공공 클라우드 환경에서 안전한 기밀데이터 공유 방법론

하병래*, 이승아*, 조기환**

전북대학교 *전자정보공학부, **컴퓨터공학부
e-mail : {blha, salee, ghcho}@jbnu.ac.kr

A Secure Scheme for Sharing Secure Data in Public Cloud Environment

Byong-Lae Ha*, Seung-Ah Lee*, Gi-Hwan Gho**

*Div. of Electronics and Information Engineering, Chonbuk National University
**Div. of Computer Science and Engineering, Chonbuk National University

요 약

공공 클라우드 컴퓨팅 환경은 대부분 사용자가 직접 데이터를 보유하지 않고 데이터 센터의 논리적으로 분리된 저장 공간에 데이터가 존재하는 환경이기 때문에 데이터의 유효한 보안은 매우 중요하다. 더군다나 데이터 센터 내에 위치한 기밀데이터를 사용자 사이에 공유하고자 하는 경우에 안전한 공유 기법이 제공되어야 한다. 본 논문에서는 공공 클라우드 컴퓨팅 환경에서 계약된 신뢰 모델을 기반으로 안전한 기밀 데이터 공유 방법을 제안한다. 공공 클라우드에서 사용자에게 데이터 제어권을 두고, 클라우드 서비스 제공자는 단지 데이터를 저장, 검색, 전송하는 프록시(Proxy) 서버 역할을 하게하여 증가하는 데이터 공유와 협업을 위한 데이터 공유 기법을 제안한다.

1. 서론

클라우드 컴퓨팅(Cloud Computing)은 많은 IT기업들에게 주목받고 있으며 기업이 당면한 과제를 해결하고 미래 로드맵을 세우기 위한 필수항목으로 떠올랐다. 클라우드 컴퓨팅은 자원의 효율적 사용과 비용절감 등의 강점을 앞세워 미래 IT산업의 핵심 키워드로 자리 잡을 가능성이 높다. 그러나 클라우드 컴퓨팅이 인터넷기술을 기반으로 서비스를 제공하기 때문에 개인PC를 이용할 때보다 보안에 취약하다는 것은 분명하다[1]. 또한 공간을 공동으로 활용하는 클라우드 컴퓨팅은 사용자와 서비스 중심의 개방형 구조이며 공유하는 자원과 데이터에 대한 제어권을 사용자가 갖지 않는 점에서 다양한 보안 이슈들이 발생한다.

사용자가 특정 장치로 인터넷을 이용하여 서비스를 제공받을 때, 이를 위한 일련의 작업은 클라우드 컴퓨팅 환경에서 이루어지지만 사용자의 개인 정보와 서비스에 대한 일부 정보는 사용자의 단말이 보유하고 있다. 이는 데이터 노출 위협을 내포하고 있으며, 노출된 데이터를 통해 사용자의 프라이버시 침해가 명료하게 드러날 것이다. 또한, 이를 통해 사용되는 데이터에 대해 유추가 가능할 것이다.

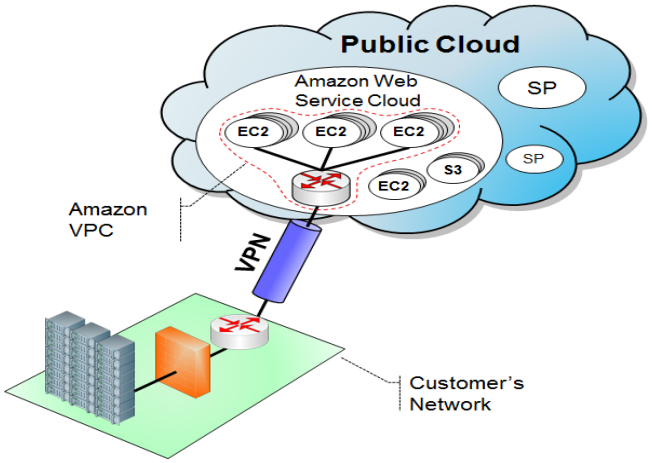
클라우드 컴퓨팅은 자원이 동일한 통제영역에 위치하는 구조적 특성으로 인하여 훌륭한 협업터전이 될 수 있다. 즉, 다수의 사용자 혹은 기업이 참여하는 협업업무를 수행하는 과정에서 시간과 장소의 제약 없이 일관성 있는 데이터 공유가 가능하다. 클라우드 컴퓨팅이 갖고 있는 고유 특성을 최적화하기위해서 적합한 사용자에게 안전한 데이터 공유 수단을 제공하는 것은 필수적이다.

