Security Concerns in Cloud Storage

Bhagyashree Patil and Pooja Sapra

March 5, 2024

Security Concerns In Cloud Storage

Bhagyashree Patil
Ph.D Scholar,
Parul University
Vadodara, Gujarat, India
patilbhagyashree89@gmail.com

Dr. Pooja Sapra
Hod of IT Department
Parul University
Vadodara, Gujarat, India
pooja.sapra24683@paruluniversity.ac.in

Abstract— **Cloud storage enables users to store their data and files online through a cloud service, which users may access via the open internet or a specialized private network connection. Cloud storage has become more and more popular among people who require additional storage space and among companies looking for a reliable off-site data backup option. In order to safeguard data integrity, stop hacking efforts, and avert file or identity theft, cloud security has grown in importance as a result of cloud storage's rising use and popularity. In this paper storage security issues, existing solutions for storage security, and security provided by popular storage providers are discussed.**

Keywords: cloud storage, cryptography, confidentiality, intrgrity

I. Introduction

Service delivery over the internet occurs through a mechanism called cloud computing. The last ten years have seen a rise in the prominence of cloud computing, a productive computing paradigm built on grid computing [1]. A model for enabling ubiquitous, practical, on-demand network access to a shared pool of reconfigurable computing resources, such as networks, servers, storage, applications, and services, is known as cloud computing. It allows for quick provisioning and release of these resources with little management work or service provider involvement [2]. Cloud storage systems become an essential component of the new era by offering data storage and management functions. Nowadays, data is being aggressively moved to the cloud by businesses, governments, and individual users. A vast volume of data can produce enormous riches. However, this increases the possible risk, for instance, unauthorized access, data leakage, sensitive information disclosure, and privacy disclosure. The benefits of cloud storage include limitless data store capacity, easy file access, rapid information backup, and inexpensive cost of use. In regard to real-world use, cloud storage can be classified into the following categories: public, private, hybrid, and pooled cloud storage [3]. In the public cloud, businesses outsource their data storage needs to cloud storage providers (like AWS and Alibaba Cloud) rather than setting up and maintaining their own infrastructures and computers. Many small and medium-sized businesses are drawn to the public cloud's benefits, which include flexibility, scalability, and cost savings. With a private cloud, businesses must set up server management and maintenance teams with qualified personnel and implement cloud storage infrastructures. Due to the organization having complete control over the data, the private cloud has stronger security than the public cloud.

A hybrid cloud combines the best features of both private and public clouds, combining them into one solution. In terms of user-friendly interfaces, scalability, and measurement resource, cloud computing and cloud storage are both built on virtualization architecture.

II. Data Security concerns with cloud storage

There could be serious repercussions if storage is not managed properly in a cloud setting. Data management and data security problems are among the problems relating to cloud storage [4][5]. In general, the following data security issues arise, while storing data in the cloud.

- **Confidentiality Issues:** Data confidentiality means the contents of the data are not made available to unauthorized users [6]. Companies outsource data is stored on distant cloud servers, outside of the control of its owners. As a result, only authorized individuals who have been granted access to this data may do so, and cloud providers are not permitted to learn anything about content that has been outsourced.
- **Integrity Issues**: The correctness and completeness of data must be maintained and ensured in accordance with the data integrity property [6]. A cloud customer anticipates that his data will be stored accurately and reliably on distant servers. In other words, data that has been transferred should not be modified with, altered, or purposefully deleted.
- **Data Access Issues:** Security regulations are the main cause of problems with accessing to data in cloud storage [4]. A cloud must follow certain security measures to prevent attackers from gaining unauthorized access to cloud resources.
- **Authentication and Authorization Issues**: Each system that requires perfect security relies on authentication, which functions as a doorway into the cloud that only authorized people can enter. Because access to sensitive information is dependent on authentication, the authentication mechanism must be strong to guarantee availability to legitimate users [4].
- **Data Breaches:** Data storage typically occurs in a cloud environment that is shared by numerous consumers. As a result, the cloud is a tempting target for attackers because a vulnerability of the cloud environment might endanger the data of all users [6].

III. Security provided by service provider

Nowadays many cloud service provider provides storage facilities to users. Dropbox, Google Drive, and One-drive are the most popular storage. These storages provide security at the server side, not the client, as discussed below:

- **Google Drive:** Google drive provides server-side security using a 128-bit AES algorithm. User data is encrypted when data is sent between the user's computer and the cloud using TLS. It also provides two-factor authentication for security.
- **Drop Box**: The data is encrypted by Dropbox both while it is in use and when it is resting using AES 256-bit encryption algorithm.
- **One drive**: OneDrive transfers data via SSL and TLS, which is sufficient to guarantee data security.

