IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10444

# Securing File Storage on the Cloud using Cryptography

**Aman Singh[1], Shivashankar Reddy Ginni[2], Dr. Advin Manhar[3]**

Final year student, Amity School of Engineering & Technology, Amity University Chhattisgarh, Raipur, India[1]

Final year student, Amity School of Engineering & Technology, Amity University Chhattisgarh, Raipur, India[2]

Assistant professor, Amity School of Engineering & Technology, Amity University Chhattisgarh, Raipur, India[3]

**Abstract**: Data security and privacy are rapidly becoming the predominant issue that forces small and medium business organizations to migrate their data from on-site to the cloud storage facilities. The recent apprehension regarding cloud storage arises mostly from the very fact that currently most of the cloud storage service providers are having unlimited access and therefore the opportunity to read the client's private and sensitive data. There is also a concern that such service providers have so far been unable to convey reasonable surety and confidence that whatever data or information they store on their cloud's infrastructure remains free from unauthorised or unwarranted access and modification in the files. Appreciably, some have managed to use either symmetric and asymmetric cryptography techniques to realize some level of security on cloud storage. This paper mainly focuses on the file securing and cloud storage security issues, giving particular attention to emerging trends and mechanisms of hybrid cryptography techniques.

**Keywords** – File Security, Cloud Computing, Cryptography, Hybrid Cryptography, Access, Authorization, Authentication Data Security, Data Privacy, File Storage

## I. INTRODUCTION

Cloud computing has been around for a short time now. it's not a completely unique technology but rather an innovative model for delivering services and knowledge using current technologies. Fundamentally, cloud computing utilizes existing internet infrastructure to facilitate communication between client nodes and services or applications that reside on a foreign server [1]. CSP's (Cloud Service Providers) are liable for offering cloud services that enable customers to make and utilize web services, very much like internet service providers (ISP's) provide access to high-speed broadband to enable internet access. Unlike the web, cloud platforms act more like an abstracted layer between computing resources and therefore the involved low-level architecture. instead of own physical computing infrastructure, cloud customers only need to pay subscription fees to a CSP to accumulate cloud infrastructure and resources [1]. The key idea with cloud computing is that the subscription model allows customers to save lots of money that they might otherwise have expended on often-expensive resources like hardware, software, and therefore the attendant licenses. CSPs provide such services. This subscription model has thus far proven fashionable [2], observing that disciplined corporate subscribers have achieved cost reductions of up to 18% on information technology (I.T.) budgets and 16% on power costs of knowledge centers.

The extensive adoption of cloud services has yet introduced various challenges for subscribers and CSPs. Various studies agree that establishing and maintaining the safety of services and knowledge stored on cloud infrastructures remains the foremost significant challenge. for instance, [3] contend that cloud-computing concerns, particularly the safety of knowledge and privacy protection, are the most factors inhibiting cloud storage's further adoption. The study observes that the safety concerns during this area of cloud computing arise from the very fact that it's third parties who are usually unknown to clients that are liable for data and infrastructure management on cloud platforms. The researchers [3] note critically that any signs of security severance may precipitate the loss of consumers and hence the cloud services business despite the efforts by CSPs to make sure the supply of highly secured password-protected accounts. [4] agree that data security is that the main issue with cloud storage and attribute the challenge to the very fact that cloud storage involves multiple users sharing an equivalent storage facility. For the researchers, the safety of knowledge and knowledge stored on cloud facilities could also be compromised thanks to weak data access control and identity management mechanisms. The challenges above have thus far necessitated the implementation of varied technological measures to reinforce the safety of knowledge and knowledge stored on cloud platforms. While there's a good range of security measures for cloud storage, this review will examine current perceptions regarding cloud storage security and hence analyze the role of hybrid cryptographic techniques and their future in cloud storage.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10444

### A. Aims and Objectives

• To investigate current perceptions regarding the safety of cloud storage.
• To analyse the implementation of hybrid cryptography because it pertains to securing file storage on cloud infrastructure.
• Investigate the longer-term direction of hybrid cryptographic techniques on securing data, information, and services residing on cloud infrastructure.

### B. Research Questions

• What are the present perceptions regarding the present state of Cloud storage security?
• How is hybrid cryptography implemented to secure file storage on the Cloud.

