情報保護學會論文誌
第 21 卷 第 4 號, 2011. 8

모바일 디바이스에서의 전자금융사고 예방을 위한 사용자입력패턴분석 기반 이상증후 탐지 방법*

서 호 진,† 김 휘 강‡
고려대학교, 정보보호대학원

Novel Anomaly Detection Method for Proactive Prevention from a Mobile E-finance Accident with User's Input Pattern Analysis*

Hojin Seo,† Huy Kang Kim‡
Graduate School of Information Security

요 약

모바일 디바이스(mobile device)를 통한 전자금융거래가 급속하게 증가하면서 이를 대상으로 한 공격시도도 점차 늘어나고 있다. 다양한 보안수단들이 적용되고 있지만, 모바일뱅킹(mobile banking)에 사용되는 디바이스에 원격으로 침입을 한 뒤 공격하는 방법 및 디바이스를 물리적으로 획득하여 전자금융사고를 유발할 수 있는 위험이 여전히 존재한다. 본 논문에서는 모바일 디바이스에서의 전자금융사고 예방 대책으로 개인별 입력패턴을 분석하여 본인에 의한 전자금융거래 시도인지 유무를 판단하여 선제적으로 대응할 수 있는 방안을 제안한다. 화면 터치(touch)를 통해 입력하는 모바일 디바이스의 특성상 터치 시간이나 압력 등의 패턴(pattern)은 개인별로 차이가 있으므로 이를 모니터링(monitoring) 함으로써 정상적인 모바일뱅킹 고객과 공격자를 구분할 수 있다. 본 논문에서 제시된 방안의 효용성을 증명하기 위해 모바일 디바이스에서의 개인별 입력패턴 정보를 실제 수집하여 실험하였고, 실험결과 입력패턴 정보 분석을 통해 전자금융사고를 효과적으로 예방할 수 있음을 확인하였다. 또한, 본 논문에서는 이러한 입력패턴 정보의 모니터링을 이용하여 불법적인 전자금융거래에 실시간으로 대응하는 방안도 제안한다.

ABSTRACT

With the increase in the use of mobile banking service, mobile banking has become an attractive target to attackers. Even though many security measures are applied to the current mobile banking service, some threats such as physical theft or penetration to a mobile device from remote side are still remained as unsolved. With aiming to fill this void, we propose a novel approach to prevent e-financial incidents by analyzing mobile device user's input patterns. This approach helps us to distinguish between original user's usage and attacker's usage through analyzing personal input patterns such as input time-interval, finger pressure level on the touch screen. Our proposed method shows high accuracy, and is effective to prevent the e-finance incidents proactively.

Keywords: Mobile banking security, Input pattern analysis, Biometric, Neural network

접수일(2010년 12월 2일), 수정일(2011년 2월 7일), 게재확정일(2011년 5월 13일)
* 본 연구는 지식경제부 및 정보통신산업진흥원의 "대학 IT 연구센터 육성·지원사업"의 연구결과로 수행되었음 (NIPA-2011-C1090-1001-0004)
† 주저자, hj3838@kftc.or.kr
‡ 교신저자, cenda@korea.ac.kr

I. 서 론

최근 스마트폰(smart phone)을 중심으로 한 모바일 디바이스의 보급이 급속하게 증가하고 있으며, 사용영역 또한 크게 확대되어 조회 및 계좌이체와 같은 전자금융거래에도 모바일 디바이스가 폭넓게 활용되고 있다. 한국은행의 발표에 따르면 2010년 3/4분기 기준 국내 스마트폰 기반 모바일뱅킹[1](이하 "모바일뱅킹" 이라 한다) 등록 고객수가 이미 137만 명을 돌파하였고, 이용 건수나 금액도 직전 분기 대비 각각 368.6%, 297.5%에 이르고 있어 그 증가속도가 매우 빠르다고 할 수 있다[1].

이와 같은 모바일뱅킹의 급속한 성장에 비례하여 모바일뱅킹을 대상으로 하는 공격시도도 점차 늘어나고 있다. 맥아피(McAfee)의 "Mobile Security Report 2009"의 조사에서도 각 보안 벤더들의 81%가 향후 가장 중점을 두어야할 보안 분야로 모바일뱅킹을 꼽고 있는 점이 이를 반증한다고 하겠다[2] 애플(Apple)의 iOS, 구글(Google)의 안드로이드(Android) 등 모바일OS별로 악성코드나 취약점 들이 속속 발견되고 있으며, 2010년 9월에는 Zeus Trojan으로 명명된 모바일 악성코드를 통해 유럽 12개 은행의 고객이 공격을 당한 사고가 보도되기도 하였다[3]. 또한, SMS(Short Message Service) 스팸(spam)을 통해 비밀번호와 같은 개인의 중요 정보를 불법 획득하는 모바일 피싱(phishing) 공격도 스미싱(SMiShing : SMs+phISHING)이란 이름으로 이미 현실화 되어 있는 상황이다[4].

이러한 보안 위협에도 불구하고 모바일 디바이스 전력의 한계, 기능 및 성능상의 제약 등으로 인해 모바일뱅킹에 PC기반 인터넷뱅킹(이하 "인터넷뱅킹" 이라 한다) 수준의 보안대책을 적용하기는 어렵다[5]. 배터리에 의존하는 전력사용이나 하드웨어(CPU, 메모리 등)의 한계 등으로 PC환경에서 동작하는 보안 프로그램들을 모바일 디바이스에서 원활하게 운영하기는 쉽지 않다. 하지만 모바일 디바이스의 개방성이나 기능, 상시 인터넷 접속이 가능한 특징 등을 고려할 때 인터넷뱅킹의 보안 위협이 모바일뱅킹에도 상존할 것으로 예상되므로 모바일뱅킹 환경에 적합한 보안대책 관련 연구가 필요하다고 하겠다.

이에 본 논문에서는 개인별 입력패턴 정보 모니터링(monitoring)을 통해 공격자에 의해 불법적으로 시도되는 전자금융거래를 탐지·차단하는 방안을 제안한다. 모바일 디바이스의 경우 PC와는 달리 대부분 스타일러스(stylus) 터치펜이나 손가락을 이용하여 입력을 하게 되며, 입력 시 누르는 압력이나 누른 후 손가락을 뗄 때까지의 시간, 손가락으로 터치 화면을 쓰다듬어 휠 액션(wheel action)을 하는 작업과 같은 입력패턴은 개인의 습관이나 신체적 특성에 기인하므로, 사용자 개개인의 고유한 특성을 나타낸다고 볼 수 있다. 이는 일종의 생체 파생 정보로 활용될 수 있는데 지문이나 홍채 정보 등과 같이 직접적으로 생체정보를 수집하지 않는다는 점에서 금융기관이 적용하기에 보다 용이하다고 할 수 있다. 이 점에 착안하여 본 논문에서는 개인별 입력패턴 정보를 탐지의 주요한 요소로 이용하였다.

전자금융거래를 위한 공인인증서 비밀번호나 보안카드 번호 등 개인의 접근매체 정보(이하 "접근매체정보"라 한다)는 악성코드 감염이나 피싱 공격 등에 의해 유출될 가능성이 있는 정보이다. 하지만 본 탐지 방안을 적용할 경우 접근매체 정보가 공격자에게 모두 유출되더라도 개인별 입력패턴 비교를 통해 비인가자의 불법 전자금융거래 시도를 즉시 확인할 수 있어 모바일 디바이스에서 전자금융사고를 효과적으로 예방할 수 있다.

이 방안의 효용성을 증명하기 위해 실제 각 개인으로부터 모바일 디바이스의 입력패턴 정보를 수집하였고, 수집한 정보들로 변별력 있게 개인을 정확히 구분해 낼 수 있는지를 판별하기 위해 신경망(neural network)알고리즘을 적용하였다. 실험 결과 본 논문에서 제안하는 방안이 98% 내외의 높은 클러스터링(clustering) 성공률과 예측력을 보임을 확인할 수 있었고, 이를 종합해볼 때 모바일 디바이스에서의 입력패턴 정보를 토대로 해당 개인의 이용패턴을 학습한 후 모바일뱅킹 이용시 생성되는 패턴 인스턴스(instance)값을 대입할 경우 본인의 실제 거래 이용 유무를 탐지할 수 있을 것으로 생각된다. 또한, 본 논문에서는 이러한 입력패턴 정보 모니터링을 통해 모바일 디바이스에서의 불법 전자금융거래에 실시간으로 대응할 수 있는 방안도 제안한다.

