한국산학기술학회논문지
Vol. 10, No. 5, pp. 1000-1008, 2009

효율적 키 관리 방식 적용을 통한 전자문서 암호화에 관한 연구

김태욱[1], 성경상[1], 오해석[1*]
[1]경원대학교 전자계산학과

A Study on the E-Document Encrypted using the Effective key Management Method

Tae-Wook Kim[1], Sung-Kyung Sang[1] and Hae-Seok Oh[1*]
[1]Dept. of Computer Science, Kyungwonwon University

요 약 전자문서의 중요성이 커지면서 효율적 운용 방안을 위한 많은 연구가 진행되고 있다. 그러나, 전자문서의 활용에 따른 많은 이점이 있음에도 불구하고 보안상의 위협에 노출되어 있다. 즉, 전자문서의 무단 유출, 파괴, 분실·훼손의 위험이 존재하며, 위·변조, 멸실방지에 대한 미비한 대응책뿐만 아니라 관리에 따른 어려움도 뒤따른다. 이러한 시점에서 전자문서 암호화 기술을 연계하여 다양한 암호 기술을 전자문서 관리 시스템에 적용함으로써 보다 안전하고 효율적인 서비스를 제공해야 한다. 따라서, 본 논문에서는 기존 전자문서 관리시스템에 적용하고 있는 암호화 방안의 문제점을 제시하고, 전자문서 보호를 위한 암호화 알고리즘의 효율적 적용 방안을 통해 문제를 개선하고자 한다. 안전성과 효율성을 고려한 모델을 위해, 본 논문에서는 빠른 연산 수행속도를 기반으로 암호화 과정을 수행하며, 전자문서의 안전한 보호를 위해 키 관리에 따른 어려움을 해결하고 사용자의 무분별한 행위 방지를 위한 키 관리의 개별적 관리 방안을 수행한다. 논문에서 제안하는 암호화 방식과 기존 전자문서 암호화 시스템과의 성능평가를 위해 기본적 요구사항 이외에 전자문서 암호화에 따른 중요 항목들의 요소들을 비교 평가 수행하였으며, 안전성과 효율성 모두 개선된 결과를 얻을 수 있었다.

Abstract It also increases the competitive power of the nation. With all these merits of electronic documents, there exist threats to the security such as illegal outflow, destroying, loss, distortion, etc. Currently, the techniques to protect the electronic documents against illegal forgery, alteration or removal are not enough. Until now, various security technologies have been developed for electronic documents. However, most of them are limited to prevention of forgery or repudiation. Cryptography for electronic documents is quite heavy that direct cryptography is not in progress. Additionally, key management for encryption/decryption has many difficulties that security has many weak points. Security has inversely proportional to efficiency. It is strongly requested to adopt various cryptography technologies into the electronic document system to offer more efficient and safer services. Therefore, this paper presents some problems in cryptography technologies currently used in the existing electronic document systems, and offer efficient methods to adopt cryptography algorithms to improve and secure the electronic document systems. To validate performance of proposed method compare with the existing cryptographies, critical elements have been compared, and it has been proved that the proposed method gives better results both in security and efficiency.

Key Words : Electronic document, cryptography technology, Computations Execution, Key Management

1. 서론

인터넷 사용의 보편화와 정보통신 기술의 발달은 종이문서에 의한 기업의 환경을 급격히 변화시키고 있으며 전자적인 방법으로의 대체를 통해 새로운 형태의 사업 기회를 제공하고 있다. 이와 같은 전자문서의 등장은 종이문서의 작성, 보관에 따른 고비용 구조를 큰 폭으로 개선시켰으며, 정보처리에 소요되는 물자와 노력이 절약되

*교신저자 : 오해석(oh@kyungwon.ac.kr)
접수일 09년 04월 10일 수정일 09년 05월 15일 게재확정일 09년 05월 27일

어 거래 비용과 시장의 투명성을 증대시킴으로써 조직의 생산성과 효율성을 확대시키고 궁극적으로는 국가경쟁력을 제고시키는 매개체가 된다[7].

그러나, 전자문서의 많은 이점이 있음에도 불구하고 보안상의 많은 위험 또한 따르고 있다. 즉, 전자문서의 무단 유출, 파괴, 분실·훼손의 위험이 항상 존재하고 있을 뿐만 아니라 관리의 어려움도 뒤따른다.

이러한 위험으로부터 전자문서에 대한 무결성·신뢰성·가독성을 유지해야 하며, 보안성을 확보하기 위한 암호 기술 및 불법복제 방지 기술, 권한 기반 접근 제어 기능, 편집기록을 관리하기 위한 시점확인 기술, 증명 기술 등이 필요하다[8]. 또한, 전자문서의 유통과 관련된 기술로는 일반적인 데이터 송수신 기술과 서버관리 기술, 로그 및 감사, 추적 기술 외에, 송·수신 데이터의 무결성을 증명하기 위한 암호 기술, 데이터 수신자 확인을 위한 인증 기술, 전자문서의 권한 위임을 지원, 관리하는 접근제어 기술 및 암호화 기술, 전자문서 유통 증적 확인을 위한 시점확인 기술, 증명 기술, 공증관련 기술 등을 필요로 한다[1].