## II. LITERATURE REVIEW

### A. Current Perceptions Regarding the safety of Cloud Storage

There's arguably little question that the emergence and increased uptake of cloud storage services by small and medium businesses (SMBs) has changed how they conduct business. SMBs have indeed reported reaping various benefits like cost savings, limited data redundancy and duplication, and protection against malware [5]. However, studies by I.S. Decisions, an enterprise that gives security and alter management solutions for major software companies, notes that some businesses that were initially hooked in to cloud storage are yet expressing diverse concerns regarding the security of the info they entrust to CSPs [6]. The survey reveals a good range of prevailing negative perceptions regarding the safety of cloud-based storage services. as an example, the survey shows that an estimated 61% of SMBs situated across the U.K. and France still believe that their organizational data is unsafe within the Cloud despite their substantial data security investment. 50% believe the principle that cloud storage services are less safe than on-site storage facilities, while 45% contend that migrating their data to the Cloud has compromised their security [6].

The study by I.S. Decisions exposes further that cloud storage services customers have reservations regarding the CSPs' ability to detect unauthorized access of their data. The survey reveals that this concern arises from the very fact that cloud storage is usually related to a scarcity of thorough access control mechanisms that make it challenging to detect persons who misuse employee data to access customer data. [7] Admit, as an example, that existing cloud storage systems overly trust the service provided to protect clients'' sensitive data. The consequence of excessive trust has been that a CSP and its employees can read documents regardless of the owner's access policy. I.S. Decisions'' survey results also indicate that detecting unauthorized access remains the most important challenge for cloud storage providers. I.S. Decisions appreciates the extent of this problem by citing that a not insignificant 32% of SMBs expressed that finding the detection of unauthorized access to data and knowledge stored on the Cloud is harder after migrating their data from on-site storage infrastructure [6]. [7] accept as true with the survey's revelation noting that whereas cloud customers endorse the convenience of cloud storage, they're yet careful in trusting providers of the service with privacy-sensitive data due to the shortage of control along user-to-cloud data transfer paths.

### B. Current Implementation of Hybrid Cryptography in Securing File Storage on Cloud Infrastructure

Users are slowly shifting far away from traditional storage devices like thumb drives, hard disks, and other physical storage devices that are gradually becoming obsolete. this alteration has arisen thanks to the globalization of business that has necessitated sharing data for collaborative working and using multiple personal devices. Cloud storage is most applicable within the new era because it facilitates easier collaboration and convenient shifts from one device to a different by providing a singular platform to attach multiple individuals and devices remotely via a stable internet connection [8]. However, cloud storage technologies yet introduce various data storage security risks like leakage, unwarranted access, and illegal modification [9]. Such risks have necessitated the implementation of hybrid cryptography and other techniques of ensuring data on cloud storage facilities is secure [10].

Information systems security experts implement hybrid cryptography by combining a minimum of two varying cryptographic algorithms. the primary approach uses RSA and AES algorithms, whereas the second uses AES and Blowfish algorithms [11]. within the first approach, RSA algorithms are used for key encryption, while AES is employed to encrypt text or data. Data uploads on the Cloud require that an ARS secret key and RSA public key be present. When a user attempts to upload to the Cloud, the file being uploaded is stored in a directory temporarily because it awaits the process of encryption. During encryption, the RSA algorithm is applied to encrypted the data then the AES algorithm is applied to the file. The ARS keys then applied to convert the file into an encoded form. The reverse occurs during the

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10444

process of decryption [12]. Studies by [13] on the primary approach show that the combined implementation of ARS alongside RSA ensures the efficiency and guarantees the cloud storage servers' consistency and reliability. The study sought to use various cryptographic techniques during digital communication while harnessing cloud computing power to enhance the safety of ciphertext and the encrypted data while simultaneously minimizing the time, cost, and the memory consumption during the process of encryption and decryption. Research findings revealed that the hybrid encryption with RSA and AES consumed significantly less time than the first RSA [13].

The second approach for the cryptography involves implementations of AES and Blowfish to supply double encryption over the keys and data. This double encryption effectively ensures a better and efficient level of security as compared to the primary approach [13]. Another study observes that this hybrid of AES and Blowfish guarantees better security by increasing the complexities [14]. AES is taken into the account to the simplest symmetric encryption algorithm and is taken into account safer than Blowfish. However, this combination's downside is that it fails to realize optimal memory usage because Blowfish itself utilizes the high quantity of memory [13].

