[6]. Cloud Security Alliance. (2017). *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. Retrieved from https://cloudsecurityalliance.org/research/sec urity-guidance

[7]. National Institute of Standards and Technology. (2013). *NIST Cloud Computing Security Reference Architecture* (NIST Special Publication 500-299). Gaithersburg, MD: U.S. Department of Commerce. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/ nistspecialpublication500-299.pdf