International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Integrating RSA Encryption in Remote Data Integrity Checking

R. Mohamed Sheriff[1], S. Nirmala Sujithra Rajini[2]

[1]PG Student, [2]Professor
Department of Computer Applications
Dr. M. G. R. Educational and Research Institute, Chennai - 95
[1]msheriff677[at]gmail.com
[2]nirmalasugirtharajini.mca[at]drmgrdu.ac.in

Abstract: ***Cloud computing storage services offer a convenient means of maintaining and managing large volumes of data at a minimal cost. However, they do not guarantee data integrity. Data is transferred to remote cloud servers that may be unsafe or untrustworthy, raising the risk of unauthorized manipulation by external entities or unintentional modification by service providers. Protecting data from potential hackers has thus become imperative to safeguard its integrity. To address this challenge, the paper proposes an Enhanced Data Integrity technique tailored for cloud computing environments. As part of this journal, I am implementing the proposed RSA (Rivest - Shamir - Adleman) algorithm. In comparison to the DES (Data Encryption Standard) algorithm, RSA offers superior security and efficiency. Upon file upload by the data owner, the data is automatically encrypted using the RSA algorithm, thereby bolstering data integrity within the cloud computing framework. when a data owner uploads a file to the cloud, it is automatically encrypted using the RSA algorithm. This encryption process is pivotal in bolstering data integrity within the cloud infrastructure, as it protects against unauthorized manipulation by external threats and unintentional modifications by service providers. By implementing this Enhanced Data Integrity technique, the paper aims to mitigate the risks associated with cloud storage and ensure the security of data in transit and at rest.***

Keywords: cloud computing, data integrity, RSA, DES, environment, efficiency, data owner, revocable, encryption, integrity.

1. Introduction

In this technology has emerged as one of the most promising technologies and has attracted a lot of attention\due to its transparency, immutability, security and decentralization. Researchers have considered running integrity services in a decentralized network, where transactions can be completed without a trusted. Ethereum and Hyper Ledger Fabric are two popular frameworks for implementing this network [1].

In applications have a scalability barrier that limits their ability to support services for large and repeated transactions, such as the computing and communication costs to verify the integrity. In addition, dynamics have rarely been studied. for most existing data\integrity methods. To solve the above problems, we propose a data integrity scheme based on bilinear mapping [2].

To protect data privacy, symmetric key homomorphic encryption is implemented and combined with homomorphic signature to verify the integrity of the compiled data. reduced the computational burden of the hash function in the signature process and used a random masking technique to preserve data privacy. Considering the specificity and complexity of the graphical database, presented two security tokens based on the hash message authentication code [3].

An evolving and popular way to access shared and dynamically configurable resources over a computer network on demand. An example of today's service is Amazon Elastic Compute (Amazon EC2), which supports virtual IT (virtual IT) and allows users to rent virtual computers to run their own computer applications [4].

The development of information technology requires us to protect the privacy of digital data. Combining cryptography with steganography is one of the most effective methods to achieve such encryption. A unique RGB unmixing algorithm is proposed in this study. The idea of RGB mixing encoding is to mix all the RGB elements to distort the image. The RGB blending technique blends the RGB values of each pixel in the image based on the password entered by the user [5].

2. Literature Survey

According to **Rizwan Akhtar**. et al., 2020 tremendous growth of cloud computing has attracted and enabled intensive computing on resource - constrained client devices. Smartphones primarily enable the deployment of data - and computing - intensive applications using the on - demand service model of remote data centers outsourcing personal and confidential data [6].

Rose Adee. et al., 2022 says that cloud computing is a rapidly growing field. It allows users to use computer system resources as needed, especially data storage and computing power, without directly controlling them. The purpose of this paper is to establish a cloud computing data security model based on data encryption and steganography, which aims to reduce existing security and privacy issues such as data loss, data manipulation and data theft [7].

