

스마트 카드 기반 사이버 교육시스템

이정우, 전성익
한국전자통신연구원
e-mail : jeow7@etri.re.kr, sijun@etri.re.kr

On the Design of Smartcard-based Cyber Education systems

Jeong-Woo Lee, Sung-Ik Jun
Electronics and Telecommunications Research Institute

요 약

뛰어난 보안성과 다기능성으로 금융, 교통 등 각종 분야에서 스마트카드의 활용이 점차 늘어나고 있다. 이런 스마트 카드의 장점을 사이버 상에서 이루어지는 교육시스템에 적용시켜 보고자 한다. 기존의 사이버 교육시스템을 중심으로 보안성이 중요시되는 지불 및 교육컨텐츠 보호관련 부분들과 타 시스템 이용에 관련된 부분들에 스마트 카드를 도입하여 보다 편리하고 안전한 시스템을 구성해 보았다.

1. 서론

최근 금융시장을 기반으로 하여 스마트 카드의 활용이 점차 확대되어 가고 있다. 기존의 마그네틱 카드의 한계를 뛰어 넘어 빠르게 발전하고 있는 스마트 카드의 성능은 조만간 거의 모든 분야에서 스마트 카드가 활용되도록 만들 것이라 생각된다. 이런 스마트 카드를 현재 사이버 상에서 이루어지고 있는 교육시스템에 도입시켜 보았다. 사이버 교육 또한 시간과 장소에 구애받지 않고 교육을 받을 수 있다는 점과 각종 멀티미디어 콘텐츠를 이용함으로써 얻을 수 있는 뛰어난 교육 효과 때문에 이미 많은 곳에서 다양한 교육 프로그램들이 행해지고 있다. 특히 이런 교육 시스템들에서는 각종 디지털 콘텐츠들이 많이 만들어지고 이용되기 때문에 이에 대한 저작권 및 사용권한에 대한 보호와 통제가 중요시 되고 있다. 또한 교육과 더불어 이루어지고 있는 각종 구매 및 지불절차는 이런 시스템에 중요한 부분이기도 하다. 이러한 부분들에 있어서 뛰어난 보안성과 안정성을 바탕으로 다양한 기능을 수용할 수 있는 스마트 카드를 활용함으로써 보다 안전하게 편리하게 교육받을 수 있는 환경을 만들어 보고자 한다. 사이버 교육과 관련된 많은 연구들이 행해지고 있으며 대부분 어떻게 하면 교육효과를 높일 수 있는가에 초점이 맞춰져 있다면 본 논문에서는 사이버 교육 시스템을 안전하고 편리하게

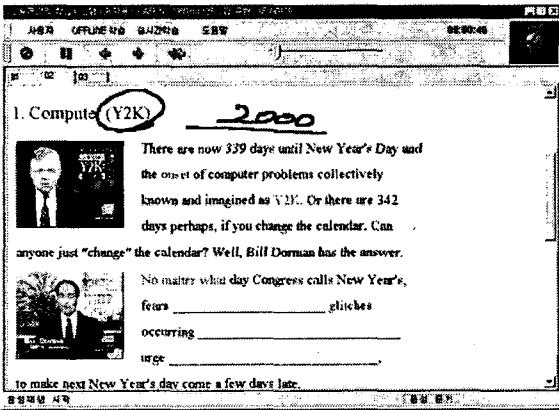
이용할 수 있는 시스템 구성의 측면에 초점을 맞추어 보고자 한다.

2. 사이버 교육의 형태

현재 다양한 분야에서 사이버 교육이 행해지고 있다. 특히 멀티미디어 기술의 발달은 다양한 형태의 수업 도구들을 만들어 냈으며 이와 더불어 네트워크 기술의 발달로 비교적 큰 크기를 가진 멀티미디어 데이터의 빠른 전송이 가능해짐에 따라 사이버 교육 시스템들이 점차 발전해 나가고 있다. 이전과 다르게 한번 교육이 아닌 평생교육으로 대두되는 새로운 교육 패러다임[1]이 생겨나면서 다양한 계층에서 다양한 교육에 대한 수요가 증가하고 있으며 이렇게 각각 시간과 장소에 구애받지 않고 자신의 수준에 맞춰 교육환경을 제공해줄 수 있는 사이버 교육에 많은 관심과 참여가 이루어지고 있는 실정이다.

