모바일 클라우드 서비스 상에서 준동형 암호 기반의 형상 관리 방안

김선주* · 김진묵** · 조인준***

Design of Configuration Management using Homomorphic Encryption in Mobile Cloud Service

Sun-Joo Kim* · Jin-Mook Kim** · In-June Jo***

요 약

스마트폰 사용자가 2,000만명을 넘어서며, 클라우드 컴퓨팅 서비스를 제공하던 기업들이 다양한 모바일 장비를 지원하려고 한다. 특히, 다양한 모바일 장비를 통해 특정 문서를 서로 공유하거나, 편집/보기 등의 작업을 수행할 수 있게 되었다. 하지만, 여러사람이 하나의 문서를 공유해서 작업하는 경우 형상관리, 기밀성, 무결성이 보장되지 않는 문제가 발생한다. 따라서, 본 논문에서는 모바일 클라우드 서비스 사용자들이 문서를 효율적으로 공유하고, 암호화된 문서에 대한 연산을 통해 문서편집을 수행하고, 무결성 검증이 가능한 준동형 암호화를 기반으로 한 형상관리 방안을 제안하고자 한다.

ABSTRACT

As smartphone users are over 20 million, companies, which offer cloud computing services, try to support various mobile devices. If so, users can use the same cloud computing service using mobile devices, as sharing document. When user share the work, there are problem in configuration management, data confidentiality and integrity. In this paper, we propose a method that cloud computing users share document efficiently, edit encrypted docuements, and manage configuration based on homomorphic encryption, which integrity is verifiable.

키워드

모바일 클라우드 서비스, 준동형 암호화, 형상관리

Key word

Mobil Cloud Service, Homomorphic Encryption, Configuration Management

* 정회원 : 한국정보통신기술협회 선임연구원
** 정회원 : 선문대학교 IT교육학부 조교수
*** 정회원 : 배재대학교 컴퓨터공학과 교수

접수일자 : 2012. 05. 24
심사완료일자 : 2012. 07. 05

Open Access http://dx.doi.org/10.6109/jkiice.2012.16.10.2217

Ⅰ. 서 론

미국의 애플사에서 아이폰을 2008년에 출시하면서 전자기기로서의 휴대폰의 용도가 달라졌다. 과거에는 휴대폰 제조사가 설치해놓은 SW만 사용할수 있었던 반면, 아이폰이 등장하면서 사용자들의 취향에 맞는 SW를 선택하여 사용할 수 있는 스마트한 모바일 장비로 변화했다. 이런 변화는 휴대폰 뿐만 아니라 다양한 모바일 장비에서 SW를 선택하여 설치 및 사용하고, 삭제가 가능하게 되었다[1].

네이버, 다음, 구글 등의 인터넷 포털사이트를 비롯한 이동통신사들은 스마트폰 사용자가 2000만명을 넘어서면서 클라우드 컴퓨팅 서비스를 다양한 모바일 장비에서 동일한 서비스를 이용할수 있도록 많은 노력을 기울이고 있다. 또한, 사용자들이 다양한 모바일 장비의 사용하면서 시간과 장소의 제약을 받지 않고, 사용자들간에 특정 문서를 공유하거나 편집/보기등의 작업을 수행할수 있는 환경이 되었다. 이로 인해, 사용자가 작성한 문서에 대한 형상관리의 중요성이 높아지게 되었다. 따라서, 본 논문에서는 모바일 클라우드 개요와 준동형 암호 알고리즘에 대해 서술하고, 사용자간에 문서를 효율적으로 공유할수 있도록 암호화된 문서에 대한 연산을 통해 문서편집을 수행하고, 무결성 검증이 가능한 준동형 암호화를 기반으로 한 형상관리 방안을 제안하고자 한다.

Ⅱ. 관련 연구

2.1. 모바일 클라우드 개요

모바일 클라우드 컴퓨팅(Cloud Computing)은 모바일 기반의 인터넷 컴퓨팅 기술로, 사용자들은 구름(Cloud) 모양의 클라우드 서비스 구조와 기술을 몰라도, 인터넷으로 접속하여 각종 서비스를 이용할 수 있다.

