

# Chapter 11

## Secure File Storage in Cloud Computing Using a Modified Cryptography Algorithm

**Manya Smriti**

*Vellore Institute of Technology, India*

**Shruti Varsha Venkatraman**

*Vellore Institute of Technology, India*


**Aashish Raj**

*Vellore Institute of Technology, India*

**Vaishnavi Raj Shukla**

*Vellore Institute of Technology, India*

**Aswani Kumar Aswani Cherukuri**

 <https://orcid.org/0000-0001-8455-9108>

*Vellore Institute of Technology, India*

### ABSTRACT

*This chapter investigates the security issues identified with the file cloud storage to ensure the security of client information in cloud information server. The authors have proposed a modified RSA algorithm with multiple keys and CRT to ensure confidentiality of data coupled with hashing through SHA-512 to maintain integrity. This work has made a secure data exchange app where files are encrypted using the RSA-CRT algorithm and hashed later. On successfully implementing the work, they observed that the proposed technique is more secure than the original RSA algorithm and RSA-CRT. Furthermore, it enhanced the algorithm performance for decryption because it employed the CRT for decryption; thus, the proposed technique proved to be faster than RSA with multi keys.*

## **INTRODUCTION**

The algorithm of RSA is an asymmetric cryptography technique. This is working on two keys, i.e. public key and private key. The proposed model in our work takes four prime evaluating techniques and discovers extension to build up a far-off information reviewing strategy that can be utilized to check the uprightness of the redistributed information in numbers for modified RSA. Instead of sending one public key directly, send two public keys to the receiver. However, there is the problem of the speed, so that in RSA decryption used the Chinese remainder theorem to enhancement the speed of RSA decryption.

## **BACKGROUND**

### **Literature Survey**

Yang et al. (Yang & Jia, 2012) proposed a proficient and intrinsically secure dynamic reviewing convention. It secures the information protection against the reviewer by consolidating the cryptography strategy with the bi-linearity property of bi-linear paring instead of utilizing the veil method. In this manner, their multi-cloud clump reviewing convention does not require any extra coordinator. Their cluster reviewing convention can likewise bolster the clump examining for numerous proprietors. Moreover, their evaluating conspire brings about less correspondence cost and less calculation cost of the evaluator by moving the registering loads of evaluating from the inspector to the worker, which enormously improves the evaluating execution and can be applied to enormous scope distributed storage frameworks.

Li et al. (Li et al., 2017) concentrated on the issue of the cloud information stockpiling and planned to give a methodology that could stay away from the cloud administrators arriving at client' delicate information. Tending to this objective, they proposed a novel methodology entitled as Security-Aware Effective Distributed Storage (SA-EDS) model. In this model, they utilized their proposed calculations, including Alternative Data Distribution (AD2), Secure Efficient Data Distributions (SED2) and Efficient Data Conflation (ED- Con) calculations. Their exploratory assessments had demonstrated that their proposed plan could viably shield significant dangers from the cloud side. The calculation time was shorter than current dynamic methodologies. Future work would address making sure about information duplications so as to increment the degree of information accessibility since any of datacentre's down will cause the disappointment of information recoveries.

Bindu et al. (Shwetha Bindu & Yadaiah, 2011), contemplated the issue of information security in cloud servers. To ensure the accuracy of clients' information in cloud information server, they proposed a viable and adaptable plan with unequivocal unique information support, including square change, delete, and join. They use erasure-correcting code in the record dissemination planning to give repetition equality vectors and assurance the information reliability. Their plan achieves the joining of capacity rightness protection and information defilement has been recognized during the capacity accuracy check over the circulated workers. Their plan is exceptionally productive and tough to Byzantine disappointment, noxious information alteration assault, and even worker intriguing assaults. They accept that information stockpiling security in Cloud Computing, a zone loaded with difficulties and of prevailing essentials, is still in its early stages to be distinguished. They imagine a few potential bearings for future examination on this territory. It permits Third Parity Auditor to review the cloud information stockpiling without requesting clients' time, likelihood.

23 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:  
[www.igi-global.com/chapter/secure-file-storage-in-cloud-computing-using-a-modified-cryptography-algorithm/291167](http://www.igi-global.com/chapter/secure-file-storage-in-cloud-computing-using-a-modified-cryptography-algorithm/291167)

## Related Content

---

### Supply and Production/Distribution Planning in Supply Chain with Genetic Algorithm

Babak Sohrabiand MohammadReza Sadeghi Moghadam (2012). *International Journal of Applied Industrial Engineering* (pp. 38-54).

[www.irma-international.org/article/supply-production-distribution-planning-supply/62987](http://www.irma-international.org/article/supply-production-distribution-planning-supply/62987)

### Industry 4.0 Privacy and Security Protocol Issues in Internet of Things

Jayapandian N. (2021). *Research Anthology on Cross-Industry Challenges of Industry 4.0* (pp. 1853-1876).

[www.irma-international.org/chapter/industry-40-privacy-and-security-protocol-issues-in-internet-of-things/276907](http://www.irma-international.org/chapter/industry-40-privacy-and-security-protocol-issues-in-internet-of-things/276907)

### Matrices

Payman Biukaghazadeh (2013). *Graph Theory for Operations Research and Management: Applications in Industrial Engineering* (pp. 14-28).

[www.irma-international.org/chapter/matrices/73147](http://www.irma-international.org/chapter/matrices/73147)

### Domiciling Truck Drivers More Strategically in a Transportation Network

Kerry Meltonand Sandeep Parepally (2014). *International Journal of Applied Industrial Engineering* (pp. 41-56).

[www.irma-international.org/article/domiciling-truck-drivers-more-strategically-in-a-transportation-network/105485](http://www.irma-international.org/article/domiciling-truck-drivers-more-strategically-in-a-transportation-network/105485)

### Performance Analysis of Cloud Systems with Load Dependent Virtual Machine Activation and Sleep Modes

Sudhansu Shekhar Patraand Veena Goswami (2018). *International Journal of Applied Industrial Engineering* (pp. 1-20).

[www.irma-international.org/article/performance-analysis-of-cloud-systems-with-load-dependent-virtual-machine-activation-and-sleep-modes/209377](http://www.irma-international.org/article/performance-analysis-of-cloud-systems-with-load-dependent-virtual-machine-activation-and-sleep-modes/209377)