정 보 보 호 학 회 지
제24권 제6호, 2014. 12

클라우드 서비스 환경에서 데이터 보호를 위한 정보보호 고려사항

장 승 재*, 손 경 호**, 이 용 필***

요 약

클라우드 컴퓨팅은 IT자원을 소유하지 않고 대여하여 사용하는 컴퓨팅 환경으로써 가상화, 정보 위탁, 자원 공유, 단말의 다양성이라는 특징을 가지고 있다. 이러한 특징 때문에 다양한 보안위협들이 존재하며, 최근에는 아이클라우드 정보유출 사건과 같은 데이터 유출 사고도 일어나고 있다. 때문에 클라우드는 기존의 IT 환경과 마찬가지로 데이터 유출 및 손상을 방지하기 위해 노력하여야 된다. 본 논문에서는 클라우드 서비스에 중요 데이터를 다량 보관·활용하면서 발생할 수 있는 보안 위험과 클라우드 서비스 환경에서 제공될 수 있는 데이터 보안 기술들을 살펴보고, 이를 토대로 데이터 보호와 관련된 정보보호 고려사항을 제안하고자 한다.

Ⅰ. 서 론

최근 IT 관리 업무의 효율성 제고 및 비용 절감을 위하여 클라우드 서비스가 차지하는 비중이 점점 높아지고 있다. 클라우드 서비스 환경 하에서 업무 서비스는 기기 접근의 다양성, 서비스 다양성, 관리 비용 절감 등과 같은 다양한 이점을 지니고 있기에 정부에서도 IT 산업의 新 성장 동력으로 활성화에 주력하고 있으며, 국내외 민간 기업뿐만 아니라 정부에서도 클라우드 서비스 도입을 서두르고 있다.

클라우드 서비스를 도입하게 되면 인프라 투자에 대한 부담이 감소해 환경 변화에 민감하게 대응할 수 있으며, 글로벌 업무 협력을 통해 시너지 효과 창출이 가능하고, IT 자원 운용과 관련된 비 핵심 업무를 아웃소싱 함으로써 조직 핵심 역량을 배가시킬 수 있다. 또한, 사물 인터넷, 빅데이터 등 인터넷 기반 신규 서비스 창출과 IT환경 전반에 영향을 미치는 파급효과가 크다. 하지만 최근 아이클라우드 정보유출 사건과 같은 해킹에 의한 장애도 늘어나는 추세로 전통적인 IT 환경과 마찬가지로 클라우드 서비스 환경에서도 데이터 유출 및 손상은 심각하게 고려해야 하는 사항이다.

더욱이 다수의 소비자들이 IT 자원을 공유하고 다양한 무선 단말기의 원격 접속이 빈번한 클라우드 서비스 환경에서는 데이터의 기밀성, 무결성, 가용성을 위해 많은 투자와 개발이 요구되고 있다. 따라서 데이터 보안을 위해서는 데이터 생명주기(데이터 생성, 저장, 사용, 배포, 파기)에 따라 클라우드 서비스 제공자가 적절한 보안 대책을 마련하여야 한다.

본 논문에서는 클라우드 서비스에 중요 데이터를 다량 보관·활용하면서 발생할 수 있는 보안 위험과 클라우드 서비스 환경에서 제공될 수 있는 데이터 보안 기술들을 살펴보고, 이를 토대로 데이터 보호와 관련된 정보보호 고려사항을 제시하고자 한다. 논문의 구성은 2장에서 클라우드 서비스 환경에서 데이터와 관련된 위협을 소개하고, 3장에서는 클라우드 서비스 환경에서 데이터 보호 기술들을 설명하며 4장에서 설명한 데이터 보호 기술을 바탕으로 클라우드 서비스 환경에서 데이터 보호를 위한 정보보호 고려사항을 제시하고 5장에서 결론을 맺는다.

