Project Ideas on Cloud Security and Self-Destructing Data

1. List of Innovative Project Ideas

1 1. Self-Destructing Data Vault using KP-TSABE and Cloud Storage
2 2. Secure Multi-User File Sharing with Time-Limited Access Control
3 3. Blockchain-Based Audit Trail for Cloud File Deletion Events
4 4. AI-Driven Access Policy Manager for Cloud Data Security
5 5. Hybrid Encryption Framework using KP-TSABE and AES for Cloud Privacy
6 6. Federated Learning Model for Secure Cloud Data Classification
7 7. Smart Contract-Based Cloud Data Deletion and Verification System
8 8. Secure IoT Data Storage with Timed Expiry in Cloud
9 9. Privacy-Preserving Cloud Collaboration Platform
10 10. Multi-Layered Access Control Framework using Attribute-Based Encryption

2. Detailed Project Ideas

Project 1: Self-Destructing Data Vault using KP-TSABE

This project focuses on creating a secure cloud storage system where users can upload, share, and manage files with a defined expiry time. Once the expiry period elapses, files automatically self-destruct, ensuring complete data privacy and protection against unauthorized access.
Novelty: Implements time-controlled access using KP-TSABE and automatic data destruction.
Future Scope: Extend to multi-user file sharing and integrate AES for advanced encryption.

Project 2: Blockchain-Based File Deletion Verification System

This system integrates blockchain with cloud storage to record file access and deletion logs immutably. Each deletion event is stored as a transaction, ensuring transparency and accountability in file lifecycle management.
Novelty: Uses blockchain for proof-of-deletion and audit verification, ensuring trust in cloud environments.
Future Scope: Combine with KP-ABE for hybrid secure access control and implement a user dashboard.

Project 3: AI-Driven Access Policy Manager for Cloud Security

An AI-powered access policy manager that learns user behavior and automatically updates access permissions or revokes rights based on risk levels. This minimizes insider threats and unauthorized data usage.
Novelty: Introduces machine learning-based adaptive access control for cloud data protection.
Future Scope: Integrate with KP-TSABE and AES-based encryption for enhanced multi-layered security.