OOXML기반의 동적 그룹키를 이용한 전자문서 관리 시스템의 설계

정회원 이 영 구*, 김 현 철**°, 정 택 영**, 전 문 석*

Design of E-Document Management System Using Dynamic Group Key based on OOXML

Young-Gu Lee*, Hyun-Chul Kim**°, Taik-Yeong Jung**, Moon-Seog Jun* ***Regular Members***

요 약

본 논문에서는 접근제어 환경에서 하나의 문서에 대하여 세분화된 페이지 정보를 권한별로 제공할 수 있는 전자문서 관리 시스템을 제안한다. 제안하는 시스템은 일방향의 특성을 가지는 해쉬 체인을 이용해 계층식별자를 생성함으로써 기존 시스템과 달리 모든 사용자의 키 정보를 소유할 필요가 없다. 또한, 해쉬 체인 기반의 계층식별자와 랜덤하게 생성한 그룹식별자를 조합해 그룹키를 생성함으로써 페이지별 대칭키를 이용한 문서 암호화 기법에 키 생성 및 관리 문제를 해결함과 동시에 그룹 구성원 이동에 따른 동적 변화에 유연하게 대처할 수 있다. 마지막으로 실험을 통해 기존 전자문서 관리 시스템과 비교, 분석한 결과 문서 암·복호화 속도, 페이지별 암·복호화 속도에서 우수함을 확인 할 수 있었다.

Key Words : OOXML, E-Document, u-Paperless, Group Key, Hash Chain

ABSTRACT

We propose a e-document management system that can provide segmented page information on a document according to different levels of authority from access control environment. The proposed system creates hierarchy identifier using a one-way hash chain and therefore does not need to own key information for all users as in existing system. Also by creating group keys by compounding hash chain hierarchy identifier with randomly formed group identifier, the system can flexibly respond to dynamic changes from group member movements while at the same time resolving the problems of key formation and management in document encoding technique using symmetric key for each page. Lastly as a result of comparative analysis through an experiment with existing e-document management systems, the proposed system showed superiority in the efficiency of encoding and decoding document and the speed of encoding and decoding by the pages.

Ⅰ. 서 론

정보통신 기술의 눈부신 발전과 초고속 네트워크에 급속한 보급은 정보화 사회 구축을 위한 초석을 마련하였으며, 오프라인 수작업 형태의 업무 환경을 온라인 자동화 형태로 전환하는 계기가 되었다[1].

이와 같은 사회 환경적 패러다임에 변화는 전자적인 방법으로의 업무 대체를 꾀하는 기업을 중심으로 시작되어 현재는 'u-Paperless Korea' 실현을 목표로 범정부 차원에서 추진되고 있다.

* 숭실대학교 컴퓨터학과(ad3927, mjun@ssu.ac.kr)
** 한국과학기술정보연구원 정보화전략팀(dmzpolice, tychung@kisti.re.kr) (° : 교신저자)
논문번호 : KICS2009-09-429, 접수일자 : 2009년 9월 23일, 최종논문접수일자 : 2009년 11월 20일

'u-Paperless'란 유비쿼터스 환경 하에서 전자문서에 이용과 종이문서에 전자적 보관을 촉진하기 위하여 언제, 어디서나 다양한 정보통신 기술을 활용하여 모든 문서의 생산, 유통 및 활용, 이관 및 보관 등의 전 과정에 걸쳐 전자적 처리가 가능한 업무 환경을 의미한다. 이와 같은 u-Paperless 환경의 도래는 종이문서 생산 제로화를 통한 비용절감 및 친환경 산업정보화 조성, 종이문서 전자화 및 전자문서 보관으로 인한 공간 및 관리 비용의 대폭적인 절감, 문서업무 전과정의 전자화를 통한 업무의 효율성과 생산성 증대를 가져온다. 이는 궁극적으로 기업의 경쟁력 강화뿐만 아니라 더 나아가 국가 경쟁력 제고에 이바지 할 수 있다[2]. 그러나 이러한 u-Paperless 환경 도래에 따른 다양한 이점에도 불구하고 그 내면에는 허가받지 않은 사용자로부터의 전자문서 무단 유출 및 불법적인 유통, 파괴, 위·변조 등의 보안상 많은 위협요소를 내포하고 있으며 또한 관리의 어려움도 뒤따르고 있다[3].

한국소프트웨어진흥원 발표자료[4]에 따르면 국내 전자문서 시장은 2008년 30억원에서 2009년 160억원에 이르며 2010년까지 도입 및 안정기를 거쳐 2012년에는 3,000억원에 가까운 시장이 형성될 것으로 예상하고 있으며, 최근 특허청이 2010년 이후 기관내 전자문서에 대한 포맷으로 OOXML(Office Open XML)[5][6]을 사용하기로 결정함에 따라 전자문서 시장의 발전 속도 및 규모의 성장은 가속화 될 것으로 보이며 이로 인한 전자문서 보안에 중요성도 한층 강화 될 것으로 예상된다.

전자문서 보안을 위한 가장 핵심적인 사항은 해당 문서에 대해 송·수신 과정에서 변경되지 않음을 보장하는 무결성, 허가된 사용자만이 문서를 열람할 수 있는 기밀성, 필요시점에 해당 문서를 열람할 수 있는 가용성에 대한 보장이다. 이를 위해 보안성을 확보하기 위한 암호 기술 및 불법복제 방지 기술, 권한 기반 접근제어 기술, 편집기록을 위한 시점확인 기술 및 진위 증명기술 등이 필요하며 이를 다각적으로 적용한 전자문서 보호 기법[3][7][8][9][10]들이 제안되었다. 그러나 대부분의 연구가 전자문서의 기밀성을 위한 것이 아닌 위·변조 및 부인방지와 같은 저작권 관리(DRM : Digital Rights Management) 부분에 국한되어 있으며, 기밀성 유지를 위한 전자문서의 암호화를 모색해야 함에도 불구하고 암호 방식의 무거움과 키 관리의 어려움으로 인해 문서 자체에 대한 직접적인 암호화는 추진하지 못하는 상황이다. 또한, 접근권한에 따른 문서 관리 방안도 부재한 실정이다[11]. 따라서 이러한 사회 환경적 패러다임 변화에 순응하고 보다 안전하고 효율적인 전자문서 서비스를 제공하기 위해서는 문서에 대한 불법적인 접근을 사전에 차단할 수 있는 접근제어 기술, 하나의 문서를 각각의 페이지로 구분하여 처리 할 수 있는 OOXML기반의 문서 처리 기술, 문서 암호화 기술, 키 생성 및 관리 기술 등이 종합적으로 접목된 전자문서 관리 방안에 대한 연구가 가시화 될 필요성이 있다.

