클라우드 저장 서비스 보안에 관한 기술

이민석
UST 정보보호공학과
minseok717@etri.re.kr

The Technique of Clouding Service About its security

MinSeok LEE

*Dept of information security engineering, UST

요 약

현재 정보이용자는 icloud, google drive등과 같은 clouding storage 서비스를 이용하여 자신의 정보를 저장한다. 하지만 서버와 사용자간의 데이터 전송 시 발생할 수 있는 데이터 손실, 서버에 저장된 데이터 삭제 및 소유권 문제 등이 발생할 수 있다. 본 논문에서는 이러한 발생 가능한 정보보안 문제를 해결하기 위한 기술들을 소개하려 한다.

1. 서론

clouding 서비스에서 기업자는 최대한 서버 저장 공간을 확보해 저장에 따른 비용을 절감하는 것을 목표로 하고 있다. 그래서 사용자는 clouding storage에 저장된 data의 삭제 여부, 훼손 여부를 확인하는 기술이 필요하다. 본 논문에선 크게 3가지의 data 저장 보안에 대한 기술을 설명하고자 한다. POR, MAC을 이용한 검증, Homomorphic Authentication 기술을 이용한 검증 기술이다.

2. 저장된 데이터 보안에 관한 기술

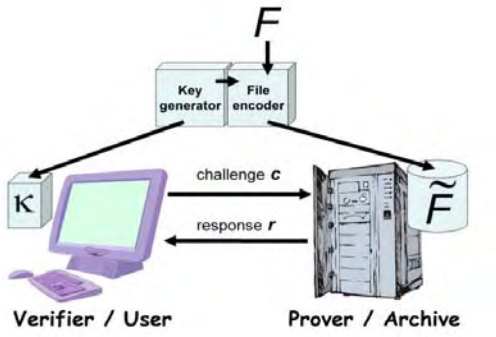
2.1. POR(Proof of Retrievability)

본 기술은 서버가 사용자의 데이터를 잘 보관하고 있는지를 알기위한 기술이다. 즉 사용자는 clouding storage에 저장된 자신의 데이터를 직접 다운받지 않고 서버의 데이터 저장 유무, 손실 여부를 확인할 수 있다. 기본 원리는 다음과 같이 요약할 수 있다.

1) 사용자는 저장할 파일 F를 encoding해서 $\tilde{F}$를 생성하고 서버에 이를 저장한다.

2) 사용자는 서버와 challenge-response protocol을 통해 $\tilde{F}$의 저장유무를 확인한 후 이를 다운로드 받아 decoding한다.

Ari Juels와 Burton S. Kaliski Jr은 저장한 파일 일부를 통해 POR을 수행할 수 있는 기술인 sentinel-based POR system을 고안했다. 다음과 같이 sentinel-based POR system의 원리를 요약할 수 있다.



[figure1. POR system 과정]

1) key generator를 통해 임의의 key pair(public key, private key)를 생성한다(키 생성과정).

2) 파일 F를 생성한 key를 통해 암호화 한다. 암호화한 파일 F에 임의의 값을 가지는 sentinel이란 check value block를 삽입한다(encoding 과정).

3) 과정 2)에서 encoding한 파일을 서버에 저장한다.

4) 사용자는 challenge로써 서버에 sentinel의 위치를 전송하고 서버에게 response로써 이에 대응하는 sentinel 값을 요구한다(challenge-response과정)

5) 사용자는 서버로부터 전송받은 response의 정오(正誤) 여부를 판단한 후 서버에 저장된 파일을 다운로드 받아 이를 decoding한다(retrieval과정).

sentinel은 encoding한 파일의 극히 일부를 차지하기 때문에 서버가 파일 대부분을 훼손하고 sentinel만 유지하여 사용자를 쉽게 속일 수 있다. 이를 방지하기 위해 error-correcting code를 이용해 파일 훼손 정도를 사용자가 파악할 수 있도록 한다.

이 방법은 파일 전체에 대한 POR을 수행하지 않고 encoding한 파일 일부에 삽입한 sentinel(encoding한 파일

의 약 2%를 차지)에 대한 POR을 수행한다. 이에 따른 장점은 서버입장으로 파일 전체에 대한 연산을 수행할 필요가 없어 연산에 따른 비용을 절감할 수 있다. 하지만 사용자 입장에선 key를 보관하는 데 따른 저장 공간 비용, 파일 F를 암호화 하는데 따른 연산 비용을 문제가 있다.

2.2. Message Authentication Codes를 이용한 cloud auditing 기술

메시지 인증코드를 이용한 clouding auditing 기술을 다음과 같다.

