

안전한 스마트워크 환경을 위한 음성인식 기반 사용자 인증 모델에 관한 연구

위유경, 박대식, 곽진
순천향대학교 정보보호학과

e-mail : ykwi@sch.ac.kr, dspark@sch.ac.kr, jkwak@sch.ac.kr

A Study on User Authentication Model based on Voice Recognition for Secure Smartwork Environment

Yoo-Kyung Wi, Dae-Sik Park, Jin Kwak
Dept of Information Security Engineering, Soonchunhyang University

요 약

정보통신기술의 발달과 스마트 디바이스의 보급률 증가로 인해 과거 사무실 안으로 한정되어 있던 업무공간이 스마트 디바이스를 활용하여 시간과 공간의 제약 없어졌다. 따라서 효율적으로 업무를 지속할 수 있는 스마트워크 환경에 대한 관심과 연구가 증가하고 있다. 그러나 국내의 스마트워크 연구는 초기 단계에 머물러 있으며 스마트워크 환경을 구축하기 위한 사용자 인증 기법에 대한 연구도 부족한 실정이다. 따라서 본 논문에서는 스마트워크 환경에서 안전한 사용자 인증을 위한 음성인식 기반 사용자 인증 기법을 제안한다.

1. 서론

정보통신기술이 발달됨에 따라 다양한 기술을 활용한 새로운 방식의 업무 환경인 스마트워크가 주목받고 있다. 스마트워크는 시간과 장소의 제약을 받지 않고 업무를 수행할 수 있도록 도와주는 유연한 근무형태로 출·퇴근 시간 감소로 인해 시간을 효율적으로 활용할 수 있고, 탄소 배출량 감소, 기업의 예산절감 등의 효과를 제공하는 등의 장점이 있다.

최근 스마트워크는 세계적으로 많은 관심을 받고 있으며 다양한 나라에서 도입을 추진하고 있다. 국외에서는 이미 미국, 일본, 네덜란드 등이 국가적인 차원에서 스마트워크를 추진하고 있다. 국내에서는 정부에서 2010년에 스마트워크 센터 2곳을 설립하여 공무원을 대상으로 시범운영하고 있으며, 2015년까지 50곳으로 확대하는 것을 목표로 정부에서 적극적으로 추진하고 있다. 하지만 다양한 형태로 스마트워크 환경이 조성되고 수많은 IT 기술이 접목되어 있어 보안 통제가 완벽하게 이루어지지 못하기 때문에 보안 취약점이 존재한다. 보안 취약점이 노출 될 경우, 업무와 관련된 중요한 정보가 유출될 수 있기 때문에 많은 경제적 손실을 입을 수 있어 스마트워크 환경에서 존재할 수 있는 보안 취약점 분석이 필요하다.

특히 스마트워크 환경에서의 모바일 서비스는 지문,

홍채 등의 생체정보를 활용하기 어려워 사용자의 음성정보와 스마트폰 USIM을 활용하여 사용자 인증 과정을 제안하고자 한다.

따라서 본 논문에서는 스마트워크 환경에 접근하는 사용자에게 대하여 음성인식 기반 사용자 인증 모델 기법을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 스마트워크, 음성인식 기술 및 스마트폰 USIM(Universal Subscriber Identity Module)의 개념을 정의하고, 3장에서는 스마트워크 환경에서 발생할 수 있는 보안 문제점을 분석한다. 4장에서는 음성인식 기반 사용자 인증 기법을 제안하고, 5장에서는 효율성에 대해 분석한다. 마지막으로 6장에서는 결론을 맺는다.

2. 관련연구

2.1 스마트워크

스마트워크는 기존에 사무실이라는 한정된 공간에서 업무를 수행하는 개념과는 다르게 시간과 장소의 제약 없이 언제 어디서나 업무를 수행할 수 있는 업무환경으로 스마트폰, 태블릿 PC 등의 모바일 기술, 광대역 통신, 클라우드 컴퓨팅 및 가상화 기술의 발달로 인해 등장하게 되었다[4].

스마트워크는 근무 장소 및 근무 방식에 따라 스마트워크 센터근무, 재택근무, 이동근무 등 3가지로 구분할 수 있다.

이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No.2011-0007755).

□ 스마트워크 센터근무

스마트워크 센터는 자택 인근에 사무실과 유사한 환경이 구축되어 있는 원격사무실에 출근을 하여 업무를 수행하는 근무유형이다.