논문의 구성은 다음과 같다. 2장에서는 국내 전자금융사고 유형 및 대응현황에 대해서 설명한다. 3장과 4장에서는 제안하는 방안에 대한 기본 개념과 구조, 구현방안에 대해 설명하고, 5장에서는 실험을 통해 본 방안의 성능과 효용성에 대해 설명한다. 마지막으로 6

1) 금융IC Chip방식의 모바일뱅킹과 VM방식의 모바일뱅킹은 본 논문의 논의대상에서 제외한다.

장에서는 요약과 함께 본 논문의 결론을 맺는다.

II. 국내 전자금융사고 유형 및 대응 현황

본 장에서는 국내 전자금융사고 유형 및 기법과 그에 따른 금융기관의 대응 현황에 대해 설명한다.

2.1 전자금융사고 유형 및 기법

2009년 9월 금융감독원에서 발표한 최근 5년간 국내 전자금융사고 내역 및 처리현황에 의하면 매년 평균 13건, 피해 금액으로는 2억 9천여만원의 전자금융사고가 발생하고 있다[6]. [표 1]은 2000년대 들어 발생한 대표적인 전자금융사고 사례를 정리한 것으로[7], 대부분의 전자금융사고가 금융기관 전자금융시스템이 아닌 고객PC 등에서 발생되고 있음을 알 수 있다. 이는 공격자에게 금융기관의 내부 시스템 보다는 고객PC가 공격하기에 용이하기 때문으로 분석된다.

인터넷뱅킹시스템과 같은 전자금융시스템은 행정안전부의 정보통신기반보호법령에 의거 주요정보통신기반시설로 지정되어 매년 정기적으로 취약점 분석·평가를 실시하고 보호대책을 수립·시행하고 있으며, 금융ISAC(Information Sharing Analysis Center)을 통해 24시간 상시 보안 관제를 실시하는 등 외부로부터의 침해공격에 철저히 대비하고 있어 공격자가 금융기관 시스템을 직접 공격하여 성공하기에는 많은 어려움이 있다.

하지만 고객PC의 경우 백신 프로그램 설치나 OS보안 업데이트(update)와 같이 기본적인 보안조치 조차 미흡한 경우가 많아 악성코드의 감염 위험성도 높고, 일부 고객은 보안카드나 공인인증서 등 접근매체 정보를 파일 형태로 보안이 허술한 이메일(e-mail)이나 웹 하드(web-hard) 등에 저장하는 경우도 있어 금융기관 전자금융시스템에 비해 상대적으로 손쉽게 공격에 성공할 수 있다. 이러한 이유로 국내 대부분의 전자금융사고는 공격자가 악성코드 등으로 고객 PC를 공격하여 접근매체 정보를 획득한 후 이를 통해 사전 공모된 대포통장으로 불법적으로 이체하는 형태로 발생된다.

2.2 인터넷뱅킹 전자금융사고 대응 현황

금융기관에서는 전자금융사고 위험성이 상대적으로 높은 고객PC 구간 보안강화를 위하여 인터넷뱅킹에

[표 1] 국내 대표적인 전자금융사고 사례 (2000년대)

년 도	내 용
2004년	텔레뱅킹 감청에 의한 비밀번호 유출 및 이체 사고
2005년	악성코드를 사용한 인터넷뱅킹 접근매체 정보 유출 및 불법 자금이체 사고 (국내 최초의 인터넷뱅킹 해킹사고)
2007년	악성코드 또는 파밍(pharming) 사이트를 통한 인터넷뱅킹 접근매체정보 유출 및 불법 자금이체 사고
2008년 2009년	개인PC, 이메일, 웹하드 해킹을 통한 인터넷뱅킹 접근매체 정보 유출 및 불법 자금이체 사고

사용자 인증, 접근매체 정보 보호를 중심으로 한 다양한 기술적 보안대책을 적용하고 있다.

2.2.1 사용자 인증 및 전자서명

인터넷뱅킹과 같은 전자금융거래는 창구거래와는 다른 비대면 거래로 사용자 및 거래에 대한 인증과 무결성 보장을 위해 공인인증서와 일회용 비밀번호를 사용하고 있다. 공인인증서는 PKI(Public Key Infrastructure)를 적용한 전자서명 기술로 사용자에 대한 인증과 거래의 무결성을 보장할 수 있고, 전자서명법에 의거 발급, 갱신 등의 과정이 엄격하게 관리되므로 인터넷뱅킹을 포함한 국내 대부분의 전자금융거래에 의무적으로 사용하도록 규정하고 있다. 일회용 비밀번호로는 보안카드가 가장 대중적으로 사용되고 있다. 보안카드는 금융기관 창구에서 대면 확인을 통해 직접 발급하고 매 거래 시마다 카드의 시리얼(serial) 번호가 변경되므로 고정된 비밀번호 보다는 보안성이 매우 높다고 하겠다. 최근에는 시리얼번호가 30여개로 한정되어 있는 보안카드의 단점을 보완하기 위해 금융기관에서 전용OTP(One Time Password)기기의 사용을 적극 권장하고 있다.

2.2.2 인터넷뱅킹 접근매체 정보 유출 방지

고객PC의 경우 인터넷에 노출되어 있고 보안조치 또한 미흡한 경우가 많아 인터넷뱅킹 접근매체 정보가 악성코드 등에 의해 쉽게 유출될 수 있다. 이를 예방하기 위해 금융기관에서는 인터넷뱅킹 시 고객PC에 악성코드 탐지 프로그램, PC방화벽, 키보드(keyboard) 보안프로그램, 웹(web) 암호화 프로그램 등

을 설치·운영하고 있다. 이러한 보안 프로그램들은 클라이언트(client) PC의 악성코드 감염 진단 및 접근매체 정보 유출 차단 등의 역할을 수행한다. 하지만 해킹(hacking) 공격기술의 진화에 따라 메모리(memory) 해킹 등 보안 프로그램 우회가 가능한 공격기법들이 지속적으로 개발되고 있어 인터넷뱅킹 보안에 큰 위협이 되고 있다. 금융기관에서는 이를 해결하기 위해 확장 E2E(End to End) 암호화 적용, 마우스(mouse)를 이용한 가상 키보드 도입 등 추가적인 보안대책을 도입·적용하고 있으나 공격 기법의 다양성 등으로 인해 효과적인 대응에 어려움을 겪고 있다.

2.2.3 고객PC 정보 모니터링

고객PC의 경우 인터넷 뱅킹시스템의 원격에 위치해 있고 금융기관의 통제 하에 있지도 않으며, 사용자 또는 악의적인 해커에 의해 무결성이 훼손될 수 있기 때문에 신뢰할 수 있는 디바이스라고 할 수 없다. 그러므로 어떠한 보안대책을 적용하더라도 접근매체 정보의 유출을 원천적으로 차단하기는 어렵다[8]. 인터넷뱅킹 보안강화를 위해 새롭게 적용된 전용OTP(One Time Password) 기기의 경우에도 단방향 인증방식 이므로 중간자 공격(Man-in-the-Middle Attack)에 취약할 수밖에 없고, OTP의 생성 메커니즘도 무작위성을 가져야하나 이 또한 프로그램을 통해 구현하므로 일정 시간이 경과하면 예측이 가능해지는 문제점이 있다[9].