1) key generator를 통해 secret key를 생성한다.
2) data에 대한 MAC을 생성한다.
3) 서버에 저장한 data에 대한 MAC을 서버에 요구한 후 이를 사용자는 MAC의 진위여부를 확인한다.

하지만 이러한 기술은 cloud data를 업데이트 할 때마다 새로운 secret key를 생성해야 하고 이를 검증자와 공유해야하는 단점을 가지고 있다. 또한 검증자는 MAC에 대한 key를 저장해 놓고 있어야 한다. 이는 저장 공간에 따른 비용을 증가시킨다.

2.3. Homomorphic Authentication

Homomorphic linear authenticator 기술은 storage verification을 위해 사용되는 기술 중 하나이다. 검증 과정을 요약하면 다음과 같다.

1) 파일 F를 K-dimension 벡터로서 본다.
2) 파일 F의 각 block마다 authentication tag t를 생성한다.
3) 사용자는 서버에게 challenge vector c를 전송한다.
4) 서버는 response로서 사용자에게 파일 벡터와 challenge벡터의 inner product값 μ를 전송한다.

각 과정을 수행하기 위해 key generator algorithm, Encode, Prove, Verify 함수가 사용된다. 앞서 요약한 것과 같이 HA를 이용한 검증 과정도 challenge-response 프로토콜을 이용한다. 4개의 함수를 통해 cloud storage가 사용자의 파일 저장 유무를 확인하는 과정을 살펴보자.

1) key generator algorithm을 이용하여 key pair(public key, private key)를 생성한다.
2) Encode 함수를 이용해 파일 F를 encoding 한다. 이때 이 함수의 input은 파일 F와 secret key이고 이에 대한 output은 파일 F의 encoding file F'과 state information st이다.
3) 사용자는 서버에 challenge 난수 c와 공용키, encoding 파일 F'을 전송한다. 서버는 이들을 input으로 해서 prove 함수를 통해 response μ(c와 F'의 inner product)를 전송한다. 이때 공용키는 F'의 각 block에 대한 인증코드(tag)를 생성하는 데 사용된다.
4) 사용자는 서버로부터 받은 response μ를 verify 함수를 통해 검증한다.

1)~4) 단계를 통해 사용자는 서버에 저장한 자신의 파일 유무를 파악할 수 있다.

3. 결론

본 논문을 통해 클라우딩 storage를 이용하는 사용자 관점에서 data 보안에 대한 기술을 알아봤다. POR, MAC, Homomorphic Authentication을 이용한 검증 기술 모두 challenge-response protocol을 기반으로 하고 있다. 특히 Ari Juels와 Burton S. Kaliski Jr가 고안한 sentinel-based POR 기술은 다른 두 가지 기술과 달리 파일 일부에 대한 검증을 통해 파일의 저장유무, 훼손, 복원 가능성을 사용자는 알 수 있다.

스마트폰 보급이 보편화 된 현재, 사용자는 자신의 PC뿐만 아니라, cellular phone을 가지고 언제 어디서나 자신의 data를 clouding storage에 저장할 수 있고 다른 사용자와 자신의 data를 공유할 수 있다. 본 논문은 사용자 관점에서의 data보안에 대해 알아봤지만 서버 입장으로서 data에 접근하는 사용자가 합법적 사용자인지에 대한 유무를 판단할 수 도 있어야 한다. 또한 서버에 대한 DDos공격과 같은 적극적 공격자에 대한 보안 기술도 확보해야 한다. 사용자 관점에서의 보안과 서버 입장으로서의 정보 보안이 서로 지켜질 수 있어야만 clouding storage의 안전성이 높아진다.

4. Reference

1. A.Juels and B.S. Kaliski Jr., "PORs:Proofs of Retrievalbility for Large Files,"Proc. 14th ACM Conf. Computer and Communications Security, 2007, p.584-585.

2. B. Kaliski and M. robshaw, "Message Authentication with MD5," RSA CryptoBytes, vol. 1, no.1, 1995.

3. D. Boneh and D.M Freeman, "Linearly Homomorphic Signatures over Binary Fields and New Tools for Lattice-Based Signatures," Proc. 14th Int'l Conf. Practice and Theory in Public Key Cryptography(PKC 11), 2011, pp.1-16

4. M.Kolhar, M.M. Abu-Alhaj and S.M. Abd El-atty, "Cloud Data Auditing Techniques with a Focus on Privacy and Security", the IEEE Computer and Reliability Society, 2017, p.42-50.