여러가지 형태로 사이버 교육[2-4]을 분류해 볼 수 있지만 교육이 이루어지는 시간을 기준으로 볼 때 실시간 교육과 비실시간 교육으로 나누어 볼 수 있다. 먼저 실시간 교육은 각기 다른 장소에 있지만 같은 시간에 이루어지는 교육을 말한다. 즉 교수와 학생이 동일한 시간상에 존재하여 즉각적인 반응이 오고 가는 형태를 이루게 된다. 이는 사이버상이 아닌 실제 교실 수업에 근접한 형태로서 화상 및 음성의 교류를 통해 사이버교육에 대한 거부감이 덜하면서 즉각적인

피드백이 이루어짐으로써 다른 형태의 시스템들에 비해 보다 나은 교육효과를 거둘 수 있다. 하지만 화상이나 음성이 오고 가는 시스템의 경우 안정적인 네트워크 사정과 데이터의 품질이 보장되지 않으면 더 많은 불편함을 초래하게 된다. 이런 문제로 인해 아직 많은 이용은 없지만 점차 이용이 증대하게 될 것이다. 비실시간 시스템의 경우 교수와 학생이 동시에 대면하지 않는 경우이다. 대부분의 사이버 교육시스템이 택하는 방식으로 대개 해당 사이트에 접속하여 교수가 미리 제작해놓은 강의 교재를 학생이 다운받는 식이다. 즉각적인 피드백이 이루어지지 않는 단점이 있기는 하지만 시간적으로 교수와 동시에 만나기 힘든 경우나 반복적으로 학습할 수 있다는 장점이 있다. 일부 시스템의 경우 단순히 그림과 문자만으로 이루어진 교재가 아니라 마치 지금 강의하는 것처럼 느낄 수 있는 멀티미디어 교재를 사용하여 학습효과를 높이고 있다. 현재 많은 수의 사이버교육이 무료로 이루어지고 있지만 점차 유료화되고 있다. 이는 우수한 콘텐츠를 만들 수 있는 배경이 될 수 있으며 단순히 교육만이 아닌 다양한 서비스를 제공할 수 있는 기회를 만들어 주게 된다. 그림 1은 이런 사이버 교육시스템에서 제공하는 멀티미디어 틀의 한 종류이다



[그림 1] 멀티미디어 콘텐츠의 재생

대부분의 사이버 교육시스템을 통해 행해지는 처리들은 다음과 같다.

- 등록 및 로그인 과정
- 교육콘텐츠 제작 및 이용
- 등록비 등 각종 지불
- 구매 등 전자상거래

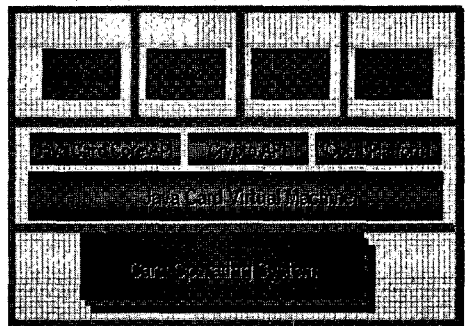
사용자는 등록과정을 거쳐 원하는 교육과정을 택하게 되고 이에 대한 대가를 지불하게 된다. 그리고 해당 교육콘텐츠를 이용하여 학습을 하게 된다. 좀 규모가 큰 시스템의 경우 각종 물품 등을 구비하여 사용자가 구매할 수 있도록 한다. 그 밖에 다른 이용자와 교류할 수 있는 공간을 마련하고 있다.