따라서 본 논문에서는 공공 클라우드 컴퓨팅 환경에서 발생하는 다양한 보안 문제점 중 이전 논문[2]에서 제안한 계약된 신뢰 계층 모델을 기반으로 안전한 기밀 데이터 공유 기법을 제안한다. 다른 클라우드 서비스 제공자를 이용하는 사용자의 데이터를 활용하기 위해서 클라우드 서비스 제공자를 프록시(Proxy) 서버처럼 사용하고, 정의된 데이터 인덱스를 이용하여 데이터를 제공받는 방법을 제안한다. 또한, 이를 위한 필요한 요소들을 정의하고 기밀 데이터 공유 절차에 대해 설명한다.

본 논문의 구성은 다음과 같다. 먼저, 2장 관련 연구에서는 공공 클라우드 환경에서 기관 별도의 추가적인 사설 클라우드 구축 없이 공공 클라우드를 이용하여 사설 클라우드처럼 활용 가능한 VPC(Virtual Private Cloud : 가상 사설 클라우드)와 P2P 환경에서 데이터 전송 시 신뢰하는 버디(Buddy)를 활용한 사용자 정보 보호 및 익명성 보호 기법을 살펴본다. 3장에서는 본 논문에서 제안하는 공공 클라우드 환경에서 안전한 기밀 데이터 공유 방법을 설명한다. 마지막으로 4장에서는 본 연구의 결론 및 향후 연구 방향을 제시한다.

2. 관련 연구

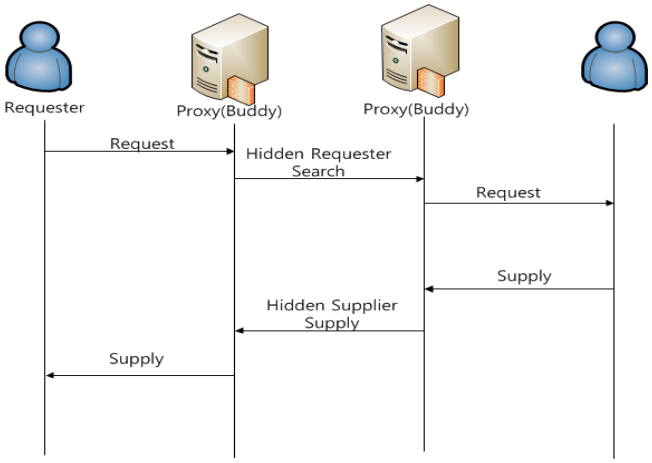
2.1 VPC(Virtual Private Cloud)[3,4]



(그림 1) Amazon VPC

VPC는 (그림 1)과 같이 공공 클라우드에서 특정한 제약사항을 통해 마치 사용자가 구축한 사설 클라우드처럼 사용하는 형태이다. 현재, Amazon, Microsoft 등의 기업들이 전통적인 정보보호 네트워크 모델인 VPN을 이용하여 서비스하고 있으며, 사용자가 사설 클라우드의 설치 비용없이 클라우드 제공자로부터 서비스를 받아 사용할 수 있다. 하지만 이러한 VPC는 CSP(Cloud Service Providers : 클라우드 서비스 제공자)들이 데이터 소유자의 내부가 아닌 외부 기관이기 때문에 데이터 소유자가 데이터를 전적으로 제어하는 것은 아니다. 자원의 통제권을 클라우드에 위탁하는 환경에서 공공 클라우드의 공유성과 개방성으로 인하여 다수의 클라우드 고객과 CSP는 여러가지 데이터 보호 위협에 직면하게 된다.