본 논문은 접근통제 환경에서의 전자문서에 대한 생성, 유통, 폐기에 이르는 일련의 라이프 사이클 동안에 전자문서의 무결성, 기밀성, 신뢰성, 가용성, 부인방지 등의 보장을 목적으로 한다. 특히 본 연구에서는 전체 문서를 암호화하여 제공하는 기존 방식의 목적 외에 정보 노출 문제를 해결하기 위하여 OOXML처리를 통하여 하나의 문서를 페이지별로 세분화 한 후 페이지에 중요도에 따라 권한을 부여하였고, 키 생성 및 관리의 효율성을 극대화하기 위하여 페이지별로 대칭키를 생성하는 방식이 아닌 권한별로 그룹키를 생성하여 분류된 페이지에 대한 암호화를 행하였다. 이를 통해 불필요한 정보 유출을 방지하고, 문서의 가독성을 향상시키며, 문서 암·복호화에 사용되는 키를 최소화함으로써 전자문서 활용의 효율성 및 보안성을 강화할 수 있는 새로운 전자문서 관리 방안을 제안하고자 한다.

Ⅱ. 관련연구

2.1 문서 전체 암호화를 이용한 보호 모델

문서 전체 암호화를 이용하는 전자문서 보호 모델은 모든 사용자에게 문서에 동일한 부분을 열람할 수 있도록 허용된 환경에 적합한 모델이다[12][13]. 이 모델은 그림 1에서와 같이 하나의 전자문서에 대하여 하나의 대칭키를 이용하여 암호화하고 암호화에 사용된 키는 사용자의 공개키로 암호화 한 후 암호화된 전자문서와 함께 전송하는 방법으로 가장 오래되고 전통적인 방법의 전자문서 보호 모델이다[4]. 이 모델은 하나의 대칭키를 이용하여 전체 문서를 암호화 한다는 점에서 동일한 문서권한, 동일한 사용자권한을 가진 시스템에 이상적이며 생성되는 키의 최소화로 인해 키 관리가 타 모델에 비해 우수하다는 장점이 있다. 그러나 권한이 서로 다른 다중 사용자 환경에서 동일한 문서에 대해 이 모델을 적용할 경우 목적 외에 정보가 노출될 수 있으며, 문서에 부분적인 수정 및 삭제가 불가능 하다는 한계

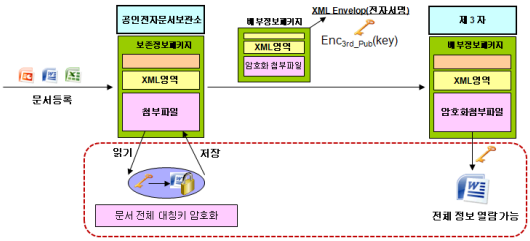


그림 1. 문서 전체 암호화를 통한 전자문서 보호 모델

점도 존재한다.

2.2 슈퍼 암호화 기반의 전자문서 보호 모델

슈퍼 암호화[14][15]를 이용한 전자문서 보호 모델은 하나의 문서를 여러 사용자가 공유할 때 정보의 접근권한 레벨에 따라 가장 중요한 부분을 먼저 하나의 키로 암호화 하고 그 다음으로 중요한 부분을 암호화하는 방법으로 전자문서를 보호한다[16].

그림 2는 슈퍼 암호화 기반의 전자문서 보호 모델을 나타내고 있으며 권한이 서로 다른 사용자 A와 B가 있을 때 사용자 B를 위해 문서의 일부분을 암호화하고 다시 사용자 A와 B를 위해 A의 키로 문서에 대한 암호화를 수행한다. A는 자신의 문서를 얻기 위해 복호화 했을 때 B의 부분을 확인 할 수 없으며, B는 자신의 문서를 얻기 위해 A에 키와 자신의 키를 모두 이용해 복호화를 수행한다[13]. 이 모델은 하나의 문서를 권한별로 세분화하여 암호화함으로써 전체 문서 암호화 모델에 목적 외 정보 노출 문제를 해결한다. 그러나 여러 개의 복수키로 하나의 문서를 중복 암호화함으로써 연산량이 많고 상위 그룹에 사용자는 하위 그룹 사용자에 대한 복호화 키도 모두 소유해야 한다는 점에서 키 관리 및 키 교환의 어려움이 존재한다.

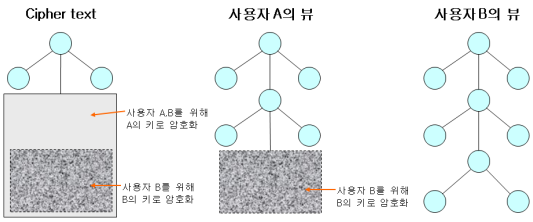


그림 2. 슈퍼 암호화 기반의 전자문서 보호 모델

2.3 다중 암호화 기반의 전자문서 보호 모델

다중 암호화[15]는 슈퍼 암호화 방식의 문제를 해결하기 위해 제안된 방식으로 그림 3과 같이 사전에 각각의 레벨에 맞는 키를 생성하고 접근권한에

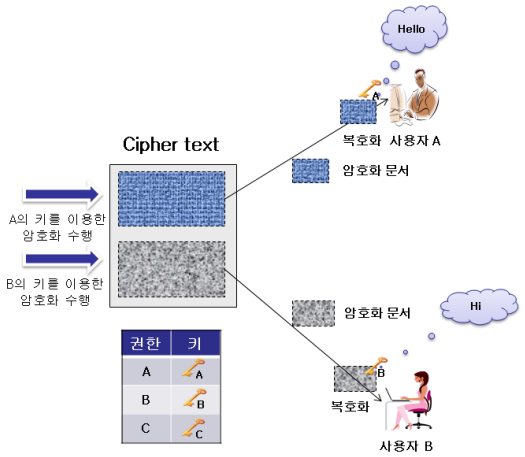


그림 3. 다중 레벨 암호화 기반의 전자문서 보호 모델

따라 필요한 부분만을 암호화하여 전달하는 모델이다[16]. 이 모델은 슈퍼 암호화 모델에 단점인 중복 암호화에 따른 연산량 문제를 해결한다. 그러나 이 모델 역시 슈퍼 암호화 모델과 마찬가지로 상위 그룹 사용자는 하위 그룹의 모든 키들을 관리해야 하는 한계를 지닌다.

