Securing File Storage on the Cloud using Hybrid Cryptography

Oluwasanmi Stephen Alabi  
*Department of Computing*  
*Bournemouth University*Bournemouth, United Kingdom  
s5228470@bournemouth.ac.uk

*Abstract*— Data security and privacy are increasingly becoming the predominant issue that affects small and medium business organisations’ readiness to migrate their data from on-site to cloud storage facilities. The prevailing apprehension regarding cloud storage arises mostly from the fact that current cloud storage service providers have unlimited access and the opportunity to read the client’s private and sensitive data. There is also concern that such providers have so far been unable to convey reasonable confidence that the data and information they store on their cloud infrastructure remains free from unwarranted access and modification. Appreciably, some have managed to deploy either symmetric and asymmetric cryptography techniques to achieve some level of security on cloud storage. This paper focuses on cloud storage security issues, giving particular attention to emerging hybrid cryptography techniques.

Keywords—Cloud Computing, Cryptography, Hybrid Cryptography, Data Security, Data Privacy, File Storage.

# Introduction

## Background

Cloud computing has been around for a while now. It is not a novel technology but rather an innovative model for delivering services and information using current technologies. Fundamentally, cloud computing utilizes existing internet infrastructure to facilitate communication between client nodes and services or applications that reside on a remote server [1]. CSP’s (Cloud Service Providers) are responsible for offering cloud services that enable customers to create and utilize web services, much as internet service providers (ISP’s) provide access to high-speed broadband to enable internet access. Unlike the internet, cloud platforms act more like an abstracted layer between computing resources and the involved low-level architecture. Rather than own physical computing infrastructure, cloud customers only have to pay subscription fees to a CSP to acquire cloud infrastructure and resources [1]. The key idea with cloud computing is that the subscription model allows customers to save money that they would otherwise have expended on often-expensive resources such as hardware, software, and the attendant licenses. CSPs provide such services. This subscription model has so far proven popular with [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 data centers.

The extensive adoption of cloud services has yet introduced various challenges for subscribers and CSPs. Various studies agree that establishing and maintaining the security of services and information stored on cloud infrastructures remains the most significant challenge. For example, [3] contend that cloud-computing concerns, particularly the security of data and privacy protection, are the main factors inhibiting cloud storage’s further adoption. The study observes that the security concerns in this area of cloud computing arise from the fact that it is third parties who are usually unknown to clients that are responsible for data and infrastructure management on cloud platforms. The researchers [3] note critically that any signs of security severance may precipitate the loss of customers and hence the cloud services business despite the efforts by CSPs to ensure the provision of highly secured password-protected accounts. [4] agree that data security is the main issue with cloud storage and attribute the challenge to the fact that cloud storage involves multiple users sharing the same storage facilities. For the researchers, the security of data and information stored on cloud facilities may be compromised due to weak data access control and identity management mechanisms. The challenges above have so far necessitated the implementation of various technological measures to enhance the security of data and information stored on cloud platforms. While there is a wide 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.

## Aims and Objectives

* To investigate current perceptions regarding the security of cloud storage.
* To analyze the implementation of hybrid cryptography as it pertains to securing file storage on cloud infrastructure.
* investigate the future direction of hybrid cryptographic techniques on securing data, information, and services residing on cloud infrastructure.

## Research Questions

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

# Literature Review

## Current Perceptions Regarding the Security of Cloud Storage

There is arguably no doubt 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 such as cost savings, limited data redundancy and duplication, and protection against malware [5]. However, studies by I.S. Decisions, an enterprise that offers security and change management solutions for major software companies, notes that some businesses that were at first enthusiastic about cloud storage are yet expressing diverse concerns regarding the safety of the data they entrust to CSPs [6]. The survey reveals a wide range of prevailing negative perceptions regarding the security of cloud-based storage services. For instance, the survey shows that an estimated 61% of SMBs situated across the U.K. and France still believe that their organisational data is unsafe in the Cloud despite their substantial data security investment. 50% believe in 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 fact that cloud storage is typically associated with a lack of thorough access control mechanisms that make it challenging to detect persons who misuse employee data to access customer data. [7] Admit, for instance, that existing cloud storage systems overly trust the service provided to guard clients’’ sensitive data. The consequence of excessive trust has been that a CSP and its employees can read documents irrespective of the owner’s access policy. I.S. Decisions’’ survey results also indicate that detecting unauthorized access remains the biggest 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 information stored on the Cloud is more difficult after migrating their data from on-site storage infrastructure [6]. [7] agree with the survey’s revelation noting that whereas cloud customers endorse the convenience of cloud storage, they are yet careful in trusting providers of the service with privacy-sensitive data because of the lack of control along user-to-cloud data transfer paths.

