DBpia

모바일 클라우드 환경에서 안전한 프록시 재암호화 기반의 데이터 관리 방식

정회원 송 유 진*, 도 정 민**

Secure Data Management based on Proxy Re-Encryption in Mobile Cloud Environment

You-jin Song*, Jeong-min Do** *Regular Members*

요 약

최근 모바일 클라우드 환경에서 공유되는 데이터의 기밀성과 유연성있는 접근제어를 보장하기 위해서 KP-ABE(Key Policy-Attribute Based Encryption)와 PRE(Proxy Re-Encryption)를 활용한 시스템 모델이 제안되었다. 그러나 기존 방식은 철회된 사용자와 클라우드 서버간의 공모 공격으로 데이터 기밀성을 침해하게 된다. 이러한 문제를 해결하기 위해서 제안 방식은 클라우드 서버에 저장되는 데이터 파일(data file)을 분산 저장하여 데이터 기밀성을 보장하고 비밀분산(Secret Sharing)를 통해서 프록시 재암호화키에 대한 변조 공격을 방지한다. 그리고 제안방식을 의료 환경에 적용한 프로토콜 모델을 구성한다.

Key Words : Key Policy-Attribute Based Encryption, Proxy Re-Encryption, Data Confidentiality, Collusion Attack, Access Control

ABSTRACT

To ensure data confidentiality and fine-grained access control in business environment, system model using KP-ABE(Key Policy-Attribute Based Encryption) and PRE(Proxy Re-Encryption) has been proposed recently. However, in previous study, data confidentiality has been effected by decryption right concentrated on cloud server. Also, Yu's work does not consider a access privilege management, so existing work become dangerous to collusion attack between malicious user and cloud server. To resolve this problem, we propose secure system model against collusion attack through dividing data file into header which is sent to privilege manager group and body which is sent to cloud server and prevent modification attack for proxy re-encryption key using d Secret Sharing, We construct protocol model in medical environment.

Ⅰ. 서 론

인터넷을 통해서 컴퓨팅 자원을 서비스로 제공하는 클라우드 컴퓨팅은 학계와 산업계에서 주목하고 있는 새로운 컴퓨팅 패러다임이다[1-3]. 이러한 클라우드 컴퓨팅 서비스가 모바일 비즈니스 영역으로의 확대가 예상된다. 최근 무선기기의 기능 향상과 네트워크의 발전에 힘입어 스마트폰 등의 모바일 기기를 기반으로 하는 클라우드 컴퓨팅 서비스인 모바일 클라우드라는 새로운 서비스 트랜드가 등장하고 있다.

연구조사기관의 보고에 따르면 향후 2014년까지

※ 이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임. (No. 2011-0027333)
* 동국대학교 정보경영학과 (song@dongguk.ac.kr), ** 동국대학교 일반대학원 전자상거래협동과정
논문번호 : KICS2011-09-431, 접수일자 : 2011년 9월 30일, 최종논문접수일자 : 2012년 4월 4일

www.dbpia.co.kr

클라우드 컴퓨팅 기술이 주로 모바일 서비스에 활용될 것이라고 전망했다[4]. 모바일 클라우드는 클라우드 컴퓨팅 기술과 모바일 서비스의 결합이다. 즉, 모바일 클라우드 서비스는 이동성을 갖는 모든 기기들(스마트폰, 노트북, PDA 등)을 통해서 클라우드 서비스를 이용한다. 그 예로써 수널(Soonr)에서 제공하는 모바일 오피스 서비스가 있다. 수널은 별도의 오피스 프로그램없이 파워포인트 파일 등과 같은 오피스 파일을 아이폰에서 열람, 백업, 인쇄 기능을 수행할 수 있는 모바일 오피스 서비스를 제공한다. 서비스 이용자가 이동 단말에 모바일 클라우드 어플리케이션을 설치하면 리모트 유저인터페이스 기술을 통해서 클라우드 서버에서 실행된 결과를 확인할 수 있다.

현재 상용화된 모바일 클라우드 서비스는 단순한 데이터 열람, 백업, 동기화 등과 같은 서비스를 제공하지만 앞으로는 언제 어디서든 인터넷에만 접속하면 클라우드 사업자로부터 무엇이든 서비스로 제공(Anything as a Service)받을 수 있는 컴퓨팅 환경이 조성될 것이다[5]. 의료 환경을 예로 들면 의사는 병원에서만이 아니라 근무지 외에서도 즉, 장소에 국한되지 않고 언제 어디서든 환자를 위한 진료 행위를 할 수 있는 서비스를 제공받을 수 있다. 자신의 모바일 기기로 특정 환자의 진료 기록을 검색하고 열람하는 것은 물론이고, 별도의 툴을 설치하지 않더라도 환자의 진료기록으로 특정 질환에 대한 이상징후를 감지하는 분석 서비스를 제공받을 수 있다. 또한, 모바일 클라우드 서비스는 컴퓨팅 자원을 사용한 만큼 과금하는 방식(Pay as you go)과 컴퓨팅 자원을 유연하고 신속하게 할당할 수 있는 능력(Self-provisioning resources) 등 클라우드 컴퓨팅의 특성을 그대로 보유하고 있다[6]. 컴퓨팅 자원을 물리적으로 소유하는 것보다 서비스로 공유, 활용하는 것이 유지, 보수 등 사후관리 비용 측면에서 효율적이기 때문에 의료 환경뿐만 아니라 다양한 어플리케이션 영역에서 제공될 것으로 예측된다.

그러나 이러한 유용한 특성에도 불구하고 모바일 클라우드 컴퓨팅을 기존의 비즈니스 환경에 도입하여 활용하기 위해서는 프라이버시 침해 등의 여러 가지 리스크를 고려해야 한다[7]. 특히, 의료데이터는 개인의 프라이버시를 침해할 수 있는 민감한 정보를 다루고 있으므로 데이터의 기밀성을 유지하는 것이 중요하다. 본 논문에서는 CSA에서 분류한 클라우드 컴퓨팅 7대 보안 위협 중 데이터 손실 및 유출, 즉 클라우드 서버에 저장되는 데이터의 기밀성 문제에 초점을 맞추어 모바일 클라우드 컴퓨팅 환경에 적합한 시스템 모델, 즉 프라이버시를 보호하면서 의료데이터를 처리하는 모바일 헬스 클라우드 모델을 구성한다[7].

한편, 데이터의 기밀성뿐만 아니라 정보의 열람 시 사용자 속성에 따른 유연성 있는 접근제어(fine-grained access control), 예를 들어 사장과 부장, 과장 등의 직책과 같은 각 사용자 속성에 따른 데이터 접근권한이 차별화되어야 한다. 또한, 특정 사용자의 데이터 열람권한을 철회하는 기능이 있어야 한다. 예를 들면, 어떤 사용자가 2010년 12월 1일에 서비스 이용 라이센스가 만료되는 경우, 철회 대상인 사용자를 시스템상에서 효율적으로 제거할 수 있는 방법이 필요하다. 이러한 방법을 제시하기 위해서 [8]에서는 KP-ABE(Key Policy-Attribute Based Encryption)를 활용하여 데이터 기밀성과 유연성있는 접근제어를 보장하고, PRE(Proxy Re-Encryption)를 통해서 클라우드 서버에 업무를 위임하는 방식을 구체화하여 다수의 사용자 이용에 따른 키 생성 등의 계산상 과부하 문제를 해결하고 있다. 또한, 시스템상의 특정 사용자를 철회할 수 있는 방법도 제시하고 있다.