2.4 해쉬 체인 키 기반의 전자문서 보호 모델

이 모델은 문서를 권한에 따라 구분하고 각 레벨에 따른 키 생성을 위해 해쉬 함수 기반의 키 체인을 이용한다. 김수희[16]는 이 모델을 이용한 의료정보 보호 방안을 제시하였으며, 박찬길[17]은 멀티미디어 콘텐츠에 대한 보호 방안을 제시하였다.

이 모델은 사용자의 그룹 역할 및 중요도에 따라 문서를 암호화 할 수 있으며, 기존의 기법들과 달리 상위 사용자가 하위 그룹에 모든 키를 소유할 필요가 없다는 장점이 있다. 그러나 그림 4에서와 같이

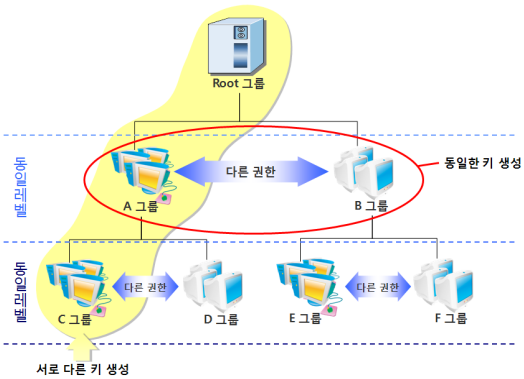


그림 4. 해쉬 체인 키 기반의 전자문서 보호 모델

동일 레벨에 다른 권한을 가진 조직 즉, 이진트리 형식에 그룹 환경에서 서로 다른 권한을 가진 그룹 간에 공통의 키를 가지는 문제가 존재한다. 따라서 하나의 레벨에 여러 개의 권한을 가진 그룹 환경에는 적합하지 않은 모델이다.

2.5 OOXML과 다중 대칭키를 이용한 전자문서 보호 모델

이 모델은 최근 국제표준으로 정의된 OOXML[6]을 통해 하나의 문서를 페이지별로 분리한 후 분리된 각 페이지에 대응되는 대칭키를 생성하여 문서를 암호화하는 모델이다. 이 모델을 응용한 연구로는 OOXML을 이용해 세분화된 페이지에 대하여 각각의 대칭키를 생성하여 암호화를 수행하고 사용자가 문서를 요청할 시점에 복호화 키와 일회용 패스워드를 함께 전송함으로써 키에 안전성 측면을 중시한 김대중[7]의 연구와 랜덤함수를 이용하여 생성한 임의값에 대하여 재배열 과정을 거쳐 대칭키를 생성한 성경상[3]의 연구가 있다.

Ⅲ. 제안하는 시스템

본 논문에서 제안하는 시스템은 문서 제공자에 의한 문서 등록 요청이 발생하면 등록 요청된 하나의 전자문서에 대해 세분화 과정을 거쳐 페이지별로 분류한다. 각각의 분류된 페이지는 사전에 정의해 놓은 규칙에 따라 권한이 부여되고 해당 권한에 따른 동적 해쉬 체인 그룹키(DHCK : Dynamic Hash Chain Key)를 통해 암호화하여 저장한다. 위와 반대로 문서 발급 요청이 발생하면 발급 요청한 사용자 권한을 확인한 후 해당 문서를 사용자의 공개키 User_Pub_Key로 암호화한 후 자신의 개인키 S_Pri_Key로 전자서명을 수행한 암호화 문서 SEPAGES와 문서 암호화에 사용된 키 정보 SEKEY를 사용자에게 전송한다. 사용자는 전달받은 키 정보를 이용해 복호화 키를 생성하고 암호화된 문서를 복호화 함으로써 원본 문서를 획득하게 된다. 본 논문에서 제안하는 전자문서 보호 시스템의 전체적인 구조는 그림 5와 같다.

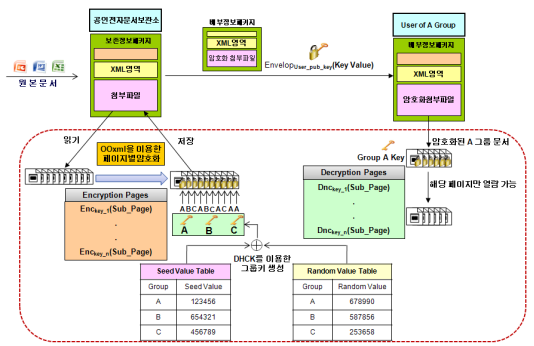


그림 5. 제안하는 시스템 구조

3.1 그룹키 생성 알고리즘

본 논문에서는 해쉬 체인 키 알고리즘을 이용해 계층식별자를 생성하고 키 서버에서 생성하여 그룹별로 부여한 그룹식별자의 논리합 연산을 통해 해당 그룹에 대한 고유 그룹키를 생성한다. 이를 통해 상위그룹 사용자는 하위그룹에 키를 소유하거나 생성할 수 있다.

