http://dx.doi.org/10.7236/JIIBC.2013.13.5.195
JIIBC 2013-5-24

암호기능을 이용한 안전한 스마트-러닝 시스템 구현

Implementation of Secured Smart-Learning System using Encryption Function

양재수*, 홍유식**, 윤은준***, 최연준****, 전상권*****

J-S Yang, Y-S Hong, E-J Yoon, Y-J Choi, S-K Chun

요 약 정부는 2011년부터 스마트 교육 및 디지털 교과서 작업을 위해서 5년 동안 정부가 많은 예산을 출원하고, 민간에서도 훨씬 더 많은 예산을 분담하는 등, 스마트 러닝 시스템 구축에 총력을 기울이기로 하였다. 이러한 시스템이 전국적으로 구축되면, 언제, 어디서나, 누구나 쉽게 스마트 기기를 이용하여 온라인 가상대학에 접속하면, 장소에 구애받지 않고, 정보격차를 해소할 수 있으며, 온라인 강의를 언제든지 공부할 수 있고 학점을 취득 할 수 있다. 그러나 이러한 편리한 시스템도 보안 기능이 취약하면, 해킹에 의해, 학점이 조작되는 심각한 문제가 발생 할 수 있다. 본 논문에서는 이러한 문제를 해결하기 위해서, 보안이 강화된 가상대학을 구상하였다. 이러한 사이버 대학을 위해, 암호 기법을 이용, 필요한 위치에 적절한 보안 솔루션을 적용하여 스마트-러닝 시스템을 모의 실험하였다.

Abstract The government has invested much budget for 5years to do the Smart-education and operate digital textbook services since 2011. The private enterprises also decided to focus on constructing Smart learning system by investing much budget. If these systems are constructed nationwide and therefore can access to cyber university by using smart devices, we can reduce the information gap and study online lectures to get a grade whenever, whoever and wherever we want to. However, these convenient systems can cause serious problems like falsifying grades by hacking if security systems are weak. In this paper, we formulated cyber university which is secured in terms of security. For this, we simulated the smart-learning system which strengthened the security, considering code algorithm and encryption technique.

Key Words : VPN security, Secured DB Encryption, Secured u-Learning System, Cyber University

I. 서 론

정부는 2015년까지 전국 초중고교를 대상으로 디지털 교과서, 유무선 통합 환경 등을 구축하는 스마트교실 사업을 추진한다. 내년 초 결정할 정부 특별교부금을 비롯해 각 시도교육청의 정보화사업 예산 전환분까지 고려하면 2조2000억원 이상을 투입한다. 가장 큰 사업비를 할당할 네트워크 분야에선 통신사(NI·SI)를 중심으로 수주전

*정회원, 단국대학교 전자전기공학부 부교수
**종신회원, 교신저자, 상지대학교 컴퓨터정보공학부 교수
***정회원, 상지대학교 한방 의료공학과 교수
****정회원, (주)신시웨이, 대표이사, 이학석사
*****정회원, (주)한국정보보안구소, 부사장, 박사
접수일자 : 2013년 9월 26일, 수정완료 2013년 10월 10일
게재확정일자 : 2013년 10월 11일

Received: 26 September, 2013 / Revised: 10 October, 2013 / Accepted: 11 October, 2013
**Corresponding Author: yshong@sangji.ac.kr
Dept. of Computer SCience, Sangji University, Wonju, Korea

준비가 한창이다. KT, LG유플러스는 스마트교실에 따른 전용회선 공급 등 네트워크·시스템통합(NI·SI)사업 수주에 총력전을 벌일 태세다. 우선 각 시도교육청 산하 학교에 설비 구축으로 기반을 구축한다는 전략이다. 업계 관계자는 “개인용 스마트기기가 늘어나며 스마트교실에 단말기를 대량 공급하는 사례는 점차 축소될 것”이라며, “일부 스펙을 뺀 다운사이징 제품을 도서, 산간 등 정보화 취약지역에 공급하는 방안 등이 대안으로 떠올랐다”고 밝혔다.