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

Users are slowly shifting away from traditional storage devices such as thumb drives, hard disks, and other physical storage devices that are gradually becoming obsolete. This change has arisen due to the globalisation of business that has necessitated sharing data for collaborative working and using multiple personal devices. Cloud storage is most applicable in the new era because it facilitates easier collaboration and convenient shifts from one device to another by providing a singular platform to connect multiple individuals and devices remotely via a stable internet connection [8]. However, cloud storage technologies yet introduce various data storage security risks such as 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 at least two varying cryptographic algorithms. The first approach uses RSA and AES algorithms, whereas the second uses AES and Blowfish algorithms [11]. In the first approach, RSA algorithms are used for key encryption, while AES is used 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 as it awaits encryption. During encryption, the RSA algorithm is applied to encrypted data; then, the AES algorithm is applied to the file. The ARS key is then applied to convert the file into an encoded form. The reverse occurs during decryption [12]. Studies by [13] on the first approach show that the combined implementation of ARS alongside RSA ensures efficiency and guarantees cloud storage servers’ consistency and trustworthiness. The study sought to apply various cryptographic techniques during data communication while harnessing cloud computing power to improve the security of ciphertext and encrypted data while simultaneously minimizing time, cost, and memory consumption during the encryption and decryption phases. Research findings revealed that hybrid encryption with RSA and AES consumed significantly less time than the original RSA [13].

The second approach for hybrid cryptography involves implementing AES and Blowfish to provide double encryption over keys and data. This double encryption effectively ensures a higher level of security than the first approach [13]. Another study observes that this hybrid of AES and Blowfish guarantees better security by increasing complexity [14]. AES is considered the best symmetric encryption algorithm and is considered more secure than Blowfish. However, this combination’s downside is that it has a lower throughput and fails to achieve optimal memory usage because Blowfish itself has utilizes high quantities of memory [13].

However, another hybridization technique involves the combination of Blowfish and ECC (Elliptic Curve Cryptography), which is an emerging alternative for traditional public-key cryptosystems, such as RSA, and which a study argues is 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 little, and the public key is short. These characteristics make it difficult to guess the keys of the encryption technique and hence render it resistant to attacks [14]. With ECC, encrypts each files and stores it on more than one Cloud. File information is stored on the aloud serve for decryption. Storing files on more than one Cloud achieves security because it ensures that an attacker attempting to acquire the original file can only get a part of it [15].

Furthermore, even when an attacker somehow finds access to any of the techniques’ keys, they may not decrypt it in a finite number of life-years [14]. This characteristic is attributable to the fact that ECC algorithms for the encoding and decoding processes require maximum time. ECC is also beneficial in that 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 other 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 higher throughputs.

Hybrid cryptography is also 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 most suitable to the type of data they intend to upload to the Cloud. The system also determines time-efficient and secure encryption algorithms that facilitate data protection as 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 a further 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 final 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 original plain-text file [16]. The study shows that a combination of Krishna and Triple DES algorithms offers the best ratio of file size to encryption time and is suitable for securing large files in the least amount of time.

Hybrid cryptography is also achieved through a combination 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 is the final cipher [17]. The reverse occurs during the decryption phase. The AES key decrypts ciphertext C2kA to C1k. Krishna then decrypts C1k further to reproduce the original plain-text file.

Overall, the implementation of hybrid cryptographic techniques is better than implementing either symmetric and asymmetric cryptography. In their analysis of cloud storage security, [18] discovered that hybrid cryptography is better poised to ensure the attainment of security techniques for data protection that have been accepted universally in the field of information security. These techniques are achieved through mechanisms of access control, authorization, authentication, and confidentiality. A 2016 study appreciates that cloud storage services subscribers can only trust the infrastructure’s data protection capabilities when the prevailing data protection system the mechanisms above into account [18].

## Future Directions for Securing File Storage on Cloud Infrastructure

Studies by [15] recommend that in the future, information security experts should consider implementing high-level security by hybridizing public key cryptography. Currently, hybridization has only been applied to private key cryptography algorithms. Hence, the research recommends steganography to conceal the existence of secret data so that it remains invisible to the public but visible to valid receivers. Steganography may prove particularly useful for text data because it enables secret data to be hidden within the text’s cover file. This approach ensures that the text cover file resembles a normal text file and does not attract a potential attacker’s interest. In the rare event that an illegitimate user finds the concealed data, they may yet be discouraged by the large amount of time it may take to recover it [15].

## CONCLUSION

In summary, the hybrid cryptography for cloud storage has emerged because the CSPs are trying to implement better techniques for securing data in their cloud storage facilities. Customers have indeed expressed significant concern regarding the safety of the data and information they entrust to cloud storage services providers. CSPs have so far achieved hybrid cryptography by combining symmetric and asymmetric encryption and decryption algorithms to secure 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 ensure that those CSPs can harness both algorithms’ advantages in a hybrid system to ensure 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.