2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

효율적이고 안전한 가상 대학 모델에 관한 연구

이덕규, 박희운, 이임영
순천향대학교 정보기술공학부
e-mail : hbrhcdbr@sec-cse.sch.ac.kr

A Study on Secure Efficient Cyber University Model.

Duk-Kyu Lee, Hee-Un Park, Im-Yeong Lee
Division of Information Technology Engineering. SoonChunHyang University

요 약

본 논문은 가상 공간에서 운영할 수 있는 가상 대학 모델에 관해 기술한다. 인터넷을 통한 가상 교육의 발달로 인하여 많은 사람들에게 교육의 기회가 부여되었다. 많은 교육의 기회의 부여는 온라인을 통하여 사용자의 자료가 도청 혹은 변경이 발생할 수 있다. 이러한 보안 문제를 해결하기 위해 전자문서의 보호와 검증에 대하여 공개키 기반 구조 모델과 OTP(One-Time Password)를 이용하여 주요시스템의 업무 및 기능을 정의한다. 기존에 사용되는 가상대학 모델의 문제점을 제시하고 새로운 가상 대학 모델을 제시하고자 한다. 제시한 방식을 통해 안전한 가상대학 모델의 하고 신뢰성을 바탕으로 사용자의 수업 참여를 확대(유도)하는 수단으로써 활용될 수 있다.

1. 서론

최근 첨단정보산업의 발전과 함께 지식정보의 시대로 펼쳐질 21 세기는 시●공간을 초월한 가상공간에서의 멀티미디어교육의 확대로 인하여 기존의 교육시스템은 새로운 패러다임으로 대체되는 커다란 변화를 겪을 것으로 예상된다. 최근 정보망을 이용하여 많은 사람들에게 교육의 기회를 부여하고 있으며, 가상대학의 시범운영을 확대하고 있다.

교육을 통해 국민으로 갖춰야 할 기본적 정보소양을 분야별, 수준별로 기준을 제시하고 희망하는 사람에 대해 정보소양 수준과 능력을 평가 인증한다. 가상 대학 운영에 있어 전자 문서, 이메일 송수신, 과제물 또는 과제물 평가에 대한 온라인 상의 송수신이 많게 된다. 이에 관련하여 전자문서에서의 당사자 신분확인, 전자업무내용의 보호 및 무결성 기능, 전자행위에 대한 부인 봉쇄 기능 등 전자업무의 중요 인증과 관련하여 신뢰할 만한 제 3 자가 확인 및 증명해주는 공개키 기반구조 하에서의 인증기관 구축이 필요하다. 인증기관의 구축을 통해 가상대학 업무의 효율성을 증진시키고 수준 높은 보안성을 제공할 수 있어 사용자에게 신뢰성을 제공할 수 있다. 이러한 신뢰를 바탕으로 사용자로 하여금 가상대학에로의 많은 교육 참여 유도를 확보할 수 있는 수단이라 할 수 있겠다.

가상대학의 모델을 제안하기 위하여 인증기관의 핵심 요소인 전자서명과 인증에 관한 개념 및 관련 암호기술을 살펴보고, 가상대학과 사용자간에 사용되는 OTP(One-Time Password)에 대하여 알아본다.[1][2][4][6]

본 논문에서는 가상대학에서의 전자문서 송수신, 이메일 송수신, 과제물 제출 및 과제물 평가 등을 보장하기 위한 인증관련 기술을 이용하여 인증업무를 수행하는 인증기관을 포함하는 가상대학의 모델을 제시함으로써 전자문서에 대한 보장과 업무 효율성을 높이는데 있다. 앞에서 다룬 내용을 바탕으로 안전하고 효율적인 가상대학의 새로운 모델을 제시한다.

2. 기존 모델들에 대한 고찰

기존 모델에 있어 크게 두 가지로 구분할 수 있다. 첫 번째로는 가상대학이 학교망 내부에 갖추어져 있는 것이며, 두 번째로는 가상대학이 학교망 외부에 존재하여 여러 대학이 협력하여 하나의 가상대학을 설립한 경우가 있을 수 있다.