3.1.1 계층식별자 생성

해쉬 체인 알고리즘은 역함수가 존재하지 않는 일방향성의 특성을 가지는 해쉬 함수를 이용하여 체인 형태의 키를 생성하는 것으로 상위 계층의 값을 통해 하위 계층의 값들을 도출해 낼 수 있으나 그 역계산은 불가능한 키 생성 알고리즘이다. 이러한 해쉬 체인 알고리즘을 통해 생성된 그룹키는 상위 계층 사용자가 하위 계층 사용자의 키를 모두 소유해야 하는 슈퍼 그룹키, 다중 레벨 그룹키 생성 모델의 문제를 해결한다. 그러나 동일한 입력에 대해 동일한 결과 값을 생성하는 해쉬 함수에 특성으로 인해 동일 계층 다른 권한을 가지는 그룹에 대해 동일한 그룹키가 생성된다는 문제가 존재한다.

따라서 본 논문에서는 이러한 해쉬 체인 알고리즘의 특성을 고려해 해쉬 체인 알고리즘을 이용하여 그룹키를 생성하는 것이 아닌 단지 그룹 계층을 구분 짓는 계층식별자를 생성하는 용도로만 사용한다.

그림 6은 해쉬 체인 알고리즘을 이용한 계층식별자 생성 과정으로써 최상위그룹 사용자는 그림 6에

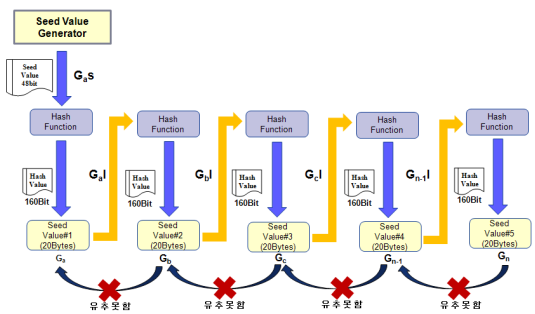


그림 6. 계층식별자 생성 과정

서와 같이 SEED값 생성기를 통해 생성된 초기 SEED값을 입력으로 160비트 크기의 계층식별자를 생성한다. 또한 자신의 계층식별자를 입력으로 자신의 서브그룹에 대한 식별자를 생성할 수도 있다. 이러한 일련의 연속된 과정을 통해 최상위그룹 사용자는 자신보다 하위에 있는 모든 그룹의 대한 식별자를 생성할 수 있게 된다.

그림 6에서와 같이 최상위그룹 G_a가 있다고 가정했을 때 최상위그룹 사용자 U는 SEED값 생성기를 통해 부여받은 초기 SEED값 G_aS에 대하여 해쉬함수를 적용한 계층식별자 G_aI를 생성할 수 있으며 생성된 G_aI를 입력으로 차상위그룹 G_b에 대한 계층식별자 G_bI를 생성할 수 있다. 이와 같은 과정을 반복해 최하위그룹인 G_n에 계층식별자 G_nI 까지 생성할 수 있게 된다.

3.1.2 그룹키 생성

그룹식별자의 생성은 다음과 같은 전제조건을 고려하여야 한다.

전 제 1 : 모든 그룹은 하나의 계층식별자와 하나의 그룹식별자를 가지며 그룹식별자는 랜덤 난수를 이용하여 생성한다.

전 제 2 : 계층식별자와 그룹식별자는 해당 그룹의 사용자 이외에는 비공개 정보이며 그룹식별자는 접근권한에 따라 적절하게 생성하여 관리한다.

전 제 3 : 계층식별자와 그룹식별자의 논리적 연산을 통해 생성된 그룹키 중 일부가 ASCII 코드 값과 충돌이 발생할 위험이 존재한다. 따라서 이러한 충돌을 방지하기 위한 별도의 키 셋 정의가 필요하며, 키 셋은 중복의 위험을 최소화할 수 있을 만큼 충분한 값을 가져야 한다.

본 논문에서 제안하는 그룹키는 해쉬 체인을 이용해 생성한 계층식별자와 그룹별로 부여된 그룹식별자의 논리합 연산을 통해 생성되며, 그룹식별자는 접근통제 매트릭스에 의해 접근권한이 있는 그룹사용자에게만 적절히 공개되어야 한다. 이때 그룹식별자는 해당 그룹의 계층을 구분 짓는 계층식별자와 달리 생성되는 그룹키의 고유성을 만족시키기 위한 요소로 사용된다. 그림 7은 본 논문에서 사용하는 동적 해쉬 체인 그룹키를 생성하는 과정을 보여주고 있다.

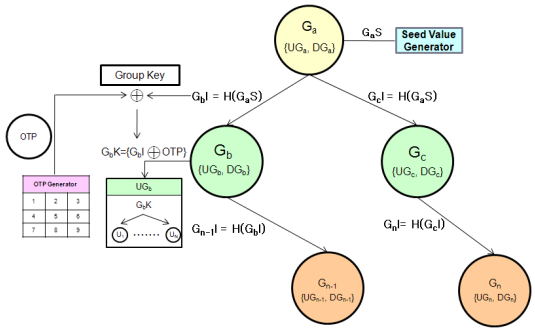


그림 7. 그룹키 생성 과정

3.2 전자문서 암호화 및 저장

그림 8은 본 논문에서 제안하는 시스템의 전자문서 암호화 및 저장 과정을 보여주고 있다.

그림 8에서와 같이 문서 제공자로부터 암호화된 원본 파일을 전송 받은 전자문서 서버는 자신의 개인키와 이용자의 공개키를 이용해 원본 파일을 복호화한 후 OOXML처리[6]를 통해 메타데이터와 OOXML문서로 분류한다. 분류된 OOXML문서는 원본문서를 구성하는 각각의 페이지로 이루어져 있으며 사전에 정의해 놓은 규칙에 따라 각 페이지에 권한이 부여된다. 권한이 부여된 페이지는 사전에 생성해 놓은 그룹키를 이용하여 암호화된 후 저장된다.

그림 9는 본 논문에서 제안하는 시스템의 전자문서 암호화 및 저장을 위한 세부 처리절차를 보여주고 있다.

과 정 1 : 사용자는 X.509 인증서를 통해 사용자 인증을 요청한다.

과 정 2 : 사용자 인증서에 대한 검증을 수행한다.