그러나 [8]의 방식은 철회된 사용자와 클라우드 서버간의 공모를 통한 불법 데이터 접근(예를 들면, 라이센스가 만료된 사용자의 데이터 열람)이 가능하다. 또한, 정당한 사용자에 대한 접근권한을 판별하여 승인하는 절차인 권한 관리(privilege management) 기능이 결여되어 있기 때문에 정보 공유 및 활용을 위한 사용자 권한관리 문제가 있다.

이러한 과제를 해결하기 위해서 본 논문에서는 클라우드 서버에 저장되는 데이터 파일의 헤더와 바디의 분리를 통해서 데이터의 기밀성을 보장한다. 기존의 방식에서 클라우드 서버에 암호문, 암호화된 키(헤더와 바디) 등 복호와 관련된 권한이 집중되어 있었다면 제안방식은 권한 관리자 그룹이라는 신뢰할 수 있는 기관을 두어 키(헤더)를 관리하고 클라우드 서버는 암호문(바디)만을 보관하여 권한을 분산한다. 그리고 비밀분산(Secret Sharing)을 도입하여 모바일 클라우드 컴퓨팅 환경에 적합한 데이터 접근권한 관리 모델을 제안한다. 특히, 비밀분산은 데이터 소유자가 데이터 복원을 위한 쉐어의 갯수인 임계값 k를 결정할 수 있는데 민감도(개인의 프라이버시를 침해할 수 있는 정보의 수위)가 높은 데이터일수록 높은 임계값을 설정하여 데이터를 보호할 수 있다. 마지막으로 제안 모델의 응용으로서 프

www.dbpia.co.kr

라이버시를 보호하면서 의료데이터를 처리하는 모바일 헬스 클라우드에 대한 시나리오를 제시한 후 공모 공격과 변조 공격에 대한 안전성을 분석한다.

Ⅱ. 관련 연구

2.1. 모바일 클라우드 컴퓨팅

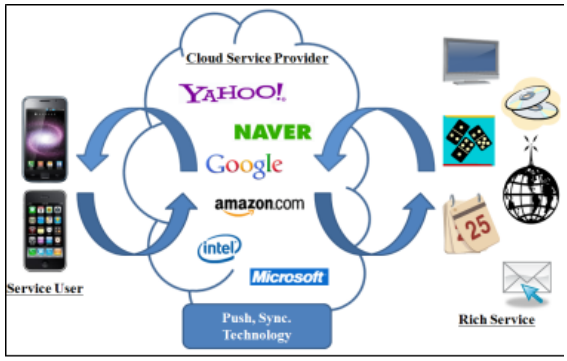

그림 1. 모바일 클라우드의 구성도
Fig. 1. Configuration of Mobile Cloud

모바일 클라우드는 클라우드 컴퓨팅 기술과 모바일 서비스의 결합이며 모바일 클라우드 서비스는 이동성을 갖는 모든 기기들(스마트폰, 노트북, PDA 등)을 통해서 클라우드 서비스를 이용한다. 모바일 클라우드 컴퓨팅은 이러한 모바일 클라우드 내에서 서비스를 제공하는 과정이다. 모바일 클라우드에는 크게 미디어 제공을 위한 데이터 스토리지 서버와 서비스를 처리하는 데이터 프로세싱 서버로 구성된다. 즉, 모바일 클라우드 컴퓨팅은 서비스 이용자에게 이동 단말을 통해 원하는 서비스를 제공하는 역할을 담당한다. 예를 들면 이동 단말에 별도의 툴을 설치하지 않고 클라우드 서버의 지원을 받아서 데이터 가공, 분석 등의 서비스를 제공받는 것이 이에 해당된다[9].

2.2. 속성기반 암호화

2.2.1. 쌍선형 사상(Bilinear Mapping)

2개의 순환군(Cyclic Group) G_1, G_2에 대해 쌍선형 사상 $\hat{e}: G_1 \times G_2 \rightarrow G_T$($G_T$는 쌍선형 사상의 출력 공간)는 다음의 성질을 갖는다.

① 쌍선형성(Bilinear) : 모든 $u \in G_1$, $v \in G_2$ 및 모든 a, $b \in Z$에 대해 $e(u^a, v^b) = e(u, v)^{ab}$가 성립된다.

② 비퇴화성(Non-degenerate) : 모든 $u \in G_1$, $v \in G_2$에 대해 $e(u, v) \neq 1$이다.

③ 계산가능성(Computable) : 모든 $u \in G_1$, $v \in G_2$에 대해서 $e(u, v)$를 계산하는 효율적인 알고리즘이 존재한다.

2.2.2. 속성기반 암호화의 개요

속성기반 암호화(Attribute Based Encryption)는 접근구조(Access Structure)가 비밀키나 암호문 중 어느 것과 관련되는가에 따라 KP-ABE(Key Policy-Attribute Based Encryption)[10]와 CP-ABE(Ciphertext Policy-Attribute Based Encryption)[11]로 구분된다. 본 논문에서는 KP-ABE를 다루고 있으므로 CP-ABE에 대한 설명은 생략한다. KP-ABE에서 사용자의 비밀키는 접근구조와 관련되며 암호문은 속성집합과 관련된다. 즉, 암호문 내의 속성집합이 사용자 비밀키의 특정 복호정책을 만족하면 암호문이 복호되는 구조이다. 이러한 복호구조는 그림 2의 접근구조로서 설명될 수 있다.

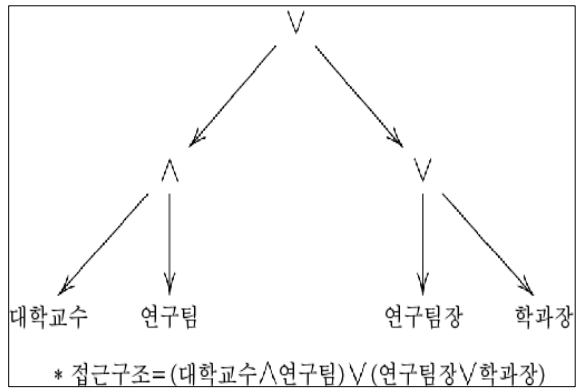

그림 2. 접근구조
Fig. 2. Access Structure

그림 2는 (대학교수, 연구팀, 연구팀장, 학과장) 속성으로 구성된 접근구조 (=((대학교수∧연구팀)∨(연구팀장∨학과장))) 이며 '∧', '∨'는 각각 AND, OR 게이트이다. 복호정책은 (대학교수이고 연구팀 또는 연구팀장이나 학과장)이다. 예를 들어 의과대학에서 신종플루에 대한 연구를 수행한다고 가정한다. 연구데이터는 속성집합 ({연구팀, 학과장})으로 암호화되어 있고 비밀키는 그림 2의 접근구조와 관련되어 있다. 연구자가 그동안 연구해 왔던 데이터에 대한 접근을 원한다면 암호문은 대학교수이고 연구팀이라는 AND 게이트는 만족하지 못하지만 학과장이라는 OR 게이트를 만족하므로 데이터에 접근가능하다.