2.2 P2P환경에서 신뢰기반 데이터공유 기법



(그림 2) P2P 환경에서 신뢰기반 데이터 공유

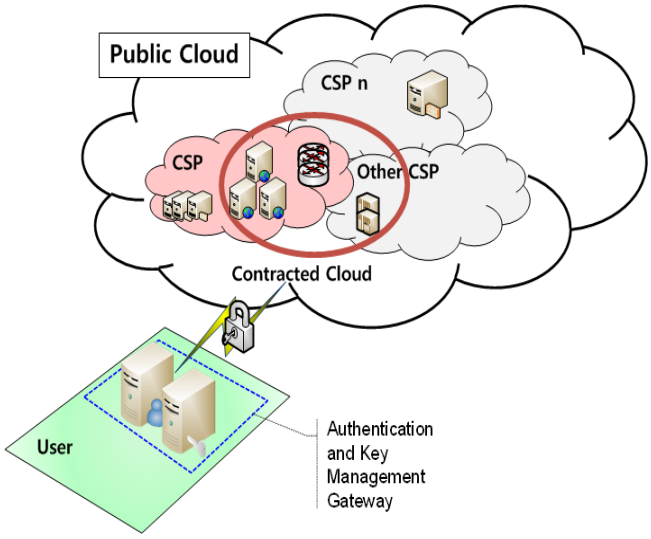
일반적으로 상대방을 알 수 있는 P2P 통신에서 프라이버시는 개인을 인식할 수 있는 정보이다. 프라이버시는 개인의 신원, 관심사항, 데이터 등을 포함한다. 이러한 프라이버시는 보호되어야하기 때문에 데이터 요구자 뿐만 아니라 제공자에 대한 확실한 프라이버시 레벨을 유지해야 한다.

Yi Lu et. al.[5]이 제시한 접근법은 (그림 2)처럼 프라이버시를 보호하기 위해 신뢰하는 서버를 사용한다. 또한 요구자와 함께 제공자의 익명성을 보장하기 위해 버디(Buddy)를 각각 활용한다. 이러한 버디는 사용자의 신뢰를 기반으로 만들어지며 버디 자신도 신뢰를 통해 믿을 수 있는 프록시 서버인지 확인하게 된다. 버디는 요구된 데이터에 대하여 검색할 수 있으며, 다수의 후보값을 보유하고 있다. 또한, 후보값을 찾기 위한 별도의 필터를 사용한다.

이러한 기법은 안전한 통신과 함께 데이터 사용자 및 제공자의 익명성 보장이 가능하지만 신뢰를 기반으로 하기 때문에 신뢰를 측정할 수 있는 정교한 알고리즘이 필요하다. 또한, 클라우드 컴퓨팅을 사용함에 따라 비용절감 효과를 극대화하려는 사용자에게 통신의 오버헤드를 부여해 비용증가를 초래한다.

3. 기밀데이터 공유 방안

3.1 기본 모델



(그림 3) 기본 모델

이전 논문[2]에서 제안된 기본 모델은 (그림 3)과 같으며, 가상화되고 분산된 공공 클라우드 환경에서 다수의 CSP가 존재할 때 사용자의 안전한 인증 및 데이터 저장과 공유를 위한 모델을 제시한다. 기본 모델은 사용자 ID 관리와 키 관리를 위한 일정한 보안수준을 수행할 수 있는 일정 규모의 기관으로 한정한다.

