OOXML 기반의 안전한 문서관리 시스템 설계

이영구*, 김현철*, 김정재*, 전문석*
*숭실대학교 컴퓨터학과
e-mail:securityhckim@gmail.com

Design of a Secure Document Management System Based on OOXML

Young-Gu Kim*, Hyun-Chul Kim*,
Jung-Jae Kim*, Moon-Seog Jun*
*Dept of Computer Science, SoongSil University

요 약

본 논문에서는 권한이 없는 불법적인 이용자로부터의 전자문서 유출을 사전에 차단하기 위한 문서관리 시스템을 제안한다. 이를 위해 각 문서를 OOXML을 이용하여 페이지별로 분리하고 분리한 페이지에 대하여 각각의 대칭키로 암호화하여 저장한다. 암호화된 문서의 복호화를 위해 각각의 대칭키를 랜덤하게 생성한 OTP로 암호화하여 서버의 개인키로 전자서명 한 후 사용자의 공개키로 암호화하여 전송한다. 사용자는 자신의 개인키를 이용하여 대칭키를 획득하여 문서를 복호화하여 열람할 수 있다.

1. 서론

최근 정보통신 기술과 인터넷 사용의 보편화는 오프라인 수작업 형태의 업무형태를 디지털 온라인 형태로 변화되어 가고 있으며 이러한 업무 형태의 변화는 종이문서를 대체할 전자문서의 도입을 촉진하는 계기가 되었다.

종이문서는 기업 활동이 확대되면서 지속적으로 보관량이 증가하고 있고, 조직개편 및 담당자 이동에 따라 분류・검색・참조가 시간이 지남에 따라 어려워진다. 이러한 시간・비용・노력의 투입에도 불구하고 분쟁해결과 자료제출에 활용되는 비율은 매우 낮다[1].

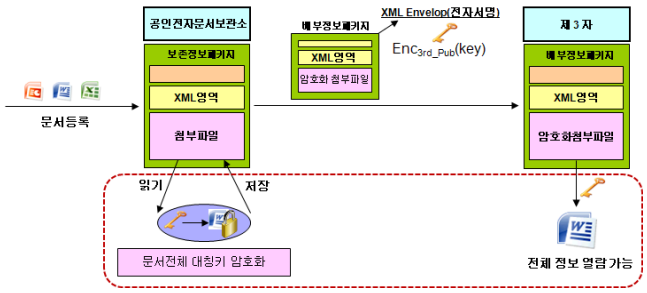
이러한 종이문서를 전자문서로 대체하면 종이문서 보관에 필요한 문서 창고를 점진적으로 감축할 수 있게 됨은 물론 검색・활용이 온라인상에서 가능하게 되어 시간과 비용을 획기적으로 절약할 수 있다. 따라서 전자문서 활용은 기업 등의 업무처리의 효율성・신속성 등을 제고함으로써 경쟁력 제고에 핵심 요인의 하나이다[2][3].

본 논문에서는 전자문서 보관 및 발급 서비스를 이용 시, 이용자가 전자문서를 등록한 후 향후 제 3자에게 발급하는 과정에서 등록된 전체의 정보가 아닌 부분정보 발급을 통해 불필요한 정보유출을 방지하고, 문서의 가독성을 향상시키며, 문서 암・복호화 키 분실 시에도 정보유출을 최소화함으로써 공전소에 등록된 문서의 정보보호를 강화할 수 있는 시스템을 제안하고 설계한다.