* 한국인터넷진흥원 (jsj81@kisa.or.kr)
** 한국인터넷진흥원 (khson@kisa.or.kr)
*** 한국인터넷진흥원 (pals@kisa.or.kr)

Ⅱ. 클라우드 서비스 환경에서 데이터와 관련된 위협

데이터 보호 관점에서 클라우드 서비스 환경이 기존 환경과 가장 큰 차이점은 데이터의 위탁, 가상화를 통한 자원 공유, 데이터를 처리 할 수 있는 단말기가 다양하다는 점이다. 이러한 차이점은 데이터 위탁에 따른 통제력 부족과 데이터 처리에 관한 투명성 부족으로 나타나고, 나아가 데이터 유출, 데이터 소실, 불안전한 데이터 삭제라는 위험으로 이어 질 수 있다.

2.1. 데이터 유출(Data Breaches)

클라우드 서비스는 기존의 서버 기반 환경보다 네트워크 접근이 용이하고 더 많은 데이터가 전송된다. 예를 들면, 분산된 클라우드 서비스 시스템에서 가상화 이미지를 동기화시키기 위해 반드시 데이터를 전송해야 하고, 이미지가 여러 대의 물리적 기기와 클라우드 서비스 인프라 등에 분산되기 때문에 상호 간의 데이터 전송 중 데이터 유출 위험이 발생한다. 또한 클라우드 서비스 제공자와 소비자 간 데이터 전송 중에도 데이터 유출 위험이 발생한다. 가능한 위협으로는 스니핑(Sniffing), 스푸핑(Spoofing), 중간자(MITM:Man-In‐The-Middle) 공격, 부채널(Side Channel) 및 재전송(Replay) 공격 등이 있다.

특히 퍼블릭 클라우드(Public Cloud)의 경우, 여러 고객들이 클라우드 서비스를 사용하기 때문에 특정 고객의 클라우드 서비스에 대한 공격이 이루어졌을 때 동일한 클라우드 서비스를 이용하는 다른 고객에게도 동일한 공격이 이루어질 가능성이 매우 높다. 클라우드 서비스의 데이터 저장과 관리는 이러한 관점의 고려가 이루어져야 하며, 이러한 문제를 해결하기 위해서는 고객이 이용하는 네트워크의 탐지 활동(포트 스캔 등)을 제한하여 클라우드 서비스 내부 네트워크의 도청을 방지하고, 암호화, 키 관리, 인증과 접근제어 등의 기술을 적절히 사용하여야 한다.

2.2. 데이터 소실(Data Loss)

클라우드 서비스의 장점은 언제, 어디서나 클라우드 서비스에 접속하면 원하는 데이터에 접근할 수 있다는 것이다. 특정 데이터는 여러 채널과 경로를 통해서 여러 사람이 동시에 접속할 수 있다. 이러한 편리함이 갖는 장점에도 불구하고, 데이터의 소실 위험 또한 증가한다. 데이터는 악의적인 공격자에 의해 소실될 수도 있지만 클라우드 서비스 제공자 내부 직원의 실수나 우발적인 삭제, 화재나 지진 등의 재해로 인해 발생할 수 도 있다.

만약 클라우드 서비스 제공자가 데이터 소실에 대한 적절한 조치를 취하지 않는다면 고객의 데이터는 영구적 손실로 이어질 수 있다. 데이터 소실을 막을 수 있는 방법으로는 데이터를 수정하거나 삭제할 수 있는 권한을 안전하게 관리하여야 하고, 수정과 삭제에 대해서는 이전 데이터를 반드시 백업해 두어야 한다.

2.3. 불완전한 데이터 삭제

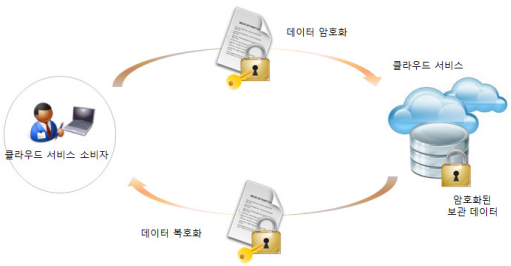
스토리지 및 백업 테이프 등의 물리적 매체에는 항상 여러 고객의 데이터가 기록되기 때문에, 특정 고객의 데이터만 지우기 위해 그 매체를 물리적으로 파괴 할 수 없다. 이는 클라우드 서비스 자원 삭제 요청이 들어와도 완전한 데이터 삭제로 이어지지 못할 수 있다. 따라서 클라우드 서비스 제공자는 고객이 삭제한 데이터에 대해서 완전히 지워줄 수 있는 기술을 도입해야 한다. 예를 들면, 데이터 저장소에 난수 등의 무의미한 데이터를 기록하여 데이터의 흔적을 지우는 방법이 있다.