According to **Ahmad O Aseeri**. et al., 2021 a cloud computing environment offers the end user a cost - effective way to store and access private data in a remote storage mode with a certain internet connection. The user has access to information anywhere and anytime. However, data via the cloud does not remain secure all the time [8].

Rubika Walia. et al., 2022 says that cloud computing is constantly evolving and moving to the cloud is becoming

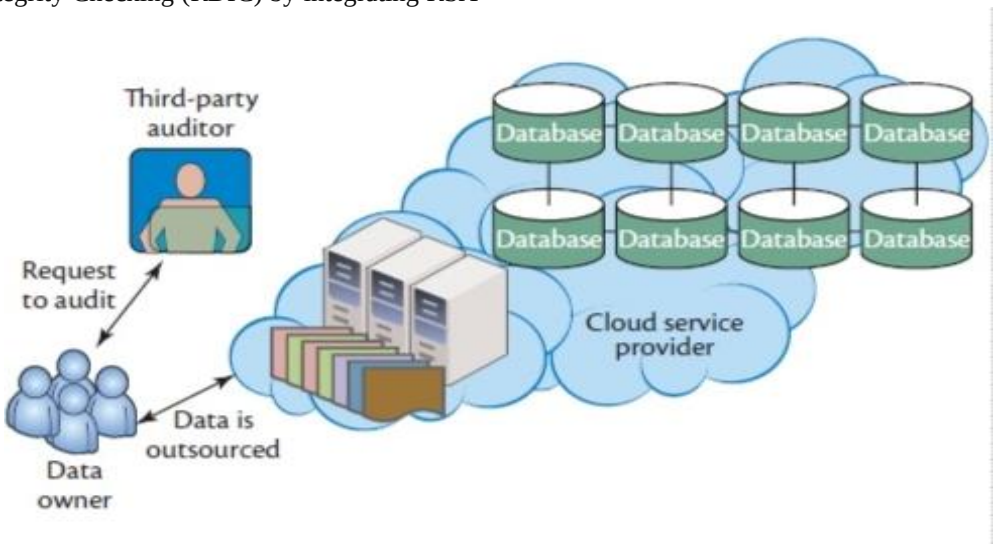
easier and easier. Several information security and data protection issues hinder the adoption of cloud services. The organizational unit, its resources and assets must be protected by a highly secure system [9].
According to **Vishal Dutt.** et al., 2023 Cloud Platforms are the most necessary gateway for remote document management with proper security standards. The concept of cloud environments is similar to a network channel. However, the cloud is considered an advanced form of networking where data can be easily stored on a server without bandwidth limitations [10].

3. Proposed System

The proposed system aims to augment the security of Remote Data Integrity Checking (RDIC) by integrating RSA encryption. This enhancement will fortify data confidentiality, integrity, and authentication, ensuring robust protection against unauthorized access and tampering. Unlike previous efforts to ensure distant data integrity, this project combines both public audit ability and dynamic data operations.

In the proposed approach, after file upload, the file is stored on the local host. If an unknown user attempts to edit the uploaded file, an HMAC (Hash - based Message Authentication Code) value is generated based on the file content. Even a minor change in the file content will result in a change in the HMAC value.

Architecture Diagram:



1) Encryption Module:
Description: This module is responsible for encrypting user data using RSA encryption before transmission.
Functionality: It generates an RSA key pair, uses the public key for data encryption, and sends the encrypted data to the remote server.

2) Hash Calculation Module:
Description: This module calculates cryptographic hash values for the original data to ensure data integrity.
Functionality: It employs a secure hash function (e. g., SHA - 3) to compute hash values, which are transmitted along with the encrypted data to the remote server.

3) Authentication Module:
Description: The Authentication Module verifies the authenticity of the sender and ensures data integrity during transmission.
Functionality: It signs the hash value with the sender's private key to create a digital signature, which is sent to the remote server for verification using the sender's public key.

4) Remote Server:
Description: The remote server stores the encrypted data, hash values, and digital signatures, and performs integrity checks upon receiving the data.
Functionality: It decrypts the received data using the private key, recalculates the hash values for integrity verification, and validates the digital signature to authenticate the sender.