2. 전자문서 보호 기법

2.1. CEK(Contents Encryption Key) Scheme

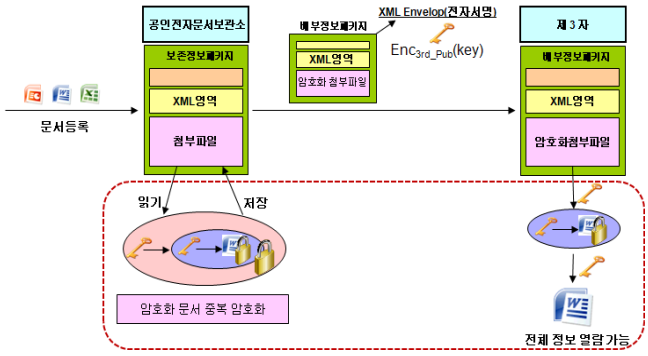
이 기법은 하나의 문서당 하나의 키만을 이용하여 문서를 암복호화는 방법이다. 따라서, 이 방법은 키 관리 및 교환이 용이하다는 장점을 가진다. 그러나 전체 문서를 암복호화함으로서 문서 암복호화에 소요되는 시간이 오래 걸리며 전체 정보 열람으로 인한 목적외 정보가 노출된다는 문제를 가지고 있다. 또한 문서의 부분적인 수정 및 삭제가 불가능하다는 단점도 있다. [그림 1]은 CEK 방법의 전체적인 구조를 보여주고 있다.



[그림 1] CEK 기반의 문서관리 기법

2.2. SCEK(Super Contents Encryption Key) Scheme

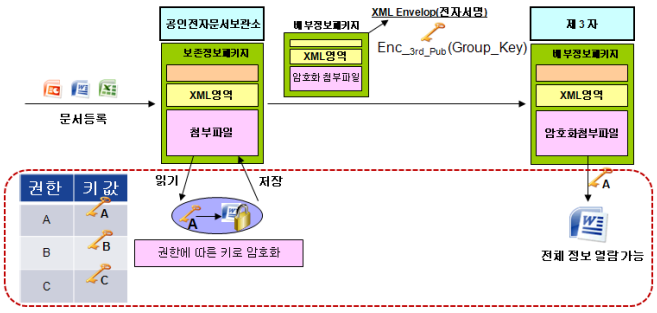
이 기법은 문서를 하나의 대칭키로 암복화를 한 후 다시 권한 별 키로 문서를 암호화하여 사용하는 방법이다. 권한별로 문서의 열람을 제안한다는 장점을 가지지만 하나의 문서당 여러개의 복수키가 필요하며 문서의 다중 암복호화의 따른 연산량증가의 문제가 존재한다. 또한 문서의 부분적인 수정 및 삭제가 불가능하다는 단점이 있다. [그림 2]는 SCEK 기반의 문서 암호 기법 구조를 보여주고 있다.



[그림 2] SCEK 문서관리 기법

2.3 MLCEK(Multi Level Contents Encryption Key) Scheme

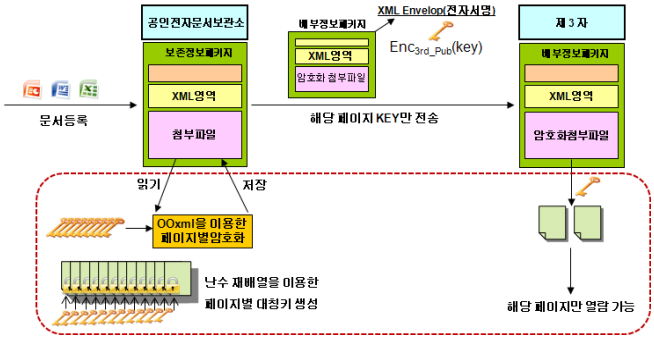
이 기법은 권한별로 키를 사전에 생성한 다음 문서 권한에 따른 키를 분배하는 방식이다. 이 기법은 권한에 따른 사용자에게만 문서를 제공한다는 장점이 존재한다. 그러나 상위 권한을 가진 사용자는 하위 사용자 권한의 대한 키를 확보하고 있어야 되며 이로 인해 키 관리 및 교환이 어렵다는 문제가 존재한다. 또한 문서의 부분적인 수정 및 삭제가 불가능하다는 단점이 존재한다. [그림 3]은 MLCEK 방법의 대한 구조를 보여주고 있다.