Ⅲ. 데이터 보호 기술

클라우드 서비스의 발전과 함께 APT 공격과 같은 진화된 다양한 공격들이 증가함에 따라, 방화벽과 같은 경계 보안으로는 안전한 데이터 보안을 이룰 수 없다. 이와 같은 공격들을 예방하고 성공적인 데이터 보호를 위해서는 데이터를 중심으로 정밀한 감사 및 통제를 실시하여 잠재적인 공격을 막고, 지속적인 모니터링과 데이터 암호화를 통해 데이터를 보호하여야 한다.

3.1. 암호화

최근 APT 공격에 대응하기 위한 수단으로 데이터 암호화가 대두되고 있다. 해커는 여러 유형의 공격을 혼합해 오랜 기간 서버에 침투해 APT 공격을 수행하는데, 이를 통해 클라우드 서비스 시스템의 계정을 획득하고,



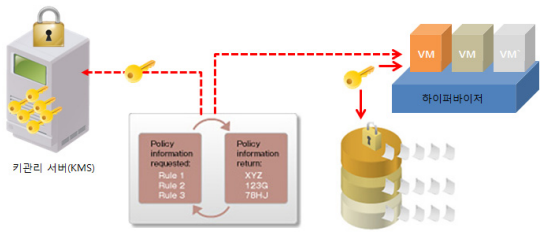
〔그림 1〕 클라우드 서비스 환경에서 데이터 암호화

데이터 파일을 작게 분할한 후 유출한다. 이러한 데이터 유출을 방지하기 위해서는 클라우드 서비스 내의 데이터를 암호화 하여 공격자가 데이터를 손에 넣었다 하더라도 암호 키 없이 내용을 열람할 수 없도록 막아야 한다.

3.2. 암호키 관리

암호 키 관리는 데이터와 별도 위치에서 관리하는 것이 바람직하다. 만약 암호화된 데이터와 이를 해독할 수 있는 암호 키를 동일한 장비에서 관리하는 경우, 해커가 계정을 획득하면 데이터와 암호 키를 동시에 확보 및 유출시킬 수 있게 되는 것이다. 따라서 암호 키는 데이터가 관리되는 장비와 다른 위치에 있는 보다 보안성이 강화된 환경에서 관리하여야 한다.

클라우드 서비스 환경에서 데이터 보호를 위해서는 데이터가 적재된 장비와 다른 키 관리만을 위한 별도의 전용 장비를 마련하고 중앙 집중화된 키 관리를 실현하여 안정성을 확보하여야 한다.



〔그림 2〕 클라우드 서비스 환경에서 키관리

3.3. 접근 제어

데이터 암호화를 하고 나면 암호화된 데이터에 대한 접근 제어 정책을 세워야 한다. APT 공격은 주로 권한을 가진 사용자의 계정 정보를 획득해 데이터를 저장하는 클라우드 서비스 서버에 접속한다. 이 때 사용자 계정 단위로 정책을 세우고 암호화 데이터에 대한 접근 제어 정책을 수립해 놓는다면, 비정상적인 접근을 방지할 수 있다. 또한 클라우드 서비스 인프라를 운영하는 시스템 관리자와 암호 키, 보안 정책을 담당하는 보안 관리자의 역할을 분리해야 한다. 일반적으로 시스템 관리자가 서버의 최상위 관리자 권한 계정을 갖고 인프라를 운영하는 경우가 많은데, 이럴 경우 내부의 악의적 의도 또는 외부 공격을 통해 관리자 계정이 유출되거나 데이터가 직접 새어나갈 수도 있으므로, 별도의 보안 관리자를 임명해 암호 키와 정책을 따로 운영하도록 구분하는 것이 바람직하다.

