1. 과제명 : 파일 분할 저장 기법을 이용한 클라우드 스토리지 보안 서비스
2. 프로젝트명 : 시크릿 가든
3. 팀원 : 박성진(PL, 23-1), 박주영(23-1), 정영진(22-2), 정일환(23-1)
4. 아이디어 제안

기존의 클라우드 서비스와는 달리 하이브리드 클라우드를 기반으로 파일 업로드 시 블록단위로 분할하여 Private(기업내 클라우드), Public(Amazon S3)클라우드에 나누어 저장한다. 다운로드 시에는 분할된 블록들의 파일정보를 가지고있는 메타데이터를 이용하여 복원한다. 메타데이터는 업로드시 생성되어 인증된 Keyfile을 가진 사용자만 접근가능한 인증서버에 의해서 보관된다. 위와 같은 방식을 이용하기 때문에 두 가지 부분에서 장점을 가진다.

첫째, 퍼블릭 클라우드의 보안성향상 : Public클라우드는 계정정보 및 데이터 유출과 같은 보안문제가 존재한다. 이러한 문제를 해결하기 위해 Private클라우드에도 분할된 데이터를 저장한다. 이를 통해 Public클라우드에서 보안사고가 발생하더라도 전체적인 파일의 보안을 유지 할 수 있도록 한다. 또한 모든 파일이 유출된 최악의 경우에도 메타데이터를 인증서버에서 관리하므로 파일의 보안을 유지한다.

둘째, 프라이빗 클라우드의 비용절감 : 위와 같은 Public클라우드의 보안문제로 인하여 대부분의 기업들은 Private클라우드를 이용 할 수 밖에 없다. 그러나 Private클라우드는 비용상의 문제로 인하여 삼성이나 현대 같은 거대기업에서만 운용, 유지, 보수가 가능하다. 본 프로젝트에서는 파일 저장 시 상대적으로 비용이 저렴한 Public클라우드도 같이 사용 함으로서 중소기업에서도 클라우드 서비스를 이용 할 수 있도록 한다.

1. 개발 방법
2. HDFS 와 Amazon SDK를 이용하여 Private – Public 클라우드 연동 Api개발
3. 하나의 파일을 분할하기 위한 알고리즘 개발 및 메타데이터 설계
4. 사용자 신원 보장용 Keyfile 설계
5. Radius 프로토콜, Kerberos을 기반으로 인증서버 구축
6. 메타 데이터의 무결성 및 손실 문제를 해결하기 위한 복제 Set 구현
7. 개발 계획



1. 평가받고 싶은 카테고리

1. 메타데이터의 무결성이 보장되는가?

2. 업로드 및 다운로드 수행시 파일의 손상이 없는가?

3. 보안 문제에 대하여 신뢰할만한 인증 과정을 제공하는가?