과 정 3 : 인증서에 대한 검증 결과를 사용자에게 전송한다. 이때 전송되는 검증 결과는

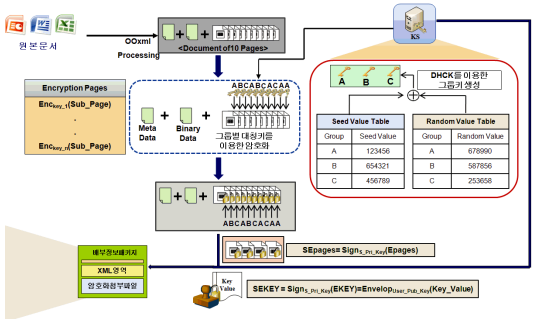


그림 8. 전자문서 세분화 및 암호화

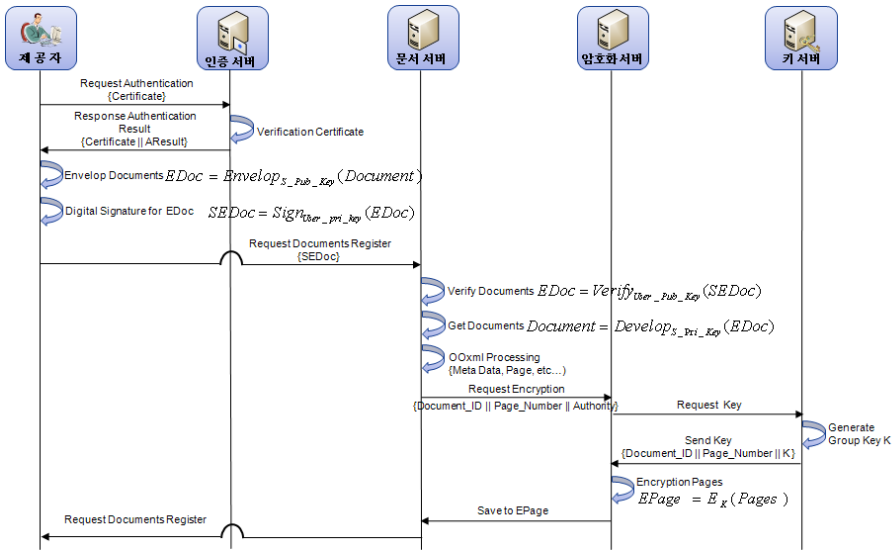


그림 9. 전자문서 암호화 및 저장을 위한 세부 처리 절차

"Good", "Revoked", "Unknown" 세 가지 값 중에 하나를 가진다. "Good"은 인증서가 유효함을 의미하고 "Revoked"는 인증서가 폐기되어 사용할 수 없음을 의미한다. 마지막으로 "Unknown"은 인증서의 존재 유·무를 확인할 수 없는 경우를 의미한다.

과 정 4 : 사용자는 저장하고자 하는 원본 문서에 대하여 서버의 공개키를 이용해 암호화를 수행한 암호화된 전자문서 EDoc를 생성한다.

$$EDoc = Envelop_{S\_Pub\_Key}(Document) \quad (1)$$

과 정 5 : 사용자는 저장을 요청하는 문서가 원본임을 증명하기 위해 암호화된 문서 EDoc에 대하여 자신의 개인키 User_Pri_Key를 이용해 전자서명을 수행한다.

$$SEDoc = Sign_{User\_Pri\_Key}(EDoc) \quad (2)$$

과 정 6 : 전자서명된 문서 SEDoc에 대한 저장을 서버에게 요청한다.

과 정 7 : 서버는 요청 받은 전자서명된 문서 SEDoc에 대하여 사용자의 공개키 User_Pub_Key를 이용하여 전자서명 검증을 수행한다.

$$EDoc = Verify_{User\_Pub\_Key}(SEDoc) \quad (3)$$

과 정 8 : 검증된 문서 EDoc에 대하여 서버 자신의 개인키를 이용해 복호화를 수행하고 원본 문서를 획득한다.

$$Document = Develop_{S\_Pri\_Key}(EDoc) \quad (4)$$

과 정 9 : 문서 모듈은 획득한 원본 문서에 대하여 OOXML처리를 수행 한 후 메타데이터, 바이너리데이터, 자료데이터로 분류한다. 이 과정을 통해 하나의 원본 문서를 각각의 페이지별로 세분화 할 수 있다.

과 정 10 : 문서 모듈은 암호화 모듈에게 세분화된 문서에 대한 암호화를 요청한다.

과 정 11 : 암호 모듈은 키 생성 모듈에게 그룹키 생성을 요청한다.

과 정 12 : 키 생성 모듈은 요청받은 문서에 대한 계층식별자와 그룹식별자를 이용해 그룹키를 생성한다.

과 정 13 : 생성한 그룹키를 암호화 모듈로 전송한다

과 정 14 : 암호화 모듈은 전송받은 그룹키를 이용해 세분화된 각각의 페이지에 대하여 암호화를 수행한다.

$$EPages = E_K(Pages) \quad (5)$$

과 정 15 : 암호화된 문서를 저장한다.

과 정 16 : 사용자에게 문서가 정상적으로 저장됨을 전송한다.

3.3 전자문서 발급 및 복호화

각각에 문서는 OOXML처리를 통해 세분화한 후 그룹키로 암호화하여 저장되어 있고 사용자가 문서 발급을 요청 했을 때 사용자 그룹에 일치하는 문서와 키 생성 정보를 선별적으로 제공하게 된다.

그림 10은 문서 제공자로부터 수신한 키 정보를 이용하여 암호화된 전자문서를 복호화 하는 과정으로써 사용자는 서버로부터 전송받은 키 정보를 이용해 암호화된 문서에 대해 복호화를 수행하고 OOXML문서를 획득한다. 획득한 OOXML문서에 대해 OOXML처리를 수행하고 최종적으로 세분화된 페이지를 획득한다.

과 정 1 : 사용자는 X.509 인증서를 통해 사용자 인증을 요청한다.

과 정 2 : 사용자 인증서에 대한 검증을 수행한다.

과 정 3 : 인증서에 대한 검증 결과를 사용자에게 전송한다.

과 정 4 : 사용자는 원하는 문서에 대해 발급을 요청한다.

과 정 5 : 문서 모듈은 인증 모듈에게 문서 발급을 요청한 사용자에 대한 권한을 요청한다.

