전자문서 유효기간 검증 기능을 탑재한 전자문서관리시스템 구현

정회원 박 중 오*, 이 승 민*, 김 상 근**, 전 문 석*

Implementation of EDMS(Electric Document Management System) with Validity Verification

Jung-Oh Park*, Seung-Min Lee*, Sang-Geun Kim**, Moon-Seog Jun* *Regular Members*

요 약

전자문서의 신뢰성과 안정성을 보장하는 공인전자문서보관소를 구축,운영하는데 있어서 "전자문서 보관 및 발급 서비스"는 핵심 서비스 중에 하나이다. 문서 소유자가 전자문서를 등록한 후 향후 제 3자에게 발급하는 과정에서 등록된 전체의 정보가 아닌 부분정보 발급을 통해 불필요한 정보유출을 방지한다. 또한 유효성 검사 모듈을 문서 자체 내에 포함시켜 문서의 유효기간을 점검하는 시스템을 제안하였다.

Key Words : E-document, EDMS, OTP

ABSTRACT

E-document deposit and issue service among other services is critical service in CEDA(Certified E-Document Deposit Authority) that assure reliability and stability of E-document. After owner's E-document is registered in CEDA, issuing partial information(a part of page) is to prevent exposure of superfluous information when owner issue E-document to 3rd party. Also we suggested that is able to verify validation of E-document as validation check module is inserted suggested system.

I. 서 론

최근 국내 기업.금융기관 등은 각종 문서 또는 서류의 유통. 보관에 연간 1조원 이상을 소요하고 있는 것으로 추정되며, 검색. 참조 등 보관 문서의 활용에도 어려움이 있는 것이 현실이다. 신용카드 매출전표의 경우 연간 15억 매가 발행되고 있는데, 이를 신용카드사가 수거하고 문서 창고에 보관하는데 약 1,200억원 가량의 비용이 소요되는 것으로 추정된다[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 핵심요인의 하나이다.

본 논문에서는 이용자가 전자문서를 전자문서보관소에 등록한 후 향후 제 3자에게 발급하는 과정에서 등록된 전체의 정보가 아닌 부분정보 발급을 통해 불필요한 정보유출을 방지하며, 발급된 문서 자체 내에 유효기간 검사 기능을 부가하여 문서의 유효기간을 검사한다. 유효기간이 지난 문서에 대해서는 문서 자체 내에서 열람이 불가능하다. 또한 문서 암.복호화 키 분실 시에도 정보유출을 최소화함으로써 전자문서 보관소에 등록된 문서의 보안을 강화하였다.

* 숭실대학교 컴퓨터학과
** 성결대학교 컴퓨터공학부(jopark2@sungkyul.edu)
논문번호 : KICS2009-12-603, 접수일자 : 2009년 12월 4일, 최종논문접수일자 : 2010년 6월 18일

논문의 구성은 다음과 같다. 2장은 선행연구 및 관련 기술로서 전자문서보관서비스 기능과 전자문서관리시스템의(EDMS) 내용과 장점을 설명하고 제안시스템에서 사용된 OTP(One Time Password)기술에 대해서 설명한다. 3장은 기존 전자문서 보관소 서비스의 문제점을 해결하기위한 전자문서의 안전한 저장과 OTP를 활용한 등록된 문서의 부분정보 발급과 유효기간 검증을 통한 전자문서의 정보보호 방안 등에 대하여 연구하였다. 4장은 기존시스템과 비교하여 제안시스템의 성능을 평가하고 보안성에 대하여 비교 분석하였으며 마지막 5장으로 결론을 맺는다.

Ⅱ. 관련연구

2.1 전자문서보관소 서비스

2.1.1 저장 및 보관 서비스

문서가 생성되어 폐기될 때까지의 안전한 보존을 목적으로 하여 문서작성, 문서변환, 문서관리, 문서검색, 문서열람 그리고 백업과 복구 등의 기능을 제공한다.

2.1.2 송수신 서비스

보존된 문서를 유통시키거나 유통만을 위해 제출된 문서에 대해 지정된 수신자에게 문서를 배달하는 서비스로서 문서의 배달, 송.수신 확인, 암호화, 연동 등의 기능을 제공한다.