모바일 클라우드 서비스의 종류로는 서비스를 위한 소프트웨어(Software as a Service: SaaS), 서비스 관리를 위한 인프라(Infrastructure as a Service: IaaS), 서비스를 위한 플랫폼(Platform as a Service: Paas)등이 있으며, 최근에는 모바일 환경에서도 유무선 모바일 장비간의 서비스(Device as a Service: DaaS)를 지원하는 기술로도 발전하고 있다.

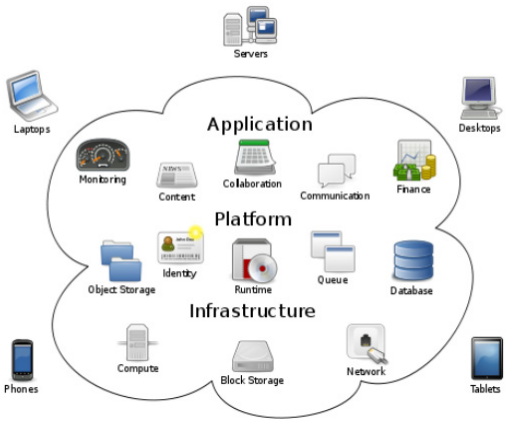

그림 1. 클라우드 컴퓨팅(출처. 위키피디아)
Fig. 1 Cloud Computing(Wikipedia)

모바일 클라우드 환경을 이용하는 대표적인 모바일 클라우드 서비스로는 [표 1]에서 보는 바와 같이, 구글의 지도 서비스와 애플사의 Mobile Me, 마이크로소프트사의 마이폰 서비스 등이 있다.

표 1. 모바일 클라우드 서비스 사례
Table. 1 Mobile Cloud service case

서비스	개요 및 특징
구글의 지도 서비스	구글 포털사이트에서만 제공되는 지도 서비스가 안드로이드 기반의 OS를 탑재한 스마트폰을 비롯한 모바일 장비에서 사용 가능함
애플의 Mobile Me	사용자의 메일, 연락처, 일정정보를 클라우드에 보관하고, iOS가 탑재된 아이폰, 노트북을 비롯한 모바일 장비에서 자동으로 동기화시켜 시간, 장소, 모바일 장비에 구애받지 않고 동일한 데이터 서비스를 제공함
마이크로소프트의 마이폰	스마트폰의 연락처, 일정, 작업, 사진, 동영상, 문자메시지, 음악 등을 클라우드에 보관하고, 윈도우 모바일 OS가 탑재된 모바일 장비에서 백업 및 동기화 서비스를 제공함

이처럼, 모바일 클라우드 서비스는 기존의 클라우드 컴퓨팅에 이동성(Mobility)을 결합한 형태로서, 모바일 장비의 저전력, 저사양이라는 제약사항을 극복하여 향후, 모바일 클라우드 시장은 급속히 확대될 것으로 전망된다.

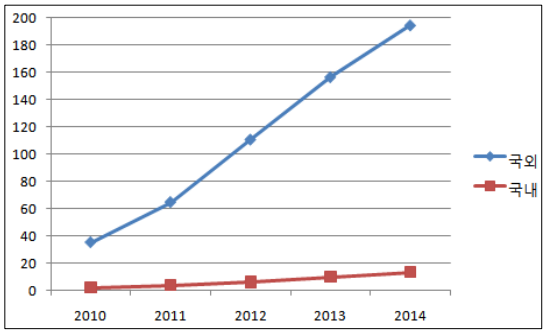

그림 2. 국내외 클라우드 시장 규모
(ABI Research, 2009)
Fig. 2 Domestic and International market for Cloud Computing(ABI Research, 2009)

위의 [그림 2]을 보면, 국외 클라우드 시장은 2010년 35억 달러에서 2014년 195억 달러 규모로 연평균 53.3%의 급격한 성장을 할것으로 예상되고, 국내시장은 2011년 2억 달러에서 2014년 13억 달러 규모로 연평균 58.1%로 성장할 것으로 전망하고 있다[1].