[그림 3] MLCEK 기반의 문서관리 기법

2.4 RRM(Random Number Rearrangement) Management

이 기법은 OOXML을 이용하여 문서를 각 페이지별로 분류하고 분류한 페이지에 대하여 랜덤한 대칭키를 생성하여 암복호화에 사용한다. 그러나 각 페이지에 따라서 암호화키와 복호화 키를 생성하기 때문에 키 생성량이 기하급수적으로 증가하며 키 관리의 대한 어려움도 존재한다. [그림 4]는 RRM 기반의 문서 관리 기법의 구조를 보여주고 있다.

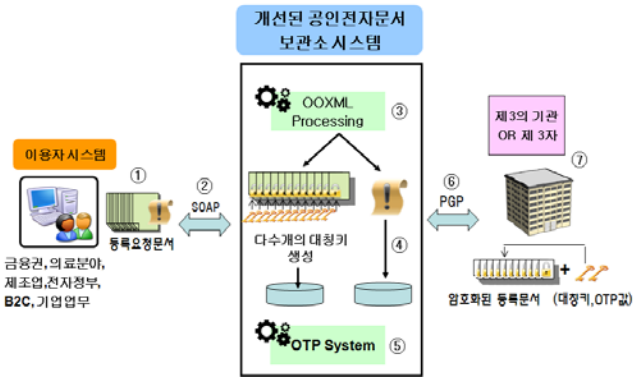


[그림 4] RRM 기반의 문서 관리 기법

3. OOXML 전자문서 시스템

3.1 제안시스템 개요

제안시스템은 [그림 5]와 같이 공전소의 기능 강화를 통하여 이용자시스템에서 등록 요청된 문서를 이용자가 정하는 기준에 따라 세분화하고, 각각 서로 다른 대칭키를 이용하여 암호화한 후 보관하여, 향후 제 3의 기관 혹은 제 3자에게 발급될 시 이용자가 원하는 정보만 공개될 수 있도록 함으로써, 문서 등록자의 정보보호를 강화하는데 목적이 있다.



[그림 5] 전자문서 등록 및 발급업무 처리 흐름도

① 이용자시스템에서 문서 등록을 요청 한다.
② 전자문서의 전송은 SOAP을 통해 이루어진다.
③ 등록 요청된 문서는 OOXML 처리 과정을 거쳐서 이용자의 분류 기준에 따라 세분화 된다.
④ 세분화된 문서는 각각 서로 다른 대칭키에 의해 각각 암호화 된 후 저장된다.
⑤ 이용자로부터 문서발급 요청시 생성된 OTP 값을 복호화용 대칭키와 함께 전송함으로써 키가 유출되더라도 발급된 문서의 정보보호를 강화한다.
⑥ 문서를 메일로 발급할때 PGP(Pretty Good Privacy)를 통해 이루어진다.
⑦ 문서를 제 3자에게 발급할때 대칭키, OTP값과 같이 2개의 복호화용 키가 암호화된 문서와 함께 전달됨으로써 보안이 강화된 문서가 전달된다.

기존의 공인 전자문서 보관소와 본 논문에서 제안하는 시스템과의 개선된 차이점은 [표 1]과 같다.

[표 1] 기존 시스템의 개선점

구 분	기존시스템	제안시스템
문서 보관 방법	전체 문서를 일괄 보관	내용별로 세분화 하여 보관
등록된 문서 중 일부 문서만 선별 발급	불가	가능
문서발급 후 가독성	-	선별발급 시 뛰어남
키 분실 시 문서 내용 유출 가능성	문서 전체 유출	일부분만 유출
등록자의 사생활 보호	-	부분정보 발급을 통한 보호 가능