스마트워크 센터는 근태관리가 용이하고 기업 본사에서 직접 관리하고, 보안 인프라가 구축되어 있어 일반 인터넷망을 사용하는 재택근무, 무선통신망을 사용하는 이동근무의 근무유형보다 보안성이 보장되어 있으며, 육아 놀이시설, 편의시설 등이 마련되어 있어 업무집중도 향상으로 인해 업무의 효율성이 향상될 수 있다[1].

□ 재택근무

자택에서 기업 내부의 네트워크에 접속하여 업무를 수행하는 유형으로 출·퇴근 시간을 소비하거나 교통비에 대한 부담을 감소시킬 수 있다. 또한 자택에 구축되어 있는 유·무선통신망을 사용하므로 업무를 수행할 수 있는 별도의 공간을 구축할 필요가 없다[1]. 또한 사무실에서 근무하기 불편한 장애인 또는 육아 휴직자, 노약자 등에게 유용한 업무 환경이다.

□ 이동근무

스마트폰, 태블릿 PC 등을 사용하여 무선통신망을 통해 기업 내부 네트워크에 접속하는 유형으로 대부분의 업무시간을 밖에서 보내는 영업 직종 및 컨설팅과 관련된 업무직종에 종사하는 인원들에 유용한 근무유형이다. 시간과 공간의 제약 없이 업무를 수행할 수 있기 때문에 신속하게 업무를 처리할 수 있다[1].

<표 1> 스마트워크 근무 유형

유형	근무형태
스마트워크 센터근무	자택 인근의 정보통신기술 환경이 갖춰진 원격 사무실에서 근무
재택근무	자택에서 기업 내 네트워크에 접속하여 근무
이동근무	모바일 오피스 환경을 이용한 현장에서 직접 근무 또는 이동 중에 현장에서 근무

2.2 음성인식 기술

음성인식은 전화, 마이크 등을 통하여 컴퓨터 또는 음성인식 시스템으로 전송된 음성으로부터 특징을 추출하고 분석하여 미리 입력된 음성데이터 목록에서 가장 근접한 결과를 찾아내는 기술이다.

음성인식 기술은 그 분류기준에 따라 여러가지 종류로 나누어진다. 사용자의 범위에 따라 화자종속 인식기술, 화자독립 인식기술로 분류되며, 인식대상 어휘수에 따라 소

어휘 인식기술, 대어휘인식기술 그리고 발성의 자연성에 따라 단어인식기술, 연속음성인식기술, 대화체인식기술 등으로 구분된다[2], [3].

□ 화자종속 음성인식 기술

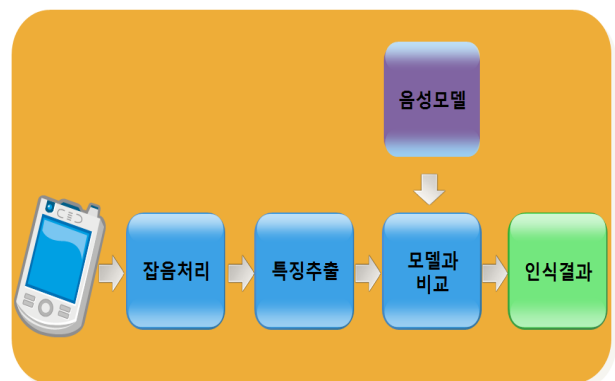
화자종속 음성인식은 화자독립 음성인식에 비해 인식이 높다. 미국의 스프린트에서 서비스하는 보이스 폰 카드는 30개까지의 이름을 저장하여 전화를 걸 때 사람 이름만 말하면 그 사람의 전화번호를 찾아 자동으로 전화를 걸어주는 기술로 화자종속 음성인식의 대표적인 예이다 [3].

□ 대어휘 음성인식 기술

대어휘 음성인식 기술은 수 만 단어 어휘까지 인식 가능하지만 인식률이 낮고 말할 때 사용자가 발음에 주의를 기울여야 하는 불편함이 있다. 80년대까지는 사용자가 정확하게 발음해야 하는 낭독체 음성인식 기술이 주로 개발됐다. 그러나 최근에는 사람과 대화하듯이 자연스럽게 말하는 대화체 음성인식 기술에 많은 연구를 집중하고 있다. 현재 2,000~3,000단어로 이루어진 대화체의 인식률은 약 70% 정도 된다[2], [3].