IV. RELATED WORK FOR CLOUD STORAGE SECURITY

Many researchers have discovered various methods to secure cloud storage. The most relevant are discussed below:

To improve data security, the author [8] proposed a Lightweight Cryptographic algorithm that used 128-bit block cipher and key to encrypt the data. The author used feistal and substitution permutation to improve the complexity of an algorithm. The suggested approach is compared with different algorithms like AES, DES, and Blowfish and it gives better security as compared to existing methods. In their research study [9], the authors offered an algorithm that will generate a key based on the data supplied and then encrypt data using the generated key. Data that has been encrypted will be transferred to a cloud storage service, and the key will be safely stored on a local computer for later decryption. In research [10], a unique DNA-based data encryption method for the cloud environment is described. Here, using DNA computing, the user's Media Access Control (MAC) address and characteristics, decimal encoding rule, and using ASCII value, a 1024-bit secret key is created which is further used for encryption. The authors [11] of this research put forth public key encryption as a secure data security method for cloud storage. Here, the user encrypts data using both a public key and a class-based cipher text identifier in addition to their public key. In order to address difficulties with data integrity and privacy, a novel paradigm based on a genetic algorithm (GA) called CryptoGA is developed [12]. In order to protect the confidentiality and integrity of cloud data, GA is used to create encryption and decryption keys that are merged with a cryptographic method. In the paper [13] authors suggested a multimodal biometric authentication system to increase the security of cloud data. In order to create a secret key, features from fingerprint, iris, and palm print extraction are combined in several steps, and then the MD-5 hashing method is used to create a hash of characters and numbers. In order to improve cloud web services, a new authentication methodology is suggested by this study to improve the encryption method based on the best key generation with Genetic Algorithm for Elliptical Curve Cryptography [14]. By improving the encryption of the files and passwords using an effective key management strategy, it is utilized to prevent unauthorized access to cloud online services. Instead of storing an entire file on one system, data are stored on various cloud servers utilizing the encryption technique suggested by authors [15]. The files will be divided into several data pieces, encrypted using a variety of ways, and then stored on different clouds using this system. The methodology presented in the paper [16] has important components including improved security and owner-specific data privacy. Utilizing adouble-round key feature, it alters the 128 AES method to accelerate the encryption procedure to 1000 blocks per second.

V. CONCLUSION

This paper mainly focused on cloud storage security issues, existing solutions for storage security, and popular storage security provided by service providers. Mostly all the service provider provides security on the server side and used AES – 256-bit encryption algorithm. The usage of cloud storage is increasing day by day and every organization switches towards cloud storage dues to the cloud's benefits hence security is the main concern. For businesses and enterprises to use cloud storage to store their sensitive data, there is a lot of research that still needs to be done.

References

[1] Gajjam, M. N. S., & Gunasekhar, T. (2021). Key challenges and research direction in cloud storage.

[2] Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

[3] Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, 131723-131740.

[4] Ghani, A., Badshah, A., Jan, S., Alshdadi, A. A., & Daud, A. (2020). Issues and challenges in cloud storage architecture: a survey. arXiv preprint arXiv:2004.06809.

[5] Kaaniche, N., & Laurent, M. (2017). Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. Computer Communications, 111, 120-141.

[6] Yu, Y., Au, M. H., Ateniese, G., Huang, X., Susilo, W., Dai, Y., & Min, G. (2016). Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage. IEEE Transactions on Information Forensics and Security, 12(4), 767-778.

[7] Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115.

[8] Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings, 2(1), 91-99.

[9] Tajammul, M., & Parveen, R. (2020). Auto encryption algorithm for uploading data on cloud storage. International Journal of Information Technology, 12, 831-837.

[10] Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R., & Shanthini, A. (2020). Towards DNA based data security in the cloud computing environment. Computer Communications, 151, 539-547.

[11] Nishoni, S., & Tenis, A. A. (2020). Secure communication with data analysis and auditing using bilinear key aggregate cryptosystem in cloud computing. Materials today: proceedings, 24, 2358-2365.

[12] Tahir, M., Sardaraz, M., Mehmood, Z., & Muhammad, S. (2021). CryptoGA: a cryptosystem based on genetic algorithm for cloud data security. Cluster Computing, 24, 739-752.

[13] Joseph, T., Kalaiselvan, S. A., Aswathy, S. U., Radhakrishnan, R., & Shamna, A. R. (2022). Retraction Note to: A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment.

[14] Dheepak, T. (2021). Enhancing the Cloud Security with ECC based Key GenerationTechnique. Annals of the Romanian Society for Cell Biology, 3874-3891.

[15] Singh, A., & Sharma, S. (2019). Enhancing data security in cloud using Split algorithm, Caesar cipher, and Vigenere cipher, homomorphism encryption scheme. In Emerging Trends in Expert Applications and Security: Proceedings of ICETEAS 2018 (pp. 157-166). Springer Singapore.

[16] Awan, I. A., Shiraz, M., Hashmi, M. U., Shaheen, Q., Akhtar, R., & Ditta, A. (2020). Secure framework enhancing AES algorithm in cloud computing. Security and communication networks, 2020, 1-16.