정 보 보 호 학 회 지
제24권 제3호, 2014. 6

멀티모달 센서를 이용한 스마트기기 사용자 인증 기술 동향

최 종 원*, 이 정 현**

요 약

스마트 환경은, 사용자가 스마트기기를 통해 시간적, 공간적 제약을 받지 않고 스마트기기 서비스를 이용하는 것을 말하며 스마트기기의 보급으로 인하여 보편화되고 있다. 그런데 스마트 환경에서 서비스를 제공받기 위한 사용자와 스마트기기 간 인터페이스에서 각종 보안에 대한 위협이 발생한다. 또 스마트기기의 특성상 사용자 입력이 간편하지 않을 뿐만 아니라 일반 사용자가 계정 종류, 보안 유형 등 전문적인 용어에 대한 지식을 알아야하는 어려움이 존재한다. 최근 이러한 문제를 해결하고자 스마트기기의 터치스크린, 카메라, 가속도 센서, 지문인식 센서 등 다양한 센서를 혼합 사용하여 사용자 인증을 거치는 멀티모달 인터페이스 연구가 각광받고 있다. 따라서 본고에서는 인간과 스마트기기 사이 상호작용 시 안전하고 편리한 스마트 환경 조성을 위하여 멀티모달 센서를 활용한 다양한 스마트기기 사용자 인증 기술 동향에 대해 소개한다.

Ⅰ. 서 론

최근 급격한 속도로 증가한 스마트기기의 보급으로 인하여 국내 IT 기기 이용행태가 변화하고 있다. `12년 PC(Personal Computer) 하루 이용시간은 61분에서 `13년 55분으로 감소한 반면에 스마트기기 하루 평균 이용시간은 약 46분에서 66분으로 증가하였다.[1]

〔표 1〕 IT 기기 하루 이용시간 변화

	2012년	2013년
스마트기기	46분	66분
PC	61분	55분

이와 같은 스마트기기 이용의 증가는 PC에서 이용했던 많은 서비스들을 시간과 공간의 제약 없이 사용할 수 있어 앞으로도 계속하여 증가할 전망이다.

스마트기기 사용자가 늘어남에 따라 스마트기기를 이용한 다양한 서비스들이 제공되고 있다. 이를 이용하기 위해 필요한 개인정보들이 스마트기기에 저장되고 있으며, 이러한 정보가 노출되지 않도록 사용자 인증의 중요성 또한 증가하고 있다. 하지만 현재 일반적으로 많이 사용되는 4자리 PIN(Personal Identification Number)의 경우 뒤에서 누군가가 사용자의 인증과정을 지켜보는 어깨너머 공격(Shoulder-Surfing Attack)이나 카메라 등의 녹화 장치를 이용하여 사용자가 인증하는 과정을 촬영해 패스워드를 알아내는 레코딩 공격(Recording Attack)에 취약한 문제점을 드러낸다.

또한 대부분의 스마트기기 서비스들은 PC의 사용자 인터페이스를 그대로 적용하여, 사용자가 스마트기기의 작은 화면을 통해 서비스를 이용하는데 불편함을 느끼게 한다. 스마트기기의 작은 터치 인터페이스로 많은 정보의 입력을 요구하는 서비스는 사용자 측면에서 사용성을 떨어뜨린다. 특히 보안이 필수적인 금융 서비스 등은 여러 번의 인증을 사용자에게 요구하는 것이 불가피하여 이러한 단점이 두드러지게 드러난다. 또한 사용자 인증방식 설정에 있어 일반 사용자는 알기 어려운 전문 용어를 통해 선택해야만 사용가능한 서비스도 있다.