정부가 폭증하는 데이터 트래픽 문제를 해결하기 위해 대대적인 민관 공동 투자를 통해 인터넷 속도를 현재의 100배 이상(유선 기준) 끌어올리기로 했다. 일선 교육현장에 스마트패드(태블릿PC)와 스마트TV 등 디지털 기기를 보급하고, 2015년까지 기존 종이 교과서를 맞춤형, 양방향 교육이 가능한 디지털 교과서로 전면 교체하기로 했다. 그러나, 이러한 편리성이 부가된 온라인 가상대학은 누구나 쉽게 인터넷 상에서 학점을 위조할 수 있는 치명적인 문제점이 발생한다. 그러므로, 이러한 문제점을 해결하기위해서 저렴하고 편리하게 VPN(가상사설망)을 이용하는 가상대학이 많아지고 있다. 그러나, VPN 아래와 같은 문제점이 발생한다. 본 논문에서는 이러한 문제점을 해결하기 위해서, 중앙 DB 서버내의 주요 데이터에 대한 암호화를 제안한다[1-4].

VPN 연결을 사용하기 전에는 일상적인 어플리케이션 프로그램을 모두 종료해야 한다. 뿐만 아니라, VPN 클라이언트 구성이 복잡하고, VPN 클라이언트는 사용하려는 네트워크에 따라 서로 다른 네트워크 ID를 가져야 하기 때문에, 복잡한 암호를 사용하지 않은 경우에는 보안상 문제점을 가지고 있다[4-9].

본 논문에서는 인터넷 환경에서 언제, 어디서나, 누구나 쉽게 지능형 가상대학을 통해서 학점을 취득 할 때에 발생 할 수 있는 학점 위조를 방지하는 알고리즘을 제시하고, 이를 모의 실험하였다.

II. 가상대학 VPN 암호화 적용

우리나라에서 2009년 처음으로 스마트폰이 도입된 이후 2012년말 이용자 수가 3200만명이 되어 세계 7위를 기록하더니, 올해들어 보급률로는 67%로서 처음으로 세계 1위에 올랐다고 한다. 2008년 0.9%에서 무려 74배나 급성장한 것이다.

VPN 유형은 2계층 프로토콜인 PPTP, L2TP, L2F와 3계층 프로토콜인 IPSec, SSL 및 2계층 스위칭 기법과 3계층 라우팅 기술을 혼합하여 이용하는 MPLS 프로토콜 방식으로 구분된다.

또한 보안 장비 중에서 침입탐지 시스템이나 네트워크 장비 중에 라우터와 VPN이 결합되기도 하나, 일반적으로 IPSec VPN과 SSL VPN이 전용 장비 형식으로 공급되고 있다. 게다가, 최근에는 모바일 단말에 사용자 보안 강화 에이전트(ESEA: Endpoint Security Enforcement Agent)를 설치하고 SSL VPN 기반의 NAC(Network Access Control) 시스템과 연동하여 사용자 단말과 데이터 정보를 안전하게 보호할 수 있는 방법이 제안되었다.

또한 스마트폰과 같은 단말기에는 사용자 인증을 위한 고유의 SIM(Subscriber Identity Module) 혹은 USIM(Universal Subscriber Identity Module) 카드내에 있는 코드를 SSL VPN 및 방화벽과 연계하도록 하는 방안이 제시되기도 했다.

이에 본 논문에서는 개별적인 모바일 단말과 사용자 특성을 고려하고 트래픽의 부하와 경제성을 고려하여 VPN 유형의 선택될 수 있다고 판단하며, 단지 비인가 내지 비정상적인 의도로 모바일 단말에서 응용서비스가 제공되는 것을 막기 위해서 2채널 사용자 인증과 함께 모바일 단말 고유의 Identity 정보(CPU, MAC 주소, SSID 등)를 서버와 연동하는 Agent를 통해 확인하는 모바일 방화벽 기능을 추가할 것을 제안한다. 물론 악성코드의 유입을 차단할 NAC과 연동은 물론이고 파일의 암호화가 적용되는 것도 바람직하다.

기존 PC의 인터넷 거래에서 스마트폰으로 2차 인증을 요청한 사례(″스마트 디바이스를 이용한 2 채널 인증방식의 전자금융거래에 관한 연구″, 동국대 김광진, p31, 2013년)를 응용하여 태블릿PC와 같은 모바일 단말에서 사용자 인증을 인증 서버에서 ID와 Password로 일차 구분하되 동시에 스마트폰으로 2차 인증을 받도록 한다. 또한 단말기 자체의 고유 정보(CPU, MAC 주소, SSID 등)를 사용자 에이전트(EA:Endpoint Agent)가 병행하여 보안 관리 서버로부터 확인을 받는다.