이런 사이버 교육시스템을 이용함에 있어서도 기타 사이버 상에서 발생하는 문제들이 나타나게 된다. 먼저 개인 정보가 유출될 수 있다는 점이다. 현재 대부

분의 시스템에서 택하고 있는 아이디와 패스워드를 이용한 인증방식에는 한계가 있다. 유출된 아이디와 패스워드는 돈을 내지않은 타인이 콘텐츠를 이용할 수 있는 기회를 제공함과 동시에 등록된 개인정보가 불법적으로 사용될 수 있다. 그리고 많은 곳에서 교육효과를 높이기 위해 단순한 텍스트 형태의 교재가 아닌 멀티미디어 교재가 사용되고 있는데 인쇄물이 아닌 이런 디지털 콘텐츠들은 그 특성상 쉽게 복제될 수 있으며 빠르게 여러 곳으로 전파될 수 있다. 특히 돈을 지불하고 이런 콘텐츠를 이용하는 측에서나 콘텐츠를 제공하고 이용료를 받는 공급자 측에서 볼 때 이런 불법 복제 및 전파는 고급 콘텐츠에 대한 제작과 이용에 많은 손해와 불평이 생기게 될 것이다. 콘텐츠에 대한 사용요금을 지불하거나 각종 구매관련 거래가 이루어지는 경우 일반 전자상거래와 같이 많은 문제가 발생할 수도 있다. 많은 사이트들의 유료화가 진행되면서 위와 같은 문제점에 대한 대책은 다른 사이트와 마찬가지로 이루어져야 하는 것이다. 이를 위해 본 논문에서는 스마트카드를 이용하여 좀 더 안전한 시스템을 구성해 보고자 한다.

3. 스마트 카드란?

스마트 카드란 마이크로프로세서와 메모리를 내장하고 있어서 카드 내에서 정보의 저장과 처리가 가능한 플라스틱 카드를 일컫는 말로써 보통 칩카드나 IC카드라 불린다.[7] 스마트카드는 외부와의 통신 방법에 따라 크게 두 가지로 나뉘는데 금도금한 접촉면을 통하는 접촉식 카드와 카드 내에 내장되어 있는 안테나를 이용하여 무선주파수를 통하는 비접촉식 카드가 있다.[8] 또한 프로세서 유무를 통해 메모리 카드와 마이크로 프로세서 카드로 나뉜다. 보통 8bit CPU 칩을 가지고 있는 것이 대부분이며 요즘 나오고 있는 것들은 16bit, 32bit의 CPU 칩들을 탑재하여 처리성능을 높이고 있다. 이런 스마트카드는 멀티 애플리케이션용으로 쓰이기에 적합하다. 현재 스마트 카드에는 JavaCardOS, MultOS, Smart Card For Windows 등을 비롯한 각종 운영체제가 사용되고 있다. 그림 2는 JavaCardOS가 사용된 스마트카드의 내부 구조이다.



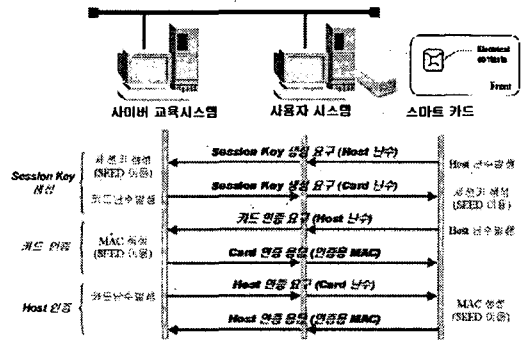
[그림 2] Java Card

스마트 카드는 세가지 형태의 메모리를 가지고 있다. 하나는 ROM(read-only memory)으로서 카드에 OS

같은 프로그램이나 영구히 저장될 데이터를 저장하는데 사용되어진다. 그 내용은 카드의 칩이 제조되어질 때 masking 작업을 통해 집어 넣어지는데 그 후에는 변경이 불가하다. 또 하나는 EEPROM(electrical erasable programmable read-only memory)으로서 이는 일반 PC에 사용되는 하드디스크와 같은 역할을 하며 파워가 꺼진 후에도 데이터가 남아 있으며 데이터를 쓰거나 변경하는 것이 가능하다. 마지막으로 일시적인 데이터들을 저장하거나 변경하는데 쓰이는 임시 작업 공간인 RAM(random access memory)이 있다. 보안쪽 응용에 사용하기 위해 설계된 스마트 카드들은 보통 암호연산을 수행하기 위한 coprocessor 을 가지고 있다.[9] 이것을 통해 RSA 를 비롯한 각종 암호연산을 수행할 수 있으며 이는 스마트 카드의 보안에 매우 중요한 요소들이 된다.

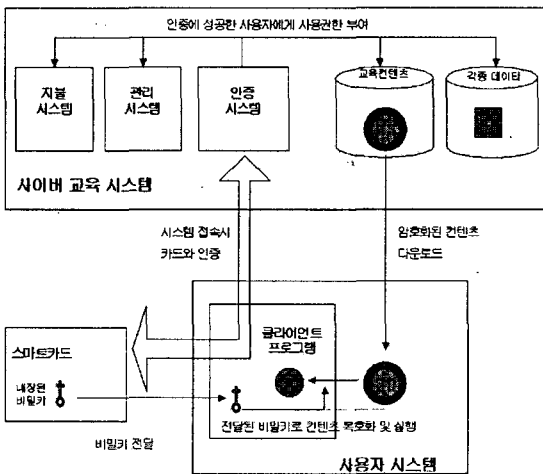
스마트 카드는 IC 카드 칩의 물리적인 안전성과 각종 암호 알고리즘 처리를 바탕으로 복제의 어려움 등 높은 보안성을 제공하며 있으며 컴퓨팅 능력을 갖춘 높은 수준의 프로세서는 다양한 응용들에 적용할 수 있는 장점들을 지니고 있다. 현재 각종 통신분야와 지능 및 뱅킹분야, 교통카드등에 이용되고 있으며 현재 널리 보급되어 있는 마그네틱 카드들은 점차 이런 스마트카드로 대체되어 질 전망이다. 현재 ETRI 에서 32Bit 스마트 카드가 개발 중이며 우리가 구성할 시스템의 사용에 적합한 다양한 기능을 보유하고 있다.

함에 있어서 이루어져야 할 인증과 보안을 담당하게 된다. 이는 스마트 카드 내의 암호 프로세서를 이용하여 SEED, 3DES, ECC, RSA 등의 알고리즘을 통해 이루어진다. 다른 분야에서 마찬가지로 뛰어난 보안성은 스마트 카드의 주요 장점 중의 하나이다. 사용자가 교육시스템에 접속할 때 스마트 카드를 통해 접속하게 된다. 이 때 스마트 카드와 시스템간의 암호화화를 통한 상호인증이 이루어지게 되며 스마트 카드 자체는 비밀번호 입력을 통해 스마트 카드의 올바른 소유주임을 알게 된다. 그림 4 는 SEED 를 이용하여 사용자 인증을 하는 예를 보여준다. 이 인증과정은 중요 데이터를 처리할 때 수시로 이루어지게 된다.



[그림 4] SEED 를 이용한 사용자 인증

4. 시스템 구성



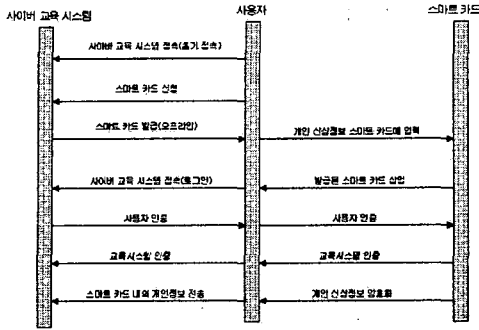
[그림 3] 전체 구성도

전체적인 구성은 다음과 같다. 스마트카드는 사용자 와 교육시스템의 중간에 위치하여 둘 간의 인터페이스 역할을 한다. 따라서 사용자는 스마트카드를 통해 교육시스템에 접속하게 되며 각종 서비스 이용시에도 스마트 카드를 거치게 된다. 이 과정에서 스마트 카드는 크게 두 가지 기능을 담당한다. 그림 3 은 제안된 시스템의 전체 구성도를 나타낸다.

