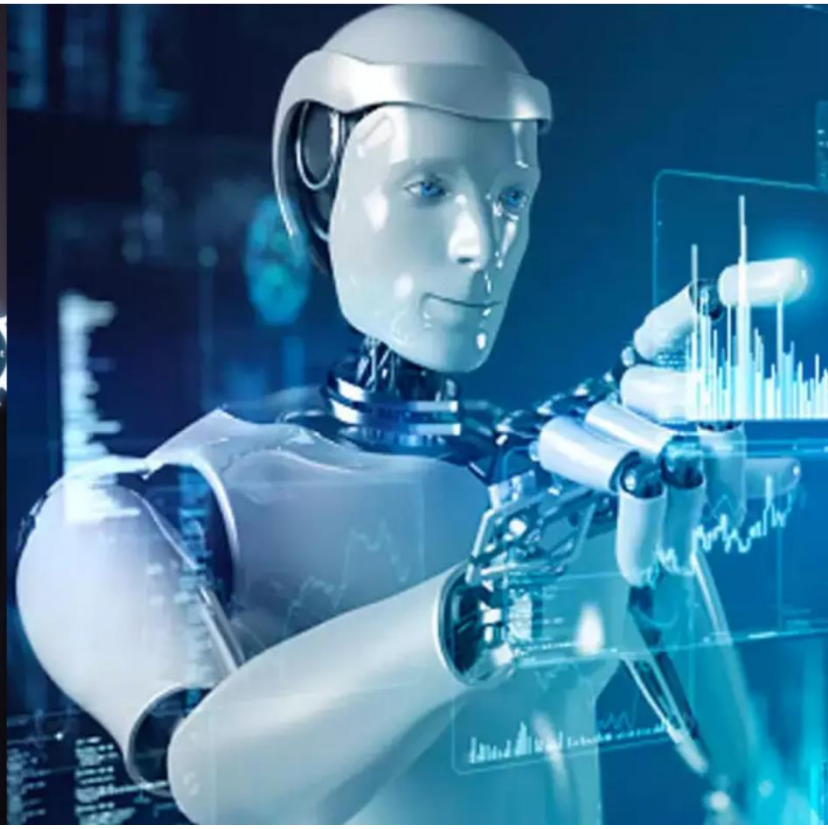
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503182|

A Multi-Format Encryption and Integrity Verification Framework for Secure Cloud Data Storage

Prof. D. J. Manowar[1], Dr. R. N. Khobragade[2]

Assistant Professor, Department of Computer Science & Engineering, Takshashila Institute of Engineering & Technology Darapur, Amravati, Maharashtra, India[1]

Associate Professor, Department of Computer Science & Engineering, Sant Gadge Baba Amravati University, Amravati, Maharashtra, India[2]

ABSTRACT: Cloud computing provides scalable storage and flexible access to computing resources. However, outsourcing sensitive information to cloud servers raises significant concerns regarding confidentiality, integrity, and user control over stored data. To address these issues, this paper proposes a multi-format encryption and decryption framework for secure cloud data storage. The proposed model encrypts different types of data including text, images, and audio using a symmetric key encryption approach combined with a key rotation mechanism. The data is divided into blocks and organized using a Block Status Table (BST), which enables efficient management of encrypted blocks. A Trusted Third Party (TTP) is introduced to verify authorized users and maintain hash values for integrity validation. During data access, the user verifies hash values received from the TTP with the encrypted blocks obtained from the cloud server before decrypting the data. The system ensures data confidentiality, integrity, and controlled access to cloud-stored information. The proposed approach is implemented using MATLAB and evaluated for computational efficiency and security. Experimental analysis shows that the framework provides secure data storage with minimal overhead while supporting encryption of multiple data formats.

KEYWORDS: Cloud Computing, Data Encryption, Key Rotation, Block Status Table, Trusted Third Party, Data Security

I. INTRODUCTION

Cloud computing has emerged as a powerful platform that enables organizations to store and access large volumes of data using remote servers. It provides on-demand access to computing resources such as storage, processing power, and applications. Despite its advantages, cloud computing introduces several security challenges because users must outsource sensitive information to third-party service providers.

When data is stored in a cloud environment, the data owner loses direct control over the storage infrastructure. This creates potential risks such as unauthorized access, data leakage, and data manipulation. Therefore, protecting cloud data through effective encryption and secure access mechanisms becomes essential.

Cryptography plays an important role in ensuring confidentiality and integrity of cloud-stored data. In symmetric cryptography, data is encrypted before being uploaded to the cloud server and decrypted by authorized users using a shared secret key. However, traditional encryption approaches often focus only on confidentiality while ignoring integrity verification and efficient data management.