그러나 스마트기기의 센서 기술의 발전은 위와 같은 문제를 해결하기 위한 방향을 제시한다. 최근 출시

본 연구는 지식경제부 및 한국산업기술평가관리원의 산업원천기술개발사업(10039180)의 일환으로 수행되었습니다.
* 숭실대학교 컴퓨터학부 석사과정 (bluster100@gmail.com)
** 숭실대학교 컴퓨터학부 조교수 (jhyi@ssu.ac.kr)

되는 스마트기기는 터치스크린, 카메라, 가속도 센서, GPS 수신기뿐만 아니라 생체 정보 인식에 기반한 지문인식 센서, 얼굴 인식 센서 등을 스마트기기에 내장한다.[2] 이를 활용한 멀티모달 인터페이스는 사용자의 동작, 소리 등의 행위를 스마트기기에 전달하고 이를 인증 방식에 활용함으로 인간과 스마트기기 사이에 편리하고 각종 보안 위협으로부터 안정성이 높은 상호작용을 할 수 있게 도와준다.

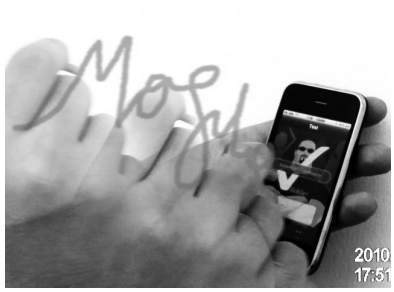
이를 토대로 본고에서는 최근 발표된 멀티모달 센서를 이용한 스마트기기 사용자 인증 기술 동향을 조사하여 인간과 스마트기기 사이에 상호작용이 보다 직관적이고 안전하게 이루어질 수 있는 방법을 소개하고자 한다.

Ⅱ. 관련 기술

인간과 컴퓨터의 상호작용의 관점에서 모달리티는 키보드, 마우스, 펜, 터치스크린과 같은 인간과 컴퓨터의 커뮤니케이션 채널을 의미한다. 사람과 사람 사이의 커뮤니케이션은 언어, 소리의 높낮이, 손짓, 얼굴 표정 등 수많은 상징체계를 사용하여 상호작용한다. 이처럼 사람사이의 상호작용은 사람의 시각, 청각, 촉각 중 하나의 모달리티가 아닌, 다중 감각을 통해 이루어진다. 멀티모달 인터페이스는 이와 같은 자연스러운 사람의 커뮤니케이션과 비슷한 방식을 인간과 컴퓨터의 상호작용에 적용하고자 하는 인간 중심적인 인터페이스이다.[3]

2.1. 지자기센서를 이용한 인증 기술

H. Ketabdar, et al. 은 지자기센서를 통해 사인을 인식하여 인증하는 MagiSign 기술을 제안 하였다.[4] 이 기술은 자석의 이동에 따른 자기장의 변화를 이용한 것으로, 자성이 있는 펜으로 모바일 기기의 허공에 사인을 하면, 지자기센서를 통해 자기장의 x, y, z 방향의 세기 변화를 확인하여 사인을 인식한다. [그림 1]은 MagiSign의 인증 예를 나타낸다.

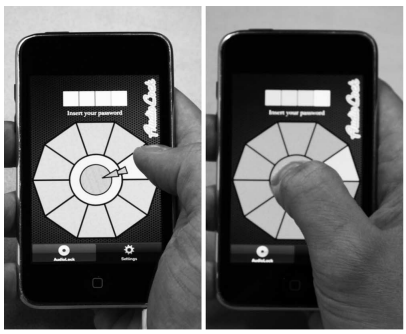


〔그림 1〕 MagiSign의 인증 예

이 기술은 자기장의 변화를 만들어내기 위해 자성이 있는 펜 또는 반지와 같은 별도의 토큰이 필요하다. 또한 복잡한 사인을 인식하기 위해서는, 기존의 스마트기기에 탑재되어 있는 지자기센서보다 정밀한 값을 얻을 수 있는 센서가 필요한 문제점이 있다.

2.2. 촉각과 음성을 이용한 인증 기술

A. Bianchi, et al. 은 촉각과 음성을 이용한 인증 기술인 The Phone Lock을 제안하였다.[5] 이 기술은 10개의 타겟 버튼에 각각의 특정 자극(음성 또는 진동)을 매칭 시켜 패스워드로 사용하고, 무작위로 발생되는 자극에 매칭 되는 버튼을 입력하는 것으로 사용자 인증을 한다. 각각의 자극은 10개의 똑같은 모양으로 구성된 타겟 버튼에 매칭 된다. 먼저 타겟 버튼을 누르면 자극이 발생되고, 자기가 원하는 타겟 버튼을 선택하여 중앙으로 드래그하는 것으로 자극과 타겟 버튼을 매칭 시킨다. [그림 2]는 자극과 타겟 버튼을 매칭 시키는 과정을 보여준다.



〔그림 2〕 자극과 타겟 버튼 매칭

Ⅲ. 멀티모달 기반 스마트폰 사용자 인증

앞서 설명한 것과 사람간의 상호작용은 다중 모달리티를 통해 이루어진다. 스마트 환경에서 멀티모달 인터페이스는 사람간의 상호작용의 다중 모달리티를 인간과 스마트기기의 상호작용에 적용하는 것이 목적이다. 즉, 인간과 스마트기기가 2개 이상의 모달리티를 이용하여 상호작용 할 수 있도록 하는 것이라고 할 수 있다. 이러한 멀티모달 기반을 통한 스마트폰 사용자 인증은 개발자나 서비스 제공업체에는 보안성 향상을 기대하게 하며 사용자에는 직관적인 인터페이스를 제공하여 사용성을 증가시킨다. 그리하여 다양한 멀티모달 인증 기술 개발이 현재 진행 중에 있으며 무궁무진한 발전 가능성이 존재하다고 생각된다.

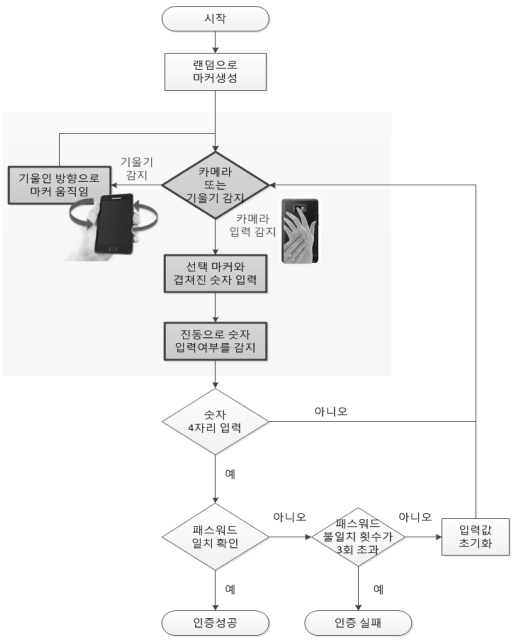
따라서 미래 인간과 스마트기기 간 상호작용의 방향에 대해 예측하고 현재의 기술동향을 진단하기 위해 최근 발표 된 멀티모달 기반 스마트폰 사용자 인증에 대해 살펴보고자 한다.

3.1. HiddenEnter[6]

어깨너머 훔쳐보기 공격, 스머지 공격, 터치로거 공격 등 PIN 방식에서 취약성을 보였던 공격에 대한 대응 기술이다. 스마트기기의 가속도 센서를 이용하여 숫자를 선택하고, 후방 카메라를 이용하여 패스워드를 입력한다. [그림 3]은 HiddenEnter의 실행화면을 보여준다.

〔그림 3〕 HiddenEnter 실행화면

패스워드 설정단계에서 사용자는 임의의 4자리 숫자 패스워드와 1가지 색상 패스워드를 선택한다. 인증 단계에서 사용자는 무작위로 생성되는 색상 마커를 확인하고, 그 중 자신이 선택한 색상인 마커를 스마트기기를 기울여 조작한다. 숫자 패스워드로 마커가 겹치면 후방 카메라를 손으로 가리는 것으로 입력한다. 예를 들어 패스워드 설정단계에서 사용자가 숫자 패스워드를 '1234'로 선택 후 색상 패스워드를 노란색으로 선택한다. 인증단계에서 랜덤하게 마커가 생성되면 스마트기기를 상, 하, 좌, 우 방향으로 기울이며 색상마커를 움직여 1이라는 숫자 위에 노란색 마커가 위치하도록 조작한다. 이때 후방 카메라를 손가락으로 가리면 스마트기기에 진동이 발생하며 첫 번째 패스워드 '1'이 입력이 된다. 이러한 과정을 4번 반복하여 '1234'를 차례로 입력한다.