2.1.3 검증 서비스

문서의 등록 증명, 배달증명, 내용증명, 원본 증명 그리고 증명서 발급 등의 기능으로 구성된다[2,3].

전자문서보관소는 전자문서의 등록, 보관, 유통 등 각종 증명서 발급 및 유통관리 서비스를 지원하며 전자문서의 송.수신 보안 업무를 수행한다. 그림 1에서와 같이 이용자는 보관소에 문서등록 의뢰를 하며 보관소는 그 문서를 저장.보관한다. 또한 허가된 제 3자에 한해서 문서 발급도 하며 등록증명, 배달증명, 내용증명, 원본증명 등의 검증업무도 수행한다[4].

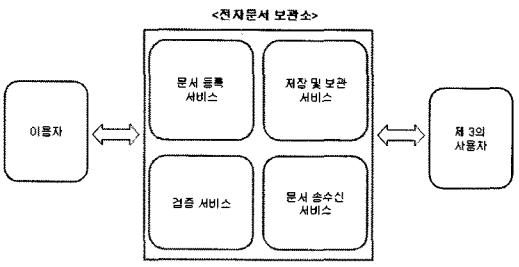


그림 1. 전자문서 보관소의 기능

2.2 EDMS(Electric Document Management System)

기업에서 사용되는 문서는 인허가 문서, 표준 운영절차서 (SOP), 마케팅 자료, 제품 시방서 등과 같이 대체로 비정형적인 문자 정보로 이루어진 문서파일의 모습을 갖고 있다. EDMS는 이러한 모든 종류의 다양한 전자 문서 컨텐츠를 회사 전체적으로 통일된 방식으로 규제 요건에 맞추어 작성하고 배포하며 관리하는 데 사용하는 정보시스템이다. EDMS는 모든 전자문서에 대해 그 생명 주기 (작성, 수정, 승인, 발행, 발효, 주기적 검토, 폐기 등)를 통하여 모든 버전을 통합적으로 수록 관리하고, 웹 기반의 인터넷/ 인트라넷을 이용하여 언제 어디서나 필요한 문서를 쉽게 찾아 활용하도록 하는 안전하고도 강력한 문서 관리 기반이다[4,5].

2.2.1 전자문서 관리시스템(EDMS)의 기능

전자 문서관리 시스템은 문서작성, 종이문서의 전자문서 변환의 기능을 제공한다. 또한 전자문서를 저장, 편집 및 출력도 가능하다. 일반 문서뿐만이 아니라 이미지, 비디오, 오디오 형태의 문서도 관리가 용이하다.

2.2.2 전자문서 관리시스템의 장점

기존의 종이 문서 형태로 행해지던 행정이 전자문서 형태로 행해짐으로써 비용이 감소한다. 또한 종이문서를 보관하던 장소나 서류함이 불필요로 하게 되고 보관장소를 다른 용도로 재사용 할 수도 있다. 종이를 수작업으로 분류/검색하던 업무는 전자문서로 대체함으로써 신속한 문서검색이 가능해졌다.

2.2.3 전자문서의 효력 및 기밀보호

정보통신망 및 컴퓨터를 이용하여 생산/처리한 전자문서도 서류문서와 동일한 효력을 유지한다. 따라서 개인 정보나 기밀 등의 전자문서는 각별히 보호해야 한다

2.3 OTP(One Time Password)

일회성 패스워드로써 매번 패스워드가 바뀌며 전에 사용한 패스워드를 다시 재사용 하지 못하므로 인증기법에서 강력한 도구로써 사용 될 수 있다[6].

2.3.1 Challenge-Response 방식

사용자가 서버가 제시한 질의 값을 알고리즘에 입

력해 응답 값을 얻고 해당 응답 값으로 자신을 인증하는 방식이다. 사용자의 입력 내용이 많아 불편하다.