5) Database:
Description: The database stores encrypted data, hash values, digital signatures, and integrity verification results**.**

4. Result and Discussion

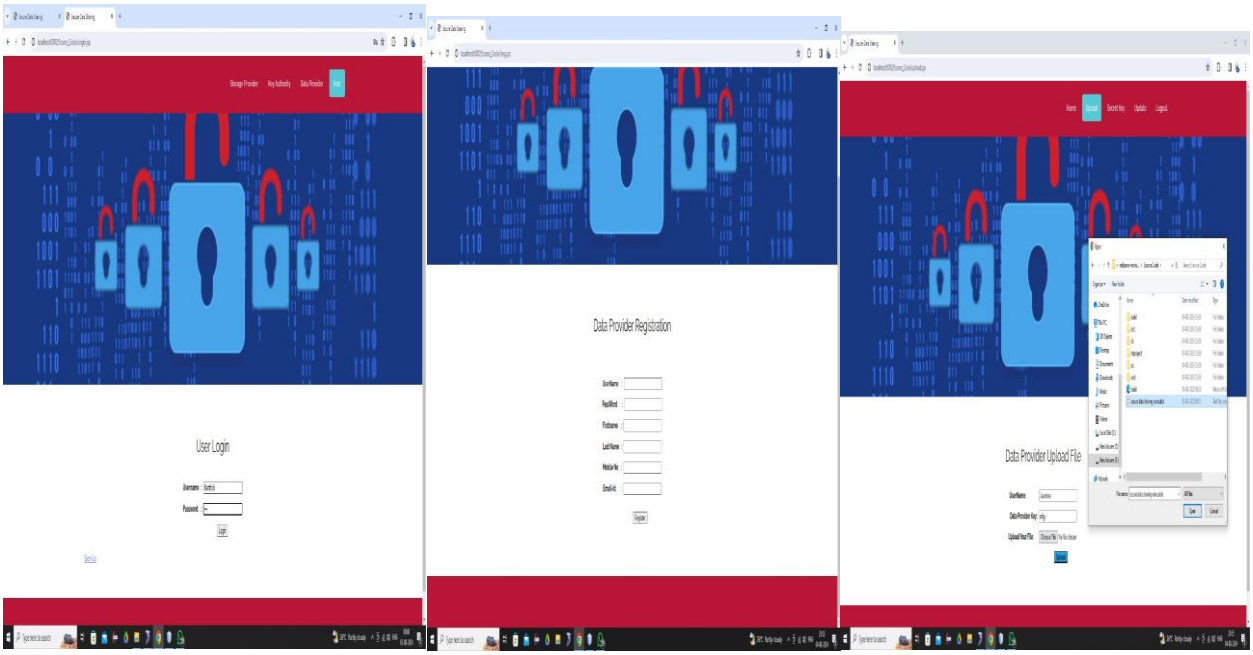


Figure 1: a) Registration 1b) Upload file 1c) Files

a) Data Provider Registration
They provide necessary information and create an account to gain access to the platform's features and functionalities.

b) Data Provider Uploads File:
Once registered, data providers can upload files to the system. These files contain the data they wish to contribute or share with other users. Upon upload, the files are stored securely.

c) File Explanation:
This refers to the process of providing context or explanation for the uploaded files. Data providers may include descriptions, metadata, or other relevant information to help users understand the content and purpose of the files. This explanation facilitates efficient utilization and interpretation of the data by other users or stakeholders**.**

