JAVA CARD기반의 생체정보 및 다중PIN을 이용한 파일접근 제어 시스템 설계 및 구현

구은희*, 신인철**
*단국대학교 전자컴퓨터공학과
**단국대학교 전기전자컴퓨터공학부
e-mail:koohee@dankook.ac.kr

Design and Implementation of File Access Control System using Multi PIN and Biometrics based on Java Card

Eun-Hee Gu*, In-Chul Shin**
*Dept of Electronics & Computer Engineering, Dankook University
**School of Electrical & Electronics & Computer Engineering, Dankook University

요 약

급속한 정보기술 및 인터넷의 발달로 인해 네트워크를 통한 정보의 교류가 활발해지고 온라인 뱅킹 등 전자상거래와 관련된 산업의 규모가 커지면서 정보보안과 휴대용이 용이한 스마트카드는 여러 활용분야에서 사용되고 있다. 계속적인 하드웨어 기술의 발전으로 스마트카드의 표준으로 자리 잡고 있는 자바카드는 스마트카드 플랫폼에 자바의 기술을 접목시킨 것으로써 객체지향 중심의 기법으로 보안상 매우 좋은 이점을 지니고 있다. 또한 특성이 다른 하드웨어에서 같은 동작을 할 수 있는 개방형 운영체제를 가짐으로써 다양한 다수의 응용 프로그램을 수용할 수 있는 유연성을 가지게 한다.

본 논문에서는 이러한 자바카드의 특성을 이용하여 하나의 회원 카드로 다수의 사용자가 사용할 수 있는 접근통제가 가능한 회원카드를 설계하였다. 사용자에게 발급된 하나의 카드에 들어있는 정보를 개인이 아닌 다수의 사용자가 서로 다른 PIN을 이용하여 카드 내에 있는 사용자 정보를 접근하여 개인 정보의 확인, 관리내용 업데이트, 내용에 따른 청구를 카드 하나로 가능하게 하였다. 이때 사용자 인증수단으로 사용되는 PIN의 보안성을 높이기 위해 개인별로 고유한 생체인식의 한 구성요소인 서명 데이터를 이용하여 패스워드가 가지는 보안상의 취약요소를 없애 보다 안전한 사용자 인증을 하고자 한다. 이러한 자바카드의 이용기술과 생체인식 및 다중PIN을 이용한 사용자 인증, 파일의 보안 등급의 차등적인 접근권한을 설계하고 마지막으로 비주얼한 응용프로그램을 구현함으로써 카드를 보다 안전하고 편리하게 사용할 수 있기를 기대한다.

1. 서론

정보통신 환경의 발달로 인하여 실생활의 많은 부분들이 사이버 세계에서도 이루어지면서 일반 사용자들은 자신들이 소유한 정보에 대한 가치를 인식해 가고 있다. 이에 수반하여 정보보호에 대한 인식도 점차 확산되어 가고 있다[1],[2].

최근 들어 사회 환경 및 거래관계가 복잡해짐에 따라 신분 확인 및 보안 유지에 대한 요구가 증가함에 따라 정보보호를 위해 다양한 기능을 수행할 수 있는 대체수단이 필요하게 되었다[3],[4].

스마트카드는 기존의 카드에 마이크로프로세서와 메모리 등을 내장한 IC 칩과, 8개의 접속단자를 통하여 외부의 리더기로부터 전원 및 데이터 송수신을 하는 독립된 연산장치이다. 이는 각별한 보안을 필요로 하는 가치이전의 수단뿐만 아니라 전화카드, 이동통신 보안수단, 신분증, 교통카드 등 그 활용분

야가 아주 다양하기 때문에 정보통신망 환경에서 스마트카드가 중요한 보안장치로 수요나 활동 면에서 급격한 증가율을 보이고 있는 실정이다[1],[3].