2.3.2 Time-Synchronous 방식

서버와 OTP 장치 간에 동기화된 시간 정보를 기준으로 특정 시간 간격마다 변하는 비밀번호를 생성한다. 따라서 사용자는 질의 값을 확인.입력할 필요가 없다. 단, 사용자가 입력 중에 비밀번호가 변할 수 있다.

2.3.3 Event-Synchronous 방식

서버와 OTP 장치가 동일한 카운트 값을 기준으로 비밀번호를 생성하는 방식이다. OTP 장치에서 여러 번 비밀번호만 생성하고 사용하지 않으면, OTP 장치와 서버 간의 카운트가 불일치 되어 OTP 장치를 다시 초기화 해야 하는 단점을 가지고 있다.

2.3.4 조합방식

시간동기화와 이벤트 방식의 단점을 보완하기 위해 마련된 방식이다. 즉, OTP 알고리즘의 입력으로 시간, 카운트 값을 모두 사용하는 것이다. 특정 시간 간격마다 비밀번호가 다시 생성되며, 같은 시간 간격 내에서 재시도 시에는 카운트 값을 증가시켜서 비밀번호가 변하도록 하는 방법이다

Ⅲ. 제안 시스템

3.1 개선한 전자문서 보관소 시스템

제안시스템은 그림2와 같이 전자문서 보관소의 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. 등록 요청된 문서의 저장 및 발급과 관련된 제안시스템의 업무처리 흐름은 다음과 같다.

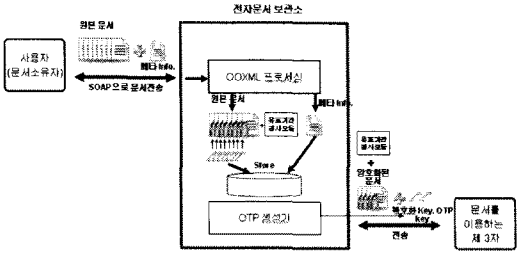


그림 2. 부문문서 생성 및 발급과정

그림 2는 문서소유자에 의한 전자문서 보관 요청시 원래의 원본문서 매 페이지마다 암호화를 적용하고 또한 유효기간 검사모듈을 탑재시켜 향후 있을 제 3자 열람 때 최소정보만을 제공하는 과정을 묘사하였다. 자세한 흐름은 아래와 같다.

① 사용자가 문서 등록을 요청한다.
② 전자문서의 전송시 SOAP을 통해 이루어진다.
③ 등록 요청된 문서는 OOXML 처리 과정을 거쳐서 이용자의 분류 기준에 따라 세분화 된다.
④ 세분화된 문서는 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. 또한 유효기간 검사 모듈이 문서 자체 내에 탑재된다.
⑥ 문서를 메일로 발급할 때 PGP(Pretty Good Privacy)또는 GPG를 통해 이루어진다.
⑦ 문서를 제 3자에게 발급할 때 대칭키, OTP값과 같이 2개의 복호화용 키, 전자문서 보관소의 개인키로 암호화 된 유효기간이 암호화된 문서와 함께 전달됨으로써 보안이 강화된 문서가 전달된다.
⑧ 문서를 이용하는 제 3자는 최초의 대칭키, OTP, 개인키로 암호화된 유효기간을 이용하여 유효기간 내에서 보안문서 열람이 가능하다

그림 3은 전자문서 보관소에 등록된 전자문서 중 부분정보 발급 요청 과정의 개념적인 흐름을 표현했다

전자문서가 저장될 시 페이지별로 암호화가 이루어지며 제 3자에 의한 부분정보 요청시 요청 페이지내에 보호된 패키지로써 "유효기간 검증모듈"과 link 키 기능이 탑재되어 제 3 자에게 발급된다. 이러한 문서를 받은 제 3자는 최초 페이지를 복호화 할 수 있는 10페이지 키와 OTP key를 가지고 다음 페이지를 복

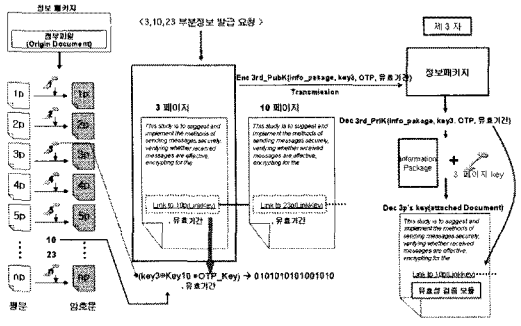


그림 3. 부분정보 발급과정

호화 할 수 있는 키를 풀어나간다. 물론 이 문서에는 유효기간 검증모듈이 보호된 패키지로써 존재하여 유효기간내에 열람만 가능토록 문서를 보호한다.