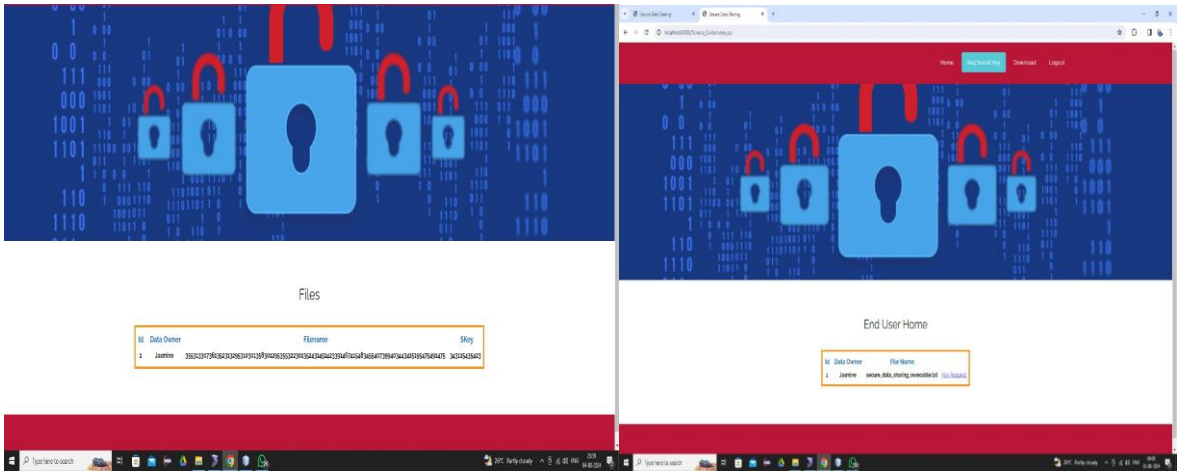


Figure 2: a) Login 2b) End User Home

a) User Login:
Users authenticate themselves by logging into the system using their credentials, such as username and password. This grants them access to the platform's functionalities and resources.

b) End User Home:
After successfully logging in, users are directed to their home page within the system. This page serves as a central hub where users can navigate various features, access their account settings, view notifications, and interact with the platform's content.

c) Generate Key:
This step involves generating cryptographic keys for encryption, decryption, or other security - related purposes. Users may be prompted to generate keys for secure communication, data protection, or access control within the system. These keys are essential for maintaining the confidentiality and integrity of sensitive information exchanged or stored within the platform.