제안 방식은 [10]의 방식을 그대로 이용한다. [10]에

www.dbpia.co.kr

서 제안한 속성기반 암호화는 Setup, Encryption, Key Generation, Decryption, 총 4개의 알고리즘으로 구성되어 있고 간단하게 각 알고리즘의 작동 원리를 설명하면 Setup 알고리즘에서 보안 파라메터 k로 PK와 MK를 출력한다. Encryption 알고리즘에서 평문 M을 속성집합 I로 암호화한 E를 출력한다. Key Generation 알고리즘에서 속성집합 I의 구성요소를 leaf node로 가지는 접근구조 T와 관련된 비밀키 SK를 생성한다. Decryption 알고리즘에서 비밀키 SK로 암호문 E를 복호하여 M을 도출한다.

2.3. 프록시 재암호화

프록시 재암호화 기법은 프록시 서버가 평문에 대한 어떠한 정보의 습득없이 A의 암호문을 B가 복호 가능하도록 재암호화하는 방식이다. 즉, A는 B에게 자신의 암호문에 대한 복호 권한을 위임하는 재암호화키(Re-encryption key)를 생성한 후, 프록시 서버에 송신한다. 그러면 프록시 서버는 재암호화키를 통해서 A의 암호문을 B의 비밀키로 복호 가능한 암호문으로 변환하여 B에게 전달한다. 그러면 B는 자신의 비밀키로 암호문을 복호한다.

제안 방식은 [12]에서 제안된 atomic proxy cryptography(이하 BBS 방식)으로 구성된다. BBS는 A의 암호문을 B의 암호문으로 변환하는 방식이다. 데이터 소유자의 키 생성 등에 대한 계산상 과부하를 줄이기 위해서 BBS 방식을 활용하여 클라우드 사업자에게 업무를 위임한다.

모바일 클라우드 컴퓨팅 환경에서 프록시 서버는 클라우드 서버의 일부기능을 담당하는 것으로 간주하여 클라우드 사업자가 저장하고 있는 데이터 접근권한을 유연성있게(fine-grained) 관리하는 방법에 대해 제시한다.

2.4. 비밀분산

비밀분산(Secret Sharing) 방식은 모든 쉐어가 모여야 평문이 복원되는 (n, n)방식과 임계치 k개만큼의 쉐어만 있으면 복원 가능한 (k, n)방식이 있다. (n, n)방식은 쉐어의 변조 및 소실 등으로 인한 복원 불가능 문제가 발생하지만 (k, n)방식은 쉐어의 변조 및 소실에 영향을 받지 않는다.

제안 방식에서는 권한 관리자 그룹(Privilege Manager Group)이 사용자의 데이터 열람권한을 판별하여 승인하는 절차를 구현하기 위해서 비밀분산을 활용한다. 즉, 프록시 재암호화키를 (k, n)방식으로 여러 개의 쉐어로 분할한 후 사용자의 데이터 열람권한을 판별하여 정당하다면 k개의 쉐어로 프록시 재암호화키를 재구성하고 정당하지 않다면 연산을 중지한다. 또한, 모든 쉐어가 있어야 평문이 복원되는 (n, n)방식이 아닌 n개의 쉐어 중 k개만 있으면 평문을 복원 가능한 (k, n)방식을 활용하여 복원에 필요한 쉐어 정보량에 따라 복원 가능성이 결정될 수 있도록 한다.

비밀분산의 활용에 대해 구체적으로 설명하면 프록시 재암호화키 $rk_{i\leftrightarrow i'} \leftarrow t_i'/t_i = R$을 (k, n) 방식으로 분할하여 각 쉐어 $R_l(1 \le l \le n)$을 권한 관리자 그룹에게 전송한다. 권한 관리자 그룹은 피위임자가 데이터를 열람하고자 할 때 사용자의 권한이 정당하다면 프록시 재암호화키 쉐어 R_l를 k개만큼 모아서 R을 재구성한다. 데이터의 민감도가 높을수록 임계값 k를 높게 설정하여 데이터가 복원되려면 더 많은 권한 관리자의 동의가 필요하게 되는 승인절차를 실현할 수 있다.

2.5. Yu 등의 기법

[8]에서는 기존의 비즈니스 환경이 클라우드 컴퓨팅 환경으로 이동해갈 것이라고 전망하고 이러한 환경에서 데이터의 기밀성을 보장할 수 있는 시스템 모델을 제안하고 있다. 클라우드 컴퓨팅 환경에서의 데이터 기밀성 문제는 클라우드 사업자가 믿을만하지 못하다는 것에서 시작된다. 각 분야와 관련된 문서들을 평문으로 수신하고 전송하게 되면 신속하고 편리하겠지만 믿을 수 없는 클라우드 사업자를 통해서 전송된다면 데이터의 기밀성이 침해된다. 이에 대해서 데이터를 속성집합으로 암호화하고 데이터의 속성집합에 만족하는 접근구조와 관련된 비밀키를 소지하고 있으면 데이터를 열람할 수 있는 KP-ABE의 컨셉을 활용한다. 즉, 비밀키 DEK(Data Encryption Key)로 데이터를 암호화하여 바디(body)를 구성하고 속성집합으로 DEK를 암호화하여 헤더(header)를 구성한다. 이러한 헤더와 바디를 결합하여 데이터 파일(data file)을 구성하여 클라우드 사업자에게 전송한다. 사용자 그룹이 데이터에 접근하고자 할 때 소지하고 있는 비밀키가 헤더의 속성집합에 만족하면 DEK를 얻고 바디의 데이터를 열람할 수 있다.

www.dbpia.co.kr

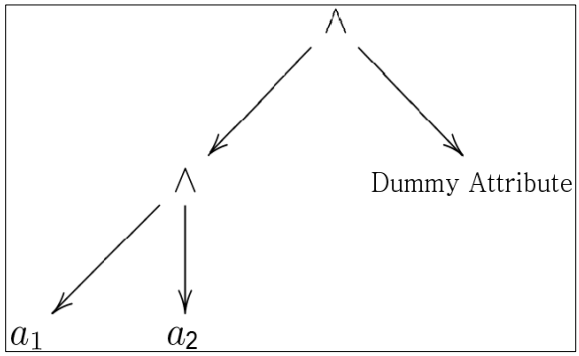

그림 3. Yu 등의 기법의 접근구조
Fig. 3. Access Structure of Yu. et. al Scheme

[8]의 방식은 데이터 소유자가 시스템 속성 집합의 정의, 시스템과 관련된 키 생성 및 설정을 하고 데이터의 암호화, 데이터를 암호화한 비밀키를 속성기반 암호화로 암호화하여 클라우드 사업자에게 전송하면 암호화된 키와 암호문의 관리는 전적으로 클라우드 사업자가 시행한다. 즉, 데이터 소유자는 온라인 상태가 아니여도 상관없다. 하지만 [8]의 방식은 철회된 사용자와 클라우드 사업자간의 공모를 통해서 데이터의 기밀성을 침해할 수 있다. [8]의 방식에서 시스템 상의 사용자를 효율적으로 철회하기 위해서 프록시 재암호화를 활용하여 속성의 버전을 업데이트하면서 사용자가 동일한 버전의 속성을 소지하고 있지 않으면 연산이 불가능하게 하고 있다. 이러한 기능을 클라우드 사업자가 수행하기 위해서 데이터 소유자는 접근구조를 그림 3과 같이 Dummy Attribute가 포함된 접근구조를 생성하여 클라우드 사업자에게는 Dummy Attribute가 제외된 접근구조를 전달함으로써 시스템 마스터키의 불법적인 사용을 막는다.