이와 같이 전자문서를 대상으로 하는 다양한 보안 기술들이 연구·제시되고 있으나, 대부분 위·변조 및 부인방지에만 국한되어 있으며, 기밀성에 대한 문제는 크게 다루지 않고 있다. 기밀성 유지를 위해, 전자문서의 암호화를 모색함에 암호 방식의 무거움으로 인해 전자문서에 대한 직접적인 암호화는 추진하지 못하고 있으며, 암·복호화 키 관리의 어려움을 이유로 보안에 대해서는 소홀히 대처하고 있다. 또한, 암호화 방식의 특성으로 부득이하게 평문 상태로 보관하게 되므로, 안전성과 효율성의 반비례 관계가 발생하고 있다[9].

현 시점에서 위와 같은 문제를 해결하기 위한 전자문서 보안 개선방안들이 소개되고 있다.

전자문서에 대한 보안 방안에는 접근권한 레벨에 따른 접근방법과 전자문서에 암호화 알고리즘을 적용하는 방법이 있다. 또한, 중요도에 따라 암호화 방법이 이용되고 있으며, 해쉬함수의 특성을 이용하여 전자문서의 연관된 관계를 응용한 일방향 키 체인 방식을 적용한 방법 그리고 선택적 암호화에 관한 방법들이 연구·제시되고 있다[10,12].

그러나, 전자문서와 사용자의 특성을 고려할 때 전자문서에 암호화 알고리즘 적용 방안에 대해서는 기술적으로나 방법적으로 많은 문제점을 가진다. 전자문서의 중요도에 따라 여러번 암호화하는 방법에는 암·복호화 시 많은 계산량을 필요로 하며, 사용자가 여러 키를 관리해야하는 문제를 갖는다. 이러한 문제를 해결하기 위해 접근 제한 모델을 통해 비밀성을 보장하고자 하였으나, 레벨적 접근 문제를 해결하지 못하고 있다. 또한, 키 관리에 따른 어려움과 전자문서의 암복호화 수행시 발생되는 비용에 대해 보상하기 어렵다는 문제를 가진다[3].

본 논문의 목적은 불규칙적으로 생성되는 난수정보 재배열 과정을 통해 키에 관한 개념을 정립시키고, 단순한 암·복호화 과정을 수행하지만, 동일한 복잡도를 지닌 XOR 연산 기법을 이용하여 키에 관한 규칙성을 부여함으로써, 키 관리에 따른 어려움을 해결하고, 전자문서의 암·복호화에 대한 안전성과 효율성을 끌어내는데 있다. 또한, 키 노출을 고려하여 분리 상태로 관리함으로써 키 관리 구조를 파악할 수 없도록 하며, 하나의 키가 유출되어도 키 생성에 따른 연관성을 배제하였으므로 키 관계를 통해 다른 키를 유추할 수 없는 구조를 지닌다.

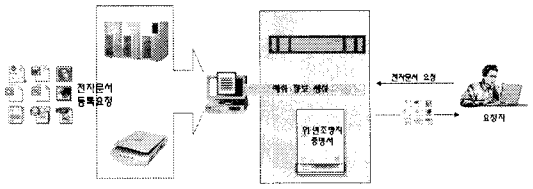
본 논문은 다음과 같은 구성을 통해 전개해 나가고자 한다. 2장에서는 관련 연구로서 전자문서 보안의 필요성을 언급하기 위해 전자문서의 위·변조방지를 위한 전자문서 보안 기술에 대해 설명한다. 3장에서는 2장에서 제기된 기존 시스템에서의 문제점을 보완할 수 있는 효율적인 키 관리를 이용한 전자문서 암호화에 대한 전체적인 시스템의 구조와 시스템을 구성하고 있는 3개의 에이전트들에 대해 설계하고, 각 구성에 따른 모듈별 처리에 대해 기술한다. 4장에서는 3장에서 기술한 내용을 기반으로 전자문서 암호화 시스템에 적용 가능한 난수정보를 이용하여 효율적인 키 관리 방안에 대해 기술함으로써, 기존 전자문서 시스템과 제안하는 개선된 전자문서 시스템의 암호화 방안에 대해 비교 분석한다. 마지막으로 5장에서는 본 연구의 정리와 4장에서 기술한 시스템 평가 결과를 기반으로 결론을 논하고, 향후 연구 방향에서는 제안하는 기법을 통해 적용 가능 방안에 대해 기술함으로써 개선안의 효과에 대해 언급한다.

2. 관련 연구 및 기술

본 장에서는 전자문서 시스템의 문제점을 분석하기 위해 전자문서 위·변조를 적용한 시스템과 전자문서에 암호 알고리즘을 적용한 시스템에 대한 문제점을 파악하고, 개선안을 제시한다.

2.1 위·변조 적용 시스템의 개선점

전자문서의 위·변조만을 검증하는 시스템 흐름은 그림 1과 같은 과정을 지닌다.