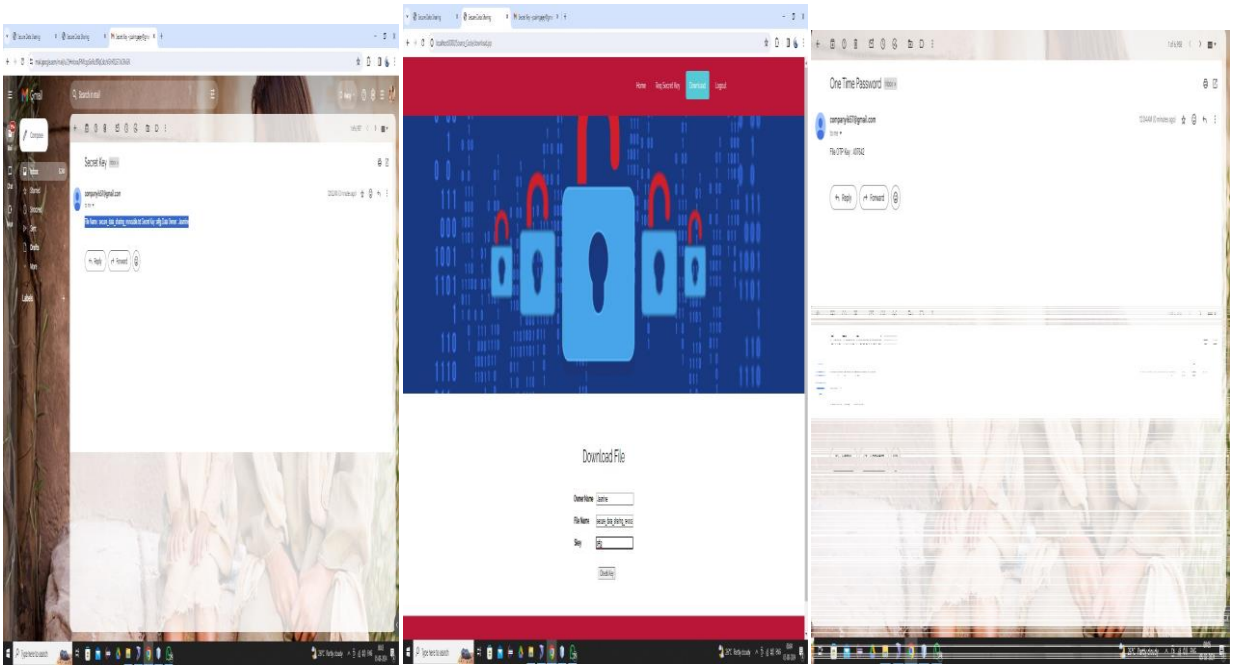


Figure 3: a) Secret Key b) Check Key c) OTP Generate on email

a) Secret Key:
A specific type of key known as a "secret key. " Secret keys are used in symmetric encryption algorithms to both encrypt and decrypt data. They are kept confidential and shared only between authorized parties to ensure secure communication.

b) Check Key:
This verification process ensures that the key is correctly generated and can be used securely for cryptographic operations.

c) OTP Generation on email:
The system generates a one - time password (OTP) for authentication or verification purposes. OTPs are temporary codes typically sent to the user's registered email or mobile device. They provide an additional layer of security by confirming the user's identity before granting Successfully.