아래 그림 4는 기존 방식의 시스템 구성도다. 아래 그림으로 설명하면 비밀키로 암호화된 암호문(바디)과 속성기반 암호화로 암호화된 비밀키(헤더)를 결합한 것(데이터 파일)을 클라우드 사업자에게 전송하고 사용자 그룹이 데이터 열람을 요구하면 데이터 파일을 전송한다. [8]의 방식은 헤더를 암호화할 때 사용된 속성의 버전을 업데이트함으로써 사용자 그룹이 데이터 파일을 받더라도 복호가 불가능하게 하고 있다. 하지만 철회된 사용자와 클라우드 사업자간의 공모가 이루어 지면 공모한 사용자를 위한 암호문의 속성의 버전을 업데이트하지 않으면 데이터에 대한 접근이 가능하다.

제안방식은 권한 관리자 그룹이라는 믿을 수 있는 공인기관을 두고 데이터 파일을 분산 저장하므로써 기존 방식의 공모 공격을 해결하고자 한다. 즉, 헤더는 권한 관리자 그룹, 바디는 클라우드 사업자에게 전송된다. 이러한 데이터 파일의 분산 저장을 통해서 사용자 그룹은 권한 관리자 그룹에게 반드시 승인을 받아야하는 방식으로 데이터의 기밀성을 보장한다.

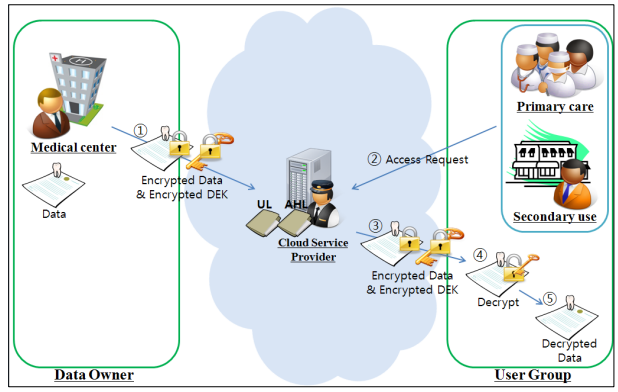

그림 4. 기존 방식의 시스템 구성도
Fig. 4. System Configuration of Existing Scheme

Ⅲ. 제안방식

3.1. 개요

제안 방식은 [8]의 방식에서 클라우드 서버에 저장되는 데이터 파일을 헤더와 바디로 나누어 각각 권한 관리자 그룹과 클라우드 사업자에게 분산 저장한다. 헤더에는 바디의 메시지를 암호화하는데 사용된 비밀키가 KP-ABE로 암호화되어 있다. 다시 말해서 사용자는 권한 관리자 그룹에게 정당성을 인정받지 못하면 헤더내의 비밀키 정보를 얻을 수 없고 실제적으로 사용자가 얻고자 하는 메시지가 포함된 바디의 복호가 원천적으로 불가능하다. 즉, 클라우드 서버에 저장된 데이터 파일을 헤더와 바디로 나누어 분산 저장함으로써 데이터의 기밀성을 보장한다. 또한, 클라우드 내에 권한 관리자 그룹을 두어 사용자 접근에 대한 정당성을 판별한다. 이러한 기능을 구체화하기 위해서 비밀분산과 타입 기반 프록시 재암호화를 활용한다.

[8]의 방식에서의 프록시 재암호화키 $rk_{i\leftrightarrow i'} \leftarrow t_i'/t_i = R$을 (k,n) 방식으로 분할하여 각 쉐어 $R_l(1 \le l \le n)$을 권한 관리자 그룹에게 전송한다. 권한 관리자 그룹은 피위임자가 데이터를 열람하고자 할 때 사용자의 권한이 정당하다면 프록

www.dbpia.co.kr

시 재암호화키 쉐어 R_l를 k개만큼 모아서 R을 재구성하고 정당하지 않다면 연산을 중지한다.

3.2. 알고리즘 상세

제안 방식의 구성요소는 데이터 소유자(Data Owner), 권한 관리자 그룹(Privilege Manager Group), 클라우드 사업자(Cloud Service Provider: CSP), 사용자 그룹(User Group) 총 4개의 집단으로 구성된다. [8]의 방식은 클라우드 서버의 명령에 따른 6개의 시스템 레벨과 시스템 레벨내에서 구체적으로 작동하는 8개의 알고리즘 레벨로 구성된다. 제안 방식은 [8]의 방식에 1가지의 알고리즘 레벨(APrivilegeMgt)을 추가한다.

표 1은 제안방식에서 사용된 기호에 대한 설명을 나타낸 표이다.

표 1. 제안 방식의 기호
Table 1. Symbol of Proposed Scheme

기 호	설 명
PK, MK	시스템 공개키와 마스터키
A_i	속성 i에 대한 공개키 콤포넌트
a_i	속성 i에 대한 마스터키 콤포넌트
SK	사용자 비밀키
sk_i	속성 i에 대한 암호문 콤포넌트
E_i	속성 i에 대한 암호문 콤포넌트
I	데이터 파일에 할당된 속성집합
DEK	데이터 m을 암호화하는데 사용된 비밀키
P	사용자 접근구조
L_P	P의 leaf node를 구성하고 있는 속성들의 집합
Att_D	Dummy Attribute
UL	시스템 사용자 리스트
AHL_i	속성 i에 대한 속성 히스토리 리스트
$rk_{i\leftrightarrow i'}$	현재 버전의 속성 i에서 업데이트된 속성 i'로 속성을 업데이트하는 프록시 재암호화키
$\delta_{O,X}$	X상의 데이터 소유자의 서명

① System Setup : 데이터 소유자가 시스템 유니버스 $U=\{1,2,...,N\}$와 보안 파라메터 k를 입력하여 PK와 MK를 출력하는 시스템 레벨 $(PK, MK \leftarrow ASetup(k))$.

- 생성자 g를 가지는 소수 위수 p의 쌍선형 그룹(bilinear group) G_1과 쌍선형 사상 $e: G_1 \times G_1 \rightarrow G_2$를 정의.
- $T_i \in G_1 (T_i = g^{t_i})$, 속성 i에 대한 $t_i \in Z_p$ $(1 \le i \le N)$, $Y \in G_2 (Y = e(g,g)^y$, $y \in Z_p)$를 생성.
- 시스템 공개키 $PK = (Y, T_1, T_2, ..., T_N)$와 시스템 마스터키 $MK = (y, t_1, t_2, ..., t_N)$를 생성하고 PK에 서명을 덧붙인 $(PK, \delta_{O,PK})$를 권한 관리자에게 전송.

② New File Creation : CSP에게 파일을 전송하기 전에 데이터 소유자가 파일을 암호화하는 시스템 레벨.