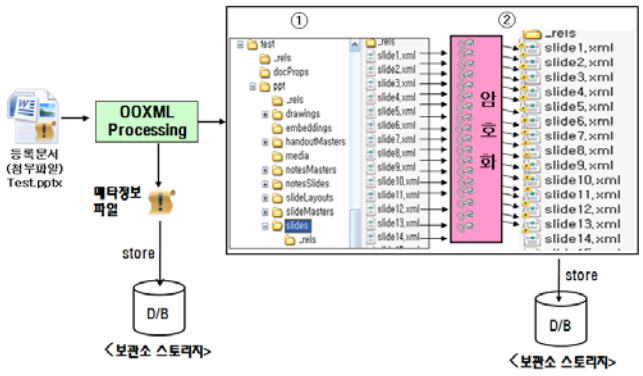
첫째, 등록 요청된 문서 전체가 하나의 파일로 암호화되어 저장되는 것이 아니라, [그림 5]의 ③,④에서와 같이 이용자의 분류기준에 의해 여러 개의 파일로 세분화된 후 각각 암호화되어 저장됨으로서 향후 등록된 문서 중 일부 문서 발급이 가능해지고, 보안이 강화된다.

둘째, [그림 5]의 ⑤와 같이 문서가 발급될 때 생성된 OTP 값이 발급문서의 암·복호화에 사용되므로, 문서가 발급될 시 같이 제공되는 복호화용 키가 유출 시에도 OTP값의 재사용이 불가능하므로 발급된 문서의 정보보호가 강화된다.

3.2 OOXML 기반의 문서 암호화

첫째, 등록 요청된 전자문서의 압축을 풀게 되면 [그림 6]의 ①과 같이 PPT\Slides 폴더에 각각의 페이지 내용 슬라이드가 포함되어 있으며, ②와 같이 각각 슬라이드 별로 서로 다른 대칭키에 의해 암호화되어 저장된다.

둘째, [그림 6]의 ①과 같이 PPT/Media 폴더의 내용에는 문서에 첨부되어 있는 모든 그림파일, 동영상 파일등이 저장되어 있으며, 이 파일 역시 PT\Slides 폴더에 있는 파일과 같은 방법으로 키를 생성한 후, Rijndael 256Bits 암호화를 수행하며, 데이터를 저장하게 된다. 여기서 암호화 키는 키 생성 모듈을 통해 키를 생성하고, 해당키를 통해 Rijndael 256Bits 암호화 방법을 수행하게 된다.



[그림 6] OOXML 기반의 문서 세분화 및 암호화

3.3 OOXML 기반 문서 부분 복호화

OTP를 이용하여 공전소에 등록된 전자문서 중 일부 문서가 제 3자에게 발급되는 세부처리 과정을 [그림7]과 같이 전자문서에 Link 키가 실제 삽입되는 과정을 통하여 표현하였으며, 세부내역은 다음과 같다.

① OTP 값을 생성한다.
② 이용자가 100페이지의 등록문서 중 3, 10, 23 페이지의 부분문서 발급을 요청했으므로, 시작 페이지인 3페이지 하단부에 10페이지 Link 정보

를 문서 발급시 생성된 OTP 값을 이용하여 계산된 값 (“10페이지 Link 정보 = 3페이지 복호화 키 ⊕ 10페이지 복호화 키⊕ OTP 값”)을 삽입한다.

③ 두번째 페이지(10페이지) 하단에는 시작 페이지와 마찬가지로 계산된 다음 페이지 Link 정보 값(“23페이지 Link 정보 = 3페이지 복호화 키 ⊕ 23페 이지 복호화 키 ⊕ OTP값”)을 삽입한다.

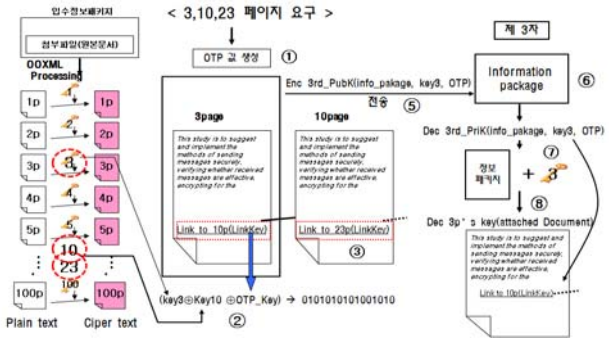
④ 마지막 페이지에는 Link 정보가 없다.