먼저 시스템과 사용자 간에 중요한 데이터를 처리

컨텐츠를 이용할 경우 암호화 과정을 통해 컨텐츠에 대한 저작권과 사용권리에 대한 보호가 이루어지게 된다. 사용자는 인증과정을 통해 컨텐츠를 다운로드할 권리를 확인한다. 컨텐츠는 암호화된 채로 사용자에게 다운로드 된다. 스마트 카드에는 사용자에게 발급될 때 이 암호화된 컨텐츠를 복호화 할 수 있는 키가 담겨진 채로 발급된다. 사용자는 다운받은 컨텐츠를 스마트카드에 담겨진 복호화 키를 이용하여 컨텐츠를 복호화 한다. 이와 같이 컨텐츠에 대한 보호 및 관리, 배포에 대한 기술을 DRM(Digital Rights Management) 기술[10]이라 일컫는다. 일반적으로 관리자 서버가 복호화 키를 전송해주는데 반해 스마트카드에 이러한 키를 미리 집어 넣은 채로 발급하였다. 이로써 네트워크 상의 비밀키 전달 문제를 해결하게 된다. 보통 비실시간 교육시스템의 경우 컨텐츠를 실행시키는 특정 툴이 존재하게 되는데 이 곳에서 스마트 카드가 전해준 복호화 키를 가지고 컨텐츠를 복호화하여 실행한다. 스마트 카드는 APDU[11]라는 형식으로 데이터를 전송해주기 때문에 이 툴은 스마트 카드와 교육시스템 간의 데이터를 전송해주는 역할을 겸하게 된다. 이렇게 스마트 카드는 암호화 과정을 통해 유료 사용자에 대한 신분확인 과 컨텐츠의 저작권 보호 및 사용권한의 통제를 할 수 있게 된다. 즉 스마트 카드를 소유한 사람만이 이런 교육시스템을 활용할 수 있게 되는 것이다. 그림 5 는 사용자가 사이버 교육시스템에 초기 접속하여 카드를 발급받고 로그인 하는 과정을 나타낸 것이다. 카드에는 비밀키가 내장된 채 발

급되며 이를 이용하여 자신의 신상정보를 암호화 하여 전송하게 된다.



[그림 5] 초기 사용자 등록 과정

스마트 카드가 담당하는 또 하나의 기능은 다양한 서비스를 제공한다는 것이다. 현재 개발된 스마트 카드는 보안과 더불어 다기능에 많은 초점이 맞춰져 있다. 즉 하나의 카드로 여러가지 일을 수행할 수 있게 된 것이다. 발급 후에도 원하는 프로그램을 추가시켜 여러 용도로 사용할 수 있게 개발되어 있다. 먼저 교육시스템을 이용하면서 발생하는 지불에 관련된 부분은 스마트 카드에 전자화폐 기능을 내장하여 이용한다. 그 밖에 물건 구매 등을 이용할 경우 역시 이 기능을 이용하게 된다. 이 시스템에 이용하는 스마트 카드는 단순히 교육시스템에만 이용하는 것이 아니라 오프라인 상에서도 이용할 수 있도록 다른 기능도 추가할 수 있다. 교통카드나 일반적인 신용카드 등의 기능을 추가시키면 단순히 한번 쓰고 버리는 카드가 아니라 일상생활에서도 사용하는 스마트 카드로 활용될 수 있다. 사이버 캠퍼스의 경우라면 오프라인 캠퍼스에서도 학생증 등의 용도로 사용할 수 있을 것이다. 심리적인 면에서도 카드의 발급으로 해당 교육사이트에 대한 소속감과 애착이 증가될 것이다.

