XML 전자서명과 암호화를 이용한 전자투표 시스템

김유희*° 홍영식**
*°신흥대학 컴퓨터정보계열 **동국대학교 컴퓨터공학과
*°euhkim@shc.ac.kr **hongys@dgu.edu

A Digital Voting System Using XML-Signature and XML-Encryption

Euhee Kim*° Young-Sik Hong**
*°Division of Computer Information, Shinheung College
**Dept. of Computer Engineering, Dongguk University

요 약

현존하고 있는 HTML(Hyper Text Markup Language)기반 인터넷 전자투표 시스템의 대안으로 웹 환경에서 XML(Xtensible Markup Language)표준기술을 이용하여 이기종간의 시스템에서 동작가능하고 HTML의 구조적 단점을 보완하며 전자투표와 관련한 데이터를 XML로 저장하고, 표준화된 XML문서 인증과 데이터 무결성, 기밀성, 송신 부인봉쇄 등의 보안 서비스를 제공할 뿐만 아니라 부분 서명과 암호화가 가능하며 구현 측면에 있어서 편리함을 제공할 수 있는 XML 기반의 전자투표 시스템을 설계한다.

1. 서 론

웹의 사용이 증가함에 따라 마크업 언어인 HTML보다 차세대 언어인 XML으로 급속히 확산되고 있는 추세이다. 현존하고 있는 HTML기반 인터넷 전자투표 시스템의 대안으로 웹 환경에서 XML표준 기술을 이용하여 이기종간의 시스템에서 동작가능하고 HTML의 구조적 단점을 보완하며 전자투표와 관련한 데이터를 XML로 저장하고, 표준화된 XML문서 인증과 데이터 무결성, 기밀성, 송신 부인봉쇄 등의 보안 서비스를 제공할 뿐만 아니라 부분 서명과 암호화가 가능하며 구현 측면에 있어서 편리함을 제공할 수 있는 XML 기반의 전자투표 시스템을 설계하고자한다.

웹 환경에서 인터넷을 이용한 전자투표 시스템은 암호프로토콜과 보안 채널 메커니즘 등으로 구성된 애플리케이션이다. 즉, 동적이고 개방된 웹 환경에서 XML을 사용하여 개발하고자 할 때 가장 염려하고 있는 것 중의 하나가 이 시스템 상에서 발생할 수 있는 비 인가된 권한사용, 서비스 거부, 데이터 노출/변경, 송수신 부인 등의 보안과 관련된 문제들이다. XML기반의 전자투표 시스템이 보안 서비스를 제공하기위해 통신할 때 보안이 필요한 데이터의 암호화와 인증처리를 기존의 비XML 보안 메커니즘 PGP(Pretty Good Privacy)[RFC 2440]나 바이너리 형태의 S/MIME(Secure Multipurpose Internet Mail Extensions)[RFC 2633]를 사용해서 기밀성과 인증을 구현할 수 있다. 하 만 이런 솔루션을 사용하려면 또 다른 비XML메커니즘을 추가해야하며, 그렇 않을 경우에는 XML기반 시스템에 손상을 주게 된다. 또한 기존의 바이너리 구문들을 사용하는 실제 구현은 계산력 소요가 커서 복잡하며, 웹 서버의 성능에 미치는 부담이 커져 효율성을 고려해 볼 때 적합하 않은 면이 있다. 이 문제를 해결하기 위해 W3C의 XML-Signature와 XML-Encryption 스펙[1][2]을 사용하여 편리하게 XML전자투표 문서의 필요한 부분에 인증과 기밀성을 적용할 수 있으며, 이들을 XML기반의 웹서비스에 자연스럽게 통합시킬 수 있다.