[그림 1] 위·변조만을 검증하는 전자문서 시스템

그림 1에서 보는 바와 같이 전자문서는 이미지 정보의 특징을 지니고 있으며, 헤더부에는 이미지의 위·변조 검증을 위한 이미지 정보를 SHA1 해쉬 알고리즘을 이용하여 해쉬화한다[3]. 전자문서 관리 서버는 해쉬된 이미지 정보를 헤더부에 삽입하고 관리하며, 이후 발생되는 문제에 대해 무결성 여부를 입증한다. 그러나, 해당 전자문서의 위·변조 여부만을 가리기 위한 방책이므로 내용 유출여부 문제에 대해서는 책임 여부를 확신할 수 없다. 또한, 전자문서는 일반 텍스트 문서의 특성이 아닌 전자화 정보를 지닌 이미지 특성을 가진다. 단일 페이지 문서라면 암·복호화하는데 큰 무리가 따르지 않겠지만, 멀티 페이지를 가진 전자문서라면 이미지 특성상 그 용량은 무시할 수 없게 된다. 이렇게 큰 문서를 암호화해서 요청자에게 전송하고, 송신자는 전달받은 암호화된 전자문서를 복호화하는데 많은 시간적 비용과 시스템적 트래픽에 대해 보장받을 수 없는 문제를 지니게 된다.

이와 같은 문제를 해결하기 위한 방안으로 빠른 연산 속도를 지닌 대칭키 기반 암호 알고리즘을 이용하여 암호화 시스템에 적용하고 있으나, 키 관리에 대한 문제점을 지닌다[4].

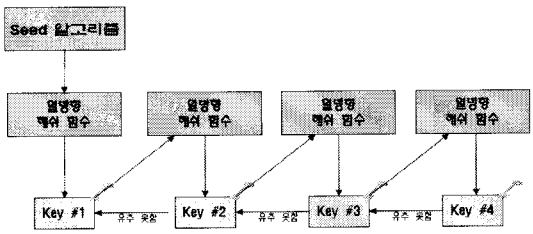
2.2 전자문서 암호화 시스템의 문제점

전자문서를 암호화하기 위한 방안으로 정보의 접근권한 레벨에 따른 암호화 방법과 중요도에 따라 여러번 암호화하는 방법이 이용되고 있으며, 해쉬함수를 이용한 키 생성을 통해 전자문서의 연관된 관계를 응용한 일방향 키 체인 방식과 전자문서에 대한 등급별 보안을 적용한 방식과 선택적 암호화에 관한 방식들이 소개되고 있다[9].

2.2.1 일방향 키 체인 방식 시스템

일방향 키 체인 방식은 역함수가 존재하지 않는다는 해쉬 함수의 특징을 이용하여 키를 생성하고 관리하는 방법으로, 기존에 존재하는 비공개키 암호화 방식에서의 키 관리에 대한 어려움을 극복하기 위해 제안된 방식이다. 이러한 방식은 상위 레벨키를 가진 사용자는 하위 레벨키들을 도출해 낼 수 있지만, 그 역은 불가능하다는 의미를 내포한다.

그림 2와 같이 일방향 해쉬 함수의 성질을 이용하여 키를 만들면 연속적인 체인 형태의 키를 만들어 낼 수 있다[5]. 이러한 방식은 상위 레벨키를 가진 사용자는 하위 레벨키들을 도출해 낼 수 있지만, 그 역은 불가능하다는 뜻이다. 다시 말해, 숫자가 낮아질수록 레벨이 높다고 가정할 경우, 만약 키 #2를 가진 사용자는 일방향 함수를 이용한 키 체인을 통해 하위키인 키 #3, 키 #4를 유도해 낼 수 있지만, 그보다 상위키인 키 #1을 알아내는 것은 불가능하다.



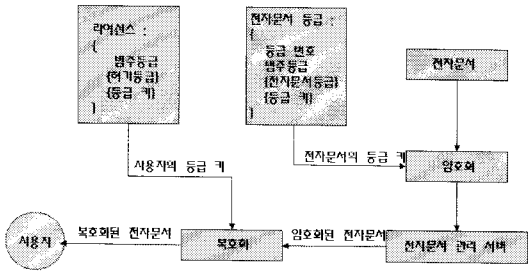
[그림 2] 일방향 키 체인 방식

이러한 방법론은 손쉽게 키 관리를 할 수 있는 장점은 가지고 있지만, 키 우선순위에 대한 개념 정립에 문제가 발생됨으로써 접근제어에 관한 권한을 부여받은 사용자의 무분별한 행위에 대해서는 보장받을 수 없다. 또한, 암호화된 전자문서의 중간에 접근하기 위해서는 차례대로 키를 복호화해야 하며, 초기 키값이 유출되거나 손상된 경우에는 해당 전자문서에 대해서는 보장받을 수 없다는 문제점을 지닌다.

2.2.2 등급별 보안을 적용한 암호화 시스템

전자문서 서비스를 제공하는 업체는 사용자와 해당 전자문서를 어떠한 기준에 의하여 여러 그룹으로 나누고, 각각에 대하여 접근 제한 정책을 사용한다. 이와 같이 사용자와 전자문서에 등급을 부여하여 접근을 제한하는 것을 등급별 보안이라 한다[6].

전자문서의 암호화 과정은 등급 정책에 부합하는 등급키를 랜덤으로 생성하고, 그림 3과 같이 전자문서 등급에 부합하는 등급키를 이용하여 암호화한다. 복호화는 사용자가 자신이 소유한 라이선스에서 복호화에 필요한 키를 추출하여 수행한다. 일반적으로 전자문서의 암호화와 복호화에 사용하는 Rijndael 암호 알고리즘을 이용하며 128비트 키를 생성하여 사용한다. 암호화 과정을 거친 전자문서는 자신의 라이선스에서 등급키를 추출한 후 복호화 과정을 수행한 후 관련 전자문서에 접근하는 과정을 거친다.



