

Problem

Cloud computing offers great advantages.

However,

- To what extent users can trust their cloud provider with their sensitive data?
- Can government agencies store nationally sensitive information on the cloud?
- How to protect information confidentiality, user privacy, and data service continuity in the cloud?
- How to achieve a trusted, reliable, and secure cloud data service using untrusted, less reliable and insecure cloud providers?

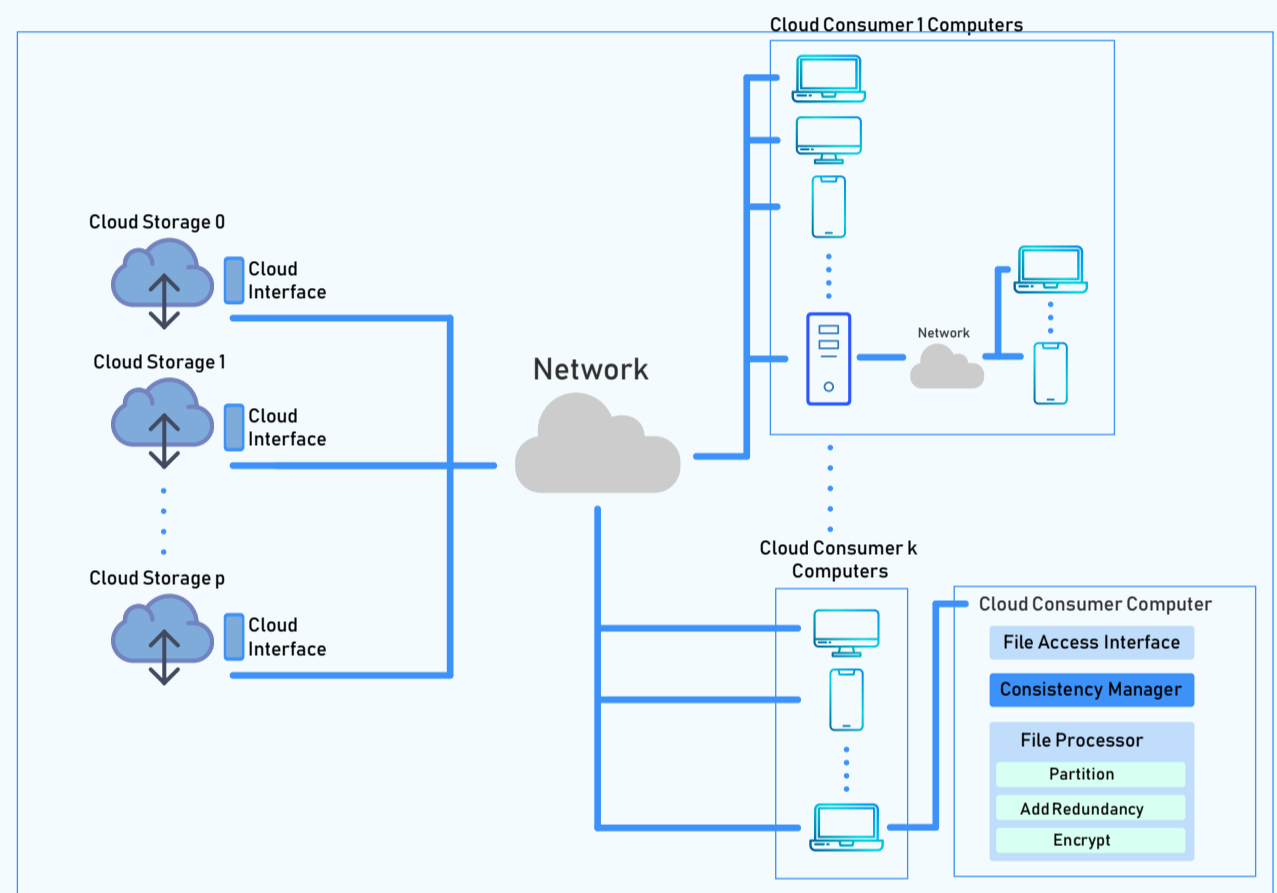
SafeDrive Overview

SafeDrive is an efficient, reliable, and secure multi-cloudfile storage system that keeps data safe and accessible even if you do not fully trust the service provider, whose systems can be compromised or become unavailable. SafeDrive relies on distributed storage on multiple clouds and employs fast techniques for tolerating multiple service outages. Data remain seamlessly accessible as long as m-out-of-n clouds are available. With SafeDrive, data and access credentials never exist in an unencrypted form outside the client's machine.

SafeDrive features

1. **Availability and reliability:** Tolerating multiple unavailable servers using optimal redundancy.
2. **Security, confidentiality:** and trust: The user does not trust anyone but himself. Hiding data content and structure from the cloud. Keeping data safe even if a cloud provider system is compromised.
3. **Performance:** Taking advantage of caching on clients' machines.
4. **Convenience and cost:** Reliable access of data from anywhere. Plus, scalability of data storage at a minimum cost

System architecture

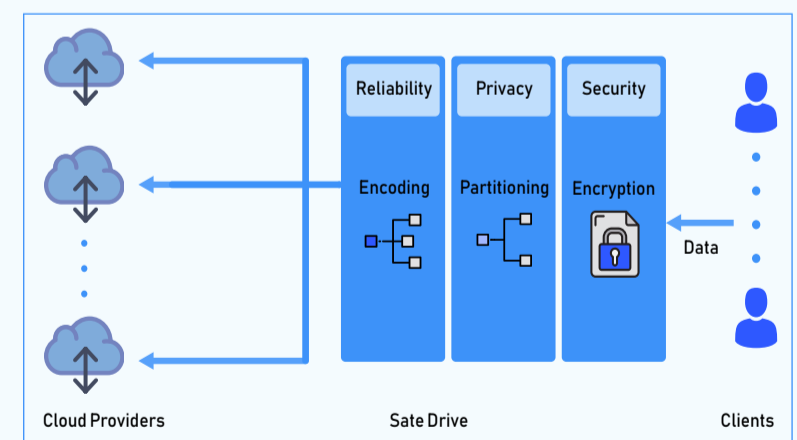
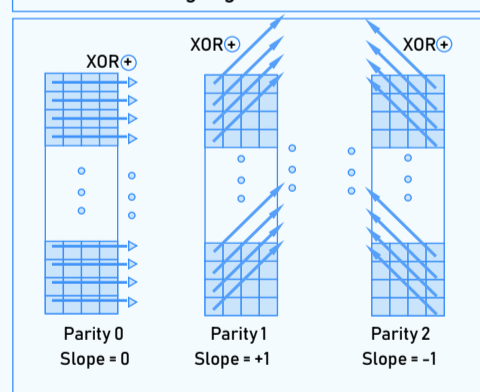


Pending patents

This work IP is protected through two pending US patents:

- Efficient Method for Tolerating Multiple Failures of Storage Nodes.
- New Method for Managing Concurrent Data Modifications in Multi-Cloud Storage Systems .

Encoding Algorithm



Decoding Algorithm