2.2. 준동형 암호 시스템(Homomorphic Cryptosystem) 개요

최근 MIT에서는 준동형 암호화(Homomorphic Encryption)를 2011년도 10대 최신기술 중 하나로 선정하였다. 준동형 암호 시스템은 1978년 Rivest, Adleman, Dertouzous에 의해 Privacy Homomorphism으로 처음 소개 되었으나, 안전성에대한 검증이 이루어지지 않아 사용하지 않았다[4]. 1996년 Domingo-Ferrer가 덧셈, 뺄셈, 곱셈 연산이 가능한 Symmetric 준동형 암호화가 제안되었지만, 비밀키를 사용자간 미리 공유해야 하고, 알려진 평문공격에 취약했다[5]. 2009년에는 Gentry가 안전성이 증명된 “Fully homomorphic encryption” 기법을 제안하였다[6]. 이 기법은 암호화된 상태에서 일정 회수까지 연산이 가능하고, 복호화에 필요한 정보와 공개키 정보를 암호문과 함께 제공하는 특징이 있다.

2.3. 형상관리 시스템(Configuration Management System) 개요

형상관리란 시스템 형상 요소의 기능적 특성이나 물리적 특성을 문서화하고, 특성의 변경을 관리하며, 변경의 과정을 기록하여 지정된 요건이 충족되었다는 사실을 검증하는 것 또는 그 과정이라 할 수 있다[7]. 따라서, 형상관리 시스템은 소프트웨어를 개발하거나 문서 작업을 통한 산출물을 식별하고, 산출물에 대한 버전 및 변경 이력 관리 등 각종 결과물들을 종합적으로 관리하고 제어하는 시스템이다. 이러한 형상관리 시스템으로는 다음 [표 2]와 같으며, 대부분이 클라이언트-서버 플랫폼 구조이다.

표 2. 형상관리 시스템 예시
Table 2. Configuration Management System case

도구명	특징
VSS	클라이언트-서버 플랫폼으로 내부 네트워크에서만 접속이 가능하다. MS 개발 도구와 호환성이 높지만 안정성(Stability)이 다른 도구에 비해 떨어지며 Repository가 중앙 서버에 연결되어 있음
CVS	클라이언트-서버 플랫폼으로 인터넷을 통해 접속이 가능하다. 형상 관리 기능인 히스토리 기능, 변경 내용 관리, 문서 병합 등을 지원하며, Repository가 중앙 서버에 연결되어 있고, 무료 버전으로 널리 사용됨
Subversion	CVS의 단점을 개선코자 Collabnet사에서 개발했으며, 클라이언트-서버 플랫폼으로 인터넷을 통한 형상관리가 가능하다. 디렉토리 및 파일 버전 관리, 오프라인 사용 관리 및 웹 인터페이스 지원 등이 가능하며, Repository가 중앙 서버에 연결되어 있음
Git	분산처리가 가능한 구조로, Repository가 분산되어 여러개가 존재하여 Offline 작업이 가능함

Ⅲ. 제안모델

서두에서 다룬바와 같이 모바일 사용자간에 공동 작업이 가능하도록 문서를 효율적으로 공유할수 있고, 준동형 암호화 기반의 기밀성과 무결성이 지원되는 형상관리시스템을 다음과 같이 제안하고자 한다.

3.1. 준동형 암호화 기반 형상관리시스템

본 논문에서는 Gentry가 제안한 “Fully homomorphic encryption”방식을 이용한다. 최초 문서 작성자는 문서 파일에 접근 레벨을 부여하여 사용자별로 문서를 보거나 편집을 할수 있도록 하고, 문서의 기밀성을 위해 해당 문서를 준동형 암호화하여 이를 형상관리 시스템에 게시하는 방식이다.

3.2. 제안시스템 파일 구조

형상관리를 위한 준동형 암호화가 적용된 파일의 구조는 다음 [그림 3]과 같다. 기존 파일 구조와 달리 제안 시스템의 파일 구조에는 File Header(이하 ‘FH’라함), Permission Bit(이하 ‘P’라함), Encryption 필드로 구성된다. 각 필드별 상세 설명은 다음 [표 3]과 같다.