[그림 3] 전자문서의 암호화와 복호화

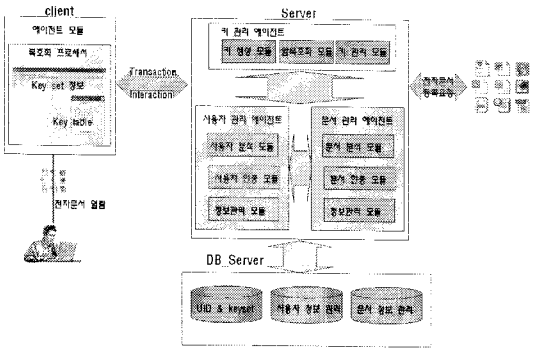
등급과 범주에 따라서 접근 제한을 두는 방법은 전자문서를 관리하는 입장에 있어서는 매우 편리하게 접근할 수 있다. 사용자의 권한보다 높은 등급의 전자문서에 접근할 수 없게 하고, 해당 등급 이하의 전자문서는 모두 접근하도록 하기 위하여 등급에 따라서 여러 개의 키를 사용하는 방법은 매우 위험할 수도 있다. 즉, 등급에 따라 구분되어지는 접근 권한 여부에 따라 자신 밑에 존재하는 모든 문서에 대해서는 슈퍼 관리자와 같은 권한이 부여되기 때문이다.

또한, 개별 인증이 아니라 등급별 인증 방법을 사용하고, 전자문서 배포시 사용자 인증절차를 요구하지 않으므로 해당 전자문서나 사용자 등급 조정에 따라 발생되는 문제점에 대해서는 전혀 고려되지 못하고 있다[3].

3. 제안하는 시스템 설계

본 장에서는 효율적인 키 관리 방안을 적용하여 안전한 전자문서 암호화의 극대화 방안을 위해 전체 시스템 구조와 제안 시스템의 구성 및 모듈별 기능과 키 관리 프로토콜 설계에 따른 처리 과정에 대해 기술한다.

3.1 제안시스템의 전체 구조



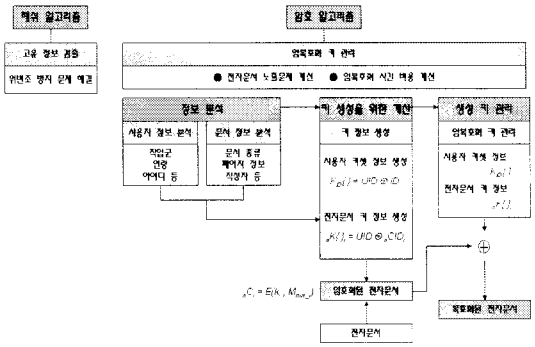
[그림 4] 제안하는 시스템 구조

개선된 전자문서 암호화 시스템 구축을 위해 제안하는 효율적인 키 관리 시스템 설계를 기반으로 하는 전체 시스템의 구조는 그림 4와 같이 구성되며, 클라이언트/서버 구조로 운용한다. 서버는 키 관리 에이전트와 사용자 관리 에이전트, 문서 관리 에이전트 그리고 데이터베이스로 구성되며 클라이언트는 암호화된 전자문서를 열람하기 위한 복호화 모듈로 구성된다.

먼저 전자문서의 등록 요청이 발생되면 정해진 규정에 따른 전자화 관리 시스템을 통해 전자화 과정을 거치게 된다. 전자화 과정속에서 문서가 갖는 속성 정보로서 문서의 작성자, 제목, 작성일, 등록일, 주제어, 설명, 보안등급 등 문서를 등록할 때 작성하는 메타데이터가 기록되며, 위와 같은 정보들은 해당 절차에 따라 관리된다. 등록된 전자문서의 분석된 정보를 기반으로 키 관리 에이전트부의 난수 재정렬 기법을 이용하여 키 생성 모듈을 통해 문서의 암호화 수행을 위한 키를 생성한다. 생성된 키를 이용하여 암·복호화 모듈에서는 전자문서의 개별 페이지 정보에 대한 암호화를 대칭키 기반의 AES 알고리즘을 이용하여 수행한다. 암호화를 수행한 키의 노출을 막기 위한 방안으로 개별 관리 방법을 이용한다. 전자문서 열람을 원하는 사용자는 정당한 인증과정을 거쳐 등록되며, 사용자 관리 에이전트부의 사용자 정보 모듈을 통해 등록된 사용자의 정보는 분석된다. 분석된 사용자 정보는 이름, 아이디, 주민등록번호, 직업 등의 메타데이터로 정리되며, 위와 같은 정보들은 해당 절차에 따라 관리된다. 사용자를 위한 s-Box 역할을 수행하는 키셋 정보 생성을 위해 사용자 인증 모듈에서는 키 관리 에이전트를 호출한다. 분석된 사용자 정보를 기반으로 난수 재정렬을 위해 규칙성 부여 방법을 적용한 키 생성 모듈을 통해 64바이트의 고유한 키셋 정보를 생성하고 관리하는 시스템 구조를 지닌다.

3.2 제안 기법의 프로세스 흐름도

효율적 전자문서 보호를 위한 방안으로 기존 전자문서 암호화 시스템의 문제를 해결해야 한다. 따라서, 요청된 전자문서의 부분정보 발급을 통해 불필요한 정보유출을 방지하고, 정보유출의 최소화를 위한 암·복호화 키 관리 방안과 안전성과 효율성의 관계를 고려한 모델이 필요하다. 위·변조 방지를 위한 해쉬 정보를 첨부한 전자문서가 개별적으로 관리 가능하다는 특성을 이용하여 부분 정보별로 암호화를 수행할 수 있도록 한다.