본 논문에서는 웹에서 전자투표와 관련한 모든 데이터를 XML로 저장하고 다른 형태의 데이터로 변환될 수 있게 함으로써 HTML의 구조적 단점을 보완하고, 구조화된 데이터 공유 및 교환을 위한 전자투표 시스템에 관련된 모든 XML문서를 XML Schema로 표준화하며, 전자투표문서의 인증 및 과 투표값의 기밀성을 동시에 적용하기위해 XML보안 메커니즘 XML-Signature와 XML-Encryption을 사용하여 인터넷을 통한 안전한 XML 기반 전자투표 시스템의 설계를 하고자 함이 연구의 목적이다.

이와 관련된 논문으로서 Devegili와 Neto는 전자투표 진행과정을 XML 스키마를 사용하여 하나의 XML 전자투표 문서의 구조를 정의했으며, XML-Signature을 적용하여 이 문서의 보안성 즉, 인증, 무결성, 송수신 부인방 를 제공하였다[3]. 하 만 이 논문에서는 전자투표의 결과 값의 기밀성에 대해서는 고려하고 있 않고 있다.

본 논문에서는 그들의 논문을 일반화하여 XML-Signature와 XML-Encryption을 사용하여 보안이 필요한 XML문서만을 선택적으로 적용해서 안전한 XML 기반의 전자투표 시스템을 설계하고자 한다. 본 논문의 구성은 2장에서 전자투표 시스템에 관련된 XML 표준 보안 기술을 소개하고. 3장에서는 XML 기반 전자투표 시스템 모델을 제안하고 관련된 구성 모듈을 설계하며 4장에서는 결론을 맺는다.

2. XML 전자서명과 암호화

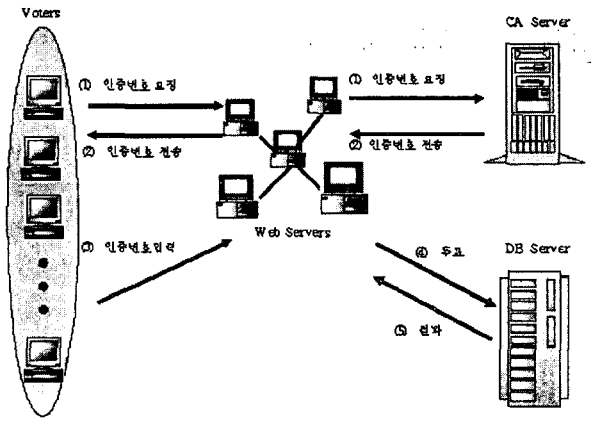
XML 전자서명(XML-Signature)은 2002년 2월 12일 권고안 상태로 W3C와 IETF(Internet Engineering Task Force)에 의해 표준화가 완료된 상태이다[1]. 기존 전자서명과 XML 전자서명의 차이점은 서명이 XML로 이루어진다는 것이다. 데이터 형식을 구분하는 것과 마찬가 로, XML 전자서명도 서명될 데이터가 XMLDSIG 요소의 내부에 있으면 이를 둘러싼 (Enveloping) 서명이라 하며, XMLDSIG 요소의 외부에 있으면서 둘러싸인 곳에 있으면 둘러싸인(Enveloped)서명이라 하는데 이 논문에서는 둘러싸인 서명방식을 사용한다.

XML 암호화(XML-Encryption)는 W3C에서 2002년 12월 10일자로 권고안 상태로 표준화가 완료되었으며, XML 기반 데이터의 기밀성을 보장하기 위해 암호화와 복호화 및 결과 표시를 위한 처리를 명시하고 있다[2]. XML 암호화의 장점은 암호화의 범위를 정할 수 있다. 즉, 전체요소를 암호화하던가. 요소의 전체 내용을 암호화하도록 제한한다. 본 논문에서는 인터넷을 통해서 사용자가 투표한 투표결과 값을 전자투표 관리자에게 공개되 않도록 투표 값의 기밀성을 보장하기 위해 XML 암호화 기술을 사용한다.