이상의 내용을 구성도로 표현하면 다음 그림 1과 같다.

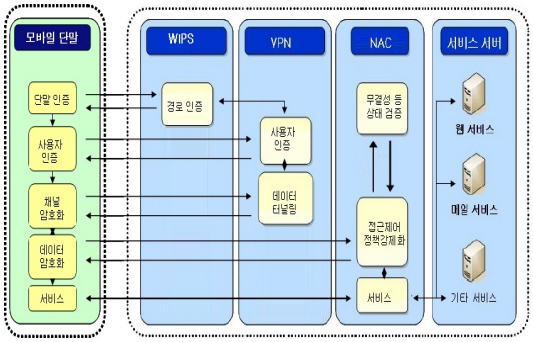

그림 1. 모바일 인증단계
Fig. 1. Mobile authentication stage

① 모바일 단말에서 서비스 인증을 요청하면 WIPS서버는 단말기내에 단말기 속성(CPU 정보, MAC 주소 등)을 파악할 수 있는 Agent를 통해 사전에 등록 여부를 확인하고 전송 경로를 인증한다.
② 이어 ID 및 Password를 통해 사용자 인증을 하되 OTP 등을 이용하여 2채널 이상의 사용자 인증을 하도록 한다.
③ 미리 지정된 공개키 기반의 암호로 작성된 주소로 가상 사설망을 구성하여 채널간 터널링을 만든다.
④ 채널을 통해 전달된 데이터의 보안 정책 여부(IP허용 등)을 확인하고 데이터내 악성 코드 유무를 통한 무결성을 확인한다.
⑤ 이상의 보안 정책이 완료되면 서비스 서버를 통한 서비스가 이루어진다.

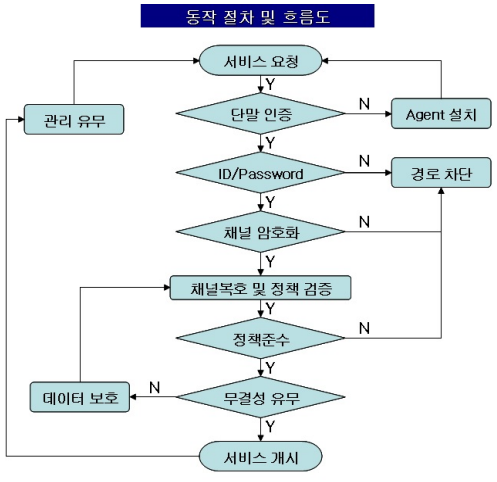

그림 2. 암호 과정
Fig. 2. encryption processing

그림 2에서는 암호화 과정의 동작 처리와 이의 흐름도를 설명하고 있다. 단말 인증에서부터 ID와 비밀번호, 채널 암호화, 보안정책 검증, 채널복호, 데이터 보호 등의 암호화 과정을 나타낸다.

III. 보안 기반 e-출석관리시스템과 가상대학 모의실험

최근에는 인터넷이 자기주도적 학습을 실현하기에 적합한 환경으로 그 잠재력을 높이 평가받고 있다. 자기주도적 학습이란 학습자가 스스로 학습 목표 설정 및 학습에 필요한 적절한 강의 선택과 실행, 평가에 이르는 일련의 과정에 자발적으로 참여하는 학습의 한 형태라 볼 수 있다. 스마트-러닝의 학습 환경은 개별 학습자가 필요에 따라 자신의 학습 과정을 선택하고 학습 과정에서 주도적인 역할을 수행하기 때문이다[3].

뿐만 아니라, 디지털 교과서를 이용한 지능형 자기주도적 학습을 하면 교사가 수준별 학습은 물론, 어떤 학생이 똑같은 점수라도 비슷한 유형의 문제를 계속해서 틀리는 오답율을 측정함으로서 어떠한 문제가 틀리는지를 알 수 있는 방법이 있다. 표 1에서는 지능형 가상대학 시스템을 도입해서 최초의 학습점수가 80점 일 때, 똑같은 문제를 반복해서 2회 실시 하였을 때, 오답율 및 출석율을 고려해서, 최근 성적 오름세를 판단하는 과정을 설명하고 있다.