[그림 5] 제안기법의 프로세스 흐름도

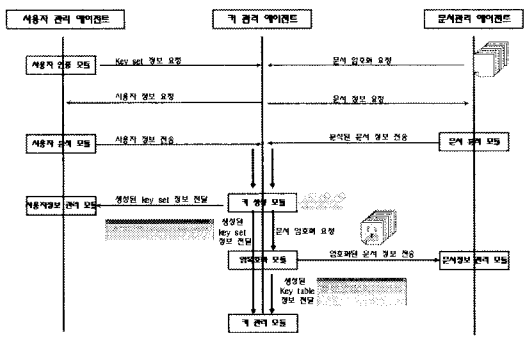
그림 5에서와 같이 해쉬 알고리즘을 이용하여 위·변조 및 부인에 대한 문제 해결을 기반으로 시스템을 구축한다. 사용자와 문서 정보를 분석하여 얻은 정보를 기반으로 키 생성을 위한 토대를 마련하며, 이를 이용하여 전자문서에 대한 암·복호화를 수행하게 된다. 또한, 키 관리에 따른 복잡한 문제도 해결하기 위해 s-Box 역할을 수행하는 사용자 키셋 정보와 암호키 역할을 수행하는 키 정보 관리 방안을 단순화하였다[3].

이와 같이 제안하는 효율적인 키 관리 방안에 관한 연구를 통해 전자문서 유출 문제를 개선하고 암·복호화 시간 비용과 시스템적 부하를 개선함으로써 전자문서 암호화 시스템에 적용 가능토록 하였다.

3.3 키 관리 프로토콜 설계

본 논문에서 제안하는 시스템은 키 관리 에이전트를 기준으로 구성되며, 생성된 키는 대칭키 기반 암호화 수행을 위한 암호키로 활용한다.

키 관리 프로토콜의 전체 구조는 그림 6과 같다.



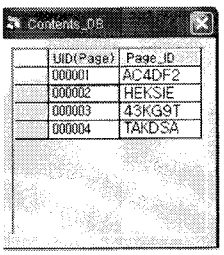
[그림 6] 키 관리 프로토콜

사용자 관리를 위한 정보를 구하기 위해 사용자 정보 관리 모듈에서는 키 관리 에이전트에게 고유키(키셋 정보)를 요청한다. 키 관리 에이전트는 키셋 정보 생성을 위해 필요한 사용자 정보를 요청하며, 사용자 분석 모듈을 통해 해당 정보를 전송한다. 사용자 정보를 기반으로 키 생성 모듈을 통해 생성된 키셋 정보는 키 관리 에이전트에 보관하고, 사용자 인증 모듈에게 해당 정보를 전송한다.

문서관리 에이전트로부터 문서 암호화 요청이 발생된 경우, 키 관리 에이전트는 암호키 생성을 위해 분석된 문서 정보를 문서 관리 에이전트부의 문서 분석 모듈을 통해 요청한다. 분석된 문서 정보를 기반으로 키 생성 모듈을 통해 암호화 수행 키를 생성한다. 암·복호화 모듈을 통해 생성된 키를 이용하여 요청된 전자문서를 암호화를 수행한 후, 키 정보는 테이블로 구성하여 키 관리 모듈에서 보관한다.

3.4 암호키 생성을 위한 설계

전자문서를 암호화하기 위한 구성요소로는 페이지를 구분할 수 있는 정보와 각 페이지의 암호화 수행을 위한 키 매칭 정보를 가져야 한다. 제안하는 시스템에서는 이와 같은 조건을 만족하기 위해 그림 7과 같은 요소로 구성하였다. UID 정보는 전자화 과정을 거쳐 분석된 페이지 넘버를 나타내며, page_ID는 각 페이지와 매칭되는 암호키 정보를 가리킨다. 이와 같이 전자문서에 대해 각 페이지별로 암호화 수행 키 정보를 테이블 형식으로 매칭시켜 관리하는 것을 목적으로 한다.



[그림 7] 문서관리를 위한 키

정의된 64개의 문자를 이용하여 불규칙적인 난수 정보에 규칙성을 부여하여 문자 6개로 구성된 키 값을 생성한다. 본 논문에서 제안하는 키 길이는 가변적 성격을 띠고 있으며, 키 길이에 따라 보안 강도는 달라진다. 문서의 중요도에 따라 키 길이가 늘어나도 XOR하는 비트 패턴을 통해 암·복호화 과정이 단순하게 이루어지지만, 동일한 복잡도와 수행시간을 가지므로 제안하는 키 관리 방식의 효율성은 뛰어나다고 할 수 있다.