그 밖에 또한 자신이 교육받은 과목, 사용요금 지불 내역, 접속 기록 등을 스마트 카드 내에 기록하여 교육시스템 이용에 대한 전반적인 내용을 조회할 수 있도록 한다든지 다운받은 콘텐츠를 이용하여 학습했는지 여부를 스마트 카드에 기록하고 다음 번 접속 시 전달하여 학습참여도를 알아보는 등의 식으로 스마트 카드를 이용할 수 있을 것이다..

5. 결론

지금까지 기존의 사이버 교육시스템에서 문제점으로 지적될 수 있었던 사용자 인증과 교육콘텐츠에 대한 저작권 보호 문제에 대해 스마트카드를 사용하여 보완한 시스템을 구성해 보았다. 즉 교육시스템은 스마트 카드를 통하여 사용자를 통제할 수 있게 되었고 사용자는 스마트 카드를 통하여 이런 권리들을 얻게 되는 것이다. 또한 스마트 카드의 다기능성을 이용하여 지불 등에 관련된 다른 서비스도 이용할 수 있었다. 점차적으로 디지털 콘텐츠에 대한 저작권이 중시되고 있기 때문에 특히 고급 콘텐츠의 제작이 중요한

교육시스템의 경우 이를 보호하기 위해 스마트 카드를 사용하는 것은 좋은 방법이 될 수 있을 것이다. 또한 하나의 카드를 다양한 용도로 사용할 수 있기 때문에 스마트 카드의 활용을 높여 스마트 카드 시장을 활성화 시키는데 기여할 수 있을 것이다. 무엇보다도 질 높은 콘텐츠의 개발이 사이버 교육에서 가장 중요한 것이 될 것이며 이렇게 만들어진 콘텐츠를 잘 보호하는 일은 그 다음일 것이다. 바꿔 생각하면 콘텐츠를 잘 보호할 수 있고 그에 대한 저작권을 인정받을 수 있는 사이버 교육시스템이 있다면 안심하고 질 높은 콘텐츠를 개발하려는 사람이 많아지리라 생각한다.

참고문헌

[1] Faisal Amir,, Samir M. Iqbal, M.Yasin, "Effectiveness of Cyber-Learning" 29th ASEE/IEEE Frontiers in Education Conference, 13a2-7, November 10, 1999
 [2] Raymond A. Dumont, "Teaching and Learning in Cyberspace", IEEE Transactions on professional communication, VOL.39, NO.4, December 1996
 [3] David J. Lilja, "Comparing Instructional Delivery Methods for Teaching Computer Systems Performance Analysis", IEEE Transactions on Education, VOL.44, NO.1, February 2001
 [4] Yoshino, T.; Munemori, J.; Yuizono, T.; Nagasawa, Y.; Ito, S.; Yunokuchi, K. Parallel Processing, 1999. Proceedings. 1999 International Conference on , p.395 -402 1999
 [5] <http://www.edunet4u.net>
 [6] <http://www.ocu.ac.kr>
 [7] The source for Java Technology, "Smart Card Overview", <http://java.sun.com/products/javacard/smartcards.html>.
 [8] 기술정보센터 정보조사분석팀, 스마트 카드 기술/시장보고서, 한국전자통신연구원, 1 쪽, 1999년 12 월.
 [9] Zhiqun Chen, Java Card Technology for Smart Cards, Addison-Wesley, p.15~16, 2000.
 [10] Joshua Duhl, Digital Rights Management: A Definition, document#:23982R, IDC reports, March 2001.
 [11] International Organization for Standard, ISO/IEC 7816-4, p.1-46, 1995.
 [12] John Elliott, "The one-card trick Multi-application smart card E-commerce prototypes", Computing & Control Engineering Journal, Vol.10 Issue 3, p.121 -128, June 1999.
 [13] <http://www.gva.co.kr>