3.4. 데이터 백업

클라우드 서비스는 중요 시스템들이 중앙에 집중되어 장애발생 시 모든 업무가 마비될 수 있으므로, 고객 데이터, 서버 접근 로드 등의 저장·관리를 이중화하고, 클라우드 서비스의 가용성을 보장하기 위해 백업체계를 구축해야 한다. 또한 백업·비상복구·변경관리·침해사고 대응 등 클라우드 서비스 시스템 운영의 전반적인 절차에 관한 표준 운용절차를 수립하여야 한다.

3.5. 감사

데이터 보호는 기술 도입만으로 끝나는 것이 아니며, 세심하고 꾸준한 관리가 필요하다. 이를 위해서 데이터 보호 상태를 확인할 수 있는 감사를 수행하여야 한다. 감사 범위는 데이터 보안의 정상 유무를 확인하는 것은 물론, 불법적인 접근 시도가 있었는지에 대한 확인도 포함한다. 또한, 향후 데이터 유출 사고가 발생할 수 있을 것에 대비해, 사건 발생 시 히스토리를 추적할 수 있도록 로그를 항상 관리하여야 한다.

Ⅳ. 클라우드 환경에서 데이터 보호를 위한 정보보호 고려사항

개인정보보호법 발효 이후, 국내 데이터 보안은 데이터베이스 암호화에 초점이 맞춰져 있었다. 하지만 클라우드 서비스 환경이 보편화되고 클라우드 서비스 보안 기술이 발전하면서 기존의 정형화된 데이터를 저장하는 데이터베이스뿐만 아니라 클라우드 서비스 환경 내에

다양한 형식의 데이터를 보호하기 위한 조치가 필요하게 되었다. 이번 장에서는 클라우드 환경에서 데이터 보호를 위한 기술적·관리적 고려사항을 제안하고자 한다.

4.1. 데이터 암호화와 관련된 정보보호 고려사항

클라우드 서비스 환경에서 데이터의 기밀성과 무결성 유지를 위해서는 반드시 암호화가 필요하고, 데이터 암호화는 저장 중, 전송 중, 처리 중 등 모든 경우에 적용되어야 한다. 암호화 방법은 매우 복합적인 요소들을 고려해야 하므로, 클라우드 서비스 제공자는 적절한 암호화 전략 및 정책을 수립을 위해 다음과 같은 사항을 고려해야 한다.

- 암호 대상 : 취급 정보 민감도 및 중요도에 따라 정의
- 암호화 대상별 암호화 방식과 알고리즘 강도 정의
- 암호 키 관리 대책
- 정보 전송 및 저장 시 암호화 방안
- 암호화 관련 시스템 운영 담당자 역할 및 책임 정의
- 암호화 관련 법적 요구사항 반영 (개인정보보호 관련 법률 등)

또한 클라우드 서비스 소비자가 암호화와 관련하여 클라우드 서비스 제공자에게서 이루어지는 작업과 자체적으로 고려해야 할 사안을 파악하려면, 클라우드 서비스 제공자가 암호화 메커니즘 및 사용된 방법에 대한 개요를 클라우드 서비스 소비자에게 제공하는 것이 좋다.

4.1.1. 저장 데이터 암호화

클라우드 서비스에서는 클라우드 서비스 소비자의 대용량 정보, 기업의 중요한 기밀정보 등을 다른 클라우드 서비스 소비자와 공동으로 사용하는 스토리지에 저장하기 때문에, 서비스 이용과 관련해 클라우드 서비스 소비자 데이터의 안전한 관리가 선행되어야 한다. 특히, 시스템 설정 파일, 시스템 구성 및 관리 문서, 개인 정보 및 계정 정보는 서비스 이용에 필수적인 클라우드 서비스 소비자 데이터로서, 반드시 암호화하여 저장하고 관리해야 한다. 저장 데이터는 정보보호를 위해 다음과 같은 사항을 고려해야 한다.