3.2 제안 시스템의 특징

3.2.1 OTP를 활용한 전자문서 발급

이용자로부터 전자문서 보관소에 전자문서 등록을 요청 받으면, 전자문서 보관소 서버는 향후 등록 된 문서 중 일부 즉 부분문서 발급을 위하여 그림 4와 같이 OOXML(Office Open XML) 처리과정을 통해 문서를 세분화하여 분리하고, 각각 서로 다른 대칭키를 이용하여 암호화 한 후 보관소 저장소에 보관한다.

문서 등록 시 이용자의 요청에 의해 100페이지의 세부 문서로 분리된다면, 이 문서 전체를 암호화 하는데 서로 다른 100개의 대칭키가 사용된다. 향후 이용자가 이 문서의 부분발급을 요청할 때 60개의 분리된 문서의 발급을 요청한다면, 60개의 문서를 발급함과 동시에 이용자에게 복호화 키 60개를 전달하여 암호화된 문서를 복호화 한다. 이 경우 복호화 키 분배의 어려움, 복호화 속도의 증가 및 다수의 키 전송에 따른 Network Overhead 등과 같은 문제점이 예상될 수 있다. 따라서 제안시스템에서는 Link기능을 이용하여 복수개의 키가 전송되는 것을 방지하고, 키 유출에 대비하여 문서 발급시 실시간으로 OTP 값을 생성하여 이를 다음 키 습득을 위한 Link 정보(Index) 생성 및 복호화에 참여시킴으로써 발급문서의 보안을 강화하였다. 실시간 OTP를 사용하는 이유는 부당한 이용자가 암호화된 원본파일에서 특정페이지에 대한 Key 값을 습득해도, 다음 링크페이지에 대한 정보를 복호화 하지 못하도록 하기 위한 것이다.

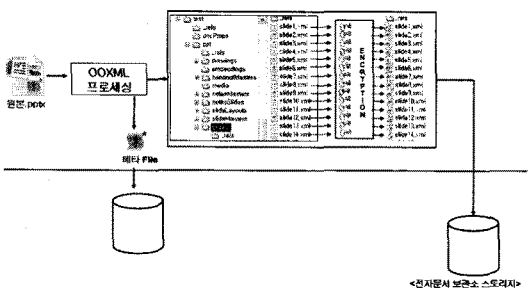


그림 4. OOXML 처리과정

3.2.2 Link와 OTP를 이용한 Key 보호와 문서 보안

이용자로부터 원본 파일을 수신 받으면 전자문서 보관소시스템은 OOXML 처리과정을 통해 원본파일을 세분화시킨 후 각각 서로 다른 대칭키를 이용하여 암호화 보관한다. 이용자로부터 받은 원본파일이 100페이지의 전자문서라 가정한다면, 제 3자가 부분정보 발급 요청시 서로 다른 키로 암호화된 100페이지 중 요청한 해당 페이지에만 OTP 값이 포함된 Link 키를 삽입하여 Key를 보호한다. OTP를 사용함으로써 Link 키 재사용이 방지된다.

예를 들어 제 3자가 등록된 문서 중 3, 10, 23 페이지의 부분문서 발급을 요청한다면, 발급된 전자문서 하단에 다음 발급될 페이지에 대한 Link 정보가 기록되므로, 그림 5의 ①과 같이 3페이지 내에 "보호된 패키지" 안에는 3페이지를 복호화 할 대칭키, 다음 발급 페이지인 10페이지 복호화키, 마지막으로 OTP 값, 이상 3개의 값을 "exclusive OR(⊕)" 하여 생성된 값을 다음 페이지(10페이지) 링크 정보 키가 정장되어있다. ② 에서는 마찬가지로 "보호된 패키지"안에 23페이지에 대한 링크 정보 키도 저장되어있다. 이러한 암호화 절차의 목적은 최초 페이지인 3페이지의 복호화 키(key3)과 OTP key 없이는 10페이지와 23페이지의 열람을 불가능하게 만드는데 있다.