금융기관에서도 이러한 한계점을 인지하고 인터넷뱅킹 접근매체 정보가 공격자에게 모두 유출되더라도 불법 전자금융거래를 탐지·차단할 수 있도록 고객PC 정보(IP주소, MAC주소, 하드디스크 시리얼번호 등) 모니터링 방안을 적용하였다[7]. 이는 개인별 인터넷뱅킹 수행 장소가 대부분 집이나 회사, 학교 등의 일부 PC로 한정되어 있다는 점을 활용한 것으로, 예를 들어 서울에서 주로 이체 거래를 하는 고객의 계좌를 통해 중국에서 이체 요청이 있을 경우 금융기관에서는 이를 의심스러운 거래로 인식할 수 있다. 이 방안은 공격자에게 접근매체정보가 모두 유출되더라도 최종 이체단계에서 거래를 제한할 수 있어 고객의 피해를 최소화할 수 있다.

하지만 이를 적용한다 하더라도 공격자의 PC 정보를 고객PC 정보로 위장할 경우 우회가 가능한 문제점이 있고, IP주소의 경우에도 국내에서 제공하는 VPN/PPTP 접속 서비스 등을 통해 손쉽게 위장이 가능하며, 해커가 트로이목마 등의 백도어(backdoor) 프로그램을 통해 고객PC의 권한을 완전히 장악한 경우도 발생할 수 있으므로 위의 방법에는 한계가 있다고 할 수 있다. 더불어 금융기관의 고객PC 정보 수집에 대한 사생활(privacy) 침해 문제가 지속적으로 제기되고 있는 점 역시 추가적인 한계점으로 작용하고 있다.

2.3 모바일뱅킹 보안대책

국내 모바일뱅킹은 대부분 iOS, 안드로이드 등 모바일OS별로 금융기관이 제공한 뱅킹전용 앱(App)을 통해 금융거래를 수행하는 방식으로, 계좌 조회나 이체는 물론 신용카드, 펀드 등의 거래까지 인터넷뱅킹에 준하는 대부분의 서비스를 제공하고 있다. 또한, 모바일OS가 PC용 OS구조를 유지하면서 모바일에 최적화된 방향으로 개발되었고, 3A(Anytime, Anywhere, Anyhow) 서비스 제공을 위해 모바일 디바이스의 상시 인터넷접속이 지원되기 때문에 인터넷뱅킹에서 발생될 수 있는 모든 보안 위협이 모바일뱅킹에도 동일하게 발생될 수 있을 것으로 예상된다[10].

이에 금융감독원에서는 "스마트폰 전자금융 안전대책"을 발표하고 모바일뱅킹에도 인터넷뱅킹 수준의 보안대책을 적용할 것을 권고하였고, 금융기관에서는 모바일 디바이스의 전력이나 성능상의 제약에도 불구하고 동 대책에 따라 높은 수준의 보안대책을 수립·시행하고 있다. 모바일 디바이스에 공인인증서를 저장하여 거래 시마다 인증 및 전자서명을 의무적으로 실시하고 있으며, 악성코드 탐지를 위한 백신 프로그램 설치는 물론 접근매체 정보 보호를 위해 E2E암호화와 무작위로 생성되는 가상키보드 등의 보안대책을 모바일뱅킹에 적용하고 있다.

하지만 모바일뱅킹의 경우에도 인터넷뱅킹과 마찬가지로 접근매체 정보 유출 위험성이 존재한다. 모바일 디바이스는 MMS(Multimedia Messaging Service), 블루투스(bluetooth), PC-Sync 등 악성코드의 감염경로가 PC에 비해 다양하고, 백신 프로그램에 대한 업데이트나 OS의 보안패치 등도 용이하지 않아 PC에 비해 악성코드 감염 위험도가 더 높다고 하겠다. 인터넷뱅킹의 고객 PC정보 모니터링 방안과 같이 모바일 디바이스의 정보(IMEI, GPS정보 등)를 수집하여 모니터링 하는 방안도 접근매체정보 유출 위험에 대한 좋은 보완책이 될 수 있으나, 이 정보 역시 공격자에 의해 위조가 가능하여 우회될 수 있

고 개인 사생활 침해 등 인터넷뱅킹의 모니터링 방안과 동일한 문제가 발생될 수 있는 단점이 있다.

III. 제안하는 방안

앞서 설명한 바와 같이 현 모바일뱅킹 보안대책은 접근매체 정보 유출 위험성이 여전히 존재하는 등 그 한계가 있다. 따라서 본 장에서는 이를 해결하기 위해 모바일 디바이스에서 개인별 입력패턴을 모니터링 하여, 불법전자금융거래를 탐지하고 이를 실시간으로 차단하는 방안을 제안한다.

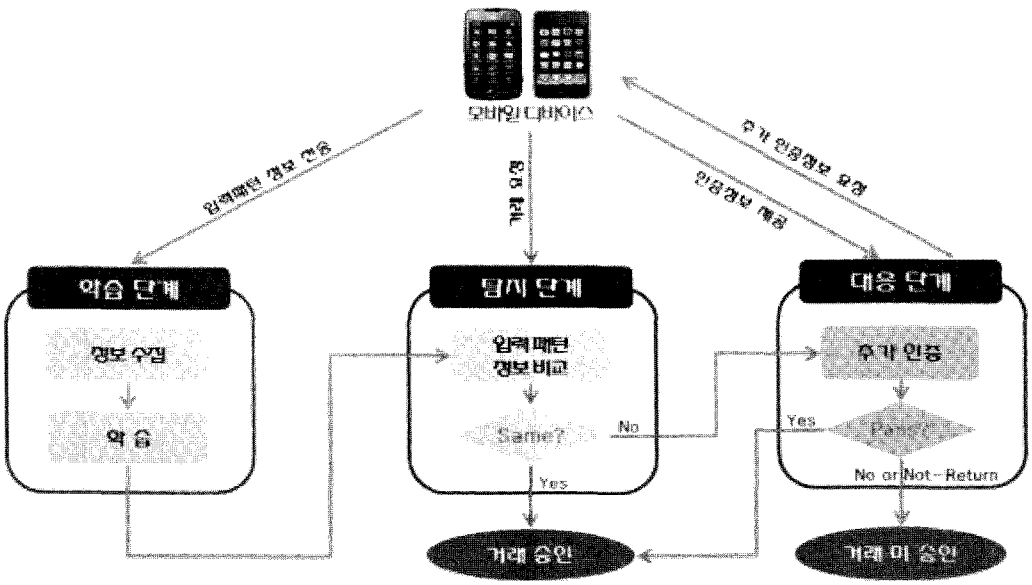
3.1 기본 개념

스마트폰과 같은 모바일 디바이스는 PC에 비해 크기가 작고 키보드, 마우스와 같이 물리적인 입력매체를 적용하기가 용이하지 않아 대부분 터치스크린(touch screen)을 입력매체로 채택하고 있다. 따라서 사람들은 모바일 디바이스 입력을 위해 손가락을 사용하게 되는데 이때 손가락으로 터치스크린을 누르는 시간이나 압력, 손가락을 움직이는 속도 등의 패턴은 사람마다 차이가 있으므로 지문, 홍채, 얼굴 모양과 같이 사람을 구분할 수 있는 생체정보로 사용할 수 있다. 생체정보는 인간이 가진 본질적인 특징에 대한 인식에 기반을 두고 있어 이를 사용하여 그 사람이 물리적으로 존재하는지에 대한 인증이 가능할 뿐만 아니라 합법적인 사용자와 공격자를 구분할 수없는 패스워드의 한계도 극복할 수 있다[11]. Liang Xie, et al의 연구에서는 모바일 디바이스에서의 입력패턴 정보를 악성코드 탐지에 활용하였는데, 입력시의 압력이나 시간, 입력 좌표값을 분석을 통해 해당 입력이 실제 사람에 의한 것인지 아니면 악성코드에 의해 임의로 생성된 것인지를 구분하였다[12].