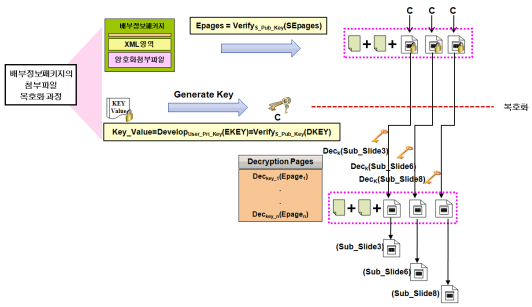


그림 10. 전자문서 발급 및 복호화 과정

과 정 6 : 인증 모듈은 문서 모듈에게 사용자 권한을 응답한다.

과 정 7 : 문서 모듈은 인증 모듈로부터 수신한 사용자 권한을 토대로 키 생성 모듈에 그룹키 생성을 위한 키 정보를 요청한다.

과 정 8 : 키 생성 모듈은 문서 모듈로부터 전송받은 사용자 권한을 토대로 권한에 맞는계층식별자와 그룹식별자를 데이터베이스로부터 가져온다.

과 정 9 : 키 생성 모듈은 계층식별자와 그룹식별자를 사용자의 공개키로 암호화한 후 자신의 개인키를 이용하여 전자서명을 수행한다.

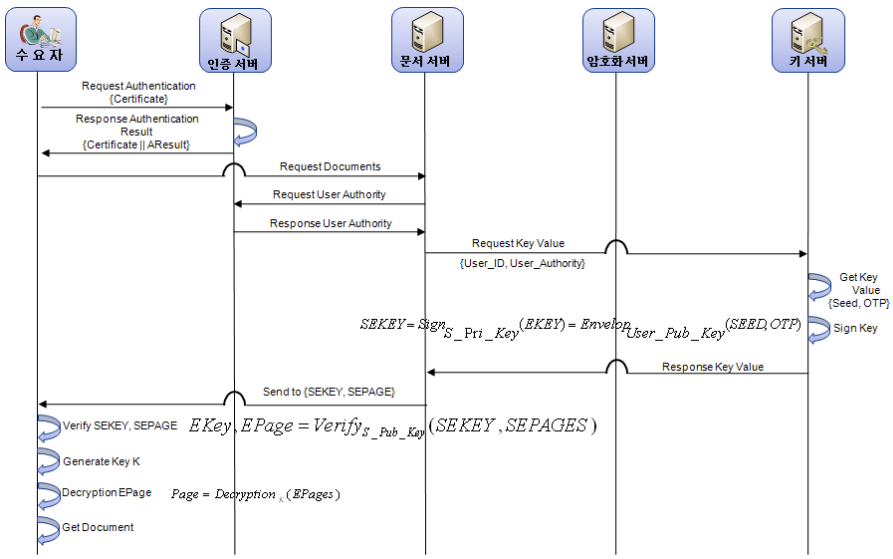


그림 11. 전자문서 발급 및 복호화를 위한 세부 처리 절차

$$SEKEY = Sign_{S\_Pri\_Key}(EKEY) = Envelop_{User\_Pub\_Key}(SEED, OTP) \quad (6)$$

과 정 10 : 암호화된 키 정보를 문서 모듈에게 전송한다.

과 정 11 : 문서 모듈은 전자서명된 암호화 문서 SEPAGES와 전자서명된 키 생성 정보 값 SEKEY를 사용자에게 전송한다.

과 정 12 : 사용자는 서버의 공개키를 이용하여 전송받은 SEPAGES와 SEKEY에 대하여 검증을 수행한다.

$$EKey = Verify_{S\_Pub\_Key}(SEKEY) \quad (7)$$

$$EPages = Verify_{S\_Pub\_Key}(SEPAGES) \quad (8)$$

과 정 13 : 사용자는 자신의 개인키를 이용하여 키 생성 정보를 획득하고 그룹키를 생성한다.

$$SEED, OTP = Develop_{User\_Pri\_Key}(Ekey) \quad (9)$$

$$KEY = SEED \oplus OTP \quad (10)$$

과 정 14 : 사용자는 생성한 그룹키를 통해 암호화된 문서에 대해 복호화를 수행하여 OOXML 문서를 획득한다.

$$Pages = Decryption_K(EPages) \quad (11)$$

Ⅳ. 실험 및 비교분석

4.1 실험 환경

제안하는 기법의 성능 평가를 위한 시스템은 Visual C# 2008과 MS-SQL 2008을 이용하여 구현하였고 정보 전송을 위한 통신 프로토콜은 단순 객체 접근 프로토콜(SOAP : Simple Object Access Protocol)을 사용하였다. 전송되는 키 값의 기밀성을 확보하기 위하여 RSA 공개키 알고리즘과 AES 대칭키 알고리즘을 각각 적용하였다. 마지막으로 실험은 Intel(R) Core2 Quad Q6600 2.40GHz, 2048M RAM의 PC에서 MS-Windows XP Professional Service Pack 3 운영체제 하에서 수행하였다.

4.2 실험 개요

문서 암·복호화 실험에서는 점진적으로 데이터를 증가해가면서 용량 및 페이지 변화에 따른 암·복호화 시간을 측정하였다. 문서 암·복호화를 위한 암호화 알고리즘으로는 AES를 사용하였으며 암호화키는 동적으로 생성한 동적 그룹키(동적 해쉬 체인키)를 사용하였다.

전자문서 암·복호화에 따른 수행시간을 측정하기 위하여 대표적인 전자문서 기법인 전체 문서 암호화, 최근 연구되어 발표된 OOXML대칭키 기법, 그리고 제안하는 동적 해쉬 체인 기법으로 한정하였다. 세부비교 항목으로는 전자문서 전체 암·복호화에 따른 수행시간과 페이지별 암·복호화 수행시간에 대하여 비교 분석하였다.

4.2.1전자문서 암호화 수행시간

그림 12는 전자문서 암호화에 소요된 시간을 측정하여 10페이지 단위로 구분해 표현한 결과로써 소요된 시간은 키 생성 시간을 제외한 문서 암호화 시간만을 측정하였다.