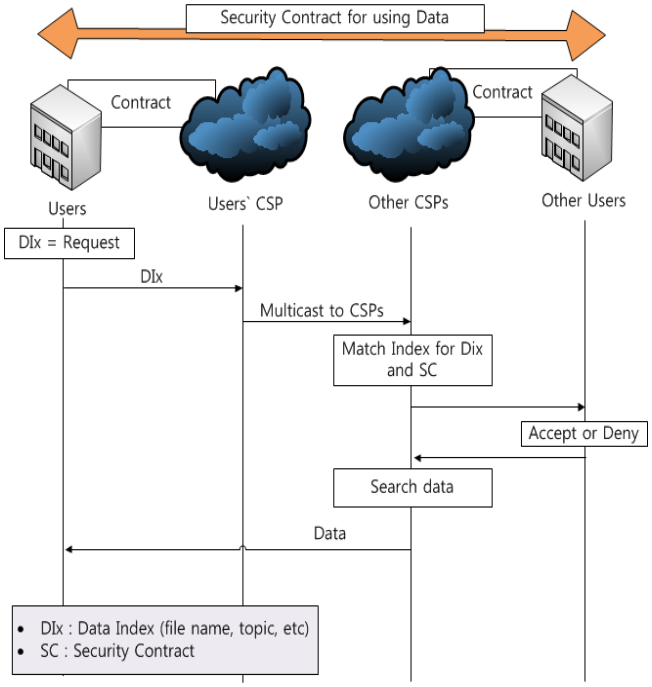
기본 모델은 공공 클라우드 계층과 계약된 신뢰 계층으로 구분된다. 계약된 신뢰 계층은 사용자와 CSP 상호간

계약에 근거한다. 사용자 ID와 Key관리는 기관의 제어 하에 운영한다. 이는 클라우드 서비스 실행이 계약에 의해서 신뢰계층을 형성하여 사용자 접근 통제 및 데이터에 대한 제어권을 기관이 갖는 것을 의미한다. 사용자 ID 관리와 키 관리를 내부 신뢰에 포함함으로써 클라우드에서도 조직은 내부 통제와 같은 수준으로 보안을 유지할 수 있다.

3.2 데이터 공유 기본 모델

데이터 공유 절차에서 요약된 용어를 정리하면 다음과 같다.

- 데이터 인덱스 (DIx : Data Index) : 데이터를 사용할 수 있는 범위와 해당 데이터를 찾을 수 있는 메타 데이터이며, 여기에는 파일명, 해시된 데이터조각, 사용자의 접근 권한 등을 포함할 수 있다. 실질적인 데이터 요청자는 데이터 인덱스를 소유할 수 없으며, 서비스를 통해 접근이 가능하다. 이를 통해 내부 사용자의 악의적인 누출이나 외부침해로부터 DIx를 보호하여 CSP가 보유한 데이터 유추, 사용자의 권한등은 유추가 불가능하다. 기관은 데이터 요구를 CSP에 요청하며, CSP는 DIx를 통해 검색하여 제공한다.
- 보안계약 (SC : Security Contract) : CSP가 사용자와 계약을 체결하여 신뢰할 수 있는 계층을 형성하고 보안계약에 따라 사용자 접근권한 및 데이터 암호화 방법 등을 수행한다.



(그림 4) 데이터 전송 모델

다른 CSP를 이용하는 소유자의 데이터를 이용하기 위해 사용자가 속한 기관은 CSP와 맺은 보안계약과 같이 다른 기관과 데이터 사용에 관한 계약을 맺는다. 계약된 관계에서 데이터 전송 요청 시 확인 후 데이터를 제공하게 된다. 적절한 서비스를 제공하기 모든 통신채널은 암호화하여 이루어진다고 가정하며, Key관리를 위한 절차는 생략한다. 제안된 모델을 바탕으로 다른 CSP에 존재하는 데이터 사용에 대한 절차는 (그림 4)와 같으며 데이터 공유 기본 모델의 절차에 대한 각각의 의미는 다음과 같다.