- 중요정보에 대해서는 안전성이 입증된 알고리즘과 키 길이를 사용하여 암호화해야 한다.
- 저장된 데이터에 대한 액세스는 알 필요(Need-to-Know) 원칙과 최소 권한을 기반으로 부여해야 한다.
- 분류된/암호화된 데이터에 대한 모든 액세스는 구축된 접근 제어 정책을 준수해야 한다.
- 절차적 접근 제어에는 추가적으로 암호화 시스템은 기본 무결성 점검 기능을 지원해야 한다.
- 전체 암호화 시스템의 무결성을 손상시키지 않고, 암호화된 데이터(단방향 해시 암호)를 비교할 수 있어야 한다.
- 데이터가 안전하게 클라우드 서비스 제공자에 전송되고 저장되어야 한다.

4.1.2. 송·수신 데이터 암호화

송·수신 데이터는 하나의 데이터 저장소에서 다른 저장소로 전송 중인 데이터, 서버나 어플리케이션, 데이터베이스에서 네트워크로 보내는 데이터를 의미한다. 전송 중인 데이터는 데이터 유출의 위험이 있기 때문에, 암호화 전송이 반드시 필요하다. 송·수신 데이터는 정보보호를 위해 다음과 같은 사항을 고려해야 한다.

- 유선, 무선 또는 기타 다른 전송 매체로 송·수신 중인 모든 중요한 데이터를 보호해야 한다.
- 기밀인 데이터가 암호화되지 않고 전송되는 경우 IPSec 또는 SSL/TLS 같은 보안 네트워크 통신 프로토콜을 사용해야 한다. 특히, 공유 네트워크나 공공 네트워크로 데이터를 전송할 때에는 반드시 보안 통신 프로토콜을 사용해야 한다.

4.1.3. 사용 중인 데이터 암호화

사용 중인 데이터는 클라우드 서비스 제공자 측에서 처리하는 데이터를 의미한다. 사용 중인 데이터 보호를 위해 다음과 같은 사항을 고려해야 한다.

- 클라우드 서비스 제공자는 고객별로 데이터를 논리적으로 분리하여야 하고 필요하다면 물리적으로도 분리해야 한다. 또한 키는 고객이 저장하고 간수해

야 한다.
- 데이터를 클라우드 저장소에서 제거하면 클라우드 서비스 제공자는 데이터가 적절히 삭제되었는지 확인해야 하며, 클라우드 서비스 제공자가 소유하거나 관리하는 모든 암호화 키가 표준과 지침에 따라 제거되었는지 확인해야 한다.
- 고객이 원할 경우 클라우드 서비스 제공자는 데이터를 보호할 수 있는 형식으로 암호화해야 한다.

4.2. 키 관리와 관련된 정보보호 고려사항

클라우드 서비스 환경에서는 암호화 키 관리가 복잡하기 때문에 클라우드 서비스 제공자는 데이터를 암호화 할 경우, 키 생명주기(키 생성, 저장, 사용, 배포, 파기)에 따라 각 단계마다 적절한 보안 조치를 실행하여야 한다. 안전한 키 관리를 위해서 필요한 정보보호 고려사항은 다음과 같다.

- 암호 키 생성, 이용, 보관, 배포, 파기에 대한 정책 및 절차를 수립하고 이행하여야 한다.
- 생성된 암호 키는 암호 키 손상 시 시스템 또는 암호화된 정보의 복구를 위하여 별도의 매체에 저장 후 안전한 장소에 보관하여야 한다.
- 암호 키의 사용기간은 최대 2년 유효기간은 최대 5년을 권고하고 있으나, 암호키 변경 시 비용과 기업의 정보자산 및 업무 중요도를 고려하여 자체적으로 정하여 적용한다.
  ※ 단, 암호 키 유출, 암호시스템 해킹이 의심되는 경우, 즉시 암호 키를 변경하여야 한다.

4.3. 접근 제어와 관련된 정보보호 고려사항

다수의 클라우드 서비스 소비자들이 IT 자원을 공유하고 다양한 무선 단말기의 원격 접속이 빈번한 클라우드 서비스 환경에서는 기존 IT 서비스 환경보다 보안성이 강화된 접근 제어가 필요하다. 따라서 클라우드 서비스 제공자는 IT 자원에 접근이 허가된 클라우드 서비스 소비자만이 서비스에 접속할 수 있도록 보장해야 되며, 제한된 영역에 대한 접근 시도와 같은 부적절한 행위에 대한 보안관제의 메커니즘을 마련하여야 한다. 접근 제어를 위한 정보보호 고려사항에 다음과 같다.