However, another hybridization technique involves the mixture of Blowfish and ECC (Elliptic Curve Cryptography), which is an emerging alternative for traditional public-key cryptosystems, like RSA, and which a study argues is that the best substitute for asymmetric encryption [13]. ECC is in itself founded on the "toughness of the discrete logarithm problem (DLP), whose network bandwidth is small, and therefore the public key's short. These characteristics make it difficult to guess the keys of the encryption technique and hence render it immune to attacks [14]. With ECC, encrypts each file and stores it on quite one Cloud. File information is stored on the aloud serve for decryption. Storing files on quite one Cloud achieves security because it ensures that an attacker attempting to accumulate the first file can only get a neighbourhood of it [15].

Furthermore, even when an attacker somehow finds access to any of the techniques' keys, they'll not decrypt it during a finite number of life-years [14]. This characteristic is due to the very fact that ECC algorithms for the encoding and decoding processes require maximum time. ECC is additionally beneficial therein it offers less overhead and executes encryption better than RSA. However, ECC suffers the disadvantage of low throughput that limits its compatibility to LTE connections. On the opposite hand, Blowfish offers higher throughput than other algorithms [14]. Hybrid cryptography consisting of Blowfish and ECC guarantees less overhead, better execution of encryption processes, and better throughputs.

Hybrid cryptography is additionally implemented by combining the Krishna and Triple DES algorithms. This hybrid cryptography system allows users of a cloud storage facility to choose an encryption algorithm that they consider best suited to the sort of knowledge they shall upload to the Cloud. The system also determines time-efficient and secure encryption algorithms that facilitate data protection because it migrates from a mobile to a cloud platform [16]. During the encryption process, a plain-text file is first encrypted using the Krishna algorithm that uses a secret key merged with public random bits and shared between sender and receiver. This strategy facilitates encryption and decryption [16]. The encryption of the file using Krishna produces a ciphertext, C1k. C1k then undergoes an extra sequence of three encryption processes using Triple DES. Triple DES key 1 creates ciphertext C2ktd1, Triple DES key 2 creates cipher text C3ktd2, and Triple DES key 3 creates the ultimate cipher text C4ktd3 [16]. During the decryption phase, Triple DES key three decrypts C4ktd3 into C4ktd2, Triple DES key 2 decrypts C4ktd2 into C4ktd1, and Triple DES key 1 decrypts C4ktd1 into C1k. The Krishna algorithm then decrypts C1k into the first plain-text file [16]. The study shows that a mixture of Krishna and Triple DES algorithms offers the simplest ratio of file size to encryption time and is suitable for securing large files within the slightest of your time.

Hybrid cryptography is additionally achieved through a mixture of Krishna and AES algorithms. During the encryption phase, the Krishna algorithm is applied to convert the plain-text file into a ciphertext, C1k. The AES algorithm is then utilized to further encrypt C1k into ciphertext C2kA that's the ultimate cipher [17]. The reverse occurs during the decryption phase. The AES key decrypts ciphertext C2kA to C1k. Krishna then decrypts C1k further to breed the first plain-text file.

Overall, the implementation of the hybrid cryptographic techniques is better than implementing either symmetric or asymmetric cryptography. In their analysis of cloud storage security, [18] discovered that hybrid cryptography is best way to make sure the attainment of security techniques for the protection of data that are accepted globally in data security. These techniques are achieved through the mechanisms of accessing control, authorization, authentication, and confidentiality. A 2016 study has appreciated that the cloud storage service subscribers can only trust the infrastructure data protection capability only when the persuading data protection system follows the mechanisms above under considerations [18].

### C. Future Directions for Securing the File Storage based on Cloud Infrastructure.

Studies by [15] recommend that within the future, information security experts should consider implementing high-level security by hybridizing public key cryptography. Currently, hybridization has only been applied to non-public key

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 4, April 2021

DOI 10.17148/IJARCCE.2021.10444

cryptography algorithms. Hence, the research recommends steganography i.e. (the practice of concealing messages or information within other non-secret text or data) to hide the existence of secret or sensitive data in order that it remains invisible to the general public but visible to valid or authenticated receivers. Steganography may be proven useful for text data because it enables sensitive or secret data to be hidden within the text's cover file. This approach ensures that the text cover file resembles a traditional document and doesn't urge an attacker's interest. within the rare event that an illegitimate user finds the concealed data, they'll yet be discouraged by the huge amount of time for recovering it [15].

