

다중모달을 이용한 전자상거래시스템 개발

장찬용^{*} · 류갑상^{*}

^{*}동신대학교

Development of a Electronic Commerce System of Multi-Modal Information

Chan-young Jang , Gab-sang Ryu^{*}

^{*}Dong shin University

E-mail : newshin2001@empal.com

요 약

다중정보를 이용한 개인 인증시스템은 음성인식, 얼굴인식, 전자서명 등의 방법을 이용하여 보안 시스템을 구축하는 기술로서 통신망 전반에 존재하는 많은 위협들로부터 중요한 정보를 보호할 수 있는 매우 효율적인 방법이다. 본 논문에서는 공개키 암호 및 전자서명 기술을 기반으로 디지털 정품 컴퓨터 S/W 및 H/W 와 관련된 제품을 인터넷 공간에서 거래할 수 있는 전자상거래 시스템(CBT-Shop)을 구현하였다. 다중정보의 개인인증 기술을 싸이버테크 인터넷 쇼핑물의 설계와 구현에 적용함으로써 보안이 고려된 상거래시스템 구현이 가능하게 됨을 설명하고 있다.

ABSTRACT

Individual authentication system that take advantage of multimodal information is very efficient method that can take advantage of method of speech recognition, face recognition, electron signature etc. and protect important information from much dangers that exists on communication network whole as skill that construct security system. This paper deal product connected with hardware from internet space based on public key sign and electron signature description embodied system. Maintenance of public security is explaining that commercial transaction system implementation that is considered is possible as applying individual authentication.

키워드

전자상거래시스템, 멀티모달 개인인증기술, 음성인식, 전자서명

1. 서 론

다중정보를 이용한 개인 인증시스템은 음성인식, 얼굴인식, 전자서명 등의 방법을 이용하여 보안시스템을 구축하는 기술로서 통신망 전반에 존재하는 많은 위협들로부터 중요한 정보를 보호할 수 있는 매우 효율적인 방법이다.

일반적으로 말하는 전자서명은 서명자의 지문이나 기타 이미지 데이터를 데이터베이스에 저장한 후 필요에 따라 꺼내어 복사하는 방식의 메커니즘을 갖는다. 이 경우에는 디지털 데이터(digital

data)의 특성상 쉽게 복제가 가능하여 저장되어 있는 이미지 데이터를 서명자이외의 사람이 그 데이터를 얻게 되면 무제한 복사가 가능해서 마치 남의 도장을 훔쳐서 마음대로 서명하는 것과 같은 결과를 초래할 수도 있다. 전자 서명 알고리즘은 메시지에 자신의 서명키로 서명하여 무결성 및 인증을 만족 시킬 수 있는 알고리즘이다. 보통 암호와 알고리즘 하나만 사용하는 것이 아니라 메시지를 One-way hash 알고리즘으로 일정한 크기의 데이터로 변환한 후에 비대칭키 암호와 알고리즘으로 암호화하는 형태이다. 서명에 대한 확

인은 복호화한 데이터와 원래 메시지를 One-way hash 알고리즘으로 변환한 데이터를 비교하여 수행한다. 화자식별은 음성에 포함되어 있는 화자 개인의 정보를 추출하여 등록된 화자를 확인하는 기술이다. 기본적으로 화자인식은 개인의 공통적인 발성의 특징을 찾아서 이를 저장 해 놓고, 입력되어 들어오는 특징과 비교하여 가장 유사한 발성을 선택하는 것이다. 화자인식을 위한 데이터 베이스는 다양한 환경의 많은 사람의 음성으로 구성되어 있다. 예를 들어 나이, 성별, 사용환경, 사용하는 마이크의 종류, 주위 잡음의 정도에 따라 구성되어 있는 수백명의 발음으로 구성되어 있다. 데이터베이스 구성 후 컴퓨터로 입력하기 위해 Analoge-Digital Converter를 거쳐 각 발성에 대한 특징을 추출하게 되는데 포먼트 정보, LPC 계수, 전체 power 성분과 같은 특징이 추출된다. 본 기술개발에서는 전자서명 기술과 음성 인식 기술을 통합하여 개인을 인증하는 그림 1과 같은 시스템을 설계하고 구현하는데 그 목적이 있다.

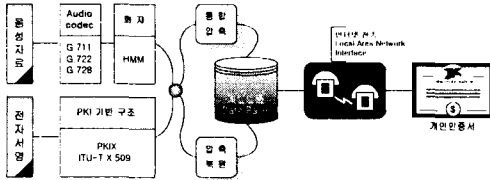


그림 1. 전체시스템 개요도

II. 시스템 설계

1 시스템 설계

공개키 암호 및 전자서명 기술을 기반으로 디지털 정품, 컴퓨터 S/W 및 H/W 와 관련된 제품을 인터넷 공간에서 거래할 수 있는 전자상거래 시스템(CBT-Shop) 을 구현하였다. CBT-Shop 시스템은 유통서버시스템, 사용자 시스템, 판매자 시스템으로 구성되어 있으며 다음 그림2 와 같은 구조로 설계되었다.

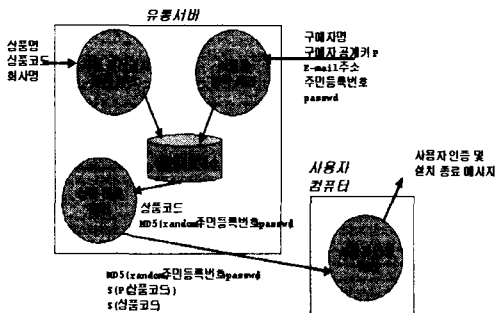


그림 2. CBT-Shop 시스템의 구조도

2 유통서버 시스템

유통서버시스템(DS: Delivery Server)은 상품의 판매 단계 중 유통을 위한 상품 등록, 사용자의 지불 이후 판매자 시스템에서 OI(Order Information)을 수신하여 탁송 처리, 탁송 내역 관리, 사용자 시스템에 디지털 상품 설치 시 온라인 등록 관리 및 사후 서비스 처리 내역 관리등을 수행하는 시스템으로 정의한다. 전달 유통 서버 시스템을 통해, 상품의 다양화와 비용을 절감할 수 있으며, 유통 기능을 통합하여 안전하게 관리할 수 있다.

1) 웹 서버(Web Server)

사용자가 유통 서버 시스템에 접근하는 동시에 지적 재산권자가 상품을 등록하는 일련의 과정을 쉽게 하는 방법은 유통 서버에 웹 서버를 설치하는 일이다. 웹 서버는 유통 시스템을 방문하는 사용자, 지적재산권 소유자 그리고 관리자로부터 데이터를 전송 받는다. 홈페이지는 서블릿(Servlet)으로 구성되어 있어서, 유통 서버 사용자가 홈페이지에 작성한 데이터는 유통 서버내의 클래스를 통하여 유통 서버 내부 모듈로 전달된다.

2) Interface(인터페이스)

CBT-Shop 시스템에서의 유통 서버는 전자 상거래의 일환으로서 전자 상거래가 가지는 모든 시스템과의 데이터 교환이 필수적이다. 따라서 이러한 필수적인 시스템과의 데이터 교환에 적용할 수 있는 인터페이스들이 필요하다. 유통 서버가 필요로 하는 인터페이스들은 다음과 같다.

- ① 사용자와 지적재산권자 그리고 유통서버 모두 믿을 수 있는 인증기관과의 인터페이스가 필요하다.
- ② 전자 상거래이므로 상품의 가격을 지불하거나, 지적 재산권 소유자에게 상품의 대금을 지불할 수 있도록 지불 기관과의 인터페이스가 필요하다.
- ③ 유통서버는 이 모든내용을 저장하고 관리하여야 하므로 데이터베이스와의 인터페이스가 필요하다.
- ④ 상품 구매 후 유통 서버와 구매자 클라이언트 환경의 메시지 교환이 필요한 경우 이를 지원하기 위한 네트워크 인터페이스가 필요하다.

3) 내부 모듈

유통 서버 내부 모듈은 웹 서버로부터 데이터를 전송 받고 이를 처리하여 다시 홈페이지를 업데이트 하는 형식을 취한다. 작업에 따라서 각각의 내부 모듈은 주변 시스템과 인터페이스를 이용하여 데이터 교환을 한다. 유통 서버가 수행해야 하는 일들을 크게 네 가지 모듈로 나눈다.

- ① 관리자 모듈은 관리자가 접속하였을 경우

유통 서버시스템 전반에 걸쳐 관리할 수 있는 기능을 지원한다. 관리자 모듈에서는 현재 진행하고 있는 모든 모듈들의 상태를 모니터 할 수 있는 동시에 조정이 가능해야 한다.

- ② 회원 관리 모듈은 회원 관리 모듈은 인증 기관과 연결하여 유통 서버를 이용하는 모든 사용자의 회원 등록, 처리, 관리를 담당한다.
- ③ 재산권자 관리 모듈은 지적 재산권자가 서버 이용시 처리를 담당하는 모듈이다. 재산권자 관리 모듈은 지적 재산권자가 등록한 상품 정보, 처리, 판매 내역 등을 관리하며, 상품 제작 모듈과 연결하여 지적 재산권자의 상품 제작 정보를 관리한다.
- ④ 사용자 관리 모듈은 유통 서버를 이용하는 사용자를 담당하는 모듈이다. 사용자 관리 모듈은 사용자의 상품을 구매하는 사용자의 정보관리, 지불처리를 담당한다.
- ⑤ 상품 패키징 모듈은 저장된 상품을 데이터베이스로부터 읽어서 상품을 사용권을 사용자의 공개키로 암호화한 후 유통 서버의 비밀키로 서명하고 사용자에게 전송한다. 제작 상품의 정보는 재산권자 관리 모듈과 연결하여 관리된다.

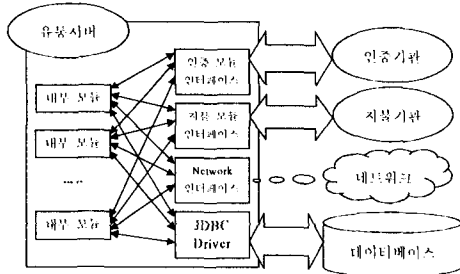


그림 3. 유통서버의 인터페이스

III. CBT-Shop 구현

1.) CBT-Shop 초기화면

싸이버테크 인터넷 쇼핑몰(CBT-Shop)은 탑메뉴(Top-Menu) 와 주메뉴(Main-Menu) 로 구성되어 있다. 탑메뉴에는 쇼핑물 안내, 고객의 소리, 주문 조회, 회원 가입의 메뉴가 있고, 주메뉴에는 컴퓨터, 컴퓨터 관련기기, 소프트웨어, 통신사무기기, 영상제품, 음향제품, 검색(search), 동호회, 사고팔고, 소모품&악세사리의 메뉴가 설계되어 전자상거래를 실현한다.

① Top-Menu

- 쇼핑물안내: 쇼핑물소개, 이용안내, 마일리지
- 고객의 소리: 공지 사항, 자유게시판, 고객의 소리, 클릭 정보
- 주문 조회: 주문 현황, 조회 이력
- 회원 가입: 쇼핑물 회원가입
- 장바구니: 쇼핑한 물건을 장바구니에 보관
- 주문: 장바구니에 쇼핑한 물건을 주문
- Sitemap: CBT-Shop 에 대한 사이트 맵

② Manin-Menu

- Sun 제품: Sun 워크스테이션과 관련된 제품
- 컴퓨터/주변기기: PC 및 주변기기 제품
- Software: 컴퓨터 소프트웨어 제품
- 통신사무기기: 통신에 관련된 사무기기
- 영상제품: 영상에 관련된 제품
- 소모품&악세사리: 컴퓨터 소모품/악세사리
- 동호회: 동호회 이용, 개설, 동호회목록
- 사고팔고 : 삽니다, 팝니다

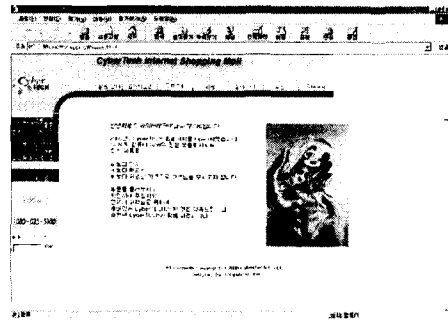


그림 4. CBT-Shop 초기화면

2) 회원 등록

CBT-Shop 사용을 위한 회원의 등록을 받는다. 제시된 이용약관에 동의한 사용자는 다음에 주어지는 필수입력사항 및 선택입력사항을 입력하고 등록 아이콘을 클릭하면 회원으로 등록이 된다. 필수 입력사항에는 주민등록번호를 입력하고, 마이크 아이콘을 클릭하여 연결된 마이크를 통해 회원의 주민등록번호를 음성으로 등록하도록 되어있다. 그림 5는 회원등록의 화면을 보인 것이다.

<표 1> 장바구니 테이블

컬럼명	데이터형	제약조건	설명
OrderNum	numeric(18,0)	NOT NULL	주문번호
Pro_ID	varchar(15)	NOT NULL	구매상품의 Prod_ID
Quantity	int	Default (1)	구매수량
Price	int	NOT NULL	구매상품의 가격