본 논문에서는 모바일 디바이스에서의 입력패턴 정보를 불법 전자금융거래 탐지에 적용한다. 사람마다 입력패턴이 다르기 때문에 이를 사전 학습 후 모니터링 하면 해당 거래가 계좌 소유주에 의한 정상 거래인지 아니면 공격자에 의한 불법적인 거래인지 확인할 수 있다. 이 방안은 고객의 접근매체 정보가 공격자에게 모두 유출되더라도 불법 이체거래 시도 시 입력패턴 정보 모니터링을 통해 실 계좌 소유주의 거래가 아님을 확인할 수 있기 때문에 고객의 피해를 최소화할 수 있다. 또한, 동 방안이 입력패턴 이라는 일종의 생체정보를 탐지에 사용하므로 공격자에 의한 위조가 불가능하고, 고객PC 정보 등과 같이 개인정보에도 해당되지 않으므로 모바일 디바이스 정보 모니터링 방안의 한계도 해결할 수 있는 장점이 있다.

3.2 불법 전자금융거래 탐지 및 대응 모델

[그림 1]은 입력패턴 모니터링을 통한 모바일 디바이스에서의 불법 전자금융거래 탐지 및 대응 모델로



[그림 1] 사용자 입력패턴 모니터링을 통한 모바일 디바이스에서의 불법 전자금융거래 탐지 및 대응 모델

크게 학습, 탐지, 대응의 3단계로 구성된다. 학습 단계는 모바일뱅킹 고객의 입력패턴 정보를 수집하고, 이를 개인의 일반화된 값으로 정형화하는(탐지 기준값을 설정)하는 과정으로 불법 전자금융거래 탐지를 위한 사전 준비단계로 볼 수 있다. 학습은 일정 수준의 연산이 요구되므로 하드웨어(hardware) 성능의 제약이 있는 개인의 모바일 디바이스 보다는 금융기관의 전자금융시스템에서 수행하는 것이 보다 효율적이며, 이 경우 학습된 결과가 디바이스에 저장되지 않으므로 디바이스가 해커에 의해 공격을 당한다 하더라도 불법 전자금융거래 탐지를 위해 쓰이는 데이터(data)들이 역으로 크래커(cracker)에 의해 수집되거나 변조되지 않게 된다.

탐지 단계는 모바일뱅킹 시 입력패턴 정보를 모니터링 하여 해당 거래가 계좌 소유주에 의한 정상적인 거래인지 여부를 확인하는 단계로 학습단계 완료 후 수행된다. 만약 신규 요청된 거래에서 수집된 입력패턴이 기존 학습된 계좌 소유주의 입력패턴에 부합할 경우 거래를 승인하고 그렇지 않은 경우 공격자에 의한 불법 전자금융거래로 의심할 수 있으므로 거래를 승인하지 않고 대응 단계로 넘어간다.

대응 단계는 탐지 단계에서 의심스러운 것으로 인지된 거래에 한해 추가적인 인증 절차를 수행하는 단계로 이를 통해 공격자의 의한 불법 전자금융거래를 명확하게 확인하여 차단할 수 있다.

IV. 설계 및 구현

4.1 사용자 입력패턴 정보의 수집

모바일뱅킹 거래 시 입력되는 값들을 분류해 보면, 크게 터치와 스크롤(scroll)로 구분할 수 있다. 터치는 버튼과 같은 위젯(widget)을 손가락으로 누르는(press) 입력이고, 스크롤은 화면 전환을 위해 손가락으로 스크린을 쓰다듬어 휠 액션을 하는 입력이다. 이러한 터치와 스크롤 입력패턴은 개인의 행동 성향이나 생체적 특성에 따라 사람마다 차이가 있게 되는데, 〔표 2〕는 이러한 차이를 발생시키는 요소들을 정리한 것이다. 표에서 보듯 많은 요소들이 개인의 입력패턴에 영향을 주게 되므로 이들이 모두 동일하거나 유사한 사람이 복수로 존재할 확률은 매우 낮다. 따라서 입력패턴이 개인을 인증하는 하나의 정보로써 활용될 수 있으며, 모바일뱅킹 시 해당 정보를 모니터링할 경우 계좌 소유주와 공격자를 효과적으로 구분할 수 있다.

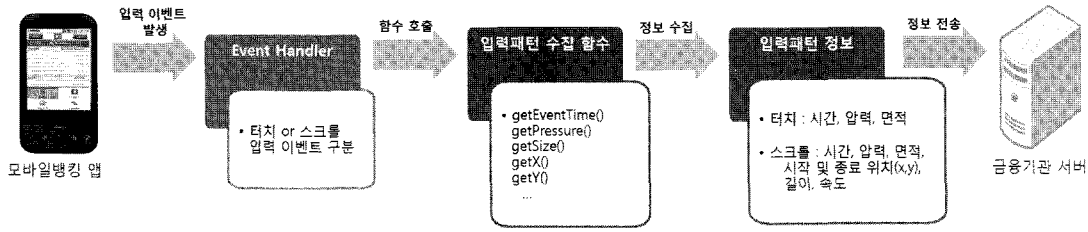
〔표 2〕 개인별 입력패턴에 영향을 미치는 요소

분 류	개인별 행동성향 및 생체적 특징	
사용하는 손과 손가락	오른손 잡이	왼손 잡이
	손가락 1개 사용	손가락 1개 사용
	엄지 사용	검지 사용
터치 및 스크롤 시간(Time)	길게 (Long)	짧게 (Short)
터치 및 스크롤 압력(Pressure)	강하게 (Strong)	약하게 (Weak)
터치 및 스크롤시 손가락이 닿는 면적(Width)	넓음 (Wide)	좁음 (Narrow)
	손가락 굵기나 입력시 손가락의 각도(눕혀서or세워서)에 영향을 받음	
스크롤 시작 및 종료 위치 (Position)	좌우, 상하 등 개인마다 스크롤 시작 및 종료 위치(좌표)가 다양	
스크롤 속도 (Speed)	빠르게 (High)	느리게 (Low)
스크롤 길이 (Length)	길게 (Long)	짧게 (Short)

기본적으로 터치는 손가락으로 누르는 입력이므로 누르는 시간(time)과 압력(pressure), 손가락이 닿는 면적(width)이 입력패턴 정보로 활용 가능하며, 스크롤은 손가락으로 화면을 누른 상태에서 이동시키는 입력으로 시간, 압력, 면적은 물론 스크롤을 시작하고 종료하는 위치 좌표(position)와 스크롤 속도(speed) 및 길이(length)가 입력패턴 정보에 추가된다. 개인별로 사용하는 손(오른손 잡이, 왼손잡이)이나 손가락(엄지, 검지 등)의 차이는 각 입력패턴 정보의 값에 영향을 미칠 수 있다. 터치 및 스크롤 입력별 패턴 정보를 요약하여 표현하면 아래와 같다.

{터치 : T_time, T_pressure, T_width}
{스크롤 : S_time, S_pressure, S_width, S_speed, S_length, S_startpos(x,y), S_endpos(x,y)}

이와 같은 사용자 입력패턴 정보의 수집은 모바일뱅킹 앱에 수집을 위한 별도의 모듈(함수)를 추가하는 방식으로 손쉽게 구현이 가능하다. iOS, Android와 같은 모바일OS는 사용자의 입력패턴 정보를 수집할 수 있는 API를 기본적으로 제공하고 있으며, 〔그림 2〕와 같이 모바일뱅킹 앱의 버튼이나 스크롤뷰(scrollview)와 같은 위젯에 사용자의 터치나 스크롤



〔그림 2〕 사용자 입력패턴 정보 수집 절차 (Android)

입력 이벤트가 발생할 경우 이벤트 핸들러(event handler)를 통해 입력패턴 수집 함수가 호출되는 방식으로 처리한다.