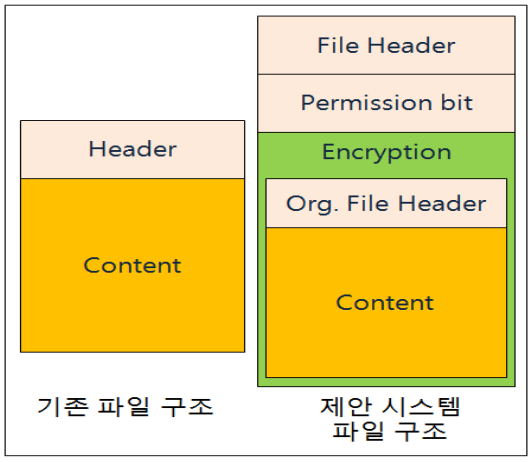

그림 3. 제안 시스템 파일 구조
Fig. 3 Proposed System File Structure

표 3. 파일 구조 별 상세 설명
Table. 3 File Structure Description

파일 구조	설명
FH	제안 시스템에서 사용하는 파일 구조임을 표시하는 16비트 값이다
P	사용자들에게 Read, Write, Access 불가를 표시하는 비트값으로 00, 01, 10을 갖는다. . 00 : 접근 불가 . 01 : READ . 10 : READ/WRITE
Encryption	기존 파일을 준동형 암호화한 결과값

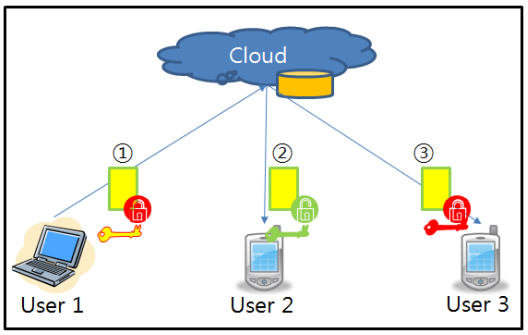

그림 4. 제안 시스템 개요
Fig. 4 Overview of the Proposed System

① User 1은 한글문서를 생성하고, 파일에 대한 접근 퍼미션과, 원본 파일에 대한 서명값을 추가하여 모바일 클라우드 서비스 망에 업로드 한다.

② User 2는 모바일 클라우드 서비스 망에서 다운로드받은 파일의 읽기/쓰기 퍼미션을 확인하고, 파일 끝에 추가된 서명값을 확인 한 다음, 퍼미션에 따라 파일을 읽거나 편집을 수행한다. 만약 서명 결과 이상이 발생하는 경우 다운로드 받은 받은 파일을 삭제하고, 편집이 완료된 경우 ①의 과정을 동일하게 수행한다.

③ User 3은 User 2와 동일한 절차로 수행하며, 파일에 대한 접근 퍼미션이 읽기만 있는 경우 해당 파일을 보기만 수행 할 수 있으며, 파일 끝에 추가된 서명값을 확인 후, 퍼미션에 따라 파일을 읽기전용으로 열어볼 수 있다.

위의 데이터 흐름을 세부 프로세스별로 나누어서 설명하면 다음 그림 5와 같으며, 상세 절차는 다음과 같다.

① User1은 원본 문서(File.org)를 작성하고, User1의 개인키로 암호화 하여 암호화된 EncSig.Content를 생성한다. 이후, FH(File Header)에 제안 시스템에서 사용하는 파일 구조임을 표시하는 16비트값과 파일에 대한 접근권한 표시(00, 01, 10)를 하고, 뒤에 EncSig.Content를 덧붙인다. 새롭게 생성된 파일(NewFile)을 모바일 클라우드 서비스 망에 업로드 한다.