- data file에 대한 ID를 선택.
- k라는 키 공간에서 symmetric 데이터 암호키 DEK를 임의로 선택하고 DEK를 이용해서 data file을 암호화. 즉, $\{DataFile\}_{DEK}$를 출력.
- data file에 대한 속성집합 I를 정의하고 DEK를 KP-ABE로 암호화. 즉, $(\tilde{E}, \{E_i\}_{i \in I}) \leftarrow AEncrypt(I, DEK, PK)$.
- 그림 5와 같은 형식으로 header는 권한 관리자, body는 CSP에 저장.

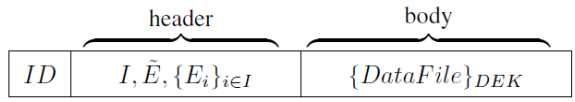

그림 5. data file의 형식
Fig. 5. Format of data file

③ New User Grant : 새로운 사용자 w가 시스템에 참가하길 원할 때, 데이터 소유자가 접근구조와 사용자 w의 접근구조 P를 할당하는 시스템 레벨.

- 접근구조 P의 각 노드 i에 대한 $p_i(x)$를 정의. 접근구조 P의 root node는 $p_r(0) = y$, leaf node는 $p_j(0)$로 정의하고 비밀키 $SK = \{sk_i\}_{i \in L} (sk_i = g^{p_i(0)/t_i})$를 생성 $(SK \leftarrow AKeyGen(P, MK))$. 접근구조의 첫 번째 Gate는 AND Gate로 시작하고 Dummy attribute Att_D를 추가.

www.dbpia.co.kr

- $\left(P, SK, PK, \delta_{O,(P,SK,PK)}\right)$를 사용자 w의 공개키로 암호화하고 C로 표시.
- $\left(T, C, \delta_{O,(T,C)}\right)$를 권한 관리자에게 전송($T$는 접근구조 P의 Dummy attribute를 제외한 접근구조).
- 권한 관리자는 $\left(T, C, \delta_{O,(T,C)}\right)$를 받는 즉시 $\delta_{O,(T,C)}$가 맞는지 확인. 시스템 사용자 리스트 UL에 T를 저장하고 사용자 w에게 C를 전달.
- 사용자 w는 C를 자신의 비밀키로 복호한 후, $\delta_{O,(P,SK,PK)}$가 맞는지 확인하고 P, SK, PK를 자신의 것으로 받아들임.

④ User Revocation : 사용자 v의 데이터 열람 권한을 철회하고, 시스템 마스터키와 공개키의 콤포넌트가 업데이트됨에 따라 재정의된 프록시 재암호화키를 출력하는 시스템 레벨.

- 접근구조의 CNF(Conjunctive Normal Form)을 설계하고 최소한의 속성집합이 있을 때, CNF 형태의 짧은 절에서 속성집합 D를 선택($D \leftarrow AMinimalSet(P)$).
- 데이터 소유자가 $t_i' \leftarrow Z_p$를 선택하고 $T_i' = g^{t_i'}$와 $rk_{i \leftrightarrow i'} \leftarrow t_i'/t_i = R$을 (k, n)방식으로 분할하여 각 쉐어 $R_l (1 \le l \le n)$을 계산($R \leftarrow AUpdateAtt(i, MK)$).
- $Att = \left(v, D, \left\{i, T_i', \delta_{O,(i,T_i')}\right\}_{i \in D}\right)$과 R_l $(1 \le l \le n)$을 권한 관리자에게 전송.
- 권한 관리자는 시스템 사용자 리스트 UL에서 사용자 v를 제거. $\left(i, T_i', \delta_{O,(i,T_i')}\right)$를 저장하고 속성 i의 히스토리 리스트 AHL_i에 R을 추가.

⑤ File Access : 사용자 u가 데이터에 접근할 때, 권한 관리자가 사용자 u의 접근권한을 판별. 이에 따라 사용자 u의 비밀키에 맞는 암호문을 습득하고 복호하는 시스템 레벨.

- 사용자 u가 데이터에 대한 접근 요구 REQ를 생성하여 권한 관리자에게 전송.
- 권한 관리자는 UL에서 사용자 u를 확인하고 (k, n)방식으로 분할된 각 쉐어 R_l $(1 \le l \le n)$를 k개 모아서 (k, n)방식으로 $rk_{i \leftrightarrow i'} \leftarrow t_i'/t_i = R$로 재구성 ($R \leftarrow APrivilegeMgt\left(\{R_l\}_{l \in k}\right)$). UL에 사용자 u가 없다면 이하의 모든 연산을 중지.
- 권한 관리자는 AHL_i에서 모든 프록시 재암호화키를 검색(i가 최신 버전이라면 연산을 수행하지 않음. 가장 최근의 MK는 $t_{i^{(n)}}$이라고 가정).
- 검색된 프록시 재암호화키로 $rk_{i \leftrightarrow i^{(n)}} \leftarrow rk_{i \leftrightarrow i'} \cdot rk_{i \leftrightarrow i''} \cdot \dots rk_{i^{(n-1)} \leftrightarrow i^{(n)}} = t_{i^{(n)}}/t_i$를 계산하여 $E_{i^{(n)}} \leftarrow \left(E_i\right)^{rk_{i \leftrightarrow i^{(n)}}} = g^{t_{i^{(n)}} s}$으로 계산($E_{i^{(n)}} \leftarrow AUpdateAtt4File\left(i, E_i, AHL_i\right)$). $\left(rk_{i \leftrightarrow i^{(n)}}\right)^{-1} \leftarrow rk_{i \leftrightarrow i'} \cdot rk_{i \leftrightarrow i''} \cdot \dots rk_{i^{(n-1)} \leftrightarrow i^{(n)}} = t_i/t_{i^{(n)}}$를 계산하여 CSP에 $\left(rk_{i \leftrightarrow i^{(n)}}\right)^{-1}$와 $\left\{sk_i\right\}_{i \in L_P}$를 전송하면 $sk_i' \leftarrow \left(sk_i\right)^{rk_{i \leftrightarrow i^{(n)}}} = g^{\left(p_i(0)/t_i\right) \cdot \left(t_i/t_{i^{(n)}}\right)} = g^{\left(p_{i^{(n)}}(0)/t_{i^{(n)}}\right)}$을 계산($sk_i' \leftarrow AUpdateSK\left(i, sk_i, AHL_i\right)$).
- $RESP_1 = \left(i^{(n)}, \widetilde{E_{i^{(n)}}}, \left\{E_{i^{(n)}}\right\}_{i^{(n)} \in I}\right)$, $RESP_2 = \left(\left\{i, sk_i', T_i', \delta_{O,(i,T_i')}\right\}_{i \in L_P \setminus Att_D}, \{DataFile\}_{DEK}\right)$를 권한관리자와 CSP는 복호를 위해 사용자 u에게 전송.
- 사용자 u는 $\delta_{O,(i,T_i')}$와 sk_i'를 확인하고 SK 안의 sk_i를 sk_i'로 대체하고 각 leaf node에 대한 $e\left(E_i, sk_i\right) = e(g, g)^{p_{i^{(0)}} s}$를 계산.
- AND Gate와 OR Gate의 연산을 통해서 $Y^s = e(g, g)^{ys}$를 계산.
- header의 E를 Y^s로 계산($E/Y^s = DEK$). body의 $\{DataFile\}_{DEK}$을 DEK로 계산하여 데이터 획득 ($DEK \leftarrow ADecrypt(P, SK, E)$).