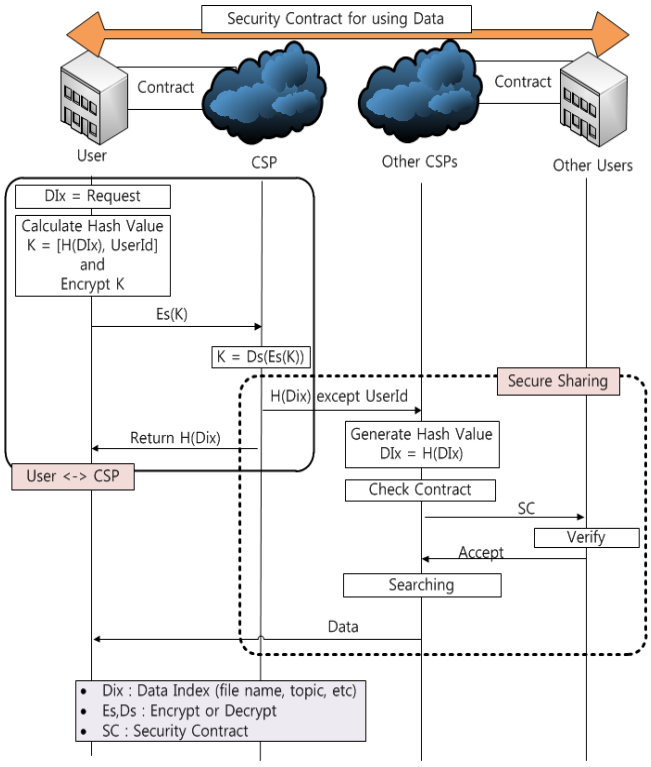
① DIx = Request
기밀 데이터를 이용하려는 사용자는 요청메시지인 DIx를 CSP에 전달

② Multicast to CSPs
CSP는 관계된 다른 CSP에게 멀티캐스트 방식으로 DIx를 전달 (멀티캐스트 방식을 사용하여 관계된 CSP에게만 전달이 가능)

③ Match Index for DIx and SA
DIx를 받은 CSP는 자신의 DIx와 비교하고, 기밀데이터의 소유자에게 보안계약을 확인한 후 기밀 데이터 사용 승인 또는 거절

④ Search data and Transfer
기밀 데이터 사용 승인 시 DIx를 활용하여 검색하고 요청한 CSP를 통해 전달

3.3 안전한 기밀 데이터 공유 기법



(그림 5) 안전한 기밀 데이터 공유 절차

데이터 전송 모델을 기반으로 사용자가 안전하게 데이터 공유를 위한 구체적인 절차는 (그림 5)와 같으며, 크게

실선으로 구분된 사용자와 CSP 그리고 점선으로 구분된 안전한 데이터 공유 기법으로 나뉘어진다. 구체적인 내용은 다음과 같다.

3.3.1 사용자와 CSP

(그림 5)에서 실선에 해당되는 부분이며 사용자가 해시된 DIx를 전달하면 CSP는 그것을 이용하여 검색하고, CSP 내부 악의적인 사용으로부터 DIx 노출을 방지하기 위해 다시 사용자에게 반납하는 부분이다. 구체적인 절차와 설명은 다음과 같다.

① DIx = Request
본 논문에서는 Request = {Filename, Access Control Level, H(UserId)}로 설정하였으며, 이를 통하여 검색과 더불어 사용자의 접근권한 전송이 가능

② Calculate Hash Value, K=[H(DIx), UserID], Encrypt K
데이터 공유 요청 사용자는 메시지인 DIx를 다른 기관과 계약된 방법으로 해시하고 CSP가 인지할 수 있는 UserId와 함께 암호화한 K를 생성 및 CSP에 전달 (사용자가 DIx를 해시하여 CSP에 전달하는 이유는 데이터를 찾기 위한 DIx를 통해 DIx 노출 시 다른 CSP를 가진 데이터에 대한 유추를 방지하기 위함)

③ K=Ds(Es(K)), Return H(DIx)
CSP는 K를 복호화하여 H(DIx)와 UserId를 확인한 뒤 사용하게 되며 UserId는 별도 저장. 사용된 H(DIx)는 데이터 공유 요청을 한 사용자에게 값을 반환 (CSP의 내부 사용자로부터 야기되는 보안위협 해소)

3.3.2 데이터 공유 기법

(그림 5)에서 점선에 해당되는 부분이며 CSP는 DIx를 이용해서 다수의 CSP에게 전달하여 데이터를 검색한다. 데이터 소유자의 CSP는 전송 전 소유자에게 보안계약을 확인하고 데이터를 제공하는 부분이며 구체적인 절차와 설명은 다음과 같다.

