**Secure Personal Cloud Storage System using AWS:**

**Tagline:**  
*A smart alternative to Google Drive with AWS-powered architecture.*

**Abstract**

This project aims to develop a secure and scalable **cloud storage platform** using Amazon Web Services (AWS), offering an experience similar to Google Drive but controlled entirely by the user. The system uses **Amazon EC2** to host a web-based user interface and **Amazon S3** for storing personal files.

**Security and privacy** are top priorities. To achieve this, the system integrates **AWS IAM** or **Amazon Cognito** for robust user authentication and authorization. Files uploaded to S3 are encrypted, and **AWS CloudWatch** is used for real-time performance and system monitoring.

The application allows users to **upload, organize, retrieve, and manage** files with complete control over the backend infrastructure. It is ideal for learners, professionals, and developers who want to explore real-world cloud-native design and architecture.

**Key Technologies Used:**

* **Amazon EC2:** Hosts the web UI and backend logic.
* **Amazon S3:** Handles secure file storage with features like versioning and lifecycle policies.
* **AWS IAM/Cognito:** Ensures authenticated and authorized access to files.
* **AWS CloudWatch:** Monitors system health and logs user activity for auditing and debugging.

**Existing System**

**Current Market Solutions:**

1. **Google Drive**
2. **Dropbox**
3. **Microsoft OneDrive**

These platforms provide:

* Seamless file synchronization across devices
* Simple UI for storage and sharing
* Cloud-based access from anywhere

**Limitations:**

* **Privacy Concerns:** Data resides in and is managed by third-party servers.
* **Vendor Lock-In:** No access to backend logic or source code.
* **Customization Constraints:** Limited user control over features or infrastructure.
* **Monetization:** Premium features such as extra storage or collaboration tools often require subscriptions.
* **Data Ownership:** Users often don’t retain full control over their content.

**Proposed System**

**Overview:**

This system proposes a **decentralized, customizable, and privacy-respecting alternative** to existing cloud storage services. By leveraging core AWS services, users can host their own cloud storage without relying on centralized service providers.

**Key Features:**

* **Personal Hosting:** Users deploy and control their own storage system using AWS EC2.
* **Secure Storage:** Files are encrypted and stored in S3 with access limited by IAM policies.
* **Scalable Architecture:** Auto-scaling and lifecycle management supported by AWS services.
* **Custom UI:** Simple, intuitive file manager interface for managing files and folders.

**System Components:**

* **EC2 Instance:** Runs the frontend (React/HTML) and backend server (Node.js/Python).
* **S3 Bucket:** Securely stores user files. Supports file versioning and access logging.
* **IAM or Amazon Cognito:** Manages users and roles with granular permission control.
* **CloudWatch:** Provides performance metrics, error logs, and alarms.

**Advantages:**

* **Privacy-Centric:** Complete control over data access and encryption.
* **Cost-Effective:** Pay-as-you-go model; no subscription fee like in Google Drive.
* **Expandable:** Can later include sharing, previewing, role-based access, etc.
* **Learning-Oriented:** Ideal for understanding AWS services, DevOps, and cloud architecture.

**Literature Survey**

**Relevant Studies and Sources:**

1. **AWS Whitepaper (2023):**  
   *"Cloud Storage Architectures on AWS"*  
   Describes EC2’s role in scalability and S3’s high durability (99.999999999%).
2. **Research Paper:**  
   *"Secure File Sharing using Cloud Platforms"*  
   Investigates privacy-focused alternatives and discusses encryption and decentralized control.
3. **AWS Official Documentation:**  
   Guides for setting up IAM, Cognito user pools, and EC2-S3 integration for real-world applications.
4. **GitHub Projects:**  
   Various open-source projects (e.g., “S3Drive”, “MyCloud”) attempt to clone Google Drive using AWS. However, most:
   * Lack proper IAM/Cognito integration
   * Do not offer encryption or user control
   * Do not use CloudWatch for monitoring

**Identified Gaps:**

* Lack of open-source, **customizable** and **secure** storage applications.
* Few existing solutions provide a full-stack **cloud-native** system using EC2, S3, IAM, and CloudWatch with a polished UI.
* Educational and deployment guides are fragmented or outdated.