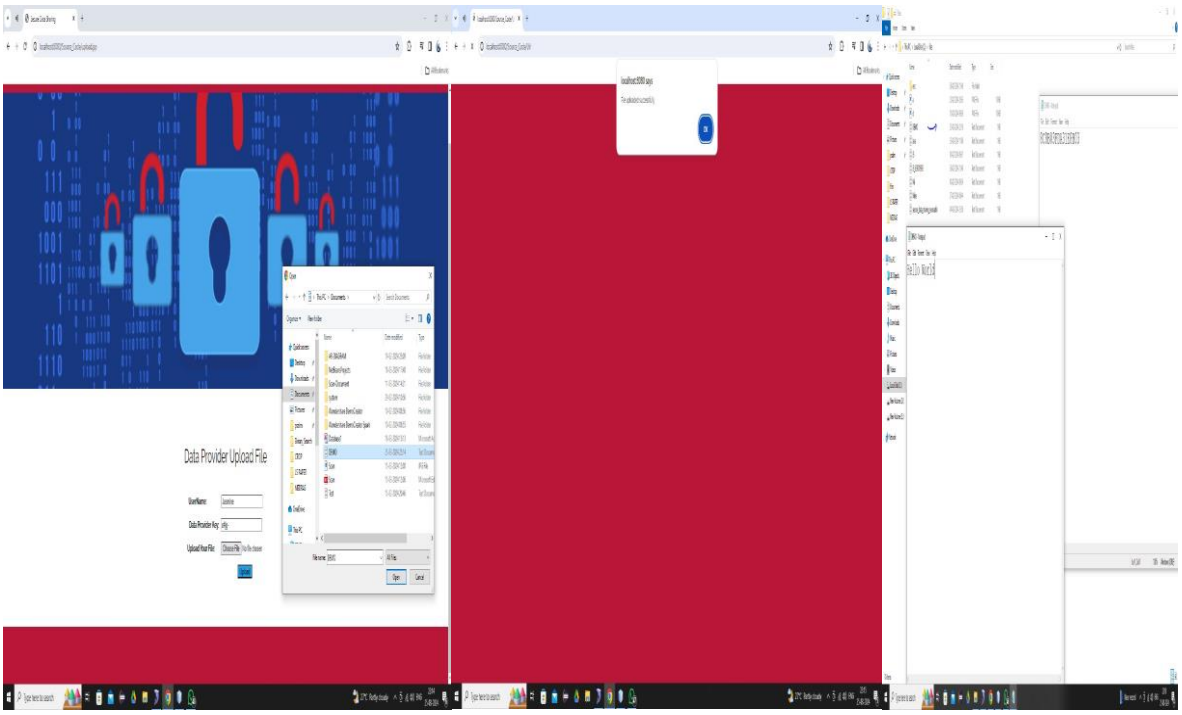


Figure 4: a) FileUpload Page b) Upload Successfully Page c) Encryption Text

a) FileUpload Page: Upon accessing the File Upload Page, users are presented with an intuitive interface to select and upload their desired files securely. The page supports various file formats and ensures data privacy during the upload process.
b) Upload Successfully Page: After successful file upload, users are redirected to the Upload Successfully Page,

which confirms the successful receipt and storage of the uploaded file. This page also provides additional information and next steps for the user.

c) Encryption Text: The Encryption Text page showcases the encrypted version of the uploaded file, transformed using RSA encryption with the public key. This page assures users of the confidentiality and security of their data through encryption.

5. Conclusion

Data integrity is one of the most difficult and pressing security issues in the cloud computing era. Bearing in mind the importance of data integrity, this study examined and compared various existing data integrity solutions as well as drawbacks. This study suggests a verifier - designated remote data integrity checking scheme. This plan can also achieve data privacy protection and resolve the semi - trusted verifier problem. In this paper we propose a new remote data integrity checking protocol for cloud storage. The proposed protocol is sultable for providing integrity protection of customers' important data. This not only addresses data integrity concerns but also tackles issues related to data privacy protection and resolves the problem of semi - trusted verifiers. By introducing a new remote data integrity checking protocol tailored for cloud storage environments, the proposed solution aims to provide robust integrity protection for customers' vital data.

References

[1] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, andD. I. Kim, ‘‘A survey on consensus mechanisms and mining strategy management in blockchain networks, ’’ IEEE Access, vol.7, pp.22328–22370, 2018.

[2] C. Wang, S. Chen, Z. Feng, Y. Jiang, and X. Xue, ‘‘Block chain - based data audit and access control mechanism in service collaboration, ’’ in Proc. ICWS, Jul.2019, pp.214–218.

[3] Zhu, Y. Yuan, Y. Chen, Y. Zha, W. Xi, B. Jia, and Y. Xin, ‘‘A secure and efficient data integrity verification scheme for based on short signature, ’’ IEEE Access, vol.7, pp.90036–90044, 2019

[4] Bolton, T Dargahi, T.; Belguith, S.; Al - Rakhami, M. S.; Sodhro, A. H. On the Security and Privacy Challenges of Virtual Assistants. Sensors 2021, 21, 2312

[5] Hadisukmana, R. N. An Approach of Securing Data using Combined Cryptography and Steganography. Int. J. Math. Sci. Comput.2020, 6, 1–9.

[6] Ijaz Ahmad Awan, Muhammad Shiraz, Muhammad Usman Hashmi, QaisarShaheen, Rizwan Akhtar, Allah Ditta (2020), Secure framework enhancing AES algorithm in cloud computing Security and communication networks 2020, pp 1 - 16.

[7] Rose Adee, HaralambosMouratidis (2022), ”A dynamic four - step data security model for data in cloud computing based on cryptography and steganography Sensors “22 (3), 1109.

[8] SabaRehman, NidaTalatBajwa, MunamAliShah, AhmadOAseeri, AdeelAnjum (2021), Hybrid AES - ECC model for the security of data over cloud storage Electronics 10 (21), 2673.

[9] Rubika Walia, Prachi Garg Mathematical (2022),” Multi Encryption Approach to Provide Security for Cloud Integrated Internet of Things” Statistician and Engineering Applications 71 (3s2), 1538 - 1544.

[10] Abhishek Kumar, Swarn Avinash Kumar, Vishal Dutt, Ashutosh Kumar Dubey, Sushil Narang (2023),”. A hybrid secure cloud platform maintenance based on improved attribute - based encryption strategies International Journal of Interactive Multimedia and Artificial Intelligence (IJIMAI),.