Introduction:  
SLA parameters of today’s cloud storage include availability of the cloud. Most of the cloud service providers like Amazon S3,Microsoft Azure or Google cloud provide SLA of availability of services for 99.95% of the time however this single properties of SLA is not convincing enough to opt for cloud storage. Cloud is not trusted at all and considered as potential for risk like data leakage, being hacked or returning manipulated data. Cloud is expected to provide securities properties like Confidentiality, Integrity, Write serializability , read freshness in their SLAs. In case of SLA breach, agreed amount can be compensated. We are trying to model mechanism which will provide proofs of security guarantees and violations if any. These proofs will be proofs by client as well as cloud to prove  
Target Scenario:  
We are targeting our model for enterprises which have privacy concerns for moving their storage to cloud. Our model has 3 roles as shown below.  
1. (Data) owner: the entity who purchases the cloud storage service. A data owner might be an enterprise with business data or a home user with personal data.

2. Cloud: the cloud storage provider.

3. (Data) users: users who are given either read or write access to data on the cloud. A user might be an employee of an enterprise or family members and friends of a home user.  
  
 Role of owner would be to carry auditing of security properties and controlling access permissions for users to cloud data.

Concept: