PDA를 이용한 실시간 모바일 귀금속·보석 B2B 시스템 구현

김영운*, 이혜정, 정성태, 정석태
원광대학교 컴퓨터공학과

{kyw1007°, redrose, stjung, stjoung}@wonkwang.ac.kr

Implementation of Realtime Mobile precious metals · jewels B2B System

Young-un Kim°, Hyae-jung Lee, Sung-tae Jung, Suck-tae Joung
Dept of Computer Engineering, Wonkwang University

요 약

귀금속·보석 분야의 업무 전산화 이전에는 원시적인 기입식 장부정리로 비효율적인 상품관리와 인적 자원낭비가 심하였다. 그러나 최근 많은 업체들이 전자적인 문서관리 시스템 도입으로 업무능력 향상과 비용절감 효과로 업체의 경쟁력이 높아지고 있다. 이에 따라 기존 텍스트 기반 정보에서 벗어나 멀티미디어 기반의 정보를 요구하고 있으며, 상품 정보의 전자카탈로그(E-Catalog) 시스템 도입으로 실시간 상품 이미지와 정보를 제공해 판매자와 고객 간의 신뢰할 수 있는 정보 제공과 모바일(Mobile) 통신의 장점인 이동성, 편재성, 실시간성, 휴대성 등을 활용한 기술개발 및 상품화가 요구되고 있다. 본 논문에서는 모바일 기술을 활용하여 휴대용 단말 장치를 이용한 귀금속·보석분야의 이동성이 보장되는 휴대용 B2B 시스템을 구축하였다.

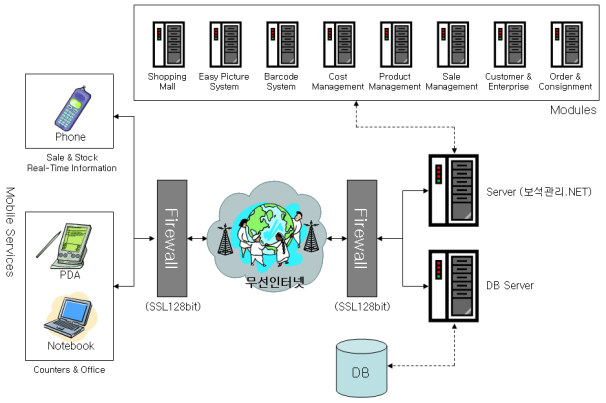
1. 서론

귀금속·보석 분야의 업무 전산화 이전에는 원시적인 기입식 장부정리로 비효율적인 상품관리와 인적 자원낭비가 심하였고, 제조, 유통 및 판매에 이르기 까지 전산화가 미흡하여 판매 및 유통에서 소매, 도매, 프랜차이즈에 이르기 까지 통합 환경 구축이 필요하였다. 그러나 최근에는 많은 업체들이 전자적인 문서관리 시스템을 도입하고 있어 업무능력 향상과 비용절감 효과로 업체의 경쟁력이 높아지고 있으며, 최근 인터넷 사용자의 급증으로 많은 시스템들이 서로 네트워크로 연결되어 정보의 공유와 효율적인 정보관리를 필요로 하고 있다. IT기술의 발달로 인터넷과 통신기술이 빠른 속도로 발전 하고 있으며, 무선인터넷과 Mobile기술을 활용한 시스템 구축이 활발해 지고 있다. 특히 귀금속·보석 분야는 판매장 내의 공간 제약과 이동성 보장이 절실한 상황이며, 이를 해결하기 위한 대안이 바로 Mobile과 무선인터넷 기술을 활용 하는 것이다. 또한 이러한 인터넷이라는 불완전한 개방형 네트워크에서 안전한 업무 실현을 위해서는 사용자의 pc접근 제어의 물리적인 보안뿐 아니라 데이터· 통신 및 거래를 보호하기 위한 추가적인 전자적 보안 수단이 필요하다.[1][2][3][4][5][6][7]

본 논문에서는 기존 유선 네트워크 환경에서 제공하는 솔루션에서 PDA기반의 유무선 통합네트워크 환경을 구축함으로서 휴대용 단말 장치를 이용하여 휴대성과 이동성이 보장되는 B2B 시스템을 구축하고 이에 필요한 보안기술에 관하여 연구하였다.

(그림 1)은 모바일기반 PDA 서비스 구성도이다. 서버 측 환경 구성은 데이터베이스 시스템과 각 세부 기능 모듈로 구성되어져 있다. 세부 모듈은 원가관리, 제품관리, 판매관리, 고객관리, 주문관리, 사진관리, 바코드관리, 온라인 쇼핑몰 등으로 이루어져 있다. 클라이언트 측 환경은 모바일 환경인 무선 환경과 유선 환경으로 나누어볼 수 있다. 클라이언트/서버 유무선 네트워크 환경은 방화벽인 보안시스템이 양 끝단에 존재하고 있으며, 128bit SSL 보안과 암호화기술, PKI 인증 모듈로 이루어져 있다. 본 논

문에서는 모바일 환경을 중심으로 시스템을 구축 하였으며, 주요 클라이언트로는 휴대폰, PDA, 노트북과 같은 이동성이 보장되는 시스템이 있다. 이중 PC 환경과 유사하고 모바일 환경 지원이 뛰어난 PDA 기반의 시스템을 기본 모델로 사용 하였으며, 운영체제는 마이크로소프트 Pocket PC 2003을 사용 하였다.[8][9]

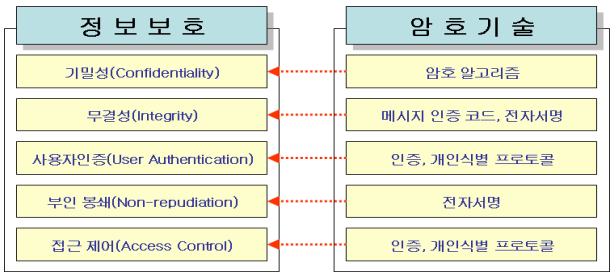


(그림 1) 시스템 구성도

2. 관련연구

클라이언트/서버(Client/Server) 기반의 통합 시스템 구축에 필요한 Mobile 기술과 보안과 인증기술을 위한 연구 내용을 보면 다음과 같다.

모바일 기술을 이용한 유·무선 통합 네트워크망을 구축하고, 3-Tier(Client/Server) 기반의 분산 미들웨어를 적용, 유·무선 네트워크 기반 PKI 및 WPKI 인증 서버 구축과 암호화 및 복구화를 위한 SSL 및 WTLS 보안 모듈, PDA 기반 인증모듈 및 보안 모듈이 있다.

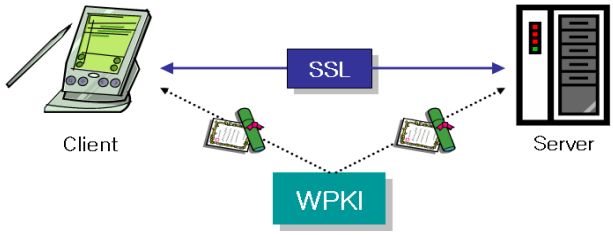


(그림 2) 정보보호와 암호기술

(그림 2)는 정보보호에 대한 암호기술들을 나타내는 그림이다.[10] 클라이언트와 서버간의 통신에 가장 필요한 것은 신뢰성이다. 이러한 신뢰성을 확보하기 위해 보안과 인증 기술이 필요하며, 정보보호의 기본 충족 조건인 기밀성, 무결성, 사용자인증, 부인봉쇄, 접근제어 등을 만족하는 암호화 기술들을 정립하고 구축해야 한다.[2][10]

정보보호에 대한 암호기술들에 대해 살펴보면 다음과 같다. 먼저 암호화에 필요한 암호 알고리즘으로는 비밀키 암호 알고리즘, 공개키 암호 알고리즘, 복합 암호 알고리즘이 있다. 비밀키 암호 알고리즘의 가장 대표전인 시스템은 DES이며, 공개키 암호 기법은 인수분해를 사용하는 RSA와 이산 대수를 사용하는 EI로 분류된다. 복합 암호 알고리즘은 비밀키와 공개키 암호 방식의 장점을 최대화하고 단점을 최소화하여 설계한 것이다. 전자서명 알고리즘(무결성/출처인증/부인봉쇄)은 전자서명의 요구 조건인 위조 불가, 서명자 인증, 재사용 불가, 변경 불가, 부인 불가 등의 요구 조건을 충족하는 “디지털 서명” 시스템을 구축 할 수 있다. 사용자 인증과 접근제어 모듈은 사용자에 대한 지식, 소유물, 신체적/행위적 특징들의 확인을 통해 접근제어 시스템을 구축하며, 비 안가된 동작들의 위협에 대해 자원을 보호하고, 접근제어정책에 의해(신분기반정책, 규칙기반정책, 직무기반정책) 보호하는 시스템을 구축 할 수 있다.[2][3][10]

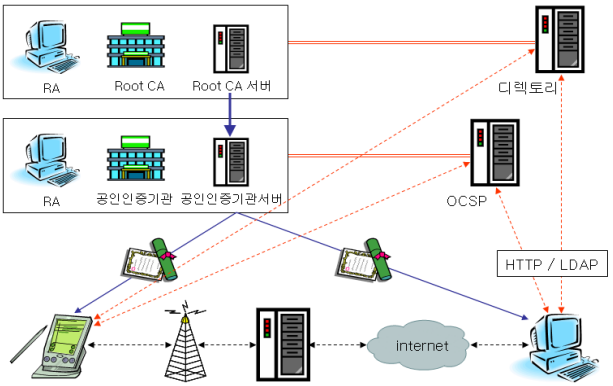
(그림 3)은 클라이언트와 서버간의 무선 인터넷 보안 그림이다.[4] 무선 인터넷 보안 시스템을 구축하기 위해서는 인증서 배포를 담당할 인증 서버 구축에 필요한 제반 기술 획득 및 시스템 구축과 WTLS/WALS 및 SSL 인증서 시스템을 구축해야 한다. 또한 Transaction Security와 Channel Security 만족하는 서비스를 제공해야 한다. Transaction Security는 응용 계층에서 전자서명을 통한 거래의 무결성, 부인봉쇄 서비스를 제공하여, Channel Security는 전송계층에서 암호화와 MAC을 통한 데이터 기밀성, 무결성 서비스를 제공한다.



(그림 3) 무선 인터넷 보안

(그림 4)는 클라이언트와 서버간의 무선 WPKI 모델이다.[4] 유선과 마찬가지로 무선 인터넷이 안전한 서비스를 제공받기 위해서는 기밀성, 무결성, 인증, 부인봉쇄와 같은 서비스를 제공하기 위한 무선 WPKI가 필요하다. 무선 WPKI 모델에서는 기본적으로 무선용 X.509 인증서를 사용하며, 단말기에서 무선용 X.509 서버 인증서의 검증 메커니즘으로는

CRL이나 OCSP를 사용하도록 한다. 서명 알고리즘으로는 RSA, ECDSA가 사용되며, 키 분배용으로 RSA, ECDH가 사용된다. 무선에서는 무선 환경에 맞는 인증서 요청 및 관리 프로토콜 규격을 사용한다.