제 3자가 원하는 부분정보가 발급됐을 때, 제 3자는 Link 정보가 생성될 때와는 반대로 복호화 키(key3과 OTP key)를 얻을 수 있다.

10페이지 복호화 키 생성은 그림 5의 ③과 같이 3페이지의 "보호된 패키지"내에 있는 10페이지에 대한 Link정보, 3페이지 복호화 키, 전자문서 보관소에서 보내온 OTP 값을 "exclusive OR(⊕)" 함으로써 10페이지에 대한 복호화 키 값을 얻을 수 있다. 마찬가지로 23페이지 복호화 키 획득은 ④와 같이 10페이지 "보호된 패키지" 내에 링크정보를 계산하여 얻을 수 있다.

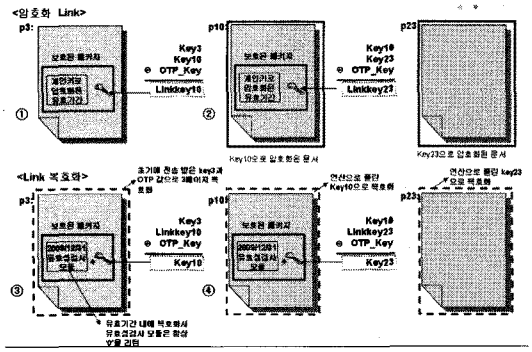


그림 5. 각 페이지별 암복호화와 유효기간 검사

3.2.3 OTP를 이용한 부분정보 발급과 유효기간 검사

발급된 부분정보(요청 페이지)는 보호된 패키지 내

에 유효성 검사모듈이 탑재되어 있어 유효기간 내에서만 열람이 가능하도록 문서를 보호한다. OTP를 이용하여 전자문서 보관소에 등록된 전자문서 중 일부 문서가 제 3자에게 발급되는 세부처리 과정과 유효기간 검증과정을 그림 6에서 표현하였다

① OTP 값을 생성한다.

② 제 3자가 100페이지의 등록문서 중 3, 10, 23 페이지의 부분문서 발급을 요청했으므로, 시작 페이지인 3페이지의 "보호된 패키지" 내에 10페이지 Link 정보를 삽입한다. 이는 문서 발급시 생성된 OTP 값을 이용하여 계산된 값 ("10페이지 Link 정보 = 3페이지 복호화 키 ⊕ 10페이지 복호화 키 ⊕ OTP 값")이다. 또한 유효성 검사를 위하여 발급기관의 개인키로 암호화된 유효기간을 삽입한다.

③ 두번째 페이지(10페이지)의 "보호된 패키지"내에 시작 페이지와 마찬가지로 계산된 다음 페이지 Link 정보 값("23페이지 Link 정보 = 3페이지 복호화 키 ⊕ 23페이지 복호화 키 ⊕ OTP값")과 발급기관의 개인키로 암호화된 유효기간을 삽입한다.

④ 마지막 페이지에는 Linkkey가 필요 없다.

⑤ 발급할 문서에 대한 준비가 끝나면, 제 3자에게 100여 개의 서로 다른 대칭키로 암호화된 발급문서, 시작페이지 복호화 키값, 실시간으로 생성된 OTP값, 암호화된 유효기간 이렇게 3개의 정보를 공개키로 암호화하여 전송한다.

