

**School of Computer Science Engineering and Information Systems (SCORE)**

**Fall Semester 2025–26**

**Review – I**

**CSE3501** - Information Security Analysis and Audit

**Lab Slot :** G2+TG2

**Faculty :** Dr. A. Anbarasa Kumar

**Title:**

**Secure File Storage Using AES-Based Fragmentation on Cloud**

**Team Members:**

PRANAVO V A – 22MIS0043

SRIRAM V-2MIS0051

**Abstract**

Data security in cloud storage is a critical concern due to increasing cyber threats, unauthorized access, and data breaches. This project, *Cloud Encryption*, proposes a secure file storage system that employs **Advanced Encryption Standard (AES)** encryption and **file fragmentation techniques** to enhance confidentiality and integrity. The system divides files into multiple fragments, encrypts each fragment with AES-256, and uploads them securely to **Dropbox cloud storage**. During retrieval, the fragments are downloaded, decrypted, and reconstructed into the original file. This approach provides an additional layer of security since unauthorized access to individual fragments does not reveal meaningful data. The project demonstrates a lightweight, efficient, and scalable model for secure file storage and retrieval in cloud environments.

**Keywords**

* Cloud Security
* AES Encryption
* File Fragmentation
* Dropbox API
* Symmetric Cryptography
* Secure File Storage
* File Reconstruction
* Data Privacy

**Introduction**

The adoption of **cloud storage services** has revolutionized data management by providing scalability, accessibility, and cost-effectiveness. However, security concerns remain a major barrier to widespread adoption. Issues such as **data breaches, insider threats, unauthorized access, and lack of encryption mechanisms** highlight the need for strong security models.

Traditional encryption methods secure files as a whole but still expose vulnerabilities in case of key leakage or partial decryption. To mitigate these challenges, our project introduces a **hybrid approach combining AES encryption with file fragmentation**. Files are divided into smaller units, each independently encrypted and stored in the cloud. This not only strengthens confidentiality but also complicates attacks since access to a single fragment is insufficient to reconstruct the original file.

In this implementation, **Dropbox** is chosen as the cloud storage platform due to its widespread availability, API support, and reliability. The system ensures secure **upload, storage, and retrieval** of files while maintaining efficiency and minimizing computational overhead.

**Literature Survey**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Title** | **Authors** | **Methodology** | **Merits** | **Demerits** |
| Secure Framework for Cloud Data Privacy Using Enhanced Hybrid Encryption | Sobia Tabassum, Omer Khalid, Nadeem Iqbal, Muhammad Ramzan | Proposed a hybrid framework combining **AES** and **RSA** for securing cloud data; performance evaluated in terms of throughput and delay. | Improved **confidentiality**, reduced **latency**, enhanced **security** for cloud storage. | Increased **computational overhead** due to hybrid encryption. |
| An Efficient and Secure Data Transmission Framework Using Elliptic Curve Cryptography in IoT | Muhammad Zubair, Waseem Iqbal, Muhammad Awais Shibli | Utilized **Elliptic Curve Cryptography (ECC)** with lightweight optimization for IoT data transfer. | **Low energy consumption**, strong security for IoT devices, efficient key management. | May face **scalability issues** in large-scale IoT deployments. |
| Enhancing Cloud Data Security Using Hybrid Cryptography: A Novel Framework | Zeeshan Anwar, Khalid Mahmood Awan, Syed Waqas Haider | Hybrid cryptographic approach combining **AES** and **Blowfish**; evaluated on cloud service scenarios. | High **encryption speed**, reduced **resource usage**, strong **data confidentiality**. | Blowfish’s **64-bit block size** limits scalability against modern attacks. |
| Secure Framework Enhancing AES Algorithm in Cloud Computing | Ijaz Ahmad Awan, Muhammad Shiraz, Muhammad Usman Hashmi, Qaisar Shaheen, Rizwan Akhtar, Allah Ditta | Modified **AES-128** with **double round key** feature; tested on cloud workloads. | Increased speed (**1000 blocks/s vs 800**), reduced **energy consumption** (14.43%), minimized **delay** (15.67%). | Only tested in **simulation**, not in large-scale real-world cloud environments. |
| Exploring Encryption Algorithms and Network Protocols: A Comprehensive Survey of Threats and Vulnerabilities | Jemin Ahn, Rasheed Hussain, Kyungtae Kang, Junggab Son | Survey of cryptographic network protocols (**TLS, SSH**) and their vulnerabilities; analyzed attacks on encryption primitives. | Provides **comprehensive review**, identifies **gaps** in securing network protocols, useful for future research. | Lacks **proposed solution**, only survey of threats and challenges. |

**References**

[1] S. Tabassum, O. Khalid, N. Iqbal, and M. Ramzan, “Secure Framework for Cloud Data Privacy Using Enhanced Hybrid Encryption,” *IEEE Access*, vol. 12, pp. 50342–50355, 2024, doi: 10.1109/ACCESS.2024.3388337.

[2] M. Zubair, W. Iqbal, and M. A. Shibli, “An Efficient and Secure Data Transmission Framework Using Elliptic Curve Cryptography in IoT,” *IEEE Access*, vol. 11, pp. 105193–105203, 2023, doi: 10.1109/ACCESS.2023.3315442.

[3] Z. Anwar, K. M. Awan, and S. W. Haider, “Enhancing Cloud Data Security Using Hybrid Cryptography: A Novel Framework,” *IEEE Access*, vol. 11, pp. 17637–17649, 2023, doi: 10.1109/ACCESS.2023.3246989.

[4] I. A. Awan, M. Shiraz, M. U. Hashmi, Q. Shaheen, R. Akhtar, and A. Ditta, “Secure Framework Enhancing AES Algorithm in Cloud Computing,” *Security and Communication Networks*, vol. 2020, pp. 1–10, Sep. 2020, doi: 10.1155/2020/8863345.

[5] J. Ahn, R. Hussain, K. Kang, and J. Son, “Exploring Encryption Algorithms and Network Protocols: A Comprehensive Survey of Threats and Vulnerabilities,” *IEEE Communications Surveys & Tutorials*, early access, pp. 1–1, Jan. 2025, doi: 10.1109/COMST.2025.3526605.