④ H(DIx) except UserId
CSP는 UserId를 제외한 해시된 DIx를 멀티캐스트방식으로 다른 CSP에게 전달 (CSP는 H(DIx)와 관련된 풀을 형성하여 반복적인 데이터 공유 시 멀티캐스트가 아닌 직접 요청하여 사용가능)

⑤ Generate Hash Value, DIx=H(DIx)
멀티캐스트를 받은 CSP는 해시된 DIx값과 자신의 DIx값을 비교하여 일치하면, 사용자에게 보안계약에 대해 확인요청, 즉 본 논문에서 정의한 DIx={Filename, Access Control Level, H(UserId)}를 통해 파일에 대한 사용자의 접근 권한을 데이터 소유자에게 확인, H(UserId)는 데이터 소유자와 사용자 양 당사자간 계약된 사항에 따라 적합한 사용자인지 확인(요청받은 CSP가 가지는 DIx는 사용자와 보안계약에 의해 요청받은 CSP가 미리 보유한다고 가정)

⑥ Check Contract
CSP는 사용자의 보안계약에 따라 데이터 사용 승인 또는 거절을 하게 되며, 처음 데이터 공유시 보안계약에 따라 데이터 요구자의 H(UserId)를 통해 보안계약을 확인함

⑦ SC, Verify, Accept
CSP가 요청한 H(UserId)를 이용하여 데이터 소유자는 데이터 요청자와 맺은 계약을 토대로 데이터 사용 승인 및 거절

⑧ Searching
데이터 사용 승인 메시지를 받으면 해당 데이터를 검색하여, 데이터를 요구한 CSP에게 전달

⑨ Data Transfer
요청한 CSP는 처음 요청 메시지를 받을 때 저장해둔 UserId를 사용하여 요청한 사용자에게 데이터 전송

4. 결론 및 향후 연구

본 연구에서는 공공 클라우드에서 사용자의 안전한 기밀 데이터에 대한 공유기법에 대해 제안하였다. 이는 인터넷을 사용하여 접근하는 클라우드에서 사용자에게 데이터 제어권을 두고, CSP는 단지 데이터를 저장, 검색, 전달하는 프록시(Proxy) 서버역할을 하게하여 증가하는 데이터 공유와 협업을 위한 안전한 기밀 데이터 공유 기법이 될 것이다. 향후 연구로는 데이터 전송 모델을 발전시켜 보완하고 검증하여 효과적으로 수행하는 연구가 필요하다.

참고문헌

[1] 김진형, 김윤정, 박춘식, “클라우드 컴퓨팅에서 신뢰하지 않는 서버 데이터의 안전한 접근,” 정보과학회지, 28(12), pp.67-74, 2010

[2] 하병래, 이승아, 조기환, “보안에 적응적인 클라우드 컴퓨팅을 위한 사용자 인증 및 데이터 관리 방안,” 제4회 정보통신분야학회 합동 학술대회(JCICT) 논문집, pp. 158-161, 2010

[3] Amazon, “Extend Your IT Infrastructure with Amazon Virtual Private Cloud,” Whitepaper, 2010

[4] H. Sato, et. al., “A Cloud Trust Model in a Security Aware Cloud,” 2010 10th Annual International Symposium on Applications and the Internet, pp. 121-124, Jul. 2010

[5] Yi Lu, et. al., “Trust-Based Preserving for Peer to Peer Data Sharing,” CERIAS Tech Report 2006-70, 2006

[6] Lotfi Ben Othmane and Leszek Lilien, "Protecting Privacy in Sensitive Data Dissemination with Active Bundles," CONGRESS '09: Proceedings of the 2009 World Congress on Privacy, Security, Trust and the Management of e-Business, pp. 202-213, 2009