3. XML 기반 전자투표 시스템 설계

본 논문에서 제안할 전자투표 시스템은 오프라인 상에서 실시되는 현행 선거프로세스를 모델로 하며, [그림 1]과 같은 인터넷을 이용한 전자투표 구성도를 제안한다. 이 전자투표 구성도에서는 투표 전 반드시 투표자는 인터넷상에서 자신을 인증하는 절차에 대한 정보를 XML 문서에 추가하고, 투표자가 투표를 하면 이에 대한 투표 결과 정보를 XML 문서에 저장하며 투표결과의 기밀성을 보장하기 위해 전자 서명과 암호화하며, 투표자가 투표 결과에 대한 정보를 확인할 수 있도록 XML 문서에 데이터를 추가하거나 수정하는 작업이 끝나고 나면 항상 XML 문서의 정보를 브라우저로 보여주어야 하는 내용이 포함된다. 전자투표 수행 절차는 다음과 같다.

1. 등록 및 인증서 발급 단계(① ② 단계).
2. 인증 단계(⑧ 단계) : CA 서버로부터 투표자의 이중투표여부를 확인.
3. 투표 단계(④ 단계) : 투표 결과 값의 암호화 및 투표자의 전자서명을 생성해서 그 결과를 데이터베이스 서버에 저장 하고, 이중 투표 여부를 확인해서 이미 투표한 경우 투표 거부 화면을 전송.
4. 개표 단계(⑤ 단계) : 데이터베이스 서버에 저장되어 있는 개표결과와 집계 결과를 공개게시판에 게시한다.

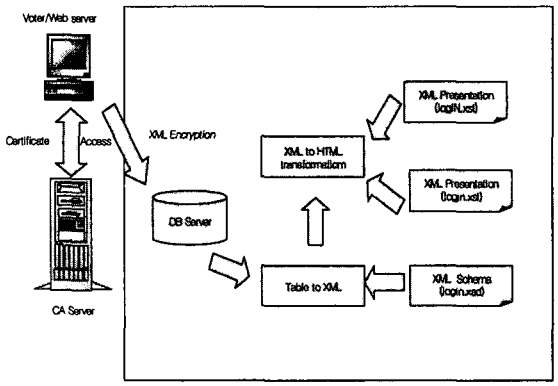


[그림 1] XML기반 전자투표 시스템 구성도

[그림 1]처럼 전자투표 시스템은 투표자 인증단계, 투표 단계, 투표 결과 및 검증 단계, 이들 간의 인터페이스 및 투표에 관련된 키 값 및 투표 결과 값들을 저장하는 인증 서버와 데이터베이스 서버로 구성되어 있다. 위에서 언급한 것처럼 제시하는 전자투표 시스템은 XML 기반의 플랫폼에 접목이 가능하도록 설계하는 것이 목적이므로 시스템 전반에 관련된 메시들과 서명이나 암호화한 결과 값이 XML 문서형태로 구성이 되도록 XML 스키마 문서를 모델로 하여 XML 문서 모듈을 설계한다.