그러나 기존의 스마트카드는 자체적으로 가진 저장능력과 계산능력의 한계, 내부적인 작동의 제한성 때문에 다양한 어플리케이션의 개발이 매우 복잡하고 어려운 환경을 가지며, 활용범위를 좁히는 결과를 가져왔다. 이러한 단점들을 해결할 수 있는 대안으로 스마트카드의 한 형태인 자바카드는 자바언어를 기본으로 지금까지의 스마트카드들이 하드웨어환경에 따라 서로 다른 어플리케이션을 사용하고, 이러한 어플리케이션의 개발이 각각의 스마트카드 하드웨어에 맞추어져 이루어지던 것의 자바의 플랫폼을 독립적인 실행 특성을 도입함으로써, 각각의 스마트카드 하드웨어에 구애받지 않는 통일된 개발환경을 구축하고, 스마트카드 어플리케이션 개발에 있어서 가장 효과적인 방법으로 자리 잡게 되었다[3].

다양한 응용 분야에 이용되는 자바카드의 엄격한 보안성을 높이기 위하여 현재까지 사용되고 있는 사용자 패스워드 또는 PIN(Personal Identification Number)만을 이용한 사용자 인증이 아닌 생체정보인 서명데이터(signature)를 이용한 사용자 인증을 이용함으로써 생체정보의 특징인 개인별로 고유한 것으로 절도나 누출에 의해 전달될 수 없으며 변경되거나 분실할 위험성이 없으므로 기존의 패스워드 또는 PIN만을 이용한 방법보다 신뢰성이 높은 신원확인을 할 수 있다. 또한 다수의 사용자가 이용하는 카드이므로 각각의 사용자들에게 접근권한을 두어 개인정보의 사용권한에 따라 사용자들의 응용프로그램이 맞추어 선택되어지는 프로그램을 설계 및 구현한다[4],[5],[7],[8].

2. 서명을 이용한 사용자 인증

대부분의 카드 사용자 인증 시스템에서는 사용자 인증의 수단으로 기본적으로 패스워드 또는 사용자 PIN을 사용하고 있는데 이들 방법은 패스워드의 분실, 유출 등의 관리문제가 생기기 때문에 보안상 많은 허점을 지니고 있다. 이를 해결하기 위하여 기존의 사용자 인증 시스템의 취약점인 신원을 확인하는 방법을 보완하여야 한다.

사용자 신원을 확인하는 방법으로는 사용자가 알고 있는 것, 사용자가 가진 것 또는 사용자의 물리적, 행동적 특성으로 사용자의 신원을 확인하여 사용자 인증을 한다.

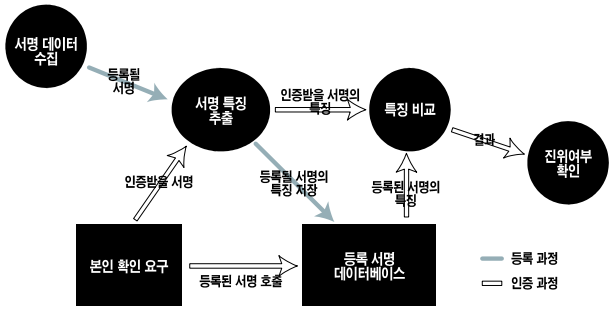
본 논문에서는 일반적으로 이용되는 가장 간단한 방법인 PIN을 이용한 사용자 인증 방법을 신체적인 특징, 즉 개인을 명백히 식별하기 위하여 생체정보 기법 중 서명(signature)을 이용하여 PIN과 함께 동시에 사용하였다. 서명을 이용함으로써 본인 이외의 다른 사람이 도용함을 막을 수 있게 되었다.

서명 인증 시스템은 전자펜 또는 stylus펜(PDA용)을 이용하여 입력된 개인의 특성을 검증하는 것으로써 서명의 특징(모양, 속도, 필압, 획 순서 등) 정보를 통합하여 비교 분석하여 본인 여부를 확인하기 위해 등록 과정과 인증 과정으로 구성된다.

수차례 서명을 입력하여 추출된 개인의 고유한 특징 파라미터를 적절한 알고리즘을 수행하여 서명 데이터 값을 만든다. 서명데이터 값은 우선 서명 데이터베이스를 구성한 후 이 데이터베이스에 등록한 후 리더기를 이용하여 카드에 저장한다.

실제 카드의 사용 시 각 사용자가 타블렛을 통하여 서명데이터를 입력하면 서명등록 데이터베이스와 연동되어 전처리(preprocessing), 특징 추출(feature extraction), 참조서명 DB(reference signature DB) 구축, 비교(comparison), 진위판별(decision making)의 과정으로 사용자 인증과정을 거치게 된다.

다음 (그림 1)은 사용 시 이루어지는 서명 인증 시스템의 구조도를 나타낸 것이다.



(그림 1) 서명 인증 시스템의 구조도

3. 파일 접근제어

사용자 인증이 이루어진 후에는 시스템의 자원과 정보에 접근하기 위하여 사용자의 ACL(Access Control List)등급에 따라 접근 권한을 부여한다. 다수의 사용자가 하나의 카드를 사용하면서도 정보의 유출이 없는 시스템을 설계하기위하여 사용자의 등급에 따라 접근을 제한하는 접근제어 시스템을 설계하였다.

파일은 카드에 Application 데이터를 저장하는 단위로서 MF, DF, EF에 의해 3레벨의 파일구조를 가진다. 파일의 종류는 DF(Dedicated File),

EF(Elementary File)로 나뉘며, DF는 파일의 디렉터리 구조를 나타낸다. DF는 다시 2종류로 나뉘어 지는데 DF들 중 루트 디렉터리에 해당하는 파일은 MF(Master File)라고 하고 이외의 파일들을 DF라고 한다. EF는 실제로 데이터가 저장되는 파일을 나타낸다. EF도 2종류로 나뉘어 지는데 카드의 운영체제가 사용하는 IEF(Internal Elementary File)와 응용 서비스의 정보를 저장하는데 사용하는 EF이다.

본 논문에서는 관리자, 일반 사용자, 보조 관리자로 나뉘어 카드가 사용된다. 관리자의 파일시스템은 일반 사용자의 개인정보 DF와 그 아래의 각종 데이터 EF와 보조 관리자의 신분 확인을 위한 DF와 그 아래 처리 EF가 있고 관리를 위한 DF와 신분 정보 및 확인을 위한 EF로 구성되어 있다. 일반 사용자의 파일 시스템은 MF 아래 개인 정보에 대한 DF와 각종 데이터를 담고 있는 EF들로 구성되어 있고, 보조 관리자의 파일 시스템은 MF 아래 신분 확인을 위한 DF와 그 아래 처리 데이터 EF들이 있다.

각각의 사용자에게 접근 권한을 정의는 접근권한 주체인 사용자를 정의하고, 인증 프로토콜을 설계하고, 접근 권한 유형을 설정한다. 인증 프로토콜은 관리자는 개인식별데이터(signature), 일반 사용자 개인식별데이터(signature), 보조 관리자 개인식별번호(PIN)로 나뉘어 진다. 각 사용자의 DF, EF의 권한 유형은 DF, EF를 접근하는 제어 목적으로 불리언 식의 규칙을 가지고 나눈다. 관리자는 파일에 접근하는 모든 권한을 주고, 보조 관리자는 보조 관리자 DF 및 EF의 모든 권한과 일반 사용자 일부 EF 일부 권한을 부여하고, 일반 사용자는 자신의 일부 EF의 모든 권한과 나머지 EF 및 DF의 일부 권한만을 부여한다. 다음 <표 1>은 본 논문에서 제안한 파일 권한을 나타내었다.

<표 1> 제안 시스템의 접근권한

		관리자(A)					일반사용자(U)					보조사용자(S)				
사용자 인증 Type		개인식별데이터 (signature)					개인식별데이터 (signature)					개인식별번호 (PIN)				
		a	r	w	e	d	a	r	w	e	d	a	r	w	e	d
DF 권한 유형	A	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
	U	x	x	x	x	x	o	o	x	x	x	x	x	x	x	x
	S	x	x	x	x	x	x	x	x	x	x	o	o	x	x	x
EF 권한 유형	A	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
	U	x	x	x	x	x	o	o	o	o	o	o	o	x	x	x
	S	x	x	x	x	x	o	o	o	o	x	o	o	o	o	o
A : 관리자, U : 일반사용자, S : 보조사용자																
a: Access, r: Read, w: Write, e: Edit, d: Delete																

4. 시스템 구현

4.1 사용자 인증 및 파일 접근권한 Applet 구현

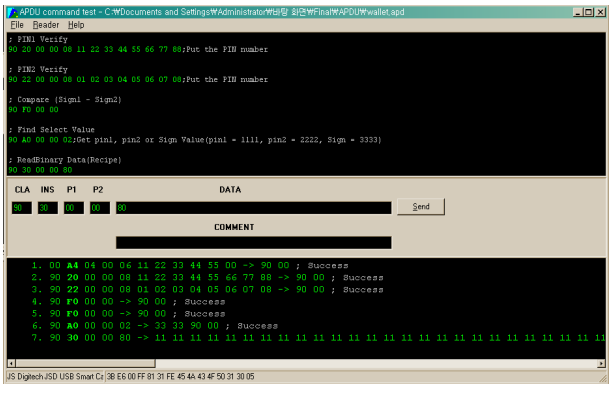
본 논문에서 제안한 시스템을 설계 및 구현하기 위하여 다음 <표 2>과 같은 환경을 이용하였다.

<표 2> 시스템 구현 환경

종류	세부사항
운영체제	Window 2000 Server
개발도구	J2se verson 1.2.2 Java(TM) Communications API specification2.0 Java_card_kit_2_2_1 서명등록 및 인증 프로그램 SMARTCAFE, PROFESSIONAL- -Toolkit V2.0
개발언어	Applet : Java, Application : Visual Basic
카드	Jcop 2.0, Smartcafelife(G&D)
단말기	SCRx31 CCID, PCT2000(G&D)
타블렛	디지타이져(WACOM)

카드와 단말기 사이의 통신을 위하여 자바카드의 Applet은 APDU(Application Protocol Data Unit)를 사용하여 통신을 하며, 생성된 Applet은 고유의 AID(Application Identifier)를 갖게 된다. 카드와 단말기 사이의 접속 시에는 항상 인증 단계가 요구되게 하였으며 TCP/IP 통신 프로토콜을 이용하여 제안된 서명 및 다중PIN을 이용한 접근권한 시스템과 통신을 한다. 각각의 사용자는 관리자, 일반사용자, 보조사용자로 애플릿으로 구현하였다.

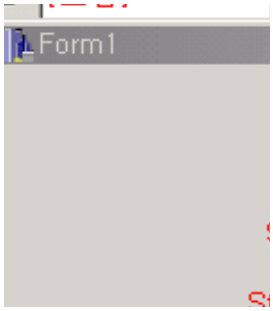
자바카드 상에서 프로그램이 진행되는 과정을 위해서는 APDU의 command와 response명령을 주고받으며 통신을 하며 response명령어가 '9000'이란 값을 지니면 그 과정이 성공 했다는 것을 의미한다.

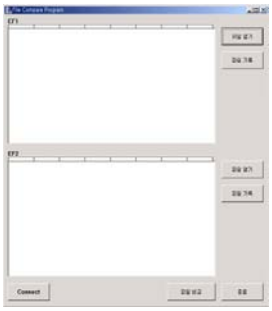


(그림 2) 접근권한 및 사용자인증 성공

(그림 2)에서 보여 지는 것은 카드에 있는 PIN값과 입력한 PIN 값이 동일한지를 비교하여 사용자를 판별하여 승인된 사용자를 보여주는 것이다. 이러한 인증과정을 거친 후 어플리케이션에 접근한다.

4.2 Application Programming 구현





(그림 3) 사용자선택 (그림 4) 인증 후 파일열기

본 논문에서 제안한 시스템을 최종적으로 구현하여 보았다. (그림 3)는 카드사용자의 PIN 정보를 받은 다음 사용자가 제시한 PIN이 정확한지를 다시 확인하는 것이고, 사용자의 인증이 이루어진 후 사용자의 권한별로 파일을 Access, Read, Write, Edit, Delete할 수 있는 것이다. (그림 4)는 파일을 선택하여 작업을 할 수 있는 환경을 보여준다.

5. 결론

본 논문에서 구축한 시스템은 자바카드 내에서 기존의 PIN의 비교를 위한 공간과 다중PIN을 넣고 비교하기위해 8byte의 공간을 할당하고 생체정보인 사용자 서명데이터를 비교하기위해 4Kbyte의 공간을 할당하여 서명데이터를 비교하였다. 또한 ACL의 등급에 따라 사용자의 권한을 제어하는 것을 가능하게 하였다. 이러한 연구의 결과 PIN이 가지는 보안상의 취약점을 해결하였고, 사용자의 접근권한을 적용함으로써 사용자와 시스템간의 신뢰를 제공하여 개인정보의 안전성과 신뢰성을 보장하는 것을 확인하였다.

향후 사용자인증을 위한 PIN을 서명데이터만이 아닌 다양한 생체정보를 이용해야 할 것이고, 접근권한을 제어하여 보다 다양한 서비스 어플리케이션의 개발과 함께 서비스의 활용성을 높이도록 해야 할 것이다.

참고문헌

[1] Jose Luis Zoreda Jose Manuel Oton, "Smart cards", Artech House Boston Sondon, 1994.

[2] Wolfgang Effing and Wolfgang Rankl, "Smart Card Handbood", Jahn Wiley & Sons, 2000.

[3] Patrice Peyret, "JavaCard Technology for Smart Cards Architecture and Programmer's Guide", Apri 2000.

[4] E. Vetillard, "Tools for Integrating the Java Card™ API into Jini™ Connection Technology", javaoneconf., 2000.

[5] Daniel Groner, et al., Java API Programming, provisorproess, 1997.

[6] Zhiqun Chen, "Java Card Technology for Smart Cards", pp.42-77, Addison-Wesley company, 2000.

[7] Sun Microsystems, "Java Card™ 2.1.1 Application Programming Interface", May 2000.

[8] Java Card™ 2.2 Virtual Machine Specification, Sun Microsystems, Inc., Early Access, 2001.

[9] Gemplus, "GemXpresso 2.4 PK User Guide, Getting Started", October 1999.

[10] J.Bigun, "Multi-modal Person Authentication", Face recognition, Sringer-Verlag, 1997.

[11] Gerd Bauer, "Data Structure for Electronic Precription", (Proposal), ISO/TC215/WG5, 2000.

[12] C. Schnorr, "Efficient Signature Generation by Smart Cards", Journal of Cryptology, Vol.4, No.3, 1991.

[13] Rescorla, Erie., "SSL and TLS(Desingning and Building Secure Systems)", Addison Wesley company, pp.175-217, 2001

[14] Window For Smart Card Toolkit 1.1 매뉴얼, 2000.

[15] Simon Wiseman, Phill Terry, Andrew Wood, "The Trusted Path betwiin SMITE and the User". British Crown Copyright, 1998.

[16] 강세나, 이기한 "IC 카드에 의한 원외 전자처방전 보안을 위한 시스템 구축", 정보처리학회 논문지, Vol.c No.3 pp.281-286, 2003.

[17] 임영이, 이윤철, 강회일, 이동일, "스마트카드 시스템의 보안 기술", 한국 전자 통신 연구원, 2000.

[18] 김연선, 이창욱, "자바카드 애플릿 설계 및 검증에 관한 연구", 한국통신정보보호학회 종합학술발표회 논문집, Vol.10 No.1 pp.805, 2000.

[19] 황선명, 염희균, "자바 카드 애플릿의 검증 방법", 정보처리학회 학회지, Vol.9 No.1 pp.489-492, 2002.

[20] 백장미, 강병모, 홍인식, "JavaCard을 이용한 마일리지 통합관리 시스템 구현", 정보과학회 학회지, Vol.28 No.2 pp.214-216, 2002.