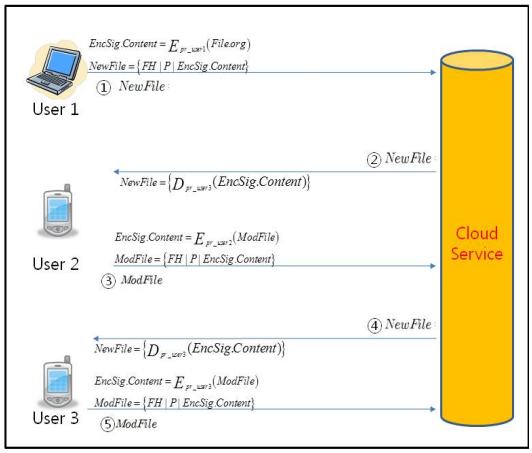

그림 5. 제안시스템 상세 절차
Fig. 5 Detailed procedures in the proposed system

② User2는 모바일 클라우드 서비스 망으로 부터 파일(NewFile)을 다운로드 받은 다음, FH가 갖는 비트값을 통해 파일의 속성을 확인하고, EncSig.Content를 필드를 준동형 암호화 알고리즘을 통해 복호화를 수행하여해 기밀성 및 무결성 검사를 수행한다.

$$ModFile = \{D_{pr\_user2}(EncSig.Content)\}$$

③ 다운로드 받은 파일에 대해 기밀성 및 무결성 검사 결과 이상이 없고, Permission이 비트인 P 비트값이 '10'으로 Write가 가능함을 확인 한 다음 해당 파일을 쓰기전용으로 OPEN하여 ①의 과정과 유사하게 수정된 파일(ModFile)를 생성하여 모바일 클라우드 서비스 망에 업로드 한다.

$$EncSig.Content = E_{pr\_user2}(ModFile)$$
$$ModFile = \{FH \mid P \mid EncSig.Content\}$$

④ User3은 모바일 클라우드 서비스 망으로 부터 파일(NewFile)을 다운로드 받은 다음, FH가 갖는 비트값을 통해 파일의 속성을 확인하고, Permission 비트값이 '01'으로 READ만 가능하다면, EncSig.Content를 구분한다. 구분된 EncSig.Content를 준동형 암호화 알고리즘을 통해 복호화하여 기밀성 및 무결성 검사를 수행 후, Permission 비트값이 READ이므로, 해당 파일을 읽기전용으로 OPEN한다. 만약에 Permission bit 값이 '00'으로 접근불가인 경우, EncSig.Content에 대해 기밀성 및 무결성 검사 없이 종료한다.

$$NewFile = \{D_{pr\_user3}(EncSig.Content)\}$$

⑤ 위의 ④번 과정에서 다운로드 받은 문서에 대한 Permission 비트값이 '10'으로 Write인 경우 ③의 과정과 동일하게 수행하고, 모바일 클라우드 서버에 수정된 파일을 업로드 한다.

$$EncSig.Content = E_{pr\_user3}(ModFile)$$
$$ModFile = \{FH \mid P \mid EncSig.Content\}$$

Ⅳ. 제안 시스템 고찰

지금까지 모바일 클라우드 서비스 환경에서 준동형 기반의 형상관리시스템을 제안하고, 동작절차를 설명하였다. 본 논문에서 제안한 시스템과 기존의 형상관리 시스템의 특징을 비교하면 다음 표4와 같다.

표 4. 제안시스템 특징
Table. 4 The proposed system features

구분	기존시스템	제안시스템
구조	중앙집중형	분산형
SW설치 위치	서버, 클라이언트	클라이언트
기밀성	X	O
무결성	X	O
가용성	높음	낮음
버전관리	O	Δ (최종버전 관리)

제안 시스템은 중앙집중형태인 기존시스템과 다르게 분산형 구조이다. 이러한 구조로 인해 다음과 같은 특성을 갖는다.

첫째, 기존시스템의 경우 서버와 클라이언트에 형상관리를 위한 프로그램이 설치되어야 하지만, 제안시스템은 클라이언트에만 형상관리 프로그램을 설치/운영하면 된다. 둘째, 기존시스템과 달리 데이터 암/복호화에 따른 데이터의 기밀성 및 무결성을 제공한다. 셋째, 기존 시스템은 서비스 제공자가 형상관리시스템과 스토리지를 함께 제공해야 하지만, 제안시스템은 별도의 형상관리시스템과 스토리지를 제공할 필요가 없다.