⑥ File Deletion : 데이터 소유자가 CSP의 데이터 파일을 삭제하기 위해서 수행. 파일을 삭제하기 위해서 데이터 소유자는 삭제할 파일의 ID에 자신의 서명을 첨부하여 권한 관리자 그룹에게 전송. 서명을 확인하여 정당성이 입증되면 권한 관리자 그룹은 CSP에 저장된 데이터를 삭제할 것을 요구하고 CSP는 데이터를 삭제하는 시스템 레벨.

www.dbpia.co.kr

Ⅳ. 의료 환경에의 응용 및 안전성 분석

4.1. 시나리오 구성

시나리오의 구성은 다음과 같다. 고혈압이 있는 환자(위임자)가 과로로 쓰러져서 입원하게 됐다. 입원 후 환자의 신뢰도에 따라 사용자 그룹(의료진, 보험회사, 연구기관 등)을 위한 타입 정보를 설정하고 환자에 대한 진료 기록은 메디컬 센터(데이터 소유자)에서 암호화된 후 CSP에 저장되어 있다. 주치의(피위임자)는 응급 상황에 대비하기 위해서 환자의 진료 기록을 스마트폰은 통해서 열람하고자 한다. 이에 대해서 권한 관리자 그룹은 주치의의 데이터 접근에 대한 정당성을 판별하고 합당하다면 접근을 승인하는 시나리오로 구성한다. 그림 6은 의료 환경에서의 제안 방식 개념도이다.

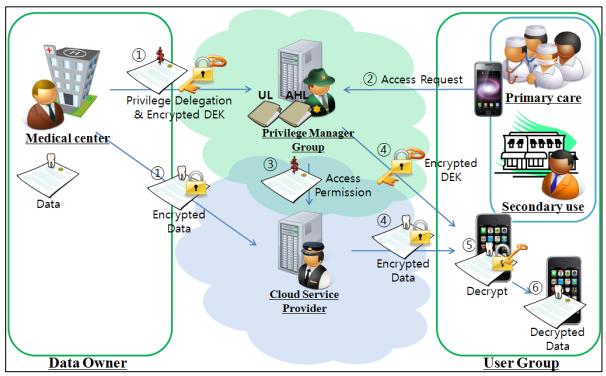

그림 6. 의료환경에의 제안 방식의 시스템 모델 구성도
Fig. 6. System Model Configuration of Proposed Scheme in Medical Environment

4.2. 세부 시스템 구성

① 메디컬 센터는 $ASetup(k)$ 알고리즘을 이용해서 공개키 PK와 마스터키 MK를 생성한다. $AEncryptB(m, DEK)$ 알고리즘으로 환자의 진료 기록 m을 DEK로 암호화한 $\{DataFile\}_{DEK}$과 $AEncryptH(I, DEK, PK)$ 알고리즘으로 DEK를 암호화한 $\left(i, \widetilde{E}_i, \{E_i\}_{i\in I}\right)$를 각각 CSP와 권한 관리자 그룹에게 전송한다. 그리고 권한 관리자 그룹이 사용자 접근의 정당성을 판별하는 권한을 행사하기 위해서 프록시 재암호화키 R을 (k, n)방식으로 권한 관리자의 수(n명)만큼 분할한 쉐어 $R_l(1 \le l \le n)$를 권한 관리자 그룹에게 전송한다.

② 주치의(사용자 그룹)의 스마트폰에 설치된 모바일 어플리케이션이 환자의 진료 기록에 대한 접근을 요구하는 REQ를 권한 관리자 그룹에게 전송한다.

③ 권한 관리자 그룹은 UL에서 보험회사 직원을 확인하고 $APrivilegeMgt\left(\{R_l\}_{l\in k}\right)$ 알고리즘으로 설정된 임계값 k개만큼의 쉐어로 재구성한 프록시 재암호화키 R과 $\{sk_i\}_{i\in L_P}$를 CSP에 전송한다.

④ CSP는 $AUpdateSK(i, sk_i, AHL_i)$ 알고리즘으로 주치의를 위한 비밀키 sk_i'를 생성하여 $\{DataFile\}_{DEK}$에 첨부하여 전송하고, 권한 관리자 그룹은 $AUpdateAtt4File(i, E_i, AHL_i)$ 알고리즘으로 비밀키 sk_i'에 대응되는 $\left(i, \widetilde{E}_i, \{E_i\}_{i\in I}\right)$를 생성하여 전송한다.

⑤ 주치의의 스마트폰에 설치된 모바일 어플리케이션은 비밀키 sk_i'와 접근구조 P로 $ADecryptH(P, SK, E)$ 알고리즘을 이용하여 DEK를 획득한다.

⑥ $ADecryptB(m\cdot DEK, DEK)$ 알고리즘을 이용하여 복호된 DEK로 $\{DataFile\}_{DEK}$를 복호하여 환자의 진료 기록 m을 획득한다.

4.3. 기존 방식과의 비교 분석

4.3.1. 기존 방식과 제안방식의 비교

표 2는 [8]의 방식과 본 논문에서 제안한 방식과의 특성을 비교하는 표이다.

표 2. 기존의 방식과 제안 방식의 비교
Table 2. Comparison of Proposed Scheme with Existing Scheme

구분	기존의 방식	제안 방식
속성철회	○	○
권한위임	×	○
공모 공격에 대한 안전성	×	○
변조 공격에 대한 안정성	×	△

[8]은 데이터의 기밀성과 유연성 있는 접근제어를 실현할 수 있는 모델을 제안하고 있다. 하지만 언급한 바와 같이 철회된 사용자와 클라우드 사업자간의 공모 공격에 취약하다. 그것은 클라우드 사업자

www.dbpia.co.kr

에게 암호문, 암호화된 키(헤더와 바디) 등 복호와 관련된 권한이 집중되어 있기 때문이다. 제안방식은 권한 관리자 그룹이라는 신뢰할 수 있는 기관을 두어 키(헤더)를 관리하게 하고 클라우드 서버는 암호문(바디)만을 보관하여 권한을 분산함으로써 공모 공격을 방지하고 데이터의 기밀성을 보장한다.

권한 관리자 그룹의 개입으로 공모 공격의 방지와 데이터 기밀성의 보장을 실현할 수 있고 비밀분산을 활용하여 사용자의 데이터 열람에 관한 접근을 승인하는 절차를 구현할 수 있다. 즉, 비밀분산을 활용하여 n명의 권한 관리자에게 쉐어(사용자의 열람을 허용할 수 있는 권한)를 나누어 주고 k명이 동의하면 키를 복원하여 데이터 열람을 가능하게 한다. 또한, 비밀분산을 사용함으로써 민감한 데이터일수록 임계값을 높임으로써 다수의 권한 관리자의 동의를 받아야만 데이터를 열람할 수 있는 구조를 실현할 수 있다.

제안방식에서 사용자 그룹은 스마트폰과 같은 컴퓨팅 자원으로 연산하여도 부담이 없도록 설계되었다. 위에서 언급했듯이 프로토콜 상에서 사용자 그룹은 자신이 소지하고 있는 키 부분에 대해서만 최소한의 계산을 수행하면 된다. 이러한 특성 때문에 기존의 방식과 비교해서 모바일 환경에 적합하다고 할 수 있다.