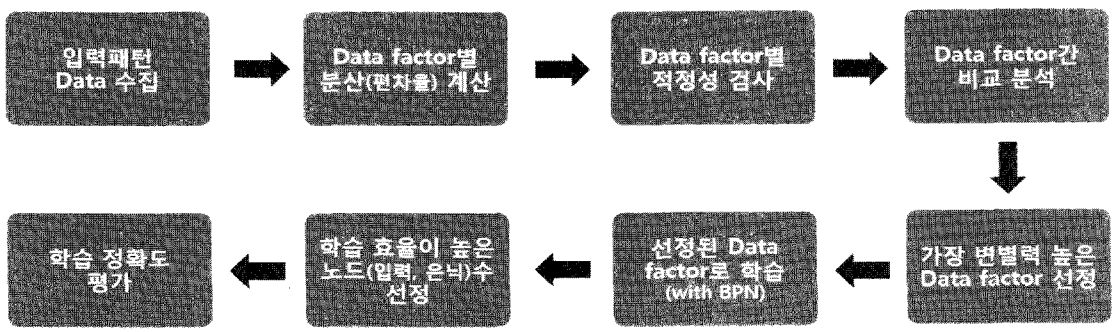
Android의 경우 MotionEvent 클래스(class)와 Gesture 클래스 등에서 입력패턴 정보 수집을 위한 함수를 제공하고 있는데, 터치 및 스크롤 입력의 발생 시간과 압력, 손가락이 닿는 면적, 시작 및 종료 좌표(x,y)값은 각각 MotionEvent 클래스의 getEventTime(), getPressure(), getSize(), getX(), getY() 함수를 호출하여 수집할 수 있으며, 스크롤 길이는 Gesture 클래스의 getLength() 함수를 사용하는 방법 등으로 수집할 수 있다. 또한 스크롤 속도는 스크롤 길이를 스크롤 시간으로 나누는 방식으로 계산이 가능하다.

4.2 학습 방법 및 절차

전체적인 학습 방법과 절차는 〔그림 3〕과 같다. 우선 학습이 가능하도록 일정 횟수 이상의 입력패턴 정보를 수집하고, 수집된 여러 종류의 입력패턴 정보 중 개인의 특성을 잘 나타내는 변별력 높은 팩터(factor)를 선정한다. 예를 들어, 어떤 사용자가 터치 시 압력과 면적에는 큰 변화가 없지만 시간의 경우 입력 시마다 편차가 크다고 가정하면 시간 정보는 사용자를 구분할 수 있는 팩터로 볼 수 없으므로 학습 요소에서 제외하는 것이 정확도나 효용성을 높이는데 도움이 된다.

사용자의 입력패턴 정보 중 학습에 활용할 수 있는 주요 팩터가 분류되면 학습을 실시한다. 본 논문에서는 입력패턴 정보에 대한 학습 알고리즘으로 신경망(neural network) 모델 중 다계층 퍼셉트론(multi-layer perceptron)을 이용한 역전파 신경망(back propagation neural network, 이하 "BPN" 이라고 한다) 알고리즘을 사용하였다. BPN은 최소자승 알고리즘(Least Square Method)의 비선형적 확장으로 볼 수 있는 지도 학습 방법으로 신경망 모델 중 패턴인식을 비롯한 여러 분야에 가장 광범위하게 사용되고 있다[13]. 입력패턴 정보 학습을 위해 BPN을 제안한 가장 큰 이유는 BPN의 오류 감내(fault tolerance) 능력이 우수하기 때문이다[14]. 학습 대상인 입력패턴 정보의 경우 터치와 같이 사람의 행동을 통해 수집되는데, 사람이 기계처럼 항상 일관된 패턴으로 입력하기는 어려우므로 입력패턴에 이전 입력과는 전혀 다른 잡음(noise)이 드물게 포함될 수 있다. 하지만 BPN은 알고리즘 특성상 잡음이 일부 포함되더라도 원하는 결과를 도출할 수 있어 타 알고리즘에 비해 학습 오류를 줄일 수 있다.

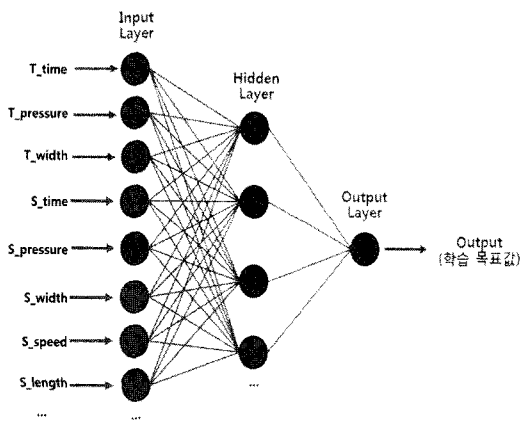
〔그림 4〕는 사용자의 입력패턴 정보 학습에 대한



〔그림 3〕 사용자 입력패턴 정보 학습 절차

BPN 구조 이다. 입력 노드(input node)에 사용자 입력패턴 값을 주면 이 신호는 각 노드에서 변환되어 은닉 노드(hidden node)에 전달되고 계산 과정을 거쳐 출력 노드(output node)에서 결과값을 출력하게 된다. 이때 출력된 값과 실제 목표값을 비교하여 이 둘간의 차이, 즉 오차를 줄여나가는 방향으로 가중치를 반복적으로 조정하여 학습 네트워크를 구성한다. 학습의 정확도나 학습에 소요되는 시간은 신경망의 계층(layer)수와 입력 및 은닉 노드수에 영향을 많이 받는다. BPN과 같은 신경망은 학습 과정에서 네트워크를 통해 할당되는 각 노드에 대한 가중치가 업데이트 되는데,업데이트된 최종 가중치의 적정성은 신경망 알고리즘을 통해 직접 유추하기는 어려우므로 최적의 신경망 구성은 계층수와 노드 수를 변화시켜가며 실험을 통해 결정하여야 한다. 또한, 구현 관점에서 보면 학습 시 입력노드 수가 많을 경우 신경망을 구성하는데 다소 오랜 시간이 걸릴 수 있으나 본 방안의 경우 사용자별 입력 노드 수가 10여개에 불과하므로 적은 연산으로도 학습이 가능하여 학습에 소요되는 시간은 실 업무에 적용하더라도 수용 가능한 수준이 될 것으로 생각된다.

실제 모니터링 과정에서 기존 학습된 입력패턴 정보를 재학습해야 하는 경우가 발생할 수 있는데 그 첫 번째 사유는 모바일뱅킹 고객이 사용하던 디바이스를 다른 기종으로 변경했을 때이다. 모바일 디바이스의 경우 제조사나 사용하는 하드웨어 및 OS에 따라 입력에 대한 반응도가 다를 수 있고, 터치스크린의 크기가 달라질 경우 터치스크린의 좌표값 설정치가 달라져 동일한 입력에 대해서도 수집되는 입력패턴 정보가 기존의 입력패턴과 상이하게 된다. 재학습이 필요한 두 번째 사유는 실제 고객의 입력패턴이 변화된 경우이다. 예를 들어 모바일뱅킹 시 하나의 손가락만 사용하던 고객이 불편함을 느껴 두개의 손가락을 사용하게 되면 입력패턴 정보가 달라져 탐지단계에서 의심스러운 거래로 인지될 수 있다. 이러한 상황이 일정 횟수이상 지속될 경우 고객의 입력패턴이 변화된 것이므로 변화된 시점부터 재학습이 필요하다.



〔그림 4〕 사용자 입력패턴 정보 학습 신경망(BPN) 구조

4.3 불법 전자금융거래 탐지 및 대응방안

사용자별 입력패턴에 대한 학습이 완료되면 이후 모바일뱅킹 거래시 수집되는 입력패턴 정보를 학습된 BPN에 입력하고 출력값이 해당 사용자와 동일한지 여부를 비교하여 실 고객에 의한 정상거래 여부를 탐지할 수 있다. 하지만, 모바일뱅킹 시 예외적으로 입력패턴에 잡음이 포함될 경우 고객의 정상적인 거래임에도 의심스러운 거래로 탐지될 수 있다. 비록 극히 낮은 확률이라 할지라도 금융 거래상에서 발생하는 오탐(false-positive)로 인해 즉시 거래를 차단을 할 경우 예상치 못한 금융거래 실패로 인한 고객의 항의가 발생할 수 있다. 따라서 탐지 즉시 거래를 차단하기 보다는 사전에 이상 증후가 발생될 경우 차단을 할 것인지, 제 3의 연락처로 연락을 취하여 고지할 것인지, 추가적인 인증을 통해 공격자에 의한 불법 전자금융거래 여부를 확인하도록 할 것인지를 사용자가 선택할 수 있도록 제공해주는 것이 필요하다. 하지만 본인이 직접 지정하여 차단을 하도록 했다고 하더라도 예기치 못한 오탐으로 인해 불만은 여전히 제기될 수 있으며, 제 3의 연락처로 고지하는 것은 사후대응이 될 수 있어 전자금융사고를 선제적으로 예방하는 효과는 없게 되므로, 본 논문에서는 이상증후가 발생한 경우 추가적인 인증을 통해 공격자를 차단하는 것을 권고한다.

추가적인 인증을 통한 공격 차단 방식은 이미 접근매체 정보가 공격자에게 모두 유출되었다는 점을 감안하여 보안성 확보 차원에서 기존과 통신경로가 다른 인증채널을 적용하는 것이 바람직한데, 이러한 인증방식을 투채널(two-channel)인증 또는 투팩터(two-factor)인증이라고 한다[15]. 모바일뱅킹 고객의 경우 거의 대부분 스마트폰을 보유하고 있다고 가정할 수 있으므로 불법 전자금융거래 대응을 위한 추가적인 인증방식으로 전화망을 통한 투채널인증(이하 "폰기반 인증"이라 함)의 적용이 가능하다. 폰기반 인증에 대한 이전의 연구들을 살펴보면 SMS나 전화연결(ARS) 방식을 이용하였는데, MinWu, et al은

SMS에 인증을 위한 별도의 모바일 웹사이트접속링크를 첨부하는 방식으로 인증하였고[16], Fadi Aloul, et al은 SMS에 OTP를 포함하여 전송하는 방안을 제안하였다[17]. 전화연결을 사용한 방식으로는 개인의 목소리 패턴정보를 수집하여 이를 고객을 인증하는데 활용하는 연구도 있었다[18].

SMS를 통한 폰기반 인증의 경우 최근 여러 취약점들이 보고되고 있는데, Collin Mulliner는 SMS의 구조 분석을 통해 iOS, Android등 대부분의 모바일OS가 SMS 대상 공격(Sniffing, Injection attack, 중간자공격)에 취약성이 있음을 공개하였고[19], 전자금융거래의 SMS 인증 코드를 탈취하는 악성코드가 발견되기도 하였다[20]. 따라서 모바일뱅킹시 폰기반 인증 방식은 SMS 보다는 전화연결 방식을 적용하는 것이 보안성을 고려할 때 바람직하다. 전화연결 방식의 폰기반 인증은 의심스러운 거래에 한해 금융기관에서 고객이 사전에 지정한 전화번호로 전화를 걸어 전자금융거래 여부를 확인 후 고객이 승인하면 결제가 진행되는 방식으로 공격자가 물리적으로 모바일 디바이스를 훔쳐가거나 복제하지 않을 경우 우회가 어려우므로 불법 전자금융거래를 효과적으로 확인하여 차단할 수 있다.

V. 실험 및 평가

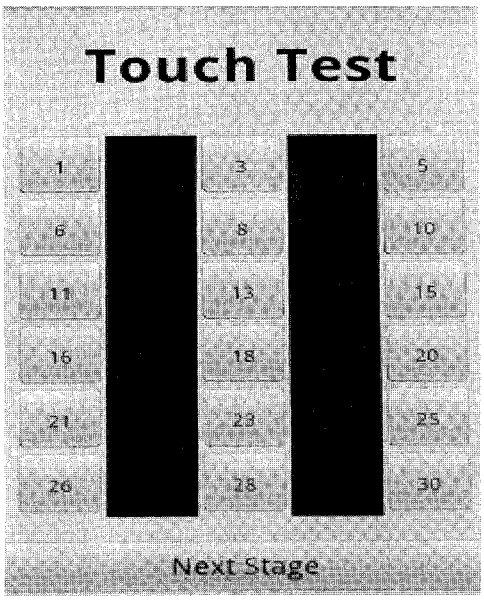
본 장에서는 실험을 통해 입력패턴 모니터링 방안의 성능 및 효용성에 대해서 평가한 결과를 기술하였다. 성능측정을 위해 모바일 디바이스에서 각 개인의 입력패턴 정보를 실제 수집하여 학습하였고, 해당 정보를 통해 각 개인을 얼마나 정확하게 클러스터링 할 수 있는지를 측정하였다. 또한, 최적의 학습조건을 찾기 위해 학습의 반복횟수(iteration)와 시간을 측정하여, 학습에 필요한 비용이 적절한지를 확인하였다.

5.1 실험 환경 및 구성

본 실험에서는 안드로이드 기반 스마트폰인 모토로이(motoroi)를 사용하였다. 모토로이는 안드로이드 2.1버전의 OS가 탑재되어 있으며, 854×480의 해상도를 가진 3.7인치 터치스크린을 사용한다. 입력패턴 정보 수집을 위해서는 별도의 앱을 개발하여 모토로이에 설치하였는데, Android API의 View.MotionEvent클래스에서 제공하는 입력패턴 정보 수집관련 함수 등을 활용하였다. 앱에서는 터치 입력패턴 수집을 위해 버튼 위젯을 사용하였으며, 버튼의 위치별로 입력패턴이 다를 수 있으므로 [그림 5]와 같이 총 18개의 버튼을 화면의 상하좌우에 균일하게 배치하였다. 터치 입력 후 스크롤 입력을 수행하도록 앱을 구성하였고, 학습을 위해 터치와 스크롤 입력은 1인당 각각 10회씩을 반복하였다.

실험은 총 50명을 대상으로 실시하였으며, 실험대상자의 연령과 직업은 모바일 디바이스 사용에 익숙한 20대 대학생을 위주로 하였다. 50명이라는 실험대상의 크기는 1인당 10회씩 입력을 수행함을 고려할 때 총 500개의 입력패턴 데이터가 학습 및 탐지에 활용되므로 제안한 방안을 실험하는데 적정한 수준으로 판단된다. 또한, 실험 대상자가 입력패턴 정보를 수집한다는 실험 목적을 알게 될 경우 이를 의식하여 입력시 영향을 받을 수가 있으므로 실험 목적을 실험 대상자에게 공개하지 않았다.

수집된 입력패턴 정보에 대한 학습 알고리즘은 BPN을 적용하였으며, 실험을 위해 Alyuda社의 신경망 시뮬레이션(simulation) 소프트웨어인 "Neuro Intelligence"를 활용하였다[21]. BPN은 1계층의 은닉노드를 사용하는 방식으로 입력노드 수와 은닉노드 수를 변화시켜가며 실험하였으며, 신경망의 활성(activation) 함수로는 시그모이드(sigmoid)를 초기 가중치(initial weight)는 ±0.3 범위 내에서 랜덤(Random)값을 선택토록 하였다. 학습 중지 조



[그림 5] 터치입력 실험을 위한 앱의 버튼 배치 화면

〔표 3〕 입력패턴 정보를 통한 클러스터링 실험 결과

구 분	입력노드 수	12				10			8
	은닉노드 수	12	10	8	6	10	8	6	8
실험결과	클러스터링 성공률(%)	97	97.6	95.8	90.2	96.2	91.6	88.4	88.6
	반복횟수(Iteration)	4705	5198	7141	10000	5714	7228	10000	7653
	학습시간(Time)	5:46	4:32	5:38	4:52	3:45	4:03	4:28	3:55