그림 12에서 확인 할 수 있듯이 전체 문서 암호화의 경우 문서 전체를 하나의 키로 암호화하기 때문에 비교 실험 대상인 다른 기법과 달리 암호화에 소요되는 시간이 다소 오래 걸림을 확인 할 수 있다. OOXML대칭키 기법의 경우 페이지별로 대칭키를 생성한 후 페이지별로 암호화를 수행하기 때문에 전체 문서 암호화에 비해 암호화에 소요되는 시간이 현격하게 줄어들었음을 확인 할 수 있다. 본 논문에서 제안한 동적 해쉬 체인 기법의 경우 각 그룹에 따른 문서에 대한 암호화 시간을 측정하였으며 그 결과 비교 대상인 다른 기법에 비해 암호화에 소요되는 시간이 다소 감소하였음을 확인할 수 있다. 그림 13은 페이지별 암호화 수행 시간을 측정한 결과를 보여주고 있다.

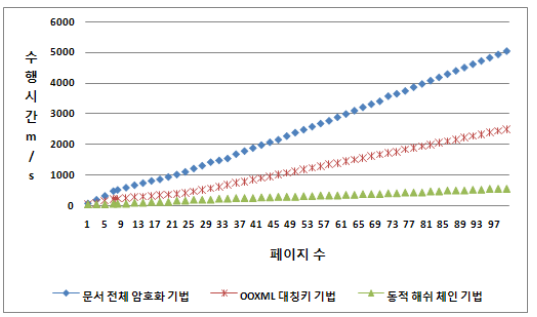


그림 12. 전체 문서 암호화 수행 시간

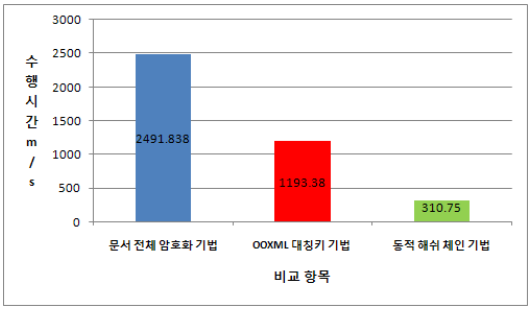


그림 13. 페이지별 암호화 수행 시간

그림 13에서 확인 할 수 있듯이 문서 전체 암호화의 페이지별 암호화 소요 시간은 다른 기법에 비해 높은 편이며 제안하는 동적 해쉬 체인 기법의 페이지별 암호화 시간은 상대적으로 매우 낮음을 확인할 수 있다.

4.2.2 전자문서 복호화 수행시간

그림 14는 전자문서 복호화에 소요된 시간을 측정하여 10페이지 단위로 구분해 표현한 것으로써 소요된 시간은 키 생성 시간을 제외한 문서 복호화 시간만을 측정하였다.

먼저 전체 문서 복호화에 경우 암호화된 전체 문서에 대하여 복호화를 수행하기 때문에 다른 기법에 비해 복호화 속도가 오래 걸림을 확인 할 수 있다.

OOXML대칭키 기법의 경우 사용자가 원하는 암호화된 페이지만을 제공하고 이에 대해서만 복호화를 수행하기 때문에 복호화 수행시간이 대폭 감소함을 확인 할 수 있다. 마지막으로 제안하는 동적 해쉬 체인 기법은 최고 권한이 설정되어 있는 암호화된 문서에 대해서만 복호화를 수행하기 때문에 비교 대상인 다른 기법에 비해 복호화 시간이 다소 적게 소요됨을 확인 할 수 있다.

그림 15는 페이지별 복호화 수행 시간으로 제안

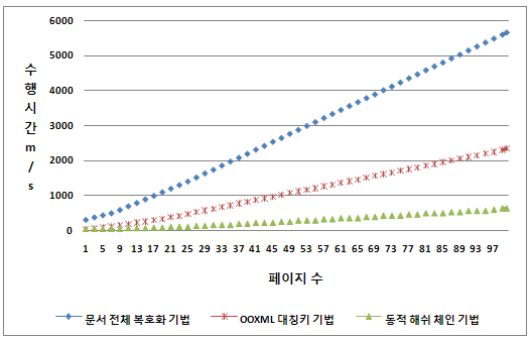


그림 14. 전체 문서 복호화 수행 시간

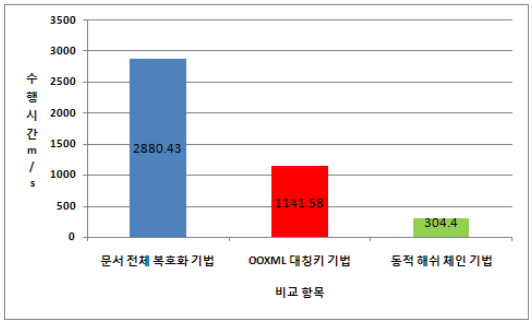


그림 15. 페이지별 복호화 수행 시간

하는 동적 해쉬 체인 기법의 페이지별 복호화 시간이 비교 대상인 다른 기법에 비해 상대적으로 매우 적음을 확인할 수 있다.

V. 결 론

본 논문에서는 조직 구성원에 이동이 빈번한 접근제어 환경에서의 효율적인 전자문서 관리를 지원하기 위한 새로운 방안을 제안하였으며 제안하는 알고리즘에 입각하여 시스템을 구현하였고, 성능 평가를 위해 기존의 전자문서 기법인 전체문서 암호화, OOXML 대칭키 기법과의 문서 암·복호화 부분에 대한 실험 및 비교 분석을 수행하였다.

먼저 입력 값의 연관성을 기반으로 연속적인 키를 생성하는 해쉬 체인 알고리즘을 통해 그룹의 계층을 구분하는 계층식별자를 생성함으로써 기존의 상위 권한 소유자로 하여금 모든 하위 권한에 키 정보를 소유해야 하는 키 관리 문제를 해결하였으며, 계층식별자와 랜덤하게 생성한 그룹식별자의 조합을 통해 동일 레벨 다른 권한을 가지는 그룹에 대한 고유키를 생성함으로써 조직 구성원 이동에 따른 동적 변화에 유연하게 대처 할 수 있도록 하였다. 또한, 최근 국제 전자문서 표준 ISO/IEC DIS 29500[6]으로 지정된 OOXML을 적용하여 전자문서를 생성하고 처리함으로써 전자문서의 부분 암호화 및 저장, 전자문서의 부분 발급 및 복호화, 전자문서의 부분 수정 및 삭제 등의 기능을 제공함과 동시에 OOXML을 지원하는 모든 문서에 적용 가능하도록 호환성 측면도 고려하였다.