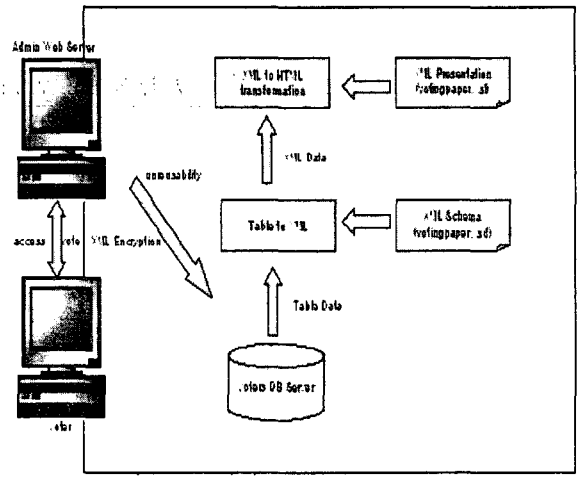
3.1 인증 문서 모듈

[그림 2]는 스키마문서와 스타일시트 문서를 사용하여 투표자 인증절차를 위한 모듈을 설계한 것이다. 즉, 투표자의 입력정보를 데이터베이스 서버에 연결하여 XML 형식의 데이터로 클라이언트에 돌려준다. 그런 다음 별도의 스키마(gin.xsd)문서를 사용해서 그것에서 정의하고 있는 규칙에 일치하도록 유효한 XML 문서를 작성한다. 또한 서버로부터 전송된 XML 형식의 데이터에 각기 다른 스타일시트(gin.xsl와 logIN.xsl)을 적용하여 인증절차와 인증확인 화면으로 진행된다.



[그림 2] 인증 절차 모듈

3.2 전자투표 문서 모듈

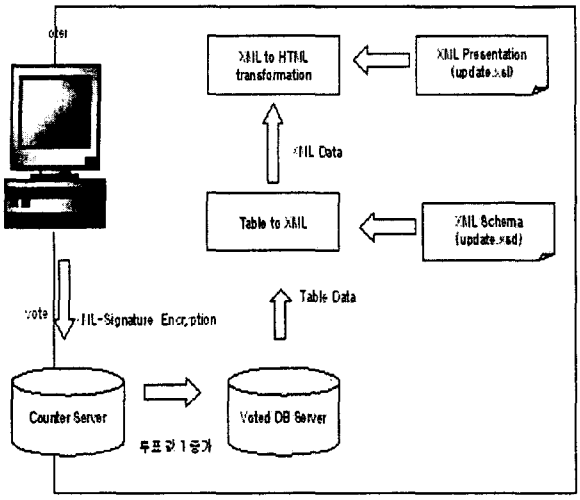


[그림 3] 전자투표 절차 모듈

[그림 3]는 투표자 인터페이스의 설계도이다. 여기서 투표자의 이중투표여부를 확인하고 유효한 투표 결과와 투표에 관련된 정보가 저장되어 있는 데이터베이스 서버로부터 전송된 XML 데이터에 스타일시트(otingpaper.xsl)와 스키마 문서(otingpaper.xsd)을 적용한다. 브라우저상에서 그 결과를 보면 XML 문서가 HTML문서로 변환된 것을 확인 할 수 있다.

3.3 투표 결과 문서 모듈

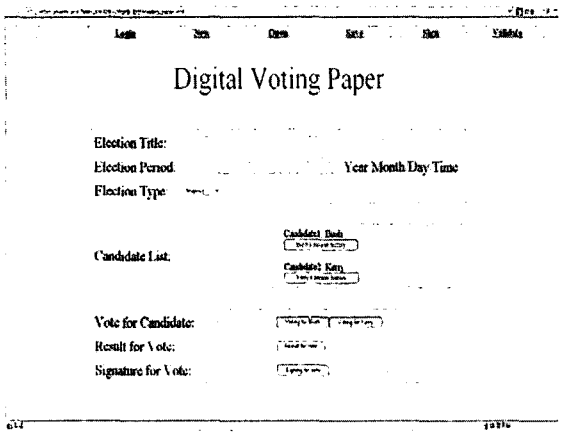
[그림 4]는 투표를 한 후, 거기에 전자서명과 암호화하면 서버상에서 투표자가 입력한 암호와 데이터베이스에 저장되어 있는 암호를 확인해서 맞으면 데이터베이스 테이블에서 투표결과 값을 읽어와 데이터베이스 서버에 저장된 유효한 투표결과를 집계하고 계수결과와 집계결과를 데이터베이스 서버에 저장한다. 이를 XML형식의 데이터로 전송하고, 별도로 작성한 스타일시트(pdate.xsl)와 스키마 문서(pdate.xsd)을 적용한 후, 투표자는 언제든 자신의 투표결과를 확인할 수 있다.