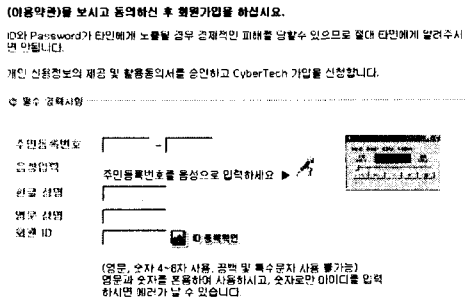


그림 5. 회원등록 예

3) 제품선택 및 장바구니

사용자가 물품을 구매하기 위해서 Main-Menu 상의 원하는 품목의 메뉴를 마우스로 클릭하면 관련된 상세한 품목의 Sub-Menu 가 나타난다. 이들 메뉴 중 원하는 품목(멀티미디어카드)의 메뉴를 클릭하면 그림6과 같은 화면이 나타나는데 VGA 카드의 'SMART TNT2 ULTRA'를 선택하고 상세보기를 클릭하면 해당 제품의 상세 정보를 보여준다. 사용자는 제공되는 제품의 상세 정보를 숙지한 후 구매를 예상하는 제품을 장바구니에 담게 된다. 그러나 장바구니에 담긴 내용만으로 구매를 한다고 볼 수 없기 때문에 수취인 정보가 입력되기 전에는 모든 정보를 Session 객체를 이용해 임시적으로 저장한다. 장바구니 테이블은 주문번호와 구매하는 상품의 Prod_ID, 구매수량, 상품의 가격을 저장한다.

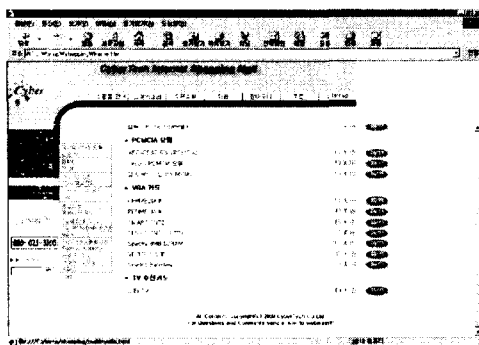


그림 6. 제품선택 화면

4)주문하기

소비자가 구매할 제품을 하나씩 장바구니에 담은 후 쇼핑을 마치고 최종적으로 구매할 제품을 주문하게 된다. 이때 사용자는 장바구니에 담은 제품의 수량을 변경하거나 항목을 삭제할 경우가 발생할 수 있으므로 그림 19 와 같이 이를 처리

할 수 있도록 설계하였고, '주문' 버튼을 실행하면 다음과 같은 결제안내와 대금지불을(카드,통장) 위한 사용자의 입력 정보를 처리하도록 개발하였다.

결제안내

1. 주문 내역

상품명	수량	단가	판매가	금액
SMART TNT2 ULTRA	1	₩ 215,000	215	₩ 215,000
스타 TV	1	₩ 68,000	68	₩ 68,000
PERMEDIA II	1	₩ 51,000	51	₩ 51,000
합계				₩ 335,000

2. 대금지불방법선택

카드

- × 할부는 5만원 이상의 상품에 대해서만 가능합니다.
- × 카드 할부 구매시 해당카드사의 수수료율에 따라 할부 수수료가 부과됩니다.
- × 카드 결제 대금 청구시 'CyberTECH' 명의로 청구됩니다.

3. 카드종류

4. 카드번호

- × 다이내믹 카드는 14자리만 기입해주세요

5. 만기일(월/년) (MM/YY)

V. 결 론

본 논문에서는 다중정보를 이용한 개인 인증시스템으로 음성인식 및 전자서명 등의 방법을 이용하여 디지털 정품, 컴퓨터 S/W 및 H/W 와 관련된 제품을 인터넷 공간에서 거래할 수 있는 전자상거래 시스템(CBT-Shop)을 설계하고 구현한 사례를 기술하였다. 기존에 발표되어 있는 기술들을 프로그램화하여 전자상거래사이트 구축에 적용함으로써 보안이 고려된 시스템 구현이 가능하게 됨을 설명하였다. 개발된 CBT-Shop은 현재 인터넷상에서 운용되고 있으며 개인인증과 관련된 기술의 지속적인 보안을 통해 사이트 품질을 개선해 가고 있다. 앞으로 음성인식을 통한 개인인증 기술을 더욱 발전시켜 손쉽게 멀티모달이 적용된 개인인증기술을 전자상거래사이트 구축에 적용할 수 있도록 연구를 계속하고자 한다.

참고문헌

- [1] 김태운, "디지털상품 정품 인증 프로토콜 설계 및 시험시스템 개발", 한국전자통신연구원, 1999.11
- [2] 이용효, "전자상거래의 신뢰성 확보를 위한 법적정비 방안", 한국전산원, 1998.6
- [3] 박성준, "공개키 기반구조 표준화 동향", 한국전산원, 1998.5
- [4] 홍승준, "화자식별과 얼굴인식을 이용한 대규모 보안시스템", 정보과학회논문집, 1999.9
- [5] R. Housley, W. Ford, W. Polk, D. Solo, X.509 Certificate and CRL Profile, <http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-part1-07.txt>, 1998. 3