〔그림 4〕 HiddenEnter를 통한 인증 방법

공격자는 사용자가 패스워드 설정 시 선택한 색상마커를 알지 못하며 화면에 직접적인 터치가 발생하지 않음으로 패스워드를 쉽게 파악하지 못할 것으로 예상된다.

HiddenEnter에서 멀티모달 적용 부분은 다음과 같다.

- 가속도 센서를 이용한 이동 : 스마트기기를 기울여 랜덤한 색상 마커 이동
- 카메라 센서를 이용한 입력 : 후면 카메라를 가리면 색상마커 아래 숫자가 입력
- 진동모터를 이용한 알림 : 숫자 입력 시 화면에 "*" 나타내는 대신 진동을 통해 촉각을 전달

3.2. 멀티모달 기반 이메일 사용자 인증기술[7]

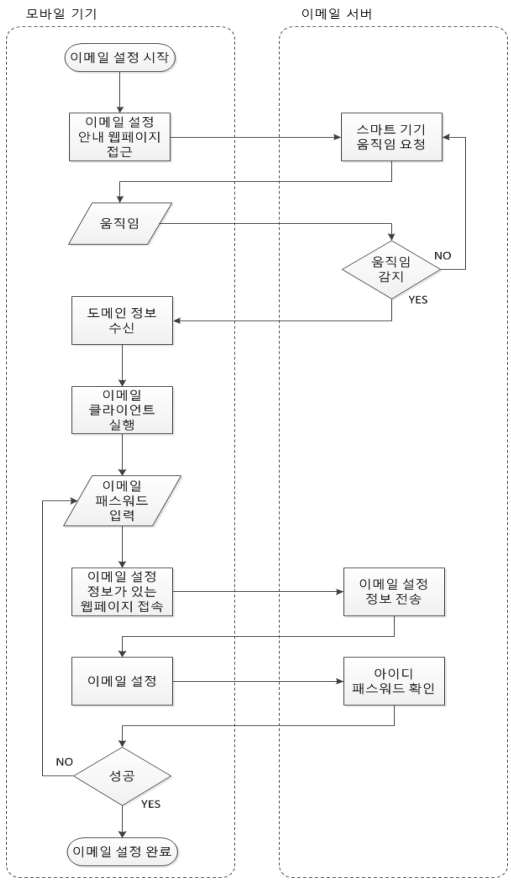
스마트워크(Smart Work) 시대에 가장 앞서 있는 애플리케이션은 이메일이다. 기업이나 연구소 등에서 업무에 관련한 내용을 이메일로 주고받는다. 그리하여 기업이나 연구소는 자체적인 이메일 서버를 만들어 운영하고 있다. 이러한 이메일 서비스는 스마트기기를 통해 외근이나 출장 시에도 시간적, 공간적 제약 없이 사용 가능하다.

그러나 스마트기기를 통한 이메일 설정은 일반 사용자에게는 다소 어렵게 느껴질 수도 있다. 주요 포털사이트 (Gmail, Naver, Daum 등)에서 제공하는 메일을 설정하기 위해서는 비교적 간단한 절차만 필요하지만 회사, 학교를 비롯하여 이메일 앱에 등록되어 있지 않은 이메일 서비스는 직접입력을 통해 설정해야 한다. 이때 이메일 계정과 패스워드만 입력해서 이메일을 설정할 수 없다.