This paper proposes a secure encryption framework that supports encryption of multiple data formats including text, image, and audio data. The proposed model introduces a Block Status Table (BST) for managing encrypted data blocks and utilizes a Trusted Third Party (TTP) to verify authorized users and maintain hash values for integrity verification. The framework ensures that encrypted data stored in the cloud cannot be modified without detection.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503182|

The main contributions of this work are:
• A multi-format encryption model supporting text, image, and audio data
• A block-level storage approach using a Block Status Table
• Integrity verification using hash values maintained by a Trusted Third Party
• Secure data access and decryption for authorized users

II. LITERATURE REVIEW

Several researchers have proposed various methods to enhance cloud data security using encryption techniques.

Jing-Jang Hwang et al. proposed a cloud computing business model where the cloud service provider is responsible for both data storage and encryption tasks. Although this approach provides centralized security management, it increases computational overhead and reduces control of the data owner.

Junzuo Lai et al. introduced an Attribute Based Encryption (ABE) scheme for secure data sharing in cloud environments. In this model, ciphertext is associated with user attributes, allowing fine-grained access control. However, this approach requires complex cryptographic operations and increases computational cost.

Fatemi Moghaddam et al. proposed a model using two separate cloud servers: one for storing data and another for storing encryption keys. While this improves security, maintaining multiple servers increases storage and operational overhead.

The limitations of these approaches highlight the need for a lightweight encryption system that ensures confidentiality, integrity, and efficient data management without introducing excessive computational overhead.

III. PROBLEM ANALYSIS

In cloud storage environments, maintaining control over encrypted data while ensuring efficient data access is a major challenge. When data is uploaded to the cloud, it is typically stored as a single file. This makes it difficult to manage, verify, or update individual portions of the data.

To address this issue, the proposed system divides the source file into smaller blocks. Each block is encrypted individually using a symmetric key encryption algorithm. A data structure called the Block Status Table (BST) is used to manage these encrypted blocks.

The BST contains two columns:
Sequence Number (SN) – represents the physical storage location of the block
Block Number (BN) – represents the logical block number of the data

Initially, the BST stores entries where SN = BN = j for each block. The BST can also support insertion, deletion, and updating of blocks using a linked list structure.

IV. PROPOSED METHODOLOGY

The proposed system consists of four main entities:
• Data Owner
• Cloud Server
• Trusted Third Party (TTP)
• Authorized User
The workflow of the proposed system is described below.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503182|

Figure 1: Architecture of Secure Cloud Data Storage using TTP and Block Status Table

Step 1: Data Encryption
The data owner divides the original file into multiple blocks and encrypts each block using a symmetric secret key with key rotation. The encrypted blocks form the cipher data.
Step 2: BST Generation
A Block Status Table is created to track the encrypted blocks and their storage locations.
Step 3: Hash Generation
The encrypted file and BST are sent to the Trusted Third Party. The TTP calculates hash values for both the encrypted file and the BST.
FH = Hash(Encrypted File)
TH = Hash(BST)
The TTP stores these hash values securely.
Step 4: Cloud Storage
Only the encrypted data blocks and BST are stored in the cloud server. The encryption key remains with the data owner.
Step 5: Data Access Request
When an authorized user requests access to the data, the request is sent to both the cloud server and the TTP.
Step 6: Verification
The cloud server sends the encrypted blocks and BST to the user. The TTP sends the stored hash values.
The user recomputes the hash values of the received data and compares them with the values from the TTP.
Step 7: Decryption
If the hash values match, the data is verified as authentic. The user then obtains the secret key and decrypts the encrypted blocks to reconstruct the original data.

V. ENCRYPTION MODEL FOR MULTIPLE DATA FORMATS

The proposed framework supports encryption of three types of data.

Text Encryption
Plain text is converted into binary format. The binary data is divided into blocks and encrypted using a symmetric encryption algorithm.