⑥ 제 3자의 시스템에서 갖고 있는 개인키를 이용하여 "첫 페이지 복호화키, 전자문서 보관소로부터 제공받은 OTP 값, 암호화된 유효기간"을 복호화한다. 이때 유효기간이 지났다면 문서를 열람되지 않는다

⑦ 10페이지 Link 정보와 23페이지 Link 정보 및 OTP값을 이용하여 10, 23페이지를 복호화 할 수 있는 키를 얻는다. 이 작업은 보호된 패키지 내에서 진행된다. 각각 얻어진 3, 10, 23 페이지 키는 유효성 검사시 마다 아래와 같이 연산된다.

$$Key10=key10 + int (today()/유효기간)$$

유효기간은 발급자의 개인키로 암호화되어 있으므로 발급기관의 공개키로 복호화한다. Today()는 오늘 일자를 반환하고, 정수화는 뒤에 생성되는 소수점을 무조건 버린다. 만약 오늘 날짜가 유효기간 내에 있다면 (Today()/유효기간) 값은 0의 값을 반환하여 key10 값의 변화는 없게 된다. 유효기간이 지났다면 (today()/유효기간)의 값은 1이상이 되므로 key10의 값에 변화를 주게 되어 정상적인 복호화 과정이 진행되지 않는다.

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

그림 7은 부분 문서 복호화시 보호된 패키지 내에서의 문서유효성에 대한 절차를 설명한 것이다. 수신된 첫페이지 복호화 키, OTP, 암호화된 유효기간은 제 3자 본인의 개인키로 복호화 된다. 그 중 유효기간은 발급기관의 개인키로 암호화 되어 있기 때문에 발급기관의 공개키로 복호화하여 유효기간을 얻는다. 물론 유효기간은 보호된 페이지 내에서 복호화 되기 때문에 변경이 불가능 하다. Int(오늘날짜/유효기간)의 연산은 나눗셈으로 인한 모든 소수점은 무조건 버린다. 오늘의 일자가 유효기간 내에 있다면 값은 0일 것이며, 유효기간이 만료 되었다면 값은 1이상일 것이다.

[수식 1] $Key_N = Key_N + int(오늘날짜/유효기간)$

[수식 1]에서 int(오늘날짜/유효기간)의 값에 따라

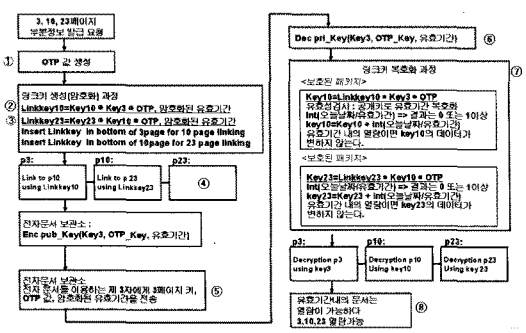


그림 6. 암복호화 세부 과정

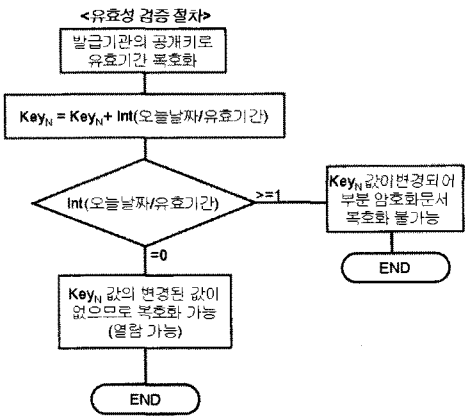


그림 7. 유효성 검증 절차

Key_N 변경일어 날 수도 있고 그렇지 않을 수도 있다. 유효기간내의 문서는 키 값이 변경되지 않으므로 열람이 가능하며 유효기간이 경과한 문서는 키 값의 변경으로 정상적인 복호화가 정상적으로 진행되지 않아 문서를 보호한다.