표 1. 학생 점수 분석
Table 1. Analysis of student scores

이름	최초 점수	2회 반복 학습점수	오답율 & 출석율	최근 성적 오름세
김기수	80	86	SMALL	POSITIVE SMALL
홍길동	80	72	BIG	NEGATIVE SMALL
한나영	50	56	BIG	Positive SMALL
권현수	86	90	SMALL	Positive SMALL
박수일	80	60	BIG	Negative BIG

가령 똑같은 최초 점수 80점이라도 김기수 학생의 경우는 똑같은 유형의 반복 시험에서 유사한 유형의 문제 오답율이 적고 출석율이 적었으므로, 반복 시험에서 86

점을 기록했으므로 최근 성적오름세가 상향세로 평가된다. 그러나, 홍길동 학생은 오답율이 많았기 때문에 최근 성적오름세가 하향세로 평가되는 과정을 보여주고 있다.

표 2. 가상대학 연관 규칙
Table 2. Association rule of cyber university

ID	연관규칙
1	미분
2	적분
3	통계
4	삼각함수
5	확율
6	2차 방정식
7	미분
8	적분
9	통계
10	미분
11	적분
12	삼각함수
13	통계
14	통계
15	확율

표 2에서는 의한 가상대학 똑같은 점수 라도 수학과목에 대한 어떠한 문제를 계속해서 틀리는지를 판단하기 위한 오답율 연관규칙을 설명하고 있다. 사실 학생이 점수를 올리려면 똑같은 어떠한 유형의 문제를 계속해서 똑같이 틀리는지를 분석하고 다음시험에는 이와 같은 실수를 방지하는 것이 제일 좋은 방법으로 사료된다. 본 논문에서는 이러한 문제점을 표 2를 이용해서 학생이 2회 반복해서 유사한 유형의 문제를 똑같이 틀렸을 때 어떠한 문제의 패턴에 취약한지를 분석하는 결과를 표 3에서 설명하고 있다.

표 3. 연관 규칙 분석 결과
Table 3. Analysis result of association rules

분야	해당 ID	신뢰도
미분	1, 7, 10	75%
적분	2, 8, 11	75%
삼각함수	4,12	50%
통계	3,9,13,14	95%
확율	5,15	50%
이차방정식	6	250%

이렇게 하여 각 단계별로 10명의 학생의 출석 평균치를 구하고, 분포대(HIGH, MED, LOW)에 따르는 메시지를 출력한다.

그러므로 수준별 학습은 종이없는 교과서가 실행되는 가상대학에서, 강사가 똑같은 점수라도 어떤 학생이 어떤 문제에 취약한지를 판단 할 수 있도록 하였다.

표 4. 학생 점수 암호화
Table 4. Student scores encryption

이름	최초 점수	2회 반복 학습점수	오답율 & 출석율	최근 성적 오름세
9b0775c440cd9e7d	06bf7ac487ed2f97	7b202af05b174aee	06bf7ac487ed2f97	cd9127635f75a09c
217d86c10e2ca4f5	06bf7ac487ed2f97	b006295f01478ec7	a878b99b3b0950e1	24ae98b2ced6ea43
facd60eb8e8d79ca	c42af71869e34b1b	b61e4845c8edf4c4	a878b99b3b0950e1	cd9127635f75a09c
549515374549b559	e89d039ed0abbbc4	6de5e7ce9e4e96a3	06bf7ac487ed2f97	cd9127635f75a09c
7e5253b7c35c031b	06bf7ac487ed2f97	43d3feac99e3b6af	a878b99b3b0950e1	b8b4be611036ba93

표 4에서는 표 1에서 분석한 소중한 학생 학생 점수를 인터넷상에서 DB로 저장 될 때에 해킹이나 변조를 예방하기 위해서 암호화된 과정을 보여주고 있다.

뿐만 아니라, 본 논문에서는 학생들이 전자(e)-출석관리 시스템으로부터 인증을 받을 때 학생신분 데이터가 유출되는 문제 방지와 보안성을 만족시키기 위해 다음과 같은 출석 인증 프로토콜을 수행하게 된다.

(1) 학생 → e-출석관리 시스템: $\{C, T\}$

학생은 자신의 RFID 태그가 탑재된 다기능 학생증을 e-출석관리 단말기에 인식시킨다. 단말기는 인식 시점의 타임스탬프 값 T를 생성한 후 태그내에 저장된 태그 식별자 ID, 수강 과목 코드 LC, 수강 날짜 정보 $Date$를 이용하여 해쉬 인증 값 $C = h(ID, LC, T, Date)$를 계산한 후 $\{C, T\}$를 e-출석관리 시스템에게 전송한다.

(2) $\{C, T\}$를 수신한 e-출석관리 시스템은 먼저 타임스탬프 T의 유효성을 검증하여 재전송 공격여부를 판단한다. T가 유효하면 그림 3에서 보여 지는 것처럼 데이터베이스 내에 저장된 태그 식별자 ID, 수강 과목 코드 LC, 수강 날짜 정보 $Date$를 이용하여 다음의 해쉬 인증 값 $C^* = h(ID, LC, T, Date)$를 계산한 후 수신한 C와

동일한지를 검증한다. 만약 $C \stackrel{?}{=} C^*$이면 e-출석관리 시스템은 학생의 출석을 인증하게 된다.

그림 3에서 보는 것과 같이, 제안한 인증 프로토콜의 적용으로 인해, 해커 또는 악의적인 공격자에 의한 송수신 메시지 도청에 따른 재전송 공격(Replay attack), 위장 공격(Impersonation attack), 익명성(Anonymity) 제공 등 다양한 암호학적 침해나 네트워크 보안 공격들에 대한 안전성을 제공한다.

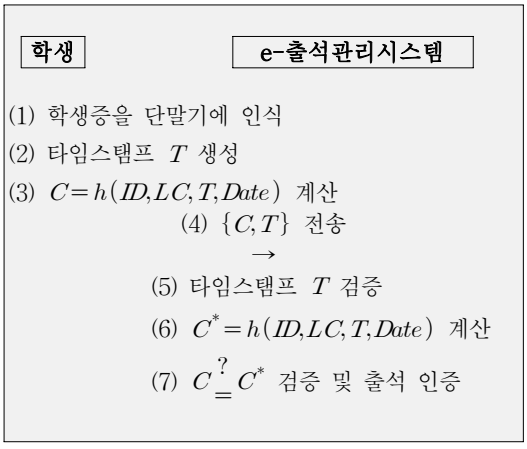

그림 3. 가상대학 인증 프로토콜
Fig. 3. Authentication protocol for Cyber university

IV. 학사정보 데이터 암호화 방안

이러한 데이터 보호의 중요성에 따라 2013년부터 개인정보보호법을 통해 주요 데이터에 대한 유출을 법으로 방지하고 있다. 주로 시스템을 망가뜨리던 악성 해커들이 근자에는 시스템은 그대로 두고 주요한 데이터만을 훔쳐가는 방식을 자주 취한다. 결국 자물쇠를 부수고 시스템을 파괴하던 방식과는 달리 조용히 문을 열고 들어와서 중요한 자산만을 훔쳐 달아나는 것이다. 악성 해커들은 물리적인 보안을 뚫고 방화벽이 대표하는 네트워크 보안시스템과 서버 보안 시스템 등을 무력화하거나 우회하여 침입하는데, 이때 데이터의 최측근에서 보호하는 시스템이 바로 데이터베이스 보안 시스템이다.

데이터베이스 보안 시스템은 앞단의 여러 보안 시스템과는 달리 매우 지능적이어야 한다. 비 정형화된 접근에 대한 의미적인 분석을 통해 데이터를 보호해야 하기 때문이다. 데이터 암호화는 데이터베이스 관련 파일의 유출시에도 그 내용을 알아보지 못하게 암호화하는 강력한 데이터 보호 방법이다. 암호화 된 개인정보는 사전에 허락된 특정 사람에 의해서만 복호화 되어 보여지게 되며, 암복호화 관련 기록은 모두 저장되어 관리된다.

이러한 기능의 구현은 데이터베이스의 기능을 활용하여 구현할 수도 있고 어플리케이션에서 암복호화 모듈을 호출하여 처리할 수도 있다. 특히, Secured 가상대학을 인터넷에서 운영 할 때에는 학생들의 성적 데이터는 매우 민감하여 단 몇 건의 유출만으로도 상당한 문제를 야기 시킬 수 있다. 이러한 이유로 본 논문에서는 중앙 DB 서버내의 주요 데이터에 대한 암호화를 제안하게 되었다.

이 구현을 위해 두 가지 방법을 고려하였는데 그 각각은 아래와 같다.

(1) 데이터를 DBMS에 넣으면 DBMS를 암호화 한 후 저장하는 방법이다. 이러한 방법은 뷰(view)를 이용하여 구현하며, 어플리케이션을 변경할 필요가 없다. 이는 간단하게 구현이 가능하지만 DBMS의 성능 저하를 야기시킬 수 있기 때문에 사전 테스트 과정이 필수적이다.

(2) 어플리케이션에서 데이터를 암호화 한 후 DBMS에 입력하는 구현 방식이 있다. 이는 성능 저하를 최소화 할 수 있으나, 어플리케이션 프로그램을 복잡하게 만든다.

본 과제에서는 첫 번째 View방식을 채택하여, 그림 4에서 보는 바와 같이, 암호화 전의 학사정보 처리의 경우와 암호화 처리 이후의 학사정보 데이터 암호화 구현 방안을 제시하였다.

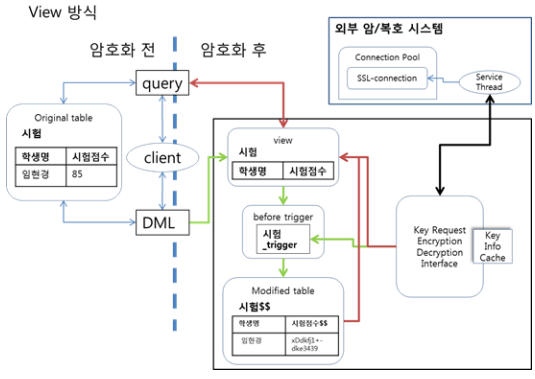

그림 4. 학사정보 데이터 암호화를 위한 View 방식 적용
Fig. 4. Adaptation of View rule in school affairs information Data Encryption

이러한 암호화의 중요한 또 하나의 부분은 암호화 키의 관리 매커니즘이며, 정교하고 안전한 매커니즘이 잘 구현되어야 한다. 국산 암호화 알고리즘에는 SEED와 ARIA 가 있다. SEED는 민간분야에서 전자상거래, 금융, 무선통신 등에서 전송되는 중요 정보를 보호하기 위해 KISA를 중심으로 개발된 128비트 블록암호알고리즘이며, ARIA는 정부 및 공공기관에서 주로 사용되는 128비트 블록암호알고리즘으로 국가정보원을 중심으로 산·학·연이 공동으로 개발한 것이다. 본 논문에서는 ARIA를 암호화 알고리즘으로 사용하였다.

복호화 실행은 인가자에 대해서만 다양한 데이터 접근에 대해 사전에 정의된 인가자들에 대해서만 복호화를 수행하여 데이터를 보호한다. 비 인가자들은 데이터에 접근해도 암호화된 데이터 혹은 마스킹된 데이터를 보게 됨으로써 주요 데이터의 유출을 막는다. 암호화 대상 데이터를 선정하고 그 데이터를 암호화 하게 된다. 그림 5에서는국가 정보원에서 개발된 ARIA 암호화 OPEN 소스를 이용해서 암호화 하였다[9].

```
/*  ARIA 암호화
* const Byte *mk: 마스터키
* Byte *rk: 라운드키
* int keyBits: 마스터키의길이
*/
int EncKeySetup(const Byte *mk, Byte *rk, int keyBits)
{
register Word t0, t1, t2, t3;
Word w0[4], w1[4], w2[4], w3[4];
int q, r;
WordLoad(WO(mk,0),w0[0]);        WordLoad(WO(mk,1),
w0[1]);
WordLoad(WO(mk,2),w0[2]);        WordLoad(WO(mk,3),
w0[3]);

q = (keyBits - 128) / 64;
t0=w0[0]^KRK[q][0]; t1=w0[1]^KRK[q][1];
t2=w0[2]^KRK[q][2]; t3=w0[3]^KRK[q][3];
FO;
if (keyBits > 128) {
WordLoad(WO(mk,4), w1[0]);
WordLoad(WO(mk,5), w1[1]);
if (keyBits > 192) {
WordLoad(WO(mk,6), w1[2]);
WordLoad(WO(mk,7), w1[3]);
} else {
w1[2]=w1[3]=0;
}
```

```
void ARIA_test() {
Byte rk[16*17], c[16], mk[32];
Byte p[16]={0x11, 0x11, 0x11, 0x11, 0xaa, 0xaa, 0xaa,
0xaa,
0x11, 0x11, 0x11, 0x11, 0xbb, 0xbb, 0xbb, 0xbb};
int i, flag;
        for (i=0; i<16; i++)
            mk[i]=i*0x11;
        for (i=16; i<24; i++)
            mk[i]=(i-16)*0x11;
Crypt(p, EncKeySetup(mk, rk, 192), rk, c);
printf("BEGIN testing basic encryption...\n");
printf("Testing whether the encryption would come out
correctly, \
for 14-round ARIA.\n");
```