4.3.2. 철회된 사용자의 공모 공격

본 제안 방식의 중요한 보안 특성은 공모 공격에 대한 안전성이다. 여기서 공모 공격이란 시스템상에서 철회된 사용자가 클라우드 서버와 공모하여 데이터를 불법적으로 열람하는 것이다. [8]의 방식에서는 철회 이벤트가 발생해도 철회된 사용자가 소지하고 있는 비밀키 SK에 직접적인 변화가 없다. 여기서, 바디내의 데이터를 암호화하는데 사용된 DEK가 KP-ABE로 암호화되어 헤더내에 포함되어 있다. 따라서 클라우드 서버가 보유하고 있는 데이터 파일의 헤더에 비밀키 콤포넌트의 업데이트를 실행하지 않고 철회된 사용자에게 전송하면 자신의 비밀키 SK로 헤더를 복호할 수 있다. 즉, DEK를 획득함으로써 데이터 m을 열람 가능하다.

의미론적으로 안전하다(semantically secure)는 것은 공격자가 암호문과 공개키를 사용해서 주어진 암호문을 만들 때 평문에 대한 어떠한 것도 습득해서는 안되는 것을 뜻한다[14]. 이러한 공모 공격에 대한 안전성의 개념은 다음과 같이 3가지로 정의한다[14].

- 사용자들간의 공모 공격을 방지해야 한다; 2명 이상의 사용자가 그들의 복호권한을 확장하기 위해서 각자의 속성집합을 조합할 수 없어야 한다.
- 프록시(클라우드 서버)와 사용자의 공모 공격을 방지하여야 한다; 접근 정책에 만족하는 비밀키를 가지고 있지 않은 사용자와 프록시간의 악의적인 협력에 의해서 암호문을 복호할 수 없어야 한다.
- 위임된 비밀키(위임자가 피위임자를 위해 생성한 비밀키 쉐어)가 안전성을 위태롭게 해서는 안된다; 위임된 비밀키를 이용한 인증기관의 마스터키 도출 등 위임된 비밀키에 의해서 안전성이 저해되어서는 안된다.

제안 방식은 데이터 파일을 헤더와 바디로 나누어 각각 권한 관리자 그룹과 클라우드 사업자에 분산 저장한다. 사용자는 권한 관리자 그룹에게 정당성을 인정받지 못하면 헤더내의 DEK에 대한 정보를 얻을 수 없기 때문에 바디의 복호가 원천적으로 불가능하다. 즉, 제안 방식은 권한 관리자 그룹의 개입으로 철회된 사용자와 클라우드 서버간의 공모 공격에 대해서 안전하다. 또한, 권한 관리자 그룹에게 사용자의 데이터 접근 정당성에 대해 판별할 수 있는 권한을 부여한다. 정당성을 판별하여 승인하는 절차는 프록시 재암호화키를 n개의 쉐어로 나누어 k개의 쉐어가 모였을 때만 재구성되는 (k, n)방식을 이용한다. 권한 관리자 그룹이 사용자의 데이터 접근 정당성을 판별하여 승인되었을 때만 k개의 쉐어로서 프록시 재암호화키를 재구성하여 다음 연산을 수행하고, 승인하지 않았을 때는 이하의 모든 연산을 중지한다.

4.3.3. 프록시 재암호화키에 대한 변조 공격

프록시 재암호화키에 대한 변조 공격이란 프록시 재암호화키 R이 소실 또는 변조를 통해서 원래의 기능을 수행할 수 없게 만드는 공격이다. [8]의 방식에서 프록시 재암호화키가 유일하므로 소실되거나 유출되어 변조된다면 재암호화를 수행할 수 없다. 이와 비교해서 제안 방식은 프록시 재암호화키에 대한 변조 공격에 대해서 비밀분산을 활용하여 프록시 재암호화키 복원에 필요한 쉐어 정보량에 따라 복원 가능성이 결정된다.

즉, 제안방식은 (k, n) 비밀분산 방식으로 프록시 재암호화키 R을 프록시 재암호화키 쉐어 R_l

www.dbpia.co.kr

$(1 \le l \le n)$로 분할하여 재조합시 k개만큼 쉐어가 모여야 프록시 재암호화키 R이 재구성된다. 예를 들어 $R_l(1 \le l \le n)$에 대해서 $k=3,\ n=5$라고 할 때 $R_1,\ R_2,\ R_3,\ R_4,\ R_5$ 중 3개의 쉐어만 있어도 R을 도출할 수 있다. k개의 쉐어만 존재하면 프록시 재암호화키를 복원할 수 있다는 점에서 안전하다.

4.4. 의료 서비스 시나리오

속성 기반 암호방식이 적용된 의료환경에서 진료시 환자의 병력을 확인할 수 있다면 효율적으로 치료가 가능할 것이다. 본 논문에서는 제안방식을 의료환경에 적용하여 환자가 의식이 없는 응급상황에서 의사가 환자의 모든 병력 등과 같은 중요한 데이터를 열람할 수 있는 시나리오를 구성한다. 본 논문에서 헬스 클라우드 서비스에 대한 시나리오는 다음과 같다.

- 심장병 환자가 심장병 악화로 의식을 잃은 채 응급실로 이송되었다. 응급실 의사는 환자의 병력을 확인하여 효과적인 진료를 하고자 한다. 따라서 환자의 병력을 확인하기 위해 환자의 진료기록에 접근하고자 한다.
- 의사가 환자의 병력을 확인하기 전에 알 수 없는 사실은 현재 환자는 심장병 환자이면서 혈우병 환자이기도 하다.

① 의사의 스마트폰에 설치된 모바일 어플리케이션이 환자의 진료 기록에 대한 접근을 요구하는 REQ를 권한 관리자 그룹에게 전송한다.

② 권한 관리자 그룹은 UL에서 보험회사 직원을 확인하고 $APrivilegeMgt\left(\{R_l\}_{l\in k}\right)$ 알고리즘으로 설정된 임계값 k개만큼의 쉐어로 재구성한 프록시 재암호화키 R과 $\{sk_i\}_{i\in L_P}$를 CSP에 전송한다.

③ CSP는 $AUpdateSK(i, sk_i, AHL_i)$ 알고리즘으로 의사를 위한 비밀키 sk_i'를 생성하여 $\{DataFile\}_{DEK}$에 첨부하여 전송하고, 권한 관리자 그룹은 $AUpdateAtt4File(i, E_i, AHL_i)$ 알고리즘으로 비밀키 sk_i'에 대응되는 $\left(i, \widetilde{E}_i, \{E_i\}_{i\in I}\right)$를 생성하여 전송한다.

④ 의사의 스마트폰에 설치된 모바일 어플리케이션은 비밀키 sk_i'와 접근구조 P로 $ADecryptH(P, SK, E)$ 알고리즘을 이용하여 DEK를 획득한다.

⑤ $ADecryptB(m\cdot DEK, DEK)$ 알고리즘을 이용하여 복호된 DEK로 $\{DataFile\}_{DEK}$를 복호하여 환자의 진료 기록 m을 획득하고 환자는 경도 혈우병 환자임이 확인되었고 의사는 심장병에 대해서만 효과적으로 치료를 시작한다.