성능 부분에 있어서도 기존의 전자문서 관리 기법과의 실험을 통한 비교 분석 결과에서 확인할 수 있듯이 제안하는 기법은 문서 암·복호화 속도, 페이지별 암·복호화 속도 등과 같은 여러 항목에서 기존 기법보다 우수함을 확인 할 수 있었다. 또한,

전체 문서를 하나의 파일로 제공하는 기존 기법과 달리 문서 요청자 권한에 부합하는 페이지만을 암호화하여 제공함으로써 가독성 향상 및 전자문서에 대한 보안을 강화할 수 있다.

향후에는 다른 전자문서 표준인 ISO/IEC 26300[18] 개방형 문서 포맷(ODF : Open Document Format)과 현재 국내 전자문서 포맷으로 사용되고 있는 ISO/IEC 19005-1 PDF/A-1(PDF for Archives Version 1)[19]과의 호환성 문제를 해결하기 위한 지속적인 연구가 요구된다.

참 고 문 헌

〔1〕 김현철, 김정재, 이종희, 오해석, 전문석, "서명자의 신원정보 해쉬값을 이용한 실시간 인증서상태 검증 메커니즘의 설계", 한국정보처리학회논문지, Vol13-C No.02, pp.147-154, 2006.

〔2〕 한국전자문서산업협회, "저탄소녹색성장과기업 경쟁력강화방안", u-paperlessKoreaforum2008, 2008.

〔3〕 성경상, "난수 재배열 기반의 키 관리 방안을 이용한 전자문서 암호화에 관한 연구", 경원대학교 대학원박사학위논문, 2009.

〔4〕 한국소프트웨어진흥원, "전자문서 시대를 앞당기는 공인전자문서보관소", 한국소프트웨어진흥원SW산업동향, 2008.

〔5〕 Office Open XML File Formats, 2008.

〔6〕 ISO/IEC DIS 29500.

〔7〕 김대중, "전자문서 보관 및 발급 서비스의 안정성 확보를 위한 시스템설계", 숭실대학교대학원박사학위논문, 2008.

〔8〕 변창우, "세밀한 XML문서 접근제어를 위한 효율적이고 안전한 질의재작성 기법", 서강대학교 대학원박사학위논문, 2007.

〔9〕 비씨큐어, "공인전자문서보관소보안및핵심솔루션소개", 2007.

〔10〕 한국전자거래진흥원, "공인전자문서보관소 구축방안 연구", 2003.

〔11〕 최훈일, 정창훈, 장영건, "원격 관리 서버 기반의 홈 네트워크 사용자인증 및 접근제어 시스템 설계 및 구현", 한국정보처리학회논문지, Vol14-D No.05, pp.545-554, 2007.

〔12〕 Gildas Avoine, Philippe Oechslin, "A Scalable and Provably Secure Hash-Based RFID Protocol", Third IEEE International Conference on Pervasive Computing, pp.110-114, 2005.

〔13〕 John Linn, "Trust Models and Management in Public Key Infrastructures", Technical Notes and Reports of RSA Laboratories, 2000.

〔14〕 Donald E.Eastlake Ⅲ, and Kity Niles, Secure XML : The New Synax for Signatures and Encryption, Pearson Education, 2003.

〔15〕 Takeshi Imamura, Blair Dillaway, Ed Simon, "XML Encryption Syntax and Processing", W3C Recommendation, 2002.

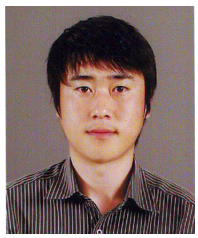
〔16〕 김수희, "의료 환경에 적용 가능한 웹서비스 보안 및 키 관리 기술 연구", 세종대학교대학원석사학위논문, 2007.

〔17〕 박찬길, 김정재, 이경석, 전문석, "DRM시스템에서 해쉬체인과 세션키교환을 이용한 암호화 기법에 관한연구", 한국정보처리학회논문지, Vol13-c No.07, pp.843-850, 2006.

〔18〕 ISO Information technology -- Open Document Format for Office Applications v1.0 ISO/IEC 26300:2006, 2006.

〔19〕 Document management -- Electronic document file format for long-term preservation -- Part 1PDF/A Standard(ISO 19005-1 :

이 영 구 (Young-Gu Lee) 정회원



2003년 숭실대학교 전자계산원
2006년 숭실대학교 컴퓨터학과 석사
2007년~현재 숭실대학교 컴퓨터학과 박사과정
<관심분야> 인터넷 보안, PKI, DRM

김 현 철 (Hyun-Chul Kim) 정회원

2003년 인제대학교 정보컴퓨터학부
2005년 경원대학교 전자계산학과 석사
2009년 숭실대학교 컴퓨터학과 공학박사
2009년 5월~현재 한국학기술정보연구원 정보화전략팀 선임연구원
<관심분야> 공전소, DRM, 보안 정책 및 전략

정 택 영 (Taik-Yeong Jung) 정회원

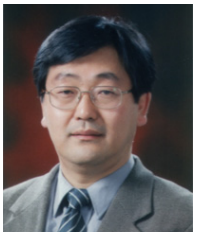
1986년 한국과학기술원 대학원 이학석사

2002년~현재 광운대학교 경영정보학과 박사과정

1986년~현재 한국과학기술정보연구원 정보화전략팀 책임연구원

<관심분야> IT전략, BSC, ERP, EA, Project Management

전 문 석 (Moon-Seog Jun) 정회원



1981년 숭실대학교 전산학과

1986년 University of Maryland 전산학 석사

1989년 University of Maryland 전산학 박사

1991년~현재 숭실대학교 컴퓨터학과 교수

<관심분야> Network Security, 정보보호, DRM