악의적인 열람 목적으로 오늘 일자를 변경(시스템의 날짜를 변경) 하여 주입한다면 열람이 가능할 수도 있다. 이것을 대비하기 위하여 오늘날짜는 NTP 타임으로 주입한다. 즉 문서 열람을 위해서는 시스템의 인터넷접근이 가능하여야 한다. 이미 발급기관의 공개키를 얻기 위하여 인터넷접근이 있어야 했기 때문에 큰 문제는 되지 않는다. 전자문서의 교환의 목적은 오프라인 상에 만나서 교환이 일어나는 것이 아니라, 편의를 위한 온라인 상에서 교환 서비스를 목적으로 한다

Ⅳ. 보안성 비교 및 성능 평가

등록 요청 받은 전자문서를 이용자의 요청으로 세분화 한 후 서로 다른 대칭키를 이용하여 암호화를 수행한 후 하므로, 공개키 암호화 기법을 사용하여 전체의 내용을 암.복호화 하는 기법보다는 빠르다. 단, 보안성 측면에서 대칭키 암호화는 키 분배 또는 키 전송시 기밀성이 공개키에 비해 약하다. 따라서 대칭키 전송시 공개키로 암호화한 후 전송하기 때문에 보안성을 보장한다.

장점: 전자문서를 페이지 별로 암호화하고 Link를 이용하여 복호화 키들을 은닉하였고, 두 개의 키를 이용하여야만 복호화가 가능하며, 두 개 중 하나의 키는 OTP 값을 이용하기 때문에 키 노출시 재사용이 불가능하다.

또한 유효기간 검사 모듈이 파일 자체 내에 탑재되어 기간을 경과한 문서에 대해서는 열람이 불가하다. 이는 향후 P2P사이트로 인해 부분별 하게 공유되는 컨텐츠에 대해 보호를 위해 이 유효기간 검사 기능을 이용해 볼만 하다.

단점 : 복호화를 위해 기존시스템은 한 개의 키 만을 전송하지만, 제안시스템에서는 두 개의 키를 전송함으로써 키 개수가 늘어났다. 매 부분 문서마다 유효성 검사 모듈이 탑재되어야 하며, 유효성 검사 모듈의 내용을 안전하게 보호해야만 한다는 위험성이 다소 있다.

기존시스템에서는 암호화에 쓰인 전자문서 암호화 키는 한 개 만을 사용하였지만 "표 1"와 같이 제안시스템에 대해서는 두개의 키를 사용하였기 때문에 한 개의 키가 유출이 되더라도 OTP 값을 알 수 없으므로 전자문서 복호화가 어려우며 또한 두개의 키가 전부 노출된다 하더라도 전자문서 전체가 복호화 되지 않아 정보유출의 위험성이 줄어든다.

표 1. 전자문서 보안성 비교표

비교항목	기존 시스템	제안 시스템
부분정보 발급기능	불가능	가 능
재전송 공격	가능	불가능 (OTP 이용)
유효기간 설정기능	불가능	가능
첨부파일 암호화 복잡도	1개의 키로 암호화	2개의 키로 암호화(Key_N, OTP)
사용 암호화 알고리즘	공개키	공개키, 대칭키
문서 해킹으로 인한 리스크 강도	큼 (전체 문서 노출)	작음 (부문 문서만 노출)

부분정보 발급기능은 현재 운영중인 공인전자문서 보관소에서는 없는 서비스 이다. 제안 시스템에서는 부분 정보 발급 서비스 기능을 지원한다. 암호화 강도를 높이기 위하여 OTP를 사용하였으므로 대칭키를 유추하기는 어렵다. 제안 시스템의 큰 특징중에 하나인 유효기간 설정기능은 기존 공인전자문서보관소에서는 없는 기능이다. 제안 시스템에서는 유효기간 설정이 가능하게 설계하였다.

기존 시스템은 발급된 문서에 대해서 유효성을 검사하는 절차가 없다. 유효기간 설정기능을 부분문서 자체 내에 탑재 하여 문서에 유효성(유효기간)을 부여할 수 있다. 현재 문제가 되는 무분별한 컨텐츠 공유에 대해서 문서를 보호하여 일정수준의 제약을 줄 수 있는 제안이다. "표 1" 에서 "부분정보 발급 기능"과 "유효기간 설정 기능"이 제안한 시스템의 핵심이라고 할 수 있다.