V. 결 론

모바일 클라우드 컴퓨팅은 컴퓨팅 자원을 서비스로서 제공하는 획기적인 컴퓨팅 패러다임이다. 모바일 클라우드 컴퓨팅은 컴퓨팅 자원에 대한 효율적인 투자가 가능하기 때문에 기존 서비스 영역이 모바일 클라우드 서비스로 확대될 것이다. 그러나 클라우드 사업자를 데이터 보안 관리상 전적으로 신뢰할 수 없기 때문에 데이터 보안 위협 및 프라이버시 침해요소를 고려해야 한다. 특히, 데이터 기밀성을 보장하는 것이 필요하다. 이러한 문제를 해결하기 위해서 [8]에서는 데이터 기밀성을 보장하면서 유연성있는 접근제어가 가능한 방식을 제안했다. 그러나 철회된 사용자와 클라우드 서버간의 공모 공격과 프록시 재암호화키에 대한 변조 공격 취약성에 의해 데이터 기밀성을 침해하게 된다.

이러한 문제점을 해결하기 위해서 본 논문에서는 클라우드 서버에 저장되는 데이터 파일의 헤더와 바디를 분산 저장하여 데이터의 기밀성을 보장했다. 또한, 비밀분산 방식의 적용을 통해서 사용자의 데이터 열람권한을 판별하여 승인하는 절차를 수행할 수 있는 방안을 구성했다. 그리고 4장에서 프라이버시를 보호하면서 의료데이터를 처리하는 모바일 헬스 클라우드 모델을 구성하고 제안 방식의 안전성을 분석했다. 본 제안 방식은 민감한 데이터를 다루는 기업 환경에서 활용될 수 있다. 정보가 곧 중요한 자산인 기업이 민감한 정보를 안전하게 공유하고 활용할 수 있다는 점에서 긍정적인 결과를 이끌어 낼 것으로 기대된다.

하지만 제안방식은 사용자 그룹의 데이터 접근 요구와 권한 관리자 그룹의 접근 승인 절차가 반복된다. 이러한 사용자의 데이터 접근 요구가 늘어나면 권한 관리자 그룹이 수행하는 승인 절차에 많은 과부하가 생길 것으로 예상된다. 또한 데이터 소유자와 사용자 그룹이 수행하는 키 생성과 암호문 복호도 과부하의 원인이 될 수 있다. 이러한 여러 계산상 과부하로 인한 서비스의 품질 문제는 향후 연

www.dbpia.co.kr

구과제로 남겨두고 있다.

한편, 모바일 클라우드 컴퓨팅 환경에서 프라이버시를 강화하기 위해서 데이터 소유자는 자기 정보에 대한 자기 통제권이 있어야 한다. 이러한 요구사항을 해결하기 위해 향후 과제로서 환자가 자신의 진료 기록에 대한 공유 및 활용을 통제(user-centric)할 수 있는 PCE(Patient Controlled Encryption)[13]에 대해 분석하고 소셜 네트워크를 의료데이터의 유통망으로서 간주하여 여러 사용자 그룹간의 의료데이터 유통 기능을 고려한 모바일 헬스 비즈니스 모델을 구성하고자 한다. 또한 다수의 클라우드 사업자간 즉, 인터클라우드(inter-Cloud) 환경에서 의료데이터를 소비하는 프라이버시 보호 메카니즘 검토가 요구된다.

현재 모바일 클라우드 서비스의 활성화를 위해서 서비스와 플랫폼간의 상호호환성을 위한 표준화 연구의 필요성이 대두되고 있다[5,9]. 이러한 연구시 CSA에서 분류한 보안 위협을 고려하여 연구가 이뤄져야할 것이다[7].

참 고 문 헌

[1] D.Kim, K.Jang, D.Shin, "Healthcare System using Agent Platform in Ubiquitous Environment,", *Korean Society For Internet Information,* Proceedings of Korean Society For Internet Information, pp. 139-142, 2006

[2] Y.Min, H.Kim, Y.Kim, "Distributed File System Technology for Cloud Computing," *Korean Institute of Information Scientists and Engineers*, pp.86-94, 2009.

[3] D.Yu, S.Jeong, T.Kim, "TIPC Application and Analysis for Network I/O Performance Evaluation in Hadoop based Distributed Computing," *Korean Institute of Information Scientists and Engineers*, pp.351-359, 2009.

[4] O.Min, H.Kim, G.Nam, "Cloud Computing Technology Trend," *ETRI*, ETTrends, Vol.24 No.4, pp.1-13, 2009.

[5] H.Kim, U.Min, G.Nam, "Mobile Cloud Computing Technology Trend," *ETRI*, ETTrends, Vol.25 No.3, pp.40-51, 2010.

[6] T. Mather, S. Kumaraswamy and S. Latif, "Cloud Security and Privacy," *O'Reilly Media*, 2009.

[7] CSA, Security Guidance for Critical Areas of Focus Cloud Computing, Vol.2.1, 2009.

[8] S.C. Yu, C. Wang, K.I. Ren and W.J. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," *INFOCOM*, 2010 Proceedings IEEE, pp.321-334, 2010.

[9] Y.Yun, B.Kim, "Mobile Cloud Computing Technology Trend", *NIPA*, Weekly Technology Trend Vol.1439, pp.28-39, 2010.

[10] V. Goyal, O.ng Pandey, A. Sahai and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," *Association for Computing Machinery*, in Proc. of CCS'06, 2006.

[11] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," *IEEE Computer Society*, Proceedings of the 2007 IEEE Symposium on Security and Privacy, pp.321-334, 2007.

[12] M. Blaze, G. Bleumer and M. Strauss, "Divertible protocols and atomic proxy cryptography", *EUROCRYPT*, Proceedings of Eurocrypt '98, Volume 1403, 1998.

[13] J. Benaloh, M. Chase, E. Horvitz and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," Association for Computing Machinery, Proceedings of the 2009 ACM workshop on Cloud computing security, pp.103-114, 2009.

[14] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel and W. Jonker, "Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes," *2009 University of Twente*, Centre for Telematics and Information Technology, Internal Report, 2009.

www.dbpia.co.kr

송 유 진 (You-jin Song) 정회원

1982년 한국항공대학교 학사
1987년 경북대학교 석사
1995년 일본 Tokyo Institute of Technology 박사
1988년~1996년 한국전자통신연구원 선임연구원
2003년~2005년 미국University of North Carolina at Charlotte 연구교수
2006년 일본 정보보호대학원대학 객원교수
1996년~현재 동국대학교 정보경영학과 교수
1998년~현재 한국정보보호학회 부회장(영남지부장)
2006년~현재 국제 e-비즈니스학회 이사
2006년~현재 한국사이버테러정보전학회 이사
2001년 ICISC2001 운영위원장
2003년 하계CISC2003 프로그램위원장
2006년 CISC-S2006 공동프로그램위원장
2007년 한국정보시스템학회 추계학술발표대회 공동조직위원장
<관심분야> Privacy Protection, Secret Sharing, 클라우드 보안 및 응용(헬스 2.0 보안), Context Aware Application Security 등

도 정 민 (Jeong-min Do) 정회원

2009년 동국대학교 정보경영학과 졸업(학사)
2010년~2011년 동국대학교 일반대학원 전자상거래협동과정 졸업(석사)
<관심분야> 정보보호, 암호이론(Secret Sharing, Attribute-Based Encryption), Context Aware Application Security 등

www.dbpia.co.kr