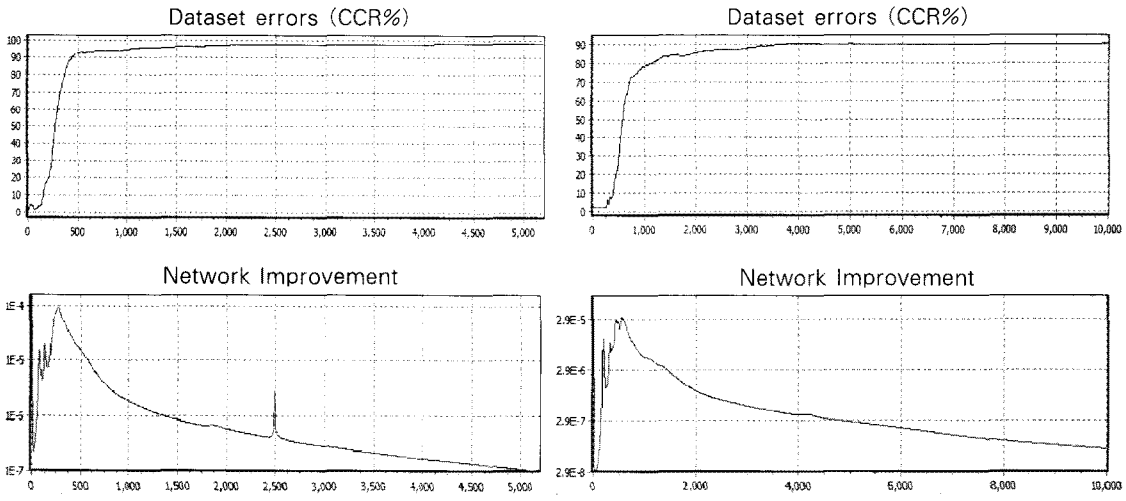
건은 반복횟수가 10000이거나 Network MSE (Mean Square Error)가 10^{-7}에 도달할 경우로 설정하였다. 또한, 학습은 1.3GHz CPU와 3G 메모리를 가진 PC 환경에서 실시하였다.

입력 패턴 정보로는 총 12가지를 수집하였는데 터치의 경우 18개 버튼의 평균값을 적용하여 시간(T_time), 압력(T_pressure), 손가락이 닿는 면적(T_width)의 3가지 정보를, 스크롤의 경우 시간(S_time), 압력(S_pressure), 손가락이 닿는 면적(S_width), 시작좌표(S_startpos), 종료좌표(S_endpos), 속도(S_speed), 길이(S_length)의 9가지 정보를 수집하였다.

5.2 실험 결과

실험은 50명의 500개 입력패턴 데이터에 대해 일괄적으로 학습한 후, 해당 데이터를 학습된 신경망에 대입하여 각 개인을 얼마나 정확하게 클러스터링 하는지를 확인하였다. 〔표 3〕은 50명의 입력패턴 정보에 대한 클러스터링 실험 결과 이다. 입력노드 수와 은닉노드 수에 따라 클러스터링 성공률에 차이를 보였는데, 입력노드 수 12, 은닉노드 수 10에서 97.6%의 가장 높은 성공률을 보였다. 실험에 활용한 입력 데이터는 지문과 같이 직접적이면서 유일한 생체정보를 활용하는 것이 아니기 때문에, 오진을 줄이기 위해서는 각 입력 데이터 분포의 편차가 적정하다면 최대한 활용하는 것이 바람직하다고 할 수 있다. 실제 실험 결과에서도 입력노드수와 은닉노드수가 많을수록 클러스터링 성공률과 정확도가 높았으며, 입력노드 수가 8개 이하일 경우에는 클러스터링 실패율이 10%를 초과하였다. 학습 반복횟수와 시간의 경우도 입력노드 수와 은닉노드 수에 영향을 많이 받는 것을 볼 수 있는데 실험결과 은닉노드 수가 10일 때 전반적으로 학습 효율이 가장 좋았다.

〔그림 6〕은 입력노드수 12에서 은닉노드수가 10인 경우와 6인 경우의 학습 그래프를 비교한 것이다. 상위 그래프는 Dataset의 에러를 측정한 것으로 학습된 신경망에 데이터 대입시 클러스터링 성공률의 변화



〔은닉노드 수 10〕 〔은닉노드 수 6〕

〔그림 6〕 입력노드수 12에서 은닉노드수에 따른 학습 그래프 비교

를 나타내며, 하위 그래프는 신경망 구성 과정에서 출력값과 목표치간의 오차가 개선되는 것을 표현한 그래프이다. 두 그래프 모두 학습 반복횟수가 늘어날수록 신경망의 적합도가 증가하는 구조이나 은닉노드수가 6인 경우 10일 경우에 비해 상대적으로 학습 에러 비율이 높음을 알 수 있다. 또한, 은닉노드수 6에서 학습 반복횟수를 10000에서 50000까지 증가시켜 가며 실험해 보았으나 클러스터링 성공률이 크게 개선되지는 않았다.

입력노드 수를 줄여나가는 기준으로는 편차율을 사용하였다. 편차율은 입력패턴 정보별 평균값과 각 데이터 사이의 거리를 분산에 대입하여 계산한 것으로 편차율이 높은 입력패턴 정보 일수록 다른 정보에 비해 입력 시 잡음이 많이 포함되거나 패턴이 균일하지 않은 정보로 볼 수 있다. 따라서 본 실험에서는 편차율 순위에 따라 해당 입력패턴 정보를 입력 노드에서 제외하는 방식을 적용하였다.

〔표 4〕는 50명의 입력패턴 정보별 평균 편차율을 계산한 것으로 전반적으로 편차율의 차이가 크지는 않았지만 터치시 손가락이 닿는 면적(T-width) 정보의 편차율이 가장 낮았으며, 스크롤시 손가락이 닿는 면적(S-width), 스크롤 종료위치의 x좌표(S-endpos_x), 스크롤 압력(S_pressure), 터치 압력(T_pressure)순으로 편차율이 높은 정보였다. 다만, 동 표의 수치는 50명 전체의 편차율을 평균한 값으로 개인별 편차율 순위는 이와 다를 수 있다.

이러한 실험결과를 종합해 볼 때 입력패턴 정보를 통해 95% 내외의 확률로 개인을 클러스터링 할 수 있

〔표 4〕 입력패턴 정보별 평균 편차율 비교

구 분	평균 편차율	편차율 순위
T_time	0.76139	7
T_pressure	0.77436	4
T_width	0.69039	12
S_time	0.75683	9
S_pressure	0.77808	3
S_width	0.78356	1
S_speed	0.76437	6
S_length	0.74074	11
S_startpos(x)	0.74611	10
S_startpos(y)	0.76094	8
S_endpos(x)	0.78256	2
S_endpos(y)	0.76531	5

〔표 5〕 입력 회차별 평균 편차율 비교

구 분	평균 편차율
1회차	1.18057
2회차	0.82278
3회차	0.83015
4회차	0.69981
5회차	0.62204
6회차	0.61444
7회차	0.65358
8회차	0.66334
9회차	0.69633
10회차	0.80422

으므로 이를 모바일뱅킹에 적용할 경우 정상적인 고객과 공격자를 입력패턴의 차이를 통해 탐지할 수 있을 것으로 생각된다. 95%라는 클러스터링 성공률은 지문이나 정맥, 얼굴모양, 손모양 등 여타 생체정보의 개인 인식율이 91~98.5% 내외인 것을 감안하면 본 방법론에 의한 학습결과가 매우 높은 정확도를 보여준다고 할 수 있다[22].

실험결과를 분석하면서 개인별 총 10회의 입력패턴 데이터 중 1회차 데이터의 평균 편차율이 타 회차에 비해 상대적으로 높음을 추가적으로 확인할 수 있었다. 〔표 5〕는 실험대상인 50명의 각 입력 회차별 데이터를 기반으로 편차율의 평균을 계산한 것으로 표에서 보는 바와 같이 1회차의 평균 편차율이 1.18로 타 회차의 평균 편차율에 비해 1.5 ~ 2배 가까이 큰 것을 볼 수 있다. 이는 1회차의 경우 실험 대상자가 실험용 앱에 대한 적응도가 낮아 잡음이 많이 포함된 것이 원인으로 1회차 입력패턴 정보를 제거한 후 실험한 결과 〔표 6〕과 같이 클러스터링 성공률이 최대 98.9%로 높아졌고 50명에 대한 전체 학습시간도 1분 이상 단축되었다. 따라서 실 모바일뱅킹 환경에서 고객의 초기 입력패턴 정보 데이터를 제외하고 뱅킹 앱에 어느 정도 적응된 후의 데이터로 학습할 경우 학습의 성능과 효용성이 보다 높아질 것으로 기대된다. 아울러 실험결과에서도 확인되었듯이, 50명에 대한 입력패턴 정보의 일괄 학습에 소요되는 시간이 PC에서 평균적으로 3분 이하로 소요되므로 개인당 학습시간은 매우 짧을 것으로 판단되며, 따라서 실제 업무환경에 적용 시 에도 시스템에 큰 부하량 없이 운영이 가능하다고 할 수 있다.