두 가지에 대해 모두 같은 문제점을 찾을 수 있다. 두 가지 모델 모두의 문제점으로는 ID 와 Password 만으로 접근이 가능하다는 것이다. 이것은 ID 와 Password 가 노출 되었을 경우 사용자의 과제물, 평가물(시험포함) 모든 것이 변조될 수 있다. 제 3 자가 불법적으로 접근해서 가상대학을 위장하여 과제물을 뽑아낼 경우 사용자는 가상대학을 인증하지 못하므로 제 3 자에게 과제물을 제출하게 된다. 또한 과제물 제출 시에도 서명없이 전달하여 보안상의 문제점 – 예를 들어 사용자 부인, 자료의 변조 등 – 을 안고 있다.[3][5]

이 모든 문제점을 본 논문에서는 다음과 같은 새로운 모델을 제시함으로써 문제점을 해결하려 한다.

3. 가상 대학에서의 요구사항

가상대학을 구성하는데 있어서 다음의 요구사항을 만족해야 한다.

요구사항 1. 사용자의 사생활은 보장되어야 한다.
학생증 요청의 행위는 Off-Line 에서 생성한다.
학생증에 대한 신상과 함께 인증서를 요청하게 되므로 학생증 요청행위는 Off-Line 으로 이루어져야 한다. Off-Line 상에서 사용자 확인 절차를 거치도록 한다

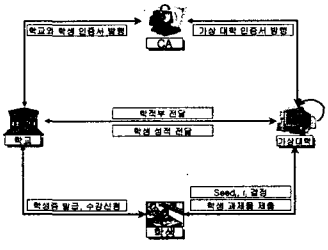
요구사항 2. 사용자와 가상대학간의 사용자 식별성을 가지고 있어야 한다.
사용자와 대학 간에 학적부 정보에 대하여 무결성이 필요하며, 사용자의 정보에 대한 권한은 사용자에게 있음을 주지한다.

요구사항 3. 가상대학은 사용자의 정보 요청에 충실해야 한다.
사용자와 가상대학에서의 Seed 값 노출은 사용자의 피해가 커진다. Seed 값은 login 시에 사용된다. 하지만 Seed 값을 이용해 안전한 통로가 개설되고, 과제물의 제출과 시험지의 제출이 이루어지기 때문에 Seed 값의 관리는 중요하다. 이러한 이유로 Seed 값에 대한 변경을 요구할 수 있다. 사용자가 Seed 값에 대한 의문이 생기는 경우와 가상대학에서 Seed 값에 대한 의문이 생기는 경우는 사용자와 가상대학 사용자의 Seed 값 변경에 대해 충실히 이행하여야 한다.

요구사항 4. 가상대학에 접근자는 크게 3 부류로 나누어야 한다.
가상대학에 접근할 수 있는 접근자는 크게 3 부류로 분류되어 있어야 한다. 교수그룹, 사용자그룹, 관리자로 분류되며, 이 3 그룹에 속하지 않은 사용자는 접근을 제한 시킨다.

4. 제안 모델

본 제안 모델에서는 인증기관과 OTP(One-Time Pass word)를 이용하여 모델을 기술한다. 제안한 모델은 다음과 같은 사항을 가진다.
학교는 가상대학의 Seed, r, Algorithm 에 대한 전달만을 한다. 학교는 가상대학의 요구사항 대로 Seed, r, Algorithm, 인증서를 학생증(Smart Card)내에 저장한다.
참고문헌 [1]를 이용해서 다음의 모델을 제안한다.
다음은 가상대학의 모델 전체의 모습을 기술한 것이다.

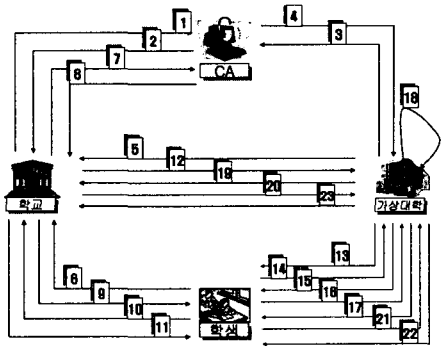


(그림 1) 가상대학 모델 개요

4.1 시스템 계수

다음은 인증서 발급과 사용자가 가상대학에 login 시에 사용되는 시스템 계수에 대해 설명한다.

Cert : 인증서 RU : 학교
VU : 가상대학 CA : 인증기관
US : 사용자
r(n) : $Seed_i$ 를 선택하기위한 난수값 생성기
Seed(n) : OTP 를 위한 초기값 생성기
AL : Algorithm m : 값의 갯수
$Seed_i$: OTP 설정 초기값
Pk : 공개키 암호화
Sk : 비밀키 암호화
ID_A : 사용자 A 의 ID
EK_{AS} : 대칭키
T_A, T_S : Time Stamp
N_A, N_S : Random Number
H : 안전한 일방향 해쉬함수
F_A, F_S : 키 구성 및 일회용 인증 요소
Xn : n 번째 일회용 패스워드

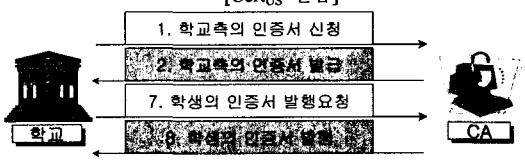


(그림 2) 가상대학 전체 흐름도

4.2 학교 · 사용자 인증서 발급 단계

다음은 학교와 사용자에 대한 인증서 발급 단계에 대해서 설명한다. 학교는 CA 에게서 인증서를 획득하게 되며 이 인증서는 사용자에게서 학교 인증시에 사용된다. 이 단계에서 사용자의 인증서는 학교가 등록기관의 역할을 대행한다.

Step 1. 학교는 CA 에게서 인증서를 요청한다.
Step 2. 학교는 CA 에게서 인증서를 발급받는다.
[$Cert_{RU}$ 발급]
Step 7. 학교는 CA 에게서 사용자 인증서 발행을 요청한다.
Step 8. CA 는 학교에 사용자 인증서를 발급한다.
[$Cert_{US}$ 발급]

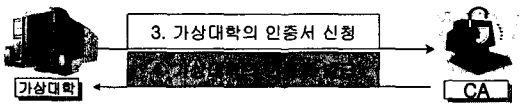


(그림 3) 학교, 사용자 인증서 발급 단계

4.3 가상 대학 인증서 발급 단계

다음은 가상 대학 인증서를 신청, 발급 받는 단계를 설명한다.

Step 3. 가상대학은 CA 에게서 인증서를 요청한다.
Step 4. 가상대학은 CA 에게서 인증서를 발급받는다.
[$Cert_{VU}$ 발급]

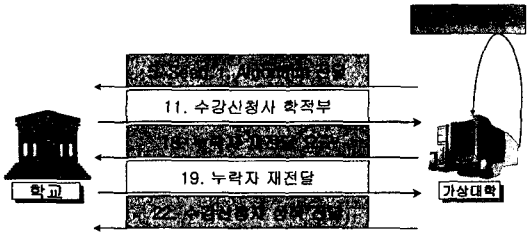


(그림 4) 가상대학 인증서 발급 단계

4.4 학교 · 가상 대학간의 학적부 전달 및 성적 전달 단계

다음은 학교와 가상 대학간의 OTP 에 필요한 인자 및 Algorithm 을 전달한다. 그 후 학적부 전달(재송부 포함), 성적 전달 단계로 이루어 진다.

Step 5. 학생증내에 포함될 Seed(n)과 r(n) 생성기와 Algorithm 전달
$PK_{RU}[Seed(n) \| r(n) \| AL]$
Step 11. 학교는 모든 사용자의 수강 신청 접수를 받아 학교의 인증서와 함께 가상대학에 학적부를 전달한다.
$PK_{VU}[SK_{RU}[학적부 \| T]]$
Step 17. 학적부와 비교하여 수강자의 진위여부 판별한다.
[신청자 학번 != 접속자 학번] ⇒ 재전송 요구
Step 18. 가상대학은 누락자에 대해 다시 학적부를 요청한다.
$PK_{RU}[SK_{VU}[누락자\ ID \| T]]$
Step 19. 학교는 누락자에 대해 확인 후 재전달 한다.
$PK_{VU}[SK_{RU}[학적부 \| T]]$
Step 22. 가상대학은 학기 마감 후 성적을 전송한다.
$PK_{RU}[SK_{VU}[ID \| 학적부 \| 성적 \| T]]$

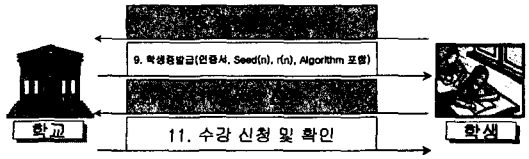


(그림 5) 학교와 가상대학 간의 자료 전송 단계

4.5 학생증 발급 및 수강 신청 단계

다음은 학생증 발급 및 수강 신청 단계로서 이 단계에서는 학생에게서 Off-Line 으로 학생증을 신청한다. 이 과정에서 학생증 내부에 포함될 인증서 신청을 한다. 학교에서 학생증을 받게 되는데 학생증에는 가상대학에서 Login 시 필요한 Seed(n), r(n), Algorithm 과 함께 인증서가 포함되어 받는다. 수강 신청은 사용자의 서명을 붙여 전송하고, 수강 신청 확인을 받는다.

Step 6. (학교는 RA 의 업무를 대신한다.) 사용자는 학교에 인증서를 신청한다. [Off-Line 으로 신청]
Step 9. 학교는 사용자 인증서, Seed(n), r(n)을 포함(Smart Card 형식으로)하여 학생증을 발급한다.
[Off-Line 으로 학생증 수령]
IC-Card[Seed(m) || r(m) || AL || 사용자정보 || $Cert_{US}$]
Step 10. 사용자는 학생증을 이용하여 수강신청을 한다.
$PK_{RU}[SK_{US}[이름 \| 학번 \| 수강과목]]$
Step 11. 학교는 수강 신청을 확인하고 확인서를 발급한다.
$PK_{US}[SK_{RU}[이름 \| 학번 \| 수강과목 \| 확인서]]$

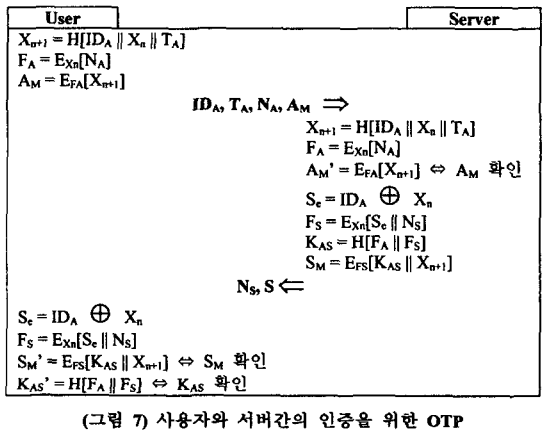


(그림 6) 사용자정보 요구 단계

4.6 가상대학 · 사용자 인증 정보 흐름 단계

다음은 가상대학과 사용자 인증 정보 흐름 단계이다. 이 단계에서는 사용자와 가상대학 사이의 r 값을 이용해 Seed 값을 가상대학이 결정하여 Seed 값을 가상 대학과 사용자가 서로 같은 값을 갖는다. 이 Seed 값은 OTP 인증에 사용되며 자료 전송 시에 안전한 통로를 개설하는데 쓰인다.

Step 12. 개강 시간을 공고한다.
Step 13. 가상대학에 사용자가 선택한 r_i 값을 전달한다.
$PK_{VU}[SK_{US}[r_i \| ID]]$
Step 14. 가상대학이 선택한 $Seed_i$ 값을 사용자에게 전달한다.
$PK_{US}[SK_{VU}[Seed_i \| r_i \| ID]]$
Step 15. 선택된 r_i, $Seed_i$ 를 이용하여 가상대학에 Login 한다.