〔그림 5〕 스마트기기 이메일 설정 예

[그림 5]와 같이 이메일 계정을 추가하기 위하여 계정 종류(POP3, IMAP), 보안 형식 및 서버 주소와 같은 복잡한 정보의 선택과 입력이 있어야 한다. 일반 사용자는 메일 계정이나 보안 유형과 같은 전문적인 용어에 대한 지식이 없어 설정 가이드를 찾아 자신의 환경에 맞는 설정을 해야만 한다. 또한, 스마트기기 기종 별로 다른 이메일 클라이언트를 제공하는데 이러한 경우 가이드에서 제공하는 이메일 클라이언트 버전과 사용자의 이메일 클라이언트 버전이 달라지는 경우가 발생한다. 이렇게 되면 사용자는 가이드의 내용과 다르기 때문에 사용자가 알아서 설정을 하거나, 별도의 설정방법을 찾아볼 불편함이 생긴다.

그리하여, 이메일 설정 간편화를 위해 멀티모달 기반 이메일 사용자 인증기술을 소개한다.



〔그림 6〕 멀티모달 기반 이메일 사용자 인증기술 동작방식

[그림 6]은 멀티모달 기반 이메일 사용자 인증기술 동작방식이다. 먼저 모바일 기기의 웹브라우저를 이용하여 이메일 서버에 있는 이메일 설정 안내 웹페이지에 접근한다. 이메일 설정 웹페이지에서는 모바일 기기에 특정한 움직임을 요청하고, 모바일 기기의 움직임을 HTML5 기능을 이용하여 서버에서 인식하게 된다. 움직임을 인식한 서버는 도메인 정보를 사용자 모바일 기기의 이메일 클라이언트로 전송하고 이메일 클라이언트가 실행되게 된다. 실행된 이메일 클라이언트에서는 사용자에게 아이디와 패스워드를 요청하고 사용자가 아이디와 패스워드를 입력하면 이메일 클라이언트에서 자동으로 이메일 설정 웹페이지에 접근하여 설정 정보를 가지고와 설정하게 된다. 마지막으로 이메일 서버에 아이디와 패스워드를 전달하여 인증에 성공하면 이메일 설정이 완료되게 된다.

실제 사용자는 [그림 7]과 같이 몇 가지 일만 수행하면 이메일 설정이 완료되는 것이다. 먼저 스마트기기를 통해 이메일 설정안내 웹페이지에 접속하고 간단한 동작을 취한다. 뒤이어 이메일 클라이언트가 실행되면 아이디와 패스워드를 입력한다. 마지막으로 계정 이름을 설정하면 모든 이메일 설정이 완료된다.

기존 스마트기기 이메일 설정 시 사용자가 가이드를 다운받아 선택 및 입력해야만 했던 복잡한 계정 종류, 보안 형식 등의 설정정보를 별다른 수고 없이 간단한 동작과 아이디 패스워드 입력만으로 완료할 수 있다. 가속도 센서를 이용하여 동작인식을 추가한 멀티모달 방식을 통하여 간편하게 이메일 설정이 완료되는 것이다.

3.3. 멀티모달 기반 스마트뱅킹 사용자 인증[6,8]

스마트기기에서 사용되는 다양한 서비스 중 금융결제 서비스는 보안이 가장 중요시 된다. 실제 직접적인 금전 피해를 입힐 가능성이 존재하기 때문이다. 따라서 복잡한 인증 절차가 불가피하다.

스마트뱅킹에서 가장 많이 이용되는 서비스는 조회서비스와 이체 서비스이다. 조회서비스는 스마트뱅킹 이용건수 중에서 89.8%를 차지하고 , 계좌이체 서비스는 나머지 10.2%를 차지한다. 그러나 조회서비스는 아이디/패스워드 입력 또는 공인인증서 비밀번호 입력만을 요구하는 비교적 간단한 절차로 이루어진다. 사용자가 조회서비스를 사용하기 위해서는 로그인만 진행하면 조회가 가능하기 때문에 크게 불편함을 호소하지 않는다. 문제는 계좌이체 서비스인데 이는 복잡한 절차를 통해 이루어진다.