그림 8은 문서에 사용할 암호키 생성을 위해 의사코드화로 표현한 것이다.

```
procedure Array Doc_key(N)
{
  if Doc_code != Enroll
    call Doc_code;
    call key_set_table;
    for i := 1 to 6
      if (i == 1)
          temp = CID XOR A(i)
      else
          temp = UID XOR A(i)
    next
    Doc_key_set(N) = temp XOR Doc_code
    return Doc_key_set(N)
}
```

[그림 8] 암호키 생성 의사코드

키 생성을 위해 등록된 문서인지 확인한 후, 등록되어 있지 않으면 Doc_code를 호출한다. 먼저 6개의 null을 생성한 후, 정의된 키셋 테이블을 통해 첫 번째 값부터 A(6)번째 열까지 채워나가는데, 첫 번째 값은 분석된 문서에 등록된 CID 정보와의 연산 수행을 통해 획득하게 되며, 생성된 이전 값과 UID 정보를 XOR 연산 수행함으로써 새로운 값을 얻게 된다. 이와 같은 과정을 반복해 얻은 값은 문서를 암호화하기 위한 키로서 대칭키 역할을 수행한다.

3.5 키 배열을 통한 인증 과정

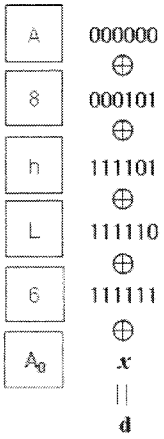
다음은 암호키와 키셋 정보를 기반으로 키 테이블을 생성하는 과정과 생성된 키 테이블의 인증 과정에 대해 살펴본다.

그림 9는 사용자에게 배부된 키셋 정보의 일부로서, 암호화된 전자문서의 키값이 "dP9KVx"라고 가정하며, 키 테이블을 생성한 이후 사용자에게 전송한다.

A	B	C	d	...	x	...
000000	000001	000011	000100	...	111000	...

[그림 9] 정의된 키셋 정보

키셋 값은 영문 대소문자와 숫자 그리고 _, Null 문자를 기반으로 64바이트 크기의 도표를 랜덤하게 생성할 수 있으며, 각 문자에 해당되는 이진 정보는 가변적으로 구성된다. 위와 같이 생성된 키셋 정보는 사용자에게는 s-Box와 같은 역할을 수행하는 기능을 제공하며, 서버측에서는 사용자의 키셋 정보를 기반으로 암호 정보가 숨겨진 키 테이블 생성역할을 수행한다.



[그림 10] 마지막 행값 생성 과정

그림 10은 미완성된 키 테이블을 완성하기 위해 마지막 행값 정보 생성을 위해 정의된 키셋 정보를 기반으로 A_0 값을 구하는 과정에 대해 나타낸 것이다. XOR 연산 수행의 특징을 이용하여 키 정보를 생성하는데, 수식 1과 같은 과정이 수행되는 규칙성을 발견하게 된다. 패딩된 키 테이블을 기반으로 정의된 키셋 정보를 기반으로 이진화 작업을 수행함으로서 생성된 이진화된 정보에 XOR 연산 수행과정을 통해 키 테이블을 구성한다. A_0에 해당되는 키 정보는 암호키값인 "d"를 숨기기 위한 역연산을 수행함으로써 구해진 "s" 정보를 가지고 그림 11과 같은 키 테이블을 완성한다.

$$A \oplus 8 \oplus h \oplus L \oplus 6 \oplus A_0 = d(key\_ID) \qquad \text{수식 1}$$

A	E	d	B	r	8
8	C	8	6	B	6
h	4	6	E	h	r
L	r	B	C	4	E
6	d	r	L	C	E
s	r	x	A	x	B

[그림 11] 완성된 키 테이블 정보

이와 같이 생성된 키 테이블 정보는 가변적인 특성을 지니고 있으며, 사용자가 서버에게 요청시마다 새로운 키 정보를 지닌 키 테이블이 생성되어 전송되므로 제 3자가

획득한다 해도 키값을 유추한다는 것이 불가능하다. 또한, 서버측에서는 키 전송 중 분실로 인한 고민을 해결할 수 있다.

4. 성능 평가 및 보안성 비교 분석

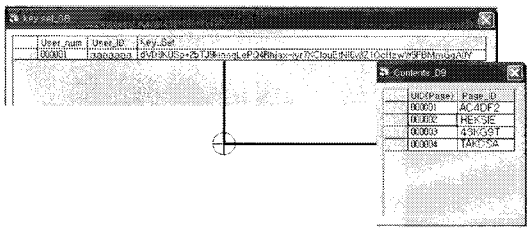
본 장에서는 구현한 시스템의 모듈 및 기능별 인터페이스에 대해 기술한다. 또한, 무분별한 난수 정보에 규칙성을 부여하여 생성된 키를 이용하여 전자문서 암호화 수행 결과에 대해 기술하고 기존 시스템과의 성능 비교를 통해 암·복호화의 안전성을 분석하며 성능평가에 대해 논한다.

4.1 구현 환경

제안하는 시스템은 클라이언트와 서버 구조로 구성되며, 서버측에서는 전자문서 관리 시스템을 기반으로 키 관리 시스템과 사용자 관리 시스템을 구축하였다. 시스템 운용을 위한 환경은 시스템 Intel(R) Pentium(R)-4 CPU 2.66GHz와 2GB RAM, 그리고 MS-Windows XP Professional 운영체제를 이용하였다. Visual Basic 6.0과 .NET을 이용하여 키 정보에 대한 전반적인 내용과 서버 및 클라이언트 인터페이스를 구현하였다. 전자문서의 UID 값과 암호키 그리고 키셋에 대한 정보를 저장하기 위한 데이터베이스는 MS-SQL 2000 프로그램을 이용하였다.