넷째, 기존시스템이 모든 문서변경이력과 모든 변경단계에서 데이터가 저장되지만, 제안시스템은 문서변경이력이 남지 않고 최종버전만 관리된다. 다섯째, 제안시스템이 개별 클라이언트에 분산되어 저장됨으로써 클라이언트가 파괴되는 경우 데이터 손실 가능성이 존재한다. 마지막으로, 데이터 암/복호화에 따른 기존의 형상관리 시스템에 비해 성능저하가 있을수 있다.

V. 결 론

본 논문에서는 모바일 사용자간에 공동 작업이 가능하도록 문서를 효율적으로 공유할수 있고, 준동형 암호화 기반의 기밀성과 무결성이 지원되는 형상 관리시스템을 제안하였다.

즉, 모바일 장비를 사용하여 사용자들간에 협업 시, 서비스 제공자의 구조 변경없이 사용자가 프로그램을 설치하여 사용자들간의 형상관리가 가능하고, 기밀성 및 무결성 제공이 가능한 형상관리 시스템을 제안하였다.

본 제안 시스템은 분산형 구조로 가장 최신버전만 관리한다는 측면서에 저용량의 모바일 장비 사용자에게 항상 최신의 자료만 관리할 수 있다는 장점이 있으며, 데이터 손실 및 암호화 성능 저하 부분은 모바일 장비의 지속적인 성능 개선과 준동형 암호 알고리즘 개선을 통해 개선될 것으로 예상한다.

참고문헌

[1] 정지범, “모바일 클라우드 시장 동향 및 시사점” 정보처리학회지, 18(5) pp. 4-10, 2011년 9월.

[2] 조남수, 장구영, “ Homomorphic Encryption의 기술동향 및 전망”, pp.15-25, 정보통신산업진흥원 주간기술동향. 2011.11.18

[3] 송유진, 박광용, “데이터베이스 아웃소싱을 위한 준동형성 암호기술,” 19(3) pp. 80-89, 2009년도 정보보호학회지, 2009.06.

[4] Rivest, Adleman, Dertouzos, "On data bank and privacy homomorphisms", pp169-180, Proceedings of the 19th Annual Symposium on Foundations of Secure Computation-FSC 1978, Academic Press

[5] J.Domingo-Ferrer, "A New privacy homo -morphism and applications", vol. 60, no.5, pp. 277-282, Information Processing letters, Dec. 1996.

[6] Craig Gentry, "Fully homomorphic encryption using ideal lattices", pp.169-178, in Proceedings of the 41st ACM Symposium on Theory of Computing - STOC 2009, ACM, 2009.05

[7] TTA 용어사전, http://word.tta.or.kr

[8] Pascal Paillier, "Public-key cryptosystems based on composite degree residuosity classes", 1999.5, 99.223-238, 1999. LNCS vol.1592 Advanced in Cryptology-Eurocrypt

저자소개

김선주(Sun-Joo Kim)

1998년 2월: 배재대학교 컴퓨터공학과 졸업
2001년 2월: 배재대학교 컴퓨터공학과 석사
2003년 8월 ~ 현재: 한국정보통신기술협회 선임연구원
※관심분야 : 클라우드 컴퓨팅, 암호화, SW테스팅, CC 평가

김진묵(Jin-Mook Kim)

1998년 2월 : 배재대학교 컴퓨터공학과 졸업
2000년 2월 : 배재대학교 컴퓨터 공학과 공학석사
2006년 2월 : 광운대학교 컴퓨터과학과 공학박사
2008년 2월 : 선문대학교 컴퓨터공학부 연구교수
2008년 3월 ~ 현재 : 선문대학교 IT교육학부 조교수
※관심분야:네트워크보안, RFID 보안, 센서 네트워크 보안, 유비쿼터스 보안, 클라우드 서비스 보안

조인준(In-June Jo)

1982년 2월: 전남대학교 계산통계학과 졸업
1985년 2월: 전남대학교 전자계산학과 석사
1999년 2월: 아주대학교 컴퓨터공학과 박사
1983년 ~ 1994년: 한국전자통신연구원 선임연구원
1994년 1월 ~ 현재: 배재대학교 컴퓨터공학과 교수
※관심분야 : 정보보호, 컴퓨터 네트워크 보안, 전산조직응용