(그림 4) 무선 WPKI 모델

3. 시스템 설계 및 구현

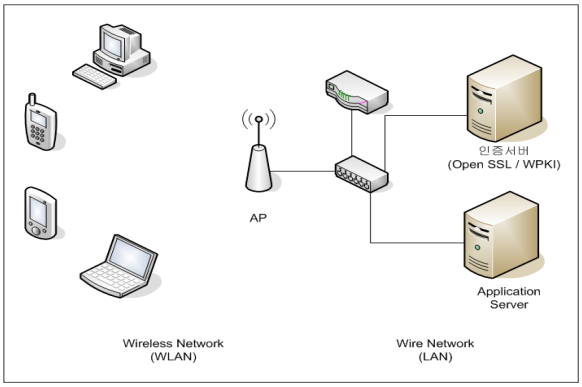
3.1 시스템 설계

가. 무선 인터넷 기반 미들웨어 환경

무선인터넷을 활용한 미들웨어환경 구축과 클라이언트/서버간의 데이터통신 방식에 대한 알고리즘 연구를 통해 실제 구현을 진행 하였다. 특히 마이크로소프트 .NET COM+기반의 미들웨어를 개발하였으며, 802.11b(WireLess LAN) 기반의 통신 모듈과 .NET Compact Framework 기반의 PDA(Pocket PC) 응용소프트웨어를 개발 하였다.

나. 무선 인터넷 보안과 인증 시스템

암호기술, PKI, 전송계층보안(SSL/TLS), 무선인터넷보안 등 크게 4개의 항목을 중심으로 구현하였다. 특히 전송계층보안은 Secure Sockets Layer (SSL v2/v3)와 Transport Layer Security (TLS v1) 프로토콜의 표준안을 사용하였다.



(그림 5) 무선 인터넷 보안과 인증 시스템 구성도

(그림 5)는 전체적인 무선 인터넷 보안과 인증 시스템을 도식화한 그림이다. Open SSL과 WPKI 서버, 어플리케이션 서버는 AP단말 장치를 통해 무선 네트워크 망을 구성한다. 클라이언트의 PDA 단말장치와 어플리케이션 서버간에 보이지 않은 보안 모듈을 제공하고 있다.

암호기술은 현대 업무가 인터넷을 통하여 수행될 때 발생 가능한 기밀성, 데이터 무결성, 메시지 인증, 사용자 인증, 부인방지와 같은 문제들을 해결해 주는 기술이다. 대표적인 암호 알고리즘은 DES, AES, DSA, SHA-1, MD5등이 있으며, 국내의 경우 SEED, KCDSA, HAS-160 등이 있다. 본 연구에서는 DES와 MD5 알고리즘을 사용하였다.[10]

PKI는 인증서 프로파일, CRL 프로파일, 인증서관리 프로토콜, 온라인 인증서 상태 검증 서비스 등의 표준이 개발되었으며, 인증서 관련 다양한 확장필드, 대리 인증 경로 검증 및 발견 서비스 등의 추가 표준 규격이 필요하다. 유선 인터넷 환경에서는 PKI, 무선 인터넷 환경에서는 WPKI, Wireless LAN (WLAN) 환경에서는 EAP-TLS 등이 적용되는데, 본 논문에서는 WPKI 기술을 사용하였다.[2][3]

무선 인터넷 보안은 무선 클라이언트와 서버간의 전송계층 및 응용 계층에서의 무선 전송계층 보안은 SSL기술과 OMA(Open Mobile Alliance)의 프로토콜 표준, 무선 공개키 기반구조, 그리고 관련 하드웨어 토큰 간의 인터페이스 표준을 중심으로 개발 하였다.[2][3]

3.2. 시스템 구현

(그림 6)은 시스템 구현 화면이며, PDA기반 보석관리.NET 초기화면과 사용자 인증 화면이다. 전체 메뉴 구성은 파일, 관리, 도움말로 구성되어져 있으며 하위 메뉴로는 고객관리, 매장관리(제품입고/제품출고), 주문관리, 재고관리 등으로 구성되어져 있다.

(그림 6) 초기화면 및 사용자 인증 화면

사용자 인증을 위한 로그인(Login)은 관리자 솔루션에 등록된 사용자만이 인증절차를 거쳐 사용할 수 있다. 즉 사용자는 보안과 인증 절차를 거쳐 허용된

기능을 사용할 수 있다. 예를 들어 매장에 근무하는 종업원은 매장관리 기능과 고객관리, 주문관리만 사용이 가능하다. 원가관리나 제품관리 등은 접근 할 수 없는 권한이므로 사용 할 수 없다.