그림 5. 데이터 암호화 처리를 위한 ARIA 암호화 소스
Fig. 5. ARIA encryption for process of Data Encryption

V. 결 론

본 논문에서는, 2015년까지 정부에서 종이없는 교과서 및 원격대학을 구축하였을 때에 인터넷 통신망에서 성적을 위조하지 못하는 VPN 암호화 알고리즘과 Secured e-출석관리시스템에 대해 모의 실험하였다. 더 나아가, 학사정보 데이터의 암호화 방안에 대해 암호화 View방식을 적용, DB 암호화 방안을 제시하였다.

본 논문을 통하여, 서버에 있는 많은 학생들의 정보보안 대책 및 방안을 알 수 있다. 또한, 학생들이 인터넷을 접속할 때 아이디 및 비밀번호 등의 노출이나 개인정보 노출 을 막기 위한 보안기능 강화와 Secured 가상대학 구현을 알 수 있다. 향후 이를 기반으로, 보안이 적용된 지능형 가상대학 시스템을 구축할 수 있을 것이다.

References

[1] Korea Education and Research Information prime, u-campus building at the University, 2006.

[2] Kimgwangjin, "smart device authentication using a two-channel study of the electronic financial transactions", Dongguk University, 2013

[3] Park,hyungKun,"Effect of learning flow analysis in relation to motivation and self-directed learning",

1993

[4] C.J.Kang,"Real-time access to the administrative computer network implementation of a mobile information processing system", korea polytechnic university, 2012

[5] "A Study of the process of organizing a special supplement of the application process step-level education curriculum, Korean Hakseong High School, Operating Manual, 2000.

[6] "According to the 7th National Curriculum achievement standards and assessment criteria research and development", Korea Institute of Curriculum and Evaluation, 2000.

[7] Kim youngae, "Education policy network issues smart education revolution in our classrooms status and development direction.", 2011

[8] Hong, YouSik, "Intelligence E- Learning System", The journal of the Institute of Webcasting, Internet and Telecommunication, vol.10 no.1, 2010

[9] http://seed.kisa.or.kr

[10] Geo-Su Yim,"On-off Map using Image Encoding Method Design and Implementation",Journal of the Korea Academia-Industrial cooperation Society, V.10, no.8, 2012

[11] Dae-Sung Park,"Reliability and Validity of the Balancia using Wii Balance Board for Assessment of Balance with Stroke Patients",Journal of the Korean Institute of Information Technology, Vol. 14, No. 6 pp. 2767-2772, 2013

저자 소개

양 재 수(정회원)

- 1988.8~1993.1 미 NJIT박사
- 1981.3~1981.12 MIC 사무관
- 1982.1~2006.1 KT
- 2006.3~2011.10 광운대 교수
- 2007.2~2011.10 경기도 정보화특보
- 2011. 11~ 단국대학교 부교수

홍 유 식(종신회원)

- 1991년-현재 : 상지대학교 컴퓨터 정보공학부 교수
- 1989년-1990년 : 삼성전자 종합기술원 연구원
- 2006년-2010년 : 대한전자공학회 컴퓨터 소사이티 회장

윤 은 준(정회원)

- 2004년 : 경북대학교 컴퓨터공학과 공학 박사
- 2011년~현재 : 경일대학교 교수
- 2010년~현재 : 대전자공학회 멀티미디어 연구회 회장

전 상 권(정회원)

- 2013. 2 한세대학교 IT융합학과 공학박사 졸업
- 1995.10 ~ 1998.11 기독교TV 기술국 기술감독
- 2012. 2 ~ (현재) 한국정보보안 연구소/한국정보보호시스템 부사장

최 연 준(정회원)

- 1991. 2 한국외국어대학교 경영정보대학원 소프트웨어공학과 이학 석사
- 1994.7~2003.3 한국 오라클 본부장
- 2003. 3~현재 ㈜ 신시웨이 사장