스마트뱅킹을 통한 이체 서비스는 언제 어디서든지 시간적, 공간적 제약 없이 수행할 수 있다. 그러나 이를 위해서는 보안카드를 항상 소지하고 있어야 하는 불편함이 따른다. 스마트기기를 통해 서비스를 제공받으려 해도 보안카드를 따로 챙기지 않아 은행 업무를 할 수 없는 경우가 빈번히 발생한다. 이에 대한 해결책으로 최근에 보안카드를 스마트기기상에서 관리할 수 있는 보안카드 관리 앱이 생겼다. 그러나 이를 통한 이체 서비스 시에도 복잡한 단계를 거쳐 수행된다. 보안카드 관리 앱을 사용하는 경우, [그림 8]과 같이 복잡한 인증 및 입력 단계가 추가된다.

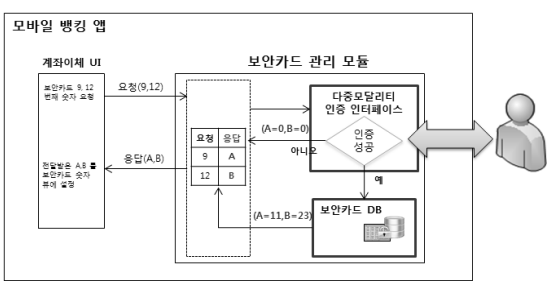
앱이 사용자에게 보안카드 번호 입력을 요청을 하면 사용자는 보안카드 관리 앱을 실행하고 해당 앱에서 요

〔그림 7〕 간단한 동작 인식을 통한 이메일 사용자 인증

〔그림 8〕 스마트뱅킹 계좌이체 시 기존의 복잡한 사용자 인증 과정

청하는 패스워드를 입력한다. 스마트기기에 저장된 보안카드를 선택하고 난후 뱅킹 앱에서 요구하는 보안카드의 번호를 검색 및 확인한다. 그 후 다시 뱅킹 앱으로 돌아와 보안카드 번호를 입력해야 한다. 계좌이체 시의 위와 같은 절차는 사용자를 불편하게 한다.

따라서 스마트뱅킹 사용자가 계좌이체 시 느끼는 불편함을 해소할 수 있는 멀티모달 기반 스마트뱅킹 사용자 인증 기술을 소개한다.



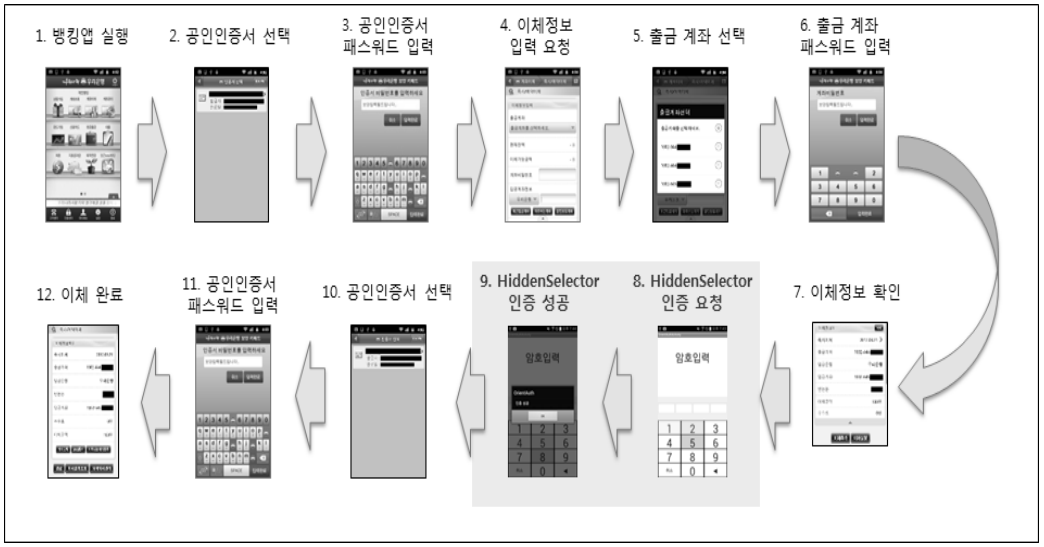
〔그림 9〕 입력 간편화를 위한 보안 프로토콜

스마트뱅킹 계좌이체서비스 이용 시, 여러 번의 사용자 인증은 보안상의 이유로 축소가 어렵다. 따라서 계좌이체 과정의 복잡도를 증가시키며, 보안카드를 안전하게 관리하는지 신뢰 할 수 없는 보안카드 관리앱을 대체할 수 있는 보안 프로토콜이 필요하며 [그림 9]와 같다.

스마트뱅킹 앱의 보안카드 관리 모듈에서 보안카드를 암호화하여 안전하게 관리 및 저장하며, 계좌이체 시 보안카드 요청을 하면 멀티모달 인터페이스 기반의 사용자 인증을 통해 암호화된 보안카드의 필요한 숫자를 복호화 하여 가져온다. 설계한 보안 프로토콜을 적용하면, 보안카드 관리 앱을 사용하는 경우와 비교해 이체 과정이 훨씬 간단해진다. [그림10]은 멀티모달 기반 스마트뱅킹 계좌이체 시 과정을 보여준다.

보안카드 앱 사용 시에는 보안카드 입력을 위해 복잡한 인증 및 입력이 필요했으나, 보안카드 관리 모듈의 멀티모달 인증 인터페이스를 통해 한 번의 인증으로 보안카드 입력을 대신하게 된다.

이와 같은 프로토콜을 통해 스마트뱅킹 앱을 통한 계좌이체 시 간단한 절차로 계좌이체를 수행할 수 있다. 해당 모듈을 사용하더라도 앱 내부적으로는 보안카드 앱 사용 시와 동일한 절차를 통해 동작하기 때문에 사용자의 입장에서는 인증 절차가 간소화되면서도 보안성 또한 기존 스마트뱅킹 계좌이체 시 인증 과정과 비교하여 떨어지지 않는다.



〔그림 10〕 개선된 보안 프로토콜 모델 적용 시 스마트뱅킹 이체 과정

Ⅳ. 결 론

우리는 현재 스마트시대에 살고 있다. 스마트폰, 태블릿 PC로 대표되는 스마트기기의 확산과 관련 기술의 발달로 사람들의 생활과 업무환경을 비롯하여 사회 모든 분야에 대혁신이 일어나고 있다. 원격으로 가사활동, 학습, 진료가 가능해지고 SNS등을 통한 광범위한 정보 공유와 새로운 사회적 관계가 형성되고 있다. 특히 최근에는 종래의 사무실 개념을 탈피하여, 언제 어디서나 편리하고 효율적으로 업무에 종사할 수 있도록 하는 스마트워크(Smart Work)가 정착되어감에 따라 업무환경 개선 및 업무효율의 극대화가 이루어지고 있다.

그러나 스마트기기는 작은 크기로 인해 휴대성과 이동성, 개방성이라는 강점을 가지고 있지만 PC환경에서 사용하던 기기와 사용자간의 인터페이스로 업무를 처리를 하는 것에는 한계가 존재한다. 또한 중요한 개인정보를 담고 있는 스마트기기는 개인 정보 노출, 사기범죄, 피싱, 스미싱 등의 각종 범죄에 표적이 되고 있는 상황이다.

이와 같은 문제 해결을 하기위한 핵심기술이 인간과 스마트기기의 상호작용 사이에 편리하고 안전한 환경을 제공하는 멀티모달 기반 인증 기술이다. 이는 인간이 스마트기기에 텍스트 형태로 명령을 내리는 것뿐만 아니라 음성, 제스처인식, 생체인식, 심지어 감성인식까지도 수행하여 마치 인간과 기기가 서로 교감을 하듯 서로 신뢰할 수 있게 만들 수 있는 기술인 것이다.

따라서 본고에서는 멀티모달 센서를 이용해 스마트기기의 사용자 인증 시 보안성, 사용 편리성 향상을 기대할 수 있는 기술을 소개하였다. 이를 통해 앞으로도 무궁무진하게 발전 가능한 인간과 스마트기기 상의 상호작용 연구에 밑거름이 될 것이라고 기대한다.