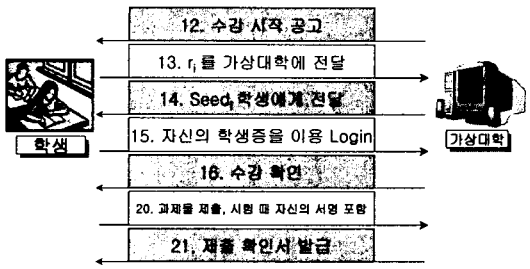
(그림 7) 사용자와 서버간의 인증을 위한 OTP

Step 16. 자신이 수강한 과목을 확인한다.(OTP 인증을 통

한 안전한 통로 개설)

Step 20. 과제물을 제출한다. (OTP 인증을 통한 안전한 통로 개설)

Step 21. 과제물 제출확인서를 발급받는다. (OTP 인증을 통한 안전한 통로 개설)



(그림 8) 가상대학 · 사용자 인증 정보 흐름 단계

4.7 각 모델별 비교 분석표

제안한 모델은 인증기관을 구축하여 업무의 효율을 증진시키고 수준 높은 보안성을 제공하고 있다. 사용자의 이메일, 전자문서에 대하여 보호 및 무결성을 제공하였다. 다음은 제안 모델과 비교 분석한 결과이다. 첫번째로 비교 분석한 것은 가상대학이 학교망 내에 존재할 경우이고(가상대학이 학교와 동일한 경우), 두 번째의 경우는 가상대학이 학교망 외부에 존재할 경우이다.(가상대학이 여러 학교가 모여 가상대학을 따로 만든 경우)

<표 1> 가상대학이 학내망 내부에 존재 할 경우.

비교표	Y 대학 모델	S 대학 모델	원격교육을 위한 메시지 필터링 기법	LAN/WAN 상에서의 멀티미디어 원격교육 시스템	제안모델
안전성	X	X	X	O	O
신원확인	X	O	O	O	O
내부결탁	Δ	O	X	O	O
신뢰성	X	O	X	O	O
효율성 (사용)	O	X	O	X	Δ
효율성 (교육)	O	Δ	O	Δ	O

<표 2> 가상 대학이 학내망 외부에 존재 할 경우(여러 대학이 가상대학을 세운 경우)

비교표	상용서비스 모델	O 가상대학	H 가상대학	제안모델
안전성	X	O	X	O
신원확인	O	O	O	O
내부결탁	O	X	X	O
신뢰성	X	X	X	O
효율성 (사용)	O	O	O	Δ
효율성 (교육)	Δ	O	O	O

5. 결론

빠르게 변화하는 교육문화에서 교육의 특수성과 시스템의 안정성이 보다 큰 문제가 되고 있다. 필수적인 체계를 통하여 교육체계의 정보화와 예산의 절감과 함께 교육문화의 흐름을 바꿀 수 있다고 본다.

본 논문에서는 PKI 의 전반적인 구성요소와 관련기술들을, 그리고 가상대학에 활용할 수 있는 인증기관 모델에 대한 시스템 구성요소 및 기능 그리고 운영절차 등 가상교육 분야에서의 모델을 제시하였다. 이를 통하여 많은 사람들에게 교육의 기회를 부여하고 올바른 교육 평가가 이루어 질 것이다. 여기서 제시한 모델은 기타 다른 조직에서의 활용할 수 있는 모델이 될 것이라 본다.

참고문헌

[1] 박희운, 이임영, "기밀성을 제공하는 상호 인증 일회용 패스워드 메커니즘 설계",춘계 멀티미디어학회, 2000

[2] 이만영, 김지홍, 류재철, 송유진, 염홍열, 이임영 공저, "전자상거래 보안기술", 생능출판사, 1999

[3] Seoul National University Virtual Campus, "http://snuvc .snu.ac.kr/"

[4] 박성준, 김지영, "공개키 기반구조에 관한 고찰", 정보처리학회 발표 자료집, P55~71, 19997

[5] 한재균, 한승조, "인터넷상에서 PKI 를 이용한 원격대학의 과제물 평가방법 개선에 관한 연구", P500~502, 1999

[6] Marc Branchaud, "A Survey of Public-Key Infrastructu- res", M.S.thesis, Department of Computer Science, McGill University, Montreal, 1997

[7] 한양사이버 학습센터, "http://cyber.hanyang.ac.kr/"

[8] 열린 사이버 대학, "http://www.ocu.ac.kr/"