[원격접속 관리 및 제한]
- 서비스 연결을 승인하기 전에 모든 단말기의 무선 접속은 정책에서 규정된 절차에 따라 인증하고, 접속로그를 관리하며 모니터링을 해야 한다.
- 무선 접속을 인증과 통신 세션의 기밀성·무결성을 보장하기 위해 암호 기술을 적용해야 한다.
- 내부정책에서 제한하는 모바일 단말기의 통제 대책을 마련해야 한다.

[계정 분할 및 권한 최소화]
- 서로 다른 이용자 계정의 충돌을 최소화하기 위하여 접근을 허용하는 영역이나 권한 등을 분리해야 한다.
- 이용자의 신분 및 지불 방식을 기술적으로 검증하는 방안을 적용해야 한다.
- 사용자에 부여하는 역할·권한을 최소한의 범위로 제한해야 한다.
- 내부정책에서 규정한 계정관리 주기에 따라 점검하고, 시스템 이용자 변경 사항은 즉시 정책에 반영해야 한다.
- 이용자의 잘못된 로그인 시도가 규정된 횟수만큼 발생할 경우, 로그인을 제한해야 한다.
- 이용자 로그인이 성공적으로 수행되었을 경우, 지난 로그인 일시 및 관련 정보 공지를 고려해야 한다.

[사용자 세션 관리]
- 서비스상의 최대 세션 수, 계정 지역, 유형 등을 고려하여 세션을 정의하여 관리해야 한다.
- 하나의 사용자가 동시에 여러 세션을 소유하는 것을 제한해야 한다.
- 내부정책에서 규정한 활성화 허용 시간을 초과한 세션은 비활성화 된 세션으로 전환해야 한다.
- 사용자 인증을 통해 활성화 된 세션이라도 이용자가 어떠한 요청도 하지 않은 채 활성화 허용시간을 초과하면 세션을 비활성화해야 한다.

4.4. 데이터 백업과 관련된 정보보호 고려사항

클라우드 서비스에서 가용성을 제공한다는 의미는 적시에 신뢰 가능한 데이터 접근 권한을 확보한다는 뜻이다. 클라우드 서비스의 가용성을 위협하는 요인으로

는 분산 서비스 거부(DDoS) 공격과 같은 악의적인 행위에 의한 서버 성능 손실이나, 클라우드 서비스 시스템의 하드웨어 고장 등과 같은 인프라 문제가 있다. 이러한 문제를 해결하기 위해서 클라우드 서비스 제공자는 여분의 네트워크 및 스토리지 확보 및 백업 메커니즘 등 장애 위험을 대처하기 위한 조치를 취하여야 한다. 데이터 백업과 관련된 정보보호 고려사항은 다음과 같다.

- 백업 정책에 따라 고객 데이터를 주기적으로 백업해야 한다.
- 고객 데이터 백업을 위한 별도의 백업 장비 구축, 장비 이중화 등 백업 방안을 마련해야 한다.
- 백업 장치 신뢰성과 데이터 무결성 검증을 위해 백업 시스템을 정해진 주기에 따라 확인하고 테스트해야 한다.
- 클라우드 서비스 제공자는 데이터에 대한 신뢰성, 비밀성, 가용성이 보장 되도록 데이터를 보관하여야 하고, 보관 데이터가 손상될 경우를 대비하여 데이터의 백업 및 복구 체계를 갖추도록 백업 준수율 99.0%를 유지해야 한다.

$$\text{백업준수율}(\%) = \frac{\text{백업실시건수}}{\text{백업계획건수}} \times 100$$

클라우드 서비스 제공자는 데이터의 중요 정도에 따라 데이터 백업주기를 정기 백업과 수시 백업으로, 백업 방법을 전체 백업과 부분 백업으로 분류하고, 백업 정보 보관 기간은 월/년 단위로 제공하여야 한다. 또한 가상화로 구현된 인프라 관련 데이터 경우 기존의 방법으로 백업이 불가능하기 때문에, 가상 이미지를 스냅샷 기반으로 백업하는 방법과 같은 대체 방안을 마련하여야 한다. 이와 더불어 내부 백업 정책에 따라 이용자 데이터의 백업을 수행하고, 주기적으로 백업 시스템을 테스트하고 점검해야 한다.