Ⅴ. 결 론

제안하는 방식은 하나의 대칭키만을 사용하는 것이 아니라 여러 개의 대칭키를 생성하여 각각의 페이지별 또는 각각의 요소 별로 추출하여 암호화 하고 여기에 같이 첨부된 파일 역시 서로 다른 키로 암호화하기 때문에 하나의 키가 노출된다 할지라도 OTP 값 없이는 복호화가 불가능하다. 또한 유효성 검사 모듈이 존재로, 시간에 관계 없이 열람이 가능하던 것을 시간적 제약을 두었다. 만약 전체적인 암호화를 실시간으로 한다면 이용자의 응답시간이 느려지겠지만 제안시스템은 기존 문서는 미리 암호화를 통해 만들어 놓고, 암호화에 사용된 키의 정보만을 암호화하기 때문에

응답시간을 좀 더 줄일 수 있다. 제안시스템을 향후 컨텐츠 보호 기술에 이용한다면, 지금 행해지는 무분별한 불법 컨텐츠 공유를 방지하고 건전한 컨텐츠 거래를 이끌어 가는데 일조 할 것으로 판단된다.

참 고 문 헌

[1] 한국무역정보통신-비씨큐어, "공인전자문서보관소 인프라 개발을 위한 연구," 2004. 6.

[2] 한국전자거래진흥원,"이용자시스템 기술규격(v1.00)", 2007

[3] 한국전자거래진흥원,"전자문서 증명서 포맷 운용절차 기술규격(v1.00)", 2007

[4] KTNET, "공인전자문서보관소 비즈니스 모델", 2006. 1.

[5] CarnegieMellonUniversity, "A Trusted Document Authority for Secure Paperless Trading," 2004. 8.

[6] 서승현, "OTP-EKE : 원-타임-패스워드 기반의 키 교환 프로토콜", 한국정보과학회 논문지 A, Vol.29 No.05 pp.291-298, 2002. 06.

박 중 오 (Jung-Oh Park) 정회원

2000년 7월 성결대학교 컴퓨터공학과

2003년 2월 명지대학교 전자계산교육 석사

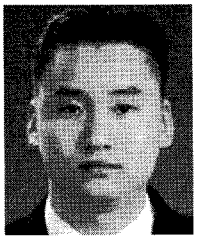
2006년 3월~현재 숭실대학교 컴퓨터학과 박사과정

2004년 3월 성결대학교 객원교수

2006년 3월~현재 성결대학교 정보산업기술연구소 전임연구원

<관심분야> 인터넷보안, RFID, 네트워크 보안, PKI, 암호알고리즘,

이 승 민 (Seung-Min Lee) 정회원



2004년 2월 한서대학교 컴퓨터정보학화

2006년 2월 숭실대학교 컴퓨터학과 석사

2006년 6월~2008년 7월 상호저축은행중앙회 IT본부 보안담당(SM)

2006년 3월~현재 숭실대학교 컴퓨터학과 박사과정

<관심분야> 네트워크 보안, RFID, PKI, EDMS, 암호알고리즘, 금융보안, 인터넷보안

김 상 근 (Sang-Geun Kim) 정회원

1987년 2월 중앙대학교 전자계산학과

1989년 2월 중앙대학교 전자계산학과 석사

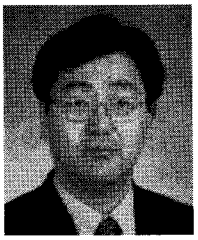
1996년 2월 중앙대학교 컴퓨터공학과 박사

1996년 3월~현재 성결대학교 컴퓨터공학부 정교수

2003년 1월~2004년 2월 University of Sydney, 객원교수

<관심분야> 정보보호, RFID, IT융합기술

전 문 석 (Moon-Seog Jun) 정회원



1981년 2월 숭실대학교 전자계산학과

1986년 2월 University of Maryland Computer Science 석사

1989년 2월 University of Maryland Computer Science 박사

1989년 3월~7월 Morgan State University 조교수

1989년 9월~1991년 2월 New Mexico State University Physical Science Lab. 책임연구원

1991년 3월~현재 숭실대학교 컴퓨터학과 정교수

<관심분야> 정보보호, 전자여권, 전자상거래