(그림 7)은 고객관리 화면이다. 고객관리는 매장관리(판매출고)에서 사용되어지며, 고객의 정보를 관리하는 기능을 담당한다. 제공 되는 기능으로는 새로운 고객을 추가 하거나, 고객 정보의 수정, 삭제, 검색 하는 기능 들을 제공한다.

(그림 7) 고객관리 화면

(그림 8)은 매장관리 화면이다. 매장관리는 제품입고와 제품출고로 나누어진다.

(그림 8) 매장관리(제품 입고/출고) 화면

제품입고는 관리자 솔루션의 제품관리에서 출고된 자료를 바탕으로 상품을 입고하는 기능을 한다. 제품출고는 입고된 상품을 고객에게 판매 하거나 입고된 상품을 관리 하는 기능을 담당한다.

보석관리.NET의 관리자 솔루션은 크게 원가관리, 제품관리, 판매관리로 이루어져 있다. 원가관리는 Jewelry, Metal, Stone과 상품의 정보를 관리 하며, 제품관리는 원가관리에서 생성된 정보를 바탕으로 본사 차원에서 상품을 관리 한다. 제품출고(제품관리) 기능을 활용해 어느 매장으로 상품을 출고할 것인지 결정되어지며, 판매관리는 제품관리에서 출고된 상품을 매장별로 관리하는 역할을 한다. 여기서 판매관리는 PDA 솔루션에서 매장관리 기능에 해당된다. 즉 PDA 솔루션에서는 관리자 솔루션에서 제공된 데이터를 받아 최종 상품의 판매관리를 담당하게 된다. 주문관리는 매장에서 고객이 요구하는 상품을 직접 주문을 받아 고객에게 판매 하는 역할을 담당 한다. 제공 기능으로는 주문서 작성, 수정, 취소 등이 있다. 재고관리는 매장에서 보유하고 있는 상품을 관리 하기위해 제공되는 기능으로 실재 매장의 재고목록을 파악 할 수 있다. 또한 바코드 신식기술을 활용해 쉽게 재고관리가 이루어 질수 있도록 제공한다.

4. 결 론

본 논문에서는 유·무선 네트워크의 통합과 이에 따른 보안에 관한 연구를 진행하여, 무선 단말 장치와 무선 AP 송수신 장치들을 무선 환경에 맞게 구축하였고, 기존 유선망과 연동하여 완벽한 유·무선 망간의 통합 시스템을 구축하였다. 특히 PDA 단말 장치를 이용해 무선 인터넷 환경과 귀금속 분야에서 사용할 수 있는 응용소프트웨어 B2B 시스템을 개발하였다. 기존 PC기반의 유선 인터넷 환경에 비해 PDA기반의 무선 인터넷 환경을 사용하기 위해서는 많은 제약과 문제점을 가지고 있다. 이런 문제점을 해결 하기위해 연구가 진행 되었으며 많은 성과를 얻을 수 있었다.

참고문헌

[1] 박성준, "C# & .NET Programming Bible", 영진닷컴

[2] 박정환, "무선 PKI 기술 규격", 한국정보보호진흥원

[3] 이용, "무선 PKI 규격", TTA

[4] Carlisle Adams, Steve Lloyd, "Understanding PKI : Concepts, Standards, and Deployment Considerations (2nd Edition)", Addison-Wesley Professional

[5] Stephen A. Thomas, "SSL and TLS Essentials Securing the Web", WILEY

[6] John Viega, "Network Security with OpenSSL", OReilly

[7] "http://www.openssl.or.kr/", OpenSSL

[8] Craig Morris, ".NET Compact Framework", Wrox

[9] 안원국, "C# .NET Mobile Programming : Pocket PC로 배우는", 영진닷컴

[10] 장관호 외, "디지털 서명을 위한 해쉬 알고리즘의 표준화 연구", 한국전산원