Ⅴ. 결 론

클라우드 서비스는 비용절감 측면과 유연성, 이동성의 장점으로 인하여 전 세계적으로 수요가 급증하고 있으며, 국내도 정부의 클라우드 활성화 계획을 통해 더욱 확산될 것으로 예상된다. 하지만 클라우드 보안문제들은 클라우드 산업 활성화에 제약으로 작용하고 있으며, 특히 자신의 정보가 업체에 위탁·관리되는 것에 대한 불안감은 클라우드 이용을 주저하게 되는 주된 이유이다.

따라서 본 논문에서는 클라우드 서비스에 중요 데이터를 다량 보관·활용하면서 발생할 수 있는 보안 위험과 클라우드 서비스 환경에서 제공될 수 있는 데이터 보안 기술들을 살펴보고, 이를 토대로 데이터 보호와 관련된 정보보호 고려사항을 제시하였다. 그러나 기본적으로 클라우드 서비스 제공자가 안전한 클라우드 서비스 제공하는 것도 중요하지만 데이터의 소유자 즉 클라우드 서비스 이용자가 정보를 위탁할 지라도 데이터를 중요도에 따라 분류하고 적절한 보안 조치 확인하는 등은 데이터 보호를 위한 지속적인 관심과 노력이 필요할 것이다.

참 고 문 헌

[1] Cloud Security Alliance, “The Notorious Nine Cloud Computing Top Threats in 2013”, Jan. 2013.

[2] Cloud Security Alliance, “SecaaS Category 2, Data Loss Prevention Implement Guidance”, Oct. 2012.

[3] Cloud Security Alliance, “SecaaS Category 8, Encryption Implement Guidance”, Oct. 2012.

[4] Dawn Song 外, “Cloud Data Protection for the Masses”, *IEEE Computer Society*, Jan. 2012.

[5] Federal Office for Information Security, “Security Recommendations for Cloud Computing Providers”, Jun. 2011.

[6] Information Commissioner’s Office,“Guidance on the use of cloud computing”, Oct. 2012.

[7] 은성경 外, “클라우드 서비스 보안 기술”, ETRI, 2009

[8] 방송통신위원회, “클라우드 서비스를 위한 SLA 가이드”, Oct. 2011.

[9] 한국인터넷진흥원, “클라우드 서비스 정보보호 안내서”, Oct. 2011.

〈저 자 소 개〉

장 승 재 (Seung Jae Jang)
비회원

2009년 2월 : 숭실대학교 컴퓨터학부 졸업
2011년 2월 : 숭실대학교 컴퓨터학과 석사
2011년 3월~현재 : 숭실대학교 컴퓨터학과 박사 수료
2012년 11월~현재 : 한국인터넷진흥원 정보보호산업기획팀
관심분야 : 네트워크 보안, 클라우드·빅데이터 보안

손 경 호 (Kyung Ho Son)
정회원

2001년 2월 : 성균관대학교 전기전자컴퓨터공학과 학사
2004년 2월~현재 : 성균관대학교 컴퓨터공학과 석·박사과정 수료
2001년 1월~현재 : 한국인터넷진흥원 정보보호산업기획팀
관심분야 : 침해사고대응기술, 융합보안, 네트워크보안, 보안 시험·평가, 클라우드·빅데이터 보안

이 용 필 (Yong Pil Lee)
정회원

1995년 : 서울대학교 경제학과
2003년 : 서울대학교 행정대학원 석사
2004년~2008년 : 서울대학교 행정대학원 박사수료
2003년 3월~현재 : 한국인터넷진흥원 정보보호산업기획팀장
관심분야 : 정보보호 정책, 기업 정보보호, IoT 보안