참 고 문 헌

[1] 김민철, “스마트폰 보유 및 이용행태 변화:2012년과 2013년의 비교”, 한국미디어패널조사, pp. 21-25, 2013.

[2] E. Miluzzo, L. Hong, D. Peebles, T. Choudhury and A.. T. Campbell, “ A Survey of Mobile Phone Sensing,” Communications Magazine, IEEE, Vol.48, No.9, pp. 140-150, 2010.

[3] 임미정, 박점, “멀티모달 인터랙션을 위한 사용자 병렬 모달리티 입력방식 및 입력 동기화 방법 설계”, Journal of the Ergonomics Society of Korea, Vol. 25, No. 2 pp. 135-146, 2006.

[4] H. Ketabdar, K. A. Yuksel, A. Jahnbekarn, M. Roshandel and D. Skirop, “MagiSign: User Identifaction /Authetication Based on 3D Around Device Magnetic Signatures,” The Fourth International Conference on Mobile Ubiqutous

Computing, Systms, Services and Technologies, 2010.

[5] Andrea Bianchi, Ian Oakley, Vassilis Kostakos, and Dong Soo Kwon, “The Phone Lock: Audio and Haptic Shoulder-Surfing Resistant PIN Entry Methods for Mobile Devices,” TEI`11 Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction, pp. 197-200, 2011.

[6] Hyunyi Yi, Yuxue Piao, and Jeong Hyun Yi, “Touch Logger Resistant Mobile Authentication Scheme Using Multimodal Sensors,” Advances in Computer Science and its Applications Lecture Notes in Electrical Engineering, Volume 279, pp. 19-26, 2014.

[7] Tajin Kim, Yuxue Piao, Changho Seo, and Jeong Hyun Yi, “Automatic Email Configuration System Using Multimodal Authentication Interfaces for Smartphones,” Applied Mechanics and Materials, Vols. 411-414, pp. 7-11. 2013.

[8] Jin-Hyuk Jung, Ju Young Kim, Hyeong-Chan Lee, and Jeong Hyun Yi, “Repackaging Attack on Android Banking Applications and Its Countermeasures,” Wireless Personal Communications, Vols. 73, Issue 4, pp. 1421-1437. 2013.

[9] Tajin Kim, Siwan Kim, Hyunyi Yi, Gunil Ma and Jeong Hyun Yi, “Mobile User Authentication Scheme Based on Minesweeper Game,” Multimedia and Ubiquitous Engineering Lecture Notes in Electrical Engineering Volume 240, 2013, pp 227-133, 2013

[10] M. Lee, B. K. Ku, and J. B. Kim, “Easy Authentication Using Smart Phones and 2-D Barcodes,” IEEE International Conference on Consumer Electronics, 2011.

[11] Z. Obrenovic and D. Starcevic, “Modeling multimodal human-computer interaction,” IEEE Computer, 2004.

〈저자소개〉

최 종 원 (Jongwon Choi)
학생회원

2013년 2월 : 숭실대학교 컴퓨터학부 졸업
2013년 3월 ~ 현재 : 숭실대학교 컴퓨터학부 석사과정
관심분야 : HCI, 모바일 플랫폼 보안, 정보보호

이 정 현 (Jeong Hyun Yi)
종신회원

1989년 2월 : 숭실대학교 전자계산학과 학사
1995년 2월 : 숭실대학교 컴퓨터학과 석사
2005년 8월 : University of California at Irvine, Computer Science 박사
1995년 2월 ~ 2001년 8월 : 한국전자통신연구원(ETRI) 연구원
2000년 4월 ~ 2001년 3월 : 미국 표준기술연구소(NIST) 객원연구원(Guest Researcher)
2005년 10월 ~ 2008년 8월 : 삼성종합기술원 수석연구원, 과제책임자
2008년 9월 ~ 현재 : 숭실대학교 IT대학 컴퓨터학부 , 조교수
관심분야 : HCI, 모바일 보안, 정보보호