## III. CONCLUSION

In summary, the mechanism of cryptography for the cloud storage has emerged because the CSPs try to implement better techniques for securing data in their cloud storage facilities. Customers have indeed expressed their significant concern regarding the security of the info and knowledge they entrust to the respective cloud storage services providers. CSPs have thus far achieved hybrid cryptography by combining the symmetric and asymmetric encryption and decryption algorithms to secure the files on cloud platforms. Hybrid cryptography systems currently use combinations of RSA and AES, AES and Blowfish, Blowfish and ECC, Krishna and Triples DES, and Krishna and AES, among various others. Such combinations make sure that those CSPs can harness both algorithms' advantages during a hybrid system to make sure access control, authorization, authentication, and confidentiality. These hybrid cryptography achievements facilitate further protecting files stored on the Cloud from unwarranted access, modification, transfer, and other potential hazards to data security.

## REFERENCES

[1] Mazrekaj, A., Shabani, I. and Sejdiu, B., 2016. Pricing schemes in cloud computing: an overview. International Journal of Advanced Computer Science and Applications, 7(2), pp.80-86.
[2] S. Carlin and K. Curran, "Cloud Computing Security", Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments, vol. 1, no. 2, pp. 12-17, 2013. Available: https://www.igi-global.com/chapter/cloud-computing-security/68920. [Accessed 8 December 2020].
[3] Jyoti, T. and Pandi, G., 2017. Achieving Cloud Security Using Hybrid Cryptography Algorithm. International Journal of Advance Research and Innovative Ideas in Education, 3(5).
[4] D. P. Timothy and A. K. Santra, "A hybrid cryptography algorithm for cloud computing security," 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, 2017, pp. 1-5, doi: 10.1109/ICMDCS.2017.8211728.
[5] Odun-Ayo, I., Ajayi, O., Akanle, B. and Ahuja, R., 2017, December. An overview of data storage in cloud computing. In 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS) (pp. 29-34). IEEE.
[6] "Cloud Storage Security Issues | A Research Report", IS Decisions, 2020. [Online]. Available: https://www.isdecisions.com/cloud-storage-security-issues/. [Accessed: 08- Dec- 2020].
[7] Xue, K., Chen, W., Li, W., Hong, J. and Hong, P., 2018. Combining data owner-side and cloud-side access control for encrypted cloud storage. IEEE Transactions on Information Forensics and Security, 13(8), pp.2062-2074.
[8] Kanatt, S., Jadhav, A. and Talwar, P., 2020. Review of Secure File Storage on Cloud using Hybrid Cryptography.
[9] Serafino, L.B., 2014. I Know My Rights, So You Go'n Need a Warrant for That: The Fourth Amendment, Riley's Impact, and Warrantless Searches of Third-Party Clouds. Berkeley J. Crim. L., 19, p.154.
[10] Sharma, S., 2019. Security in Cloud Computing using Hybrid Cryptographic Algorithms.
[11] Kumar, M.A. and Karthikeyan, S., 2012. Investigating the efficiency of Blowfish and Rejindael (AES) Algorithms. International Journal of Computer Network and Information Security, 4(2), p.22.
[12] Mahalle, V.S. and Shahade, A.K., 2014, October. Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm. In 2014 International Conference on Power, Automation and Communication (INPAC) (pp. 146-149). IEEE.
[13] Bhandari, A., Gupta, A. and Das, D., 2016, January. Secure algorithm for cloud computing and its applications. In 2016 6th International Conference-Cloud System and Big Data Engineering (Confluence) (pp. 188-192). IEEE.
[14] Timilsina, S. and Gautam, S., 2019. Analysis of Hybrid Cryptosystem Developed Using Blowfish and ECC with Different Key Size. Technical Journal, 1(1), pp.10-15.
[15] Bala, B., Kamboj, L. and Luthra, P., 2018. SECURE FILE STORAGE IN CLOUD COMPUTING USING HYBRID CRYPTOGRAPHY ALGORITHM. International Journal of Advanced Research in Computer Science, 9(2).
[16] Taha, A.A., Elminaam, D.S.A. and Hosny, K.M., 2018. An improved security schema for mobile cloud computing using hybrid cryptographic algorithms. Far East Journal of Electronics and Communications, 18(4), pp.521-546.
[17] Chennam, K.K., Muddana, L. and Aluvalu, R.K., 2017, May. Performance analysis of various encryption algorithms for usage in multistage encryption for securing data in Cloud. In 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (pp. 2030-2033). IEEE.
[18] Jakimoski, K., 2016. Security techniques for data protection in cloud computing. International Journal of Grid and Distributed Computing, 9(1), pp.49-56.