〔표 6〕 1회차 입력패턴 데이터 포함시와 제외시의 클러스터링 성공률 및 학습시간 비교

구 분		1회차 입력패턴 데이터 포함		1회차 입력패턴 데이터 제외	
입력노드 수	은닉노드 수	클러스터링 성공률 (%)	학습 시간	클러스터링 성공률(%)	학습 시간
12	12	97	5:46	98.9	2:04
	10	97.6	4:32	98	2:38
	8	95.8	5:38	98.2	4:02
10	10	96.2	3:45	98	2:37
	8	91.6	4:03	95.1	2:40
	6	88.4	4:28	91.8	3:21

VI. 결 론

본 논문에서는 모바일 디바이스에서의 전자금융사고 예방을 위한 개인별 입력패턴 모니터링 방안을 제안하였고, 실 모바일 디바이스 환경에서의 실험을 통해 동 방안의 성능과 효용성을 검증하였다. 제안한 방안은 모바일뱅킹 고객의 접근매체 정보가 모두 유출되더라도 공격자에 의한 불법 전자금융거래를 탐지·차단할 수 있고, 멀티 팩터(multi-factor)인증을 위해 지문이나 홍채정보와 같이 민감한 생체정보를 요구하는 경우 정보의 수집과 보존, 안전한 관리에 어려움이 크고 과다한 정보 보유로 인한 금융기관의 부담도 발생될 수 있으나, 본 논문에서 제시한 방법은 사용자의 생체적 특성, 습관으로 인해 유발되는 부가정보를 이용한 것이므로 공격자에 의해 위조하기 어려운 정보임과 동시에 해당 정보가 사생활을 침해하는 개인정보에 해당되지 않는다는 점에서 그 장점이 크다고 하겠다.

또한, 과거 모바일뱅킹의 오랜 숙제 중 하나였던 것으로 모바일뱅킹 시 인증에 쓰이는 정보들이 저장되어 있는 단말기가 도난당하거나 분실당한 상황에서도 본인인지 유무를 원격에서 능동적으로 감지할 수 있어 그 활용도가 높을 것으로 기대되며, 입력패턴 정보가 모바일뱅킹 과정에서 자연스럽게 수집되므로 동 방안 적용을 위해 고객에게 추가적인 작업이나 절차를 요구하지 않음은 물론 적은 비용으로 구현이 가능하다는 점과 학습에 소요되는 시간도 적다는 것도 장점이 되겠다.

향후 새로운 모바일 디바이스가 모바일뱅킹에 이용되거나, 뱅킹 전용 앱이 아닌 태블릿PC에서 모바일 웹페이지를 통한 전자금융거래가 이용될 때에도 새로운 학습과정 없이 적용될 수 있도록, 이용 환경 및 디바이스 하드웨어 환경과 독립적으로 사용자의 입력과 이용 패턴을 탐지할 수 있는 알고리즘 개발이 필요할 것으로 생각된다.

참고문헌

〔1〕 한국은행, "2010년 3/4분기 국내 인터넷뱅킹서비스 이용 현황," 2010년 10월.

〔2〕 "Mobile Security Report 2009", McAfee, 2009. http://www.mcafee.com/us/resources/reports/

〔3〕 "Zeus Strikes Mobile Banking," BankInfo Security, Oct. 2010. http://www.bankinfosecurity.com/articles.php?art_id=3005

〔4〕 A. Castiglione, R.D. Prisco, and A. De Santis, "Do Your Trust Your Phone?," EC-Web 2009, LNCS 5692, pp. 50-61, 2009.

〔5〕 A.D. Schmidt, F. Peters, F. Lamour, C. Scheel, S.A. Çamtepe, and S. Albayrak, "Monitoring Smart phones for Anomaly Detection," Mobile Network and Applications, vol. 14, no. 1, pp. 92-106, Nov. 2008.

〔6〕 금융감독원, "최근 5년간 전산보안사고 내역 및 처리현황," 2009년 9월.

〔7〕 김소이, "전자금융사고 발생유형 및 대응현황," 금융결제원, 지급결제와 정보기술, pp. 34-62, 2009년 10월.

〔8〕 P. Hanaeek, K. Malinka, and J. Schafer, "e-Banking Security - A Comparative Study," IEEE A&E SYSTEMS MAGAZINE, vol. 25, no. 1, pp. 29-34, Apr. 2010.

〔9〕 B.R. Cha, K.J. Kim, and H.S. Na, "Random Password Generation of OTP System using Changed Location and Angle of Fingerprint Features," IEEE 8th

International Conference on Computer and Information Technology 2008, pp. 420-425, Jul. 2008.

[10] J. Nie and X. Hu, "Mobile Banking Information Security and Protection Methods," Computer Science and Software Engineering International Conference, pp. 587-590, Dec. 2008.

[11] J. Mäntyjärvi, K. Nybergh, J. Himberg, and K. Hjelt, "Touch Detection System for Mobile Terminals," Mobile HCI 2004, LNCS 3160, pp. 331 - 336, 2004.

[12] L. Xie, X. Zhang, J.P. Seifert, and S. Zhu, "pBMDS: A Behavior-based Malware Detection System for Cellphone Devices," Third ACM Conference on Wireless Network Security, pp. 37-48, Sep. 2010.

[13] R. Hecht-Nielsen, "Theory of the Backpropagation Neural Network," International Joint Conference on Neural Network, pp. 593-605, Jun. 1989.

[14] J.I. Miinnix, "Fault Tolerance of the Backpropagation Neural Network Trained on Noisy Inputs," International Joint Conference on Neural Network, pp. 847-852, Jun. 1992.

[15] B. Schneier, "Two-Factor Authentication : Too Little, Too Late," AprilRisks, Communication of the ACM, vol. 48, no. 4, pp. 27, Apr. 2005.

[16] M Wu, S Garfinkel, and B Miller, "Secure Web Authentication with Mobile Phones," DIMACS Workshop on Usable Privacy and Security Software, pp. 9-10, Jul. 2004.

[17] F Aloul, S Zahidi, and W El-Hajj, "Two Factor Authentication Using Mobile Phones," IEEE/ACS International Conference on Computer Systems and Applications, pp. 641-644, May. 2009.

[18] P Ho and J Armington, "A Dual-Factor Authentication System Featuring Speaker Verification and Token Technology," AVBPA 2003, LNCS 2688, pp. 128-136, 2003.

[19] C Mulliner, "Fuzzing the Phone in your Phone," TU-Berlin/T-Labs. BlackHat USA, Jun. 2009, http://www.blackhat.com/presentations /bh-usa-09/MILLER/

[20] "ZeuS Variants Targeting Mobile Banking," F-Secure, Sep. 2010, http://www.f-secure.com /weblog/archives/0000-2037.html.

[21] Alyuda, "Alyuda Neuro Intelligence," http://www.alyuda.com/neural-networks-software.html

[22] N.L. Clarke and S.M. Furnell, "Advanced user authentication for mobile devices," Computers & Security, vol. 26, no. 2, pp. 109-119, Mar. 2007.

〈著者紹介〉

서 호 진 (Hojin Seo) 정회원
2002년 9월: 부산대학교 전자계산학과 학사
2002년 4월 ~ 현재: 금융결제원
2010년 3월 ~ 현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 e-financial 보안, 스마트폰 보안, 네트워크 보안

김 휘 강 (Huy Kang Kim) 종신회원
1998년 2월: KAIST 산업경영학과 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업및시스템공학과 박사
2004년 5월 ~ 2010년 2월: 엔씨소프트 정보보안실장, Technical Director
2010년 3월 ~ 현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 온라인게임 보안, 네트워크 보안, 네트워크 포렌직