Image Encryption
Images consist of pixels containing Red, Green, and Blue components. Each component is converted into binary form and encrypted to generate an encrypted image object.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

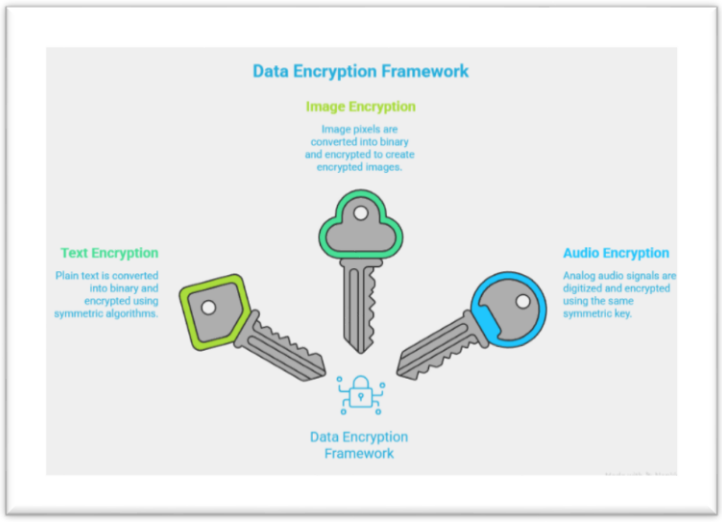
Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503182|

Audio Encryption

Audio signals are converted from analog to digital form using sampling techniques. The resulting digital data is encrypted using the same symmetric key.

This approach enables encryption of multiple data formats using a single encryption framework.



VI. IMPLEMENTATION

The proposed system is implemented using MATLAB.

MATLAB provides a high-performance computing environment suitable for cryptographic operations, data manipulation, and visualization. It simplifies the implementation of mathematical models and encryption algorithms.

Key features of MATLAB used in this implementation include:

- Matrix-based computation
- Data visualization tools
- Support for signal and image processing
- Efficient algorithm prototyping

VII. RESULTS & DISCUSSION

Data Type	File Size	Encryption Time (sec)	Decryption Time (sec)
Text File	200 KB	0.65	0.61
Image File	1 MB	1.42	1.38
Audio File	3 MB	3.18	3.05

Table 1: Encryption and Decryption Performance of Proposed Model

Feature	Traditional Encryption	Proposed Model
Data Confidentiality	Yes	Yes
Data Integrity Check	No	Yes
Multi-format Encryption	Limited	Supported

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 3, March 2026

|DOI: 10.15680/IJIRSET.2026.1503182|

Feature	Traditional Encryption	Proposed Model
Block Level Operations	No	Yes
Third Party Verification	No	Yes

Table 2: Comparison of Proposed System with Traditional Encryption Methods

VIII. APPLICATIONS

The proposed encryption framework has several applications in cloud computing environments.
- Secure storage of organizational data
- Protection of medical records and multimedia data
- Secure cloud backup systems
- Data protection for enterprises using cloud services
- Secure transmission of multimedia files

IX. CONCLUSION

This paper presented a multi-format encryption and integrity verification framework for secure cloud data storage. The proposed system encrypts data using symmetric key encryption combined with a key rotation mechanism. The Block Status Table enables efficient block-level operations, while the Trusted Third Party provides integrity verification through hash value comparison.

The framework ensures confidentiality, integrity, and controlled access to outsourced cloud data. Experimental implementation using MATLAB demonstrates that the proposed approach provides secure data storage with minimal computational overhead.

Future work may focus on improving dynamic block operations, implementing advanced key management mechanisms, and integrating the framework with real cloud platforms.

REFERENCES

1. J. R. Winkler, Securing the Cloud: Cloud Computing Security Techniques and Tactics, Elsevier, 2011.
2. U.S. Health Insurance Portability and Accountability Act (HIPAA), 1996.
3. Tim Mather, Subra Kumaraswamy, Shahed Latif, Cloud Security and Privacy, O'Reilly Media, 2009.
4. Security Architecture for Cloud Computing Environments, White Paper, 2011.
5. Jing-Jang Hwang et al., "A Business Model for Cloud Computing Based on Separate Encryption and Decryption Services," ICISA, 2011.
6. Junzuo Lai et al., "Attribute-Based Encryption with Verifiable Outsourced Decryption," IEEE Transactions on Information Forensics and Security, 2013.
7. Fatemi Moghaddam et al., "Real-Time Encryption in Cloud Computing Environments," IEEE CloudNet Conference, 2013.
8. R. J. and M. D., "Enhanced Cloud Security Model with Hybrid Encryption Approach for Advanced Data Security in Cloud Computing," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 4, pp. 432–439, 2023.
9. A. K. Shukla and A. Sharma, "Cloud Data Security by Hybrid Machine Learning and Cryptosystem Approach," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, 2023.
10. Ravindrakumar, "Data Encryption Techniques for Securing Cloud Storage and Communication," ShodhKosh Journal, vol. 5, no. 4, pp. 861–869, 2024.
11. G. Saini, "A Survey of Various Encryption Techniques in Multi-Cloud to Reduce Information Leakage," International Journal of Intelligent Systems and Applications in Engineering, 2024.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details