[그림 4] 계수 절차 모듈

4. 결론

본 논문에서 제안한 시스템의 구현 결과는 [그림 5]와 같다. 투표자 인증 절차 구현, 투표 절차 구현, 투표결과 보기 구현의 3 부분으로 구성되어 있는 투표자 인터페이스에서 투표자가 필요로 하는 정보를 컴퓨터 모니터 화면을 통해서 보여주고 투표자가 원하는 작업을 시받아 수행할 수 있도록 하는 화면이다.



[그림 3] 전자투표 문서

이를 구현하기 위해 필요한 구현 환경 설정은 [표1]와 같다. 일반적인 JSP 애플리케이션에서는 클라이언트의 요청에 대해 HTML 형식의 데이터를 전송하 만, 이 논문에서 구현한 XML 전자투표 시스템은 클라이언트의 요청에 대한 HTTP 응답메시로 HTML이 아닌 XML 형식의 데이터로 전송을 한다. 그리고 XSL 기술을 이용해서 서버로부터 클라이언트로 전송한 XML 형식의 데이터에 스타일시트를 별도로 만들어 콘텐츠와 스타일을 분리해서 처리하여 전자투표 프로세스의 내용은 동일하 만 사용자별로 다른 스타일이 적용된 전자투표를 서비스할 수 있다.

제안한 XML 기반 전자투표 시스템은 전자투표의 요구사항을 모두 충족한다. XML-Signature와 XML Encryption 기술을 사용하여 "Enveloped" 서명과 암호화를 생성하기 위해 XML Security Suite의 XML-Signature Implementation와 XML Encryption Implementation을 참조해야 한다[4][5]. 즉, 투표값의 기밀성은 XML 암호화을 이용하여 이루어 고 투표에 관련된 전자문서의 안전성은 XML 전자서명을 적용하여 달성된다. 서버와 클라이언트간의 인증은 공개키 기반 구조에서 제공하는 인증서를 사용해서 투표자의 이중투표방 와 인증서를 가진 사람만이 투표할 수 있도록 X.509 V3 표준을 기반으로 인증서를 구성해서 인증절차를 수행할 수 있다.

또한 투표결과의 검증은 전자문서의 유효성 검증에 의해 이루어진다. 여기서는 XML 문서의 유효성을 검증하기 위해 XML 파서를 이용하였다.

[표 1] XML 전자투표 시스템 구현 환경

항 목	버전
XML Security Suite	XML-Signature/Encryption Implementation
XML 파서	Apache Xerces-J
Java 환경	J2SDK1.4.1_04
Java 암호 라이브러리	JCA/JCE
JSP환경	Jakarta-Tomcat-3.3.1

본 연구에서 구현한 시스템 모델을 Devegili와 Neto가 제안한 시스템과 비교하여 위의 기술한 내용을 간단히 표로 나타내자면 다음과 같다.

[표 2] 구현 시스템 평가

요구사항	Devegili&Neto의 전자투표 시스템	제안한 전자투표 시스템
무결성	0	0
이중투표 불가성	0	0
투표값의 기밀성	X	0

5. 참고문헌

[1] W3C, XML-Signature Syntax and Processing, http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/, 2002.
[2] W3C, XML Encryption Syntax and Processing, http://www.w3.org/TR/2002/CR-xmlenc-core-20020802/,2002.
[3] A. J. Devegili and H. E. V. T. Neto, "Applying XML Signatures to the Definition of an XML Schema for Digital Ballots," Computer Communications, Vol. 27(3), 2002.
[4] IBM, XML Security Suite, XML-Signature Implementation, http://www.trl.ibm.com/projects/xml/xss4j/docs/dsig.html,2002
[5] IBM, XML Security Suite, XML Encryption Implementation, http://www.trl.ibm.com/projects/xml/xss4j/docs/enc-readme.html, 2002.