⑤ 발급할 문서에 대한 준비가 끝나면, 이용자에게 100여개의 서로 다른 대칭키로 암호화된 발급문서, 시작페이지 복호화 키값, 실시간으로 생성된 OTP값, 3개의 정보를 공개키로 암호화하여 전송한다.

⑥ 이용자시스템에서 갖고 있는 개인키를 이용하여 “첫 페이지 복호화키, 공전소로부터 제공받은 OTP 값”을 복호화 한다.

⑦ 10페이지 Link 정보와 23페이지 Link 정보 및 OTP값을 이용하여 10, 23페이지를 복호화 할 수 있는 키를 얻는다.

⑧ 얻어진 복호화용 3개의 대칭키로 각각 암호화된 해당 문서를 읽는다.

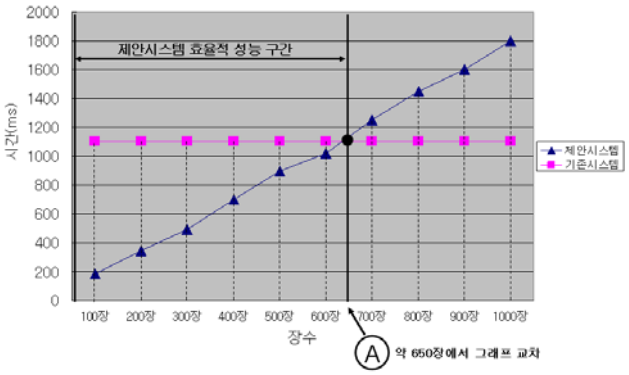


[그림 7] OTP를 이용한 전자문서 부분발급

4. 실험 및 분석

본 논문에서 실험 평가를 위해 63Kbytes 크기의 실제 사용되는 전표 스캔 문서 1000장을 데이터로 사용하였고, 기존시스템에서의 암호화 방법은 1024 Bit의 공개키 및 개인키를 사용하였다. 제안시스템 역시 1024 Bit의 공개키 및 개인키를 사용하였으며, 문서를 암호화할 대칭키 암호화는 AES 암호화 방법을 사용하여 평가를 수행하였다.

암호화에 대한 시간을 비교 분석한 결과는 [그림 4-3]과 같이 기존시스템의 1,000장 전체 암호화를 기준으로, 제안시스템은 [그림 8]의 Ⓐ와 같이 약 650장을 초과하면서 암호화 시간이 제안시스템보다 증가하기 시작했으며, 다른 데이터인 수표 이미지 데이터를 사용하여 다시 측정한 결과 기존시스템 1,000장 암호화를 기준으로 평균 600~700장 사이에서 기존시스템보다 제안시스템 암호화 시간이 증가하기 시작했다.



[그림 8] 기존시스템과 제안시스템의 암호화 시간 비교

수표 이미지 데이터를 이용하여 측정을 하였을 경우에도 마찬가지로 600~700장 사이에서 제안시스템 그래프와 기존시스템 그래프가 교차했다.

5. 결론

제안시스템을 설계하고 구현한 후 성능 평가를 위해 실 사용되는 다양한 크기의 이미지 파일을 이용하여 시스템 성능평가를 위한 실험을 수행하였다. 제안시스템은 부분정보 발급을 목적으로 하였기 때문에 전체파일을 복호화 하는 기존시스템 방법과 비교하여 전체 파일의 60%~70% 이내에서는 효율적이지만, 이용자가 등록된 전체 문서의 발급을 요청할 경우에는 오히려 기존시스템의 복호화 방법이 더 효율적이다. 제안시스템이 부분정보 발급 목적으로 사용되어 약 60%~70% 이내의 부분정보 발급 요청에 대해서는 상당히 효율적이라 판단된다.

참고문헌

[1] 한국전자거래진흥원, “공인전자문서보관소 구축 방안 연구,” 2003.

[2] 한국전자거래진흥원,“전자문서 정보패키지 기술규격 V1.10,” 2007.

[3] 한국전자거래진흥원,“전자화문서의 생성 방법 및 절차에 관한 지침 소개”, 2006