4.2 실험 개요

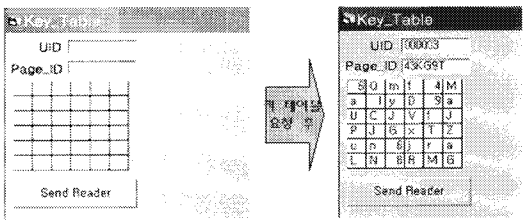
키 테이블이 생성되는 순간까지 암호키 정보는 노출되지 않으며, 단지 UID 정보만을 통해 일련의 과정을 수행하므로, 관리자도 해당 문서에 대한 키 정보를 알 수 없는 구조를 가진다. 이는 키 관리를 개별적으로 관리함으로써 키가 노출되거나 유추될 수 있는 문제를 미연에 방지하기 위한 방안이다.



[그림 12] 키 정보 생성 과정

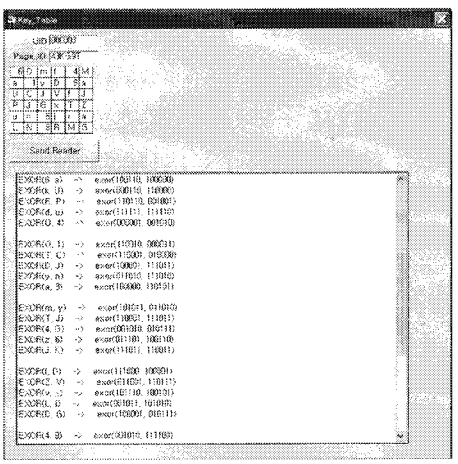
그림 12와 같이 사용자의 키셋을 기반으로 요청된 전자문서의 키 정보를 이용하여 그림 13과 같은 키 테이블을 생성한다. 생성된 키 테이블은 연산 수행시 마다 새로운 키 테이블이 생성되지만, 복호화를 유추하기 위한 결과값과 일치되는 키 테이블을 생성하는 수행 결과를 보인다.

복호키 정보를 지닌 키 테이블은 요청자에게 전송되며, 요청자는 자신의 키셋 정보를 기반으로 수신한 키 테이블 정보를 이용하여 복호키 유추 과정을 통해 암호화된 전자문서를 복호화한 후 열람하는 일련의 과정을 수행한다.



[그림 13] 키 테이블 생성 과정

그림 14는 키 테이블을 생성할 때 정당성을 보이기 위한 검증 과정을 보인것으로, 현재 보여지는 UID 3번의 Page_ID 값은 43KG9T로서 암호키 정보를 대체한다. 패스워드 정보를 유추하는 과정은 키 테이블의 첫 번째 열 부분을 통해 계산한다. 즉, 6과 a를 XOR 연산과정을 수행하면 k가 나오며, k와 U를 XOR 연산 수행하면 R의 결과값을 얻게 된다. 이와 같은 방식으로 계속 수행하며, 마지막 키 테이블에 위치한 L값은 도출된 O와 패스워드 4를 XOR 역연산 수행한 결과가 된다.



[그림 14] 키 테이블 검증 과정

4.3 실험 및 평가

본 논문에서는 제안하는 시스템에 대한 성능 평가를 위해 기존 전자문서 시스템에 적용하고 있는 암·복호화 방식과 비교 평가하였다. 평가 방법에는 암호화에 대한 비교 항목들을 정한 후 정성적 방법을 통해 분석하였다. 안전성 평가 부분에서는 전자문서의 안전성과 키 관리에 대한 안전성을 평가함으로써 기존 시스템에 비하여 안전성 측면에서 개선되었음을 확인할 수 있었다. 또한, 시스템 평가를 통해 암·복호화의 효율성과 전자문서 사용에 따른 불편함을 개선하였으며, 서비스 품질을 유지함과 동시에 시스템의 유연성에 대해 개선된 결과를 확인할 수 있었다.

본 논문에서 제안하는 전자문서 암호화의 효율성을 RSA 암호화 방식 그리고 등급키를 이용한 방식과 비교 분석하였다. 이들 암호화 시스템을 본 논문에서 제안하는 모델과 비교하여 문서를 암·복호화 하기 위해 사용자가 갖는 실질적인 키 개수, 계산 부하량, 암호화 시 문서 크기, 암·복호키 사이의 관계 등 대표적인 몇 가지 항목들을 비교하여 표 1로 나타내었다.

[표 1] 전자문서 암호화에 따른 중요 항목들에 대한 비교 평가

	RSA 이용한 암호화	등급키 이용한 암호화	제안하는 방식 적용 암호화
사용자가 갖는 키 개수 (x : 암호화 필드 수)	1	등급기준에 따라 달라짐	1
암·복호화에 따른 계산량 (n : 데이터 개수)	Me mod n	$Ke_i = \bigoplus_{i=1}^{n} \left\{ \bigoplus_{j=0}^{n} K_{ij} \right\}$	Ĕ (Rpub, M)
암호화 시 문서크기 (y:암호화 데이터 필드)	y	y	y
암호키	사용자 공개키	사용자의 등급을 이용한 키 사용	난수 정보와 전자문서의 특성을 이용한 키 사용

표 1에서 보는 바와 같이 암호화하는 데이터에 따른 사용자가 가져야 할 키 개수를 비교하고 있다. 기존의 방법들은 데이터에 따라 키의 수가 필요했지만, 제안하는 난수재배열 방법을 이용한 암호화는 모든 사용자가 단지 자신만의 고유 키셋 정보만을 보유한 상태로 일정하게 유지된다.

또한, 암·복호화에 따른 계산량을 표로 나타내 본 결과 제안하는 암호화 기법과 RSA 방식을 적용한 암호화 방식은 연산 수행의 어려움으로 인하여 계산량은 많은 반면 노출 위험성 문제를 개선할 수 있다.

5. 결론 및 향후 연구방향

전자문서의 중요성이 커지면서 정보유출을 방지하기 위한 방안들이 운영되고 있으며 많은 노력을 투자하고 있다. 전자문서의 생성·유통은 법률상 전자서명으로 그 안전성을 보장하고 있지만, 보관단계에서는 위·변조, 멸실 방지에 대한 방안이 미비하다. 이와 같은 필요성을 기반으로 전자문서의 암호화를 모색함에 암호 방식의 무거움으로 인해 전자문서에 대한 직접적인 암호화는 추진하지 못하는 실정이다. 또한 암·복호화 키 관리의 어려움을 이유로 전자분서 보안에 대한 관리적 측면에서는 소홀히 대처하고 있으며, 이로 인해 안전성과 효율성의 반비례 관계가 발생하고 있다.

이러한 시점에서 전자문서 암호화 기술을 연계하여 다양한 암호 기술을 전자문서 관리 시스템에 적용함으로써 보다 안전하고 효율적인 서비스를 제공해야 한다. 따라서, 본 논문에서는 난수 재배열 방법을 이용한 효율적인 키 관리 방안에 관한 연구를 통해 전자문서의 보안적 측면을 개선할 수 있는 방안에 대해 제안하였으며, 보다 개선된 결과를 얻을 수 있었다.

향후 전자문서에 대한 보안적 측면이 확산되었을 때, 제안하는 효율적 키 관리 방안 적용을 통한 암호화 수행과 알고리즘을 기반으로 다양한 응용분야에서 기본 모델로 활용이 가능하다. 또한, 제안 시스템의 LOG 정보를 활용하여 지능형 선호도 계산 알고리즘을 적용함으로써 사용자가 관심 갖고 열람했던 기록 정보들을 활용하여 관심 정보 추출을 통해 사용자에게 추천해주는 부분에까지 활용할 수 있는 전자문서 시스템으로 발전이 가능하다.

참고문헌

[1] 산자부고시2007-85호, "전자문서의 작성절차 및 방법에 관한 규정," 2007.

[2] 이진호, "ebXML을 이용한 문서 암호화 시스템 설계 및 구현," 한신대학교 대학원 석사학위 논문, 2003.

[3] 성경상, "난수 재배열 기반의 키 관리 방안을 이용한 전자문서 암호화에 관한 연구," 경원대학교 대학원 박사학위 논문, 2009.

[4] 윤은준, "다양한 환경을 위한 토큰 기반의 인증된 키 설정 프로토콜," 경북대학교 대학원 석사학위 논문, 2007.

[5] 김진성, "Yihl-Chun Hu, M. Jakobsson and A. Perrig, "Efficient Constructions for One-Way Hash Chains," In proceedings of ACNS 2005 LNCS Vol. 3531, pp.423-441, 2005.
[6] 김진성, "멀티미디어 컨텐츠에 대한 등급별 보안," 경상대학교 대학원 박사학위 논문, 2007.
[7] 김대중, "전자문서 보관 및 발급 서비스의 안전성 확보를 위한 시스템 설계," 숭실대학교 대학원 박사학위 논문, 2008.
[8] 김희원, "암호학에 관한 연구," 신라대학교 대학원 석사학위 논문, 2005.
[9] 김정재, "멀티미디어 데이터 보호를 위한 대칭키 암호화 시스템에 관한 연구," 숭실대학교 대학원 박사학위 논문, 2005.
[10] 이원우, "EC 환경에서의 XML 보안기술 연구," 순천향대학교 대학원 석사학위논문, 2005.

김 태 욱(Tae-Wook Kim) **[정회원]**

- 2004년 2월 : 호원대학교 전자계산학과 졸업(이학사)
- 2007년 2월 : 경원대학교 대학원 전자계산학과 졸업(공학석사)
- 2007년 2월 ~ 현재 : 경원대학교 대학원 전자계산학과 박사과정

<관심분야>
경영정보시스템, 정보통신, 텔레매틱스

성 경 상(Kyung-Sang Sung) **[정회원]**

- 2001년 2월 : 호원대학교 전자계산학과 졸업(이학사)
- 2003년 2월 : 숭실대학교 대학원 컴퓨터학과 졸업(공학석사)
- 2004년 2월 ~ 현재 : 경원대학교 대학원 컴퓨터학과 박사과정

<관심분야>
전자거래학, 유비쿼터스, 보안, 정보경영

오 해 석(Hae-Seok Oh) **[정회원]**

- 1981년 3월 : 서울대학교 대학원 계산통계학과졸업(박사)
- 2003년 1월 ~ 2003년 12월 : 한국정보처리학회 회장(역임)
- 1982년 2월 ~ 2003년 10월 : 숭실대학교 컴퓨터학부 교수/부총장(역임)
- 2003년 10월 ~ 2008년 3월 : 경원대학교 부총장(역임)
- 2003년 10월 ~ 현재 : 경원대학교 IT대학 교수

<관심분야>
Multimedia, Database, 지식경영