□ 연속음성인식 기술

연속음성인식 기술은 문장을 인식하기 때문에 사용자가 단어 단위로 끊어 발음하지 않아도 된다. 이 시스템은 종전까지 인식률이 95% 이하였고, 인식 어휘 수도도 제약이 많았다. 그러나 최근에 알고리즘의 개선, 인간공학기술 사용 등으로 1,000~3,000 어휘의 95% 이상의 인식률을 보이고 있다[3].



(그림 1) 음성인식 시스템의 기본 구성도

2.3 USIM

USIM은 SIM(Subscriber Identity Module) 카드와 UICC(Universal IC Card)가 결합된 용어로서 사용자 인증과 글로벌 로밍, 전자상거래 등 여러 기능을 손톱 크기의 카드에 담은 것이다. 가입자 인증을 하는 SIM카드와 교통카드 및 신용카드 등의 기능을 담을 수 있는 범용 IC카드

의 역할을 한다. USIM은 소형 CPU와 메모리로 구성되는데 CPU는 압·복호화 기능으로 사용자를 식별하고, 메모리는 부가서비스를 위한 저장 공간으로 사용된다. OTA(Over The Air) 기술을 이용해 은행 및 카드 서비스의 승인만 받으면 별도로 칩을 발급받지 않고도 서비스를 이용할 수 있다[4].

3. 보안 문제점 분석

스마트워크 환경은 기본적으로 유·무선 디바이스를 사용하여 기업 외부에서 기업 내부로 네트워크를 통해 접근하여 업무를 수행하기 때문에 사용자의 정당한 인증 과정이 필요하다.

스마트워크 환경에서는 디바이스가 다수의 기업에 접근하게 되며, 다루게 되는 정보 또한 기업의 기밀정보 등 높은 등급의 보안 수준을 요구하는 경우도 많다.

스마트워크 센터의 경우에는 일정한 보안 수준을 만족하기 위하여 보안 인프라가 구축되어 보다 안전한 수준의 접근이 가능하다. 그러나 이동근무나 재택근무와 같은 경우 보안에 대한 위험이 스마트워크 센터에 비해 상대적으로 높다. 또한 스마트워크 센터가 상대적으로 안전하다 하더라도 정당한 사용자에 대한 검증이 수행되지 않는다면 스마트워크 센터 내 시스템에 불법프로그램, 악성코드 등으로 인한 문제가 발생할 수 있다[3].

따라서 이와 같은 보안 문제를 해결하기 위해서 스마트워크 환경에서 안전한 사용자 인증 기법에 대한 연구가 필요하다.

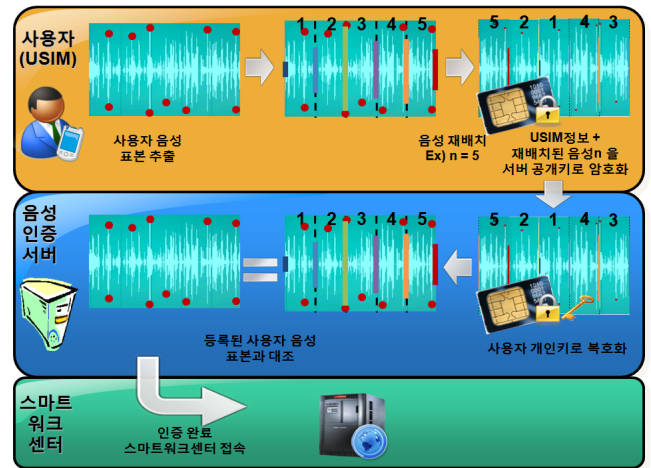
4. 음성인식 기반 사용자 인증 모델

본 논문에서는 안전한 스마트워크 모바일 서비스 환경을 구축하기 위하여 안전성이 향상된 사용자와 스마트워크 센터 간 음성인식 기반 사용자 인증 기법을 제안한다.

4.1 제안방식

사용자 음성을 이용하여 스마트워크센터 사내망에 안전하고 편리한 접속을 위해 스마트폰을 이용한 음성인식 기반 사용자 인증을 제안하고자 한다. 사용자의 음성 데이터를 사용하여 스마트폰과 스마트워크 센터간의 인증을 통해 보다 편리하고 안전한 인증 기법을 제공한다. 본 제안 방식은 음성 등록 단계, 인증 단계로 구분 된다.

(그림 2)는 본 논문에서 제안하는 음성인식 기반 사용자 인증 모바일 서비스 시스템의 개념도를 나타낸다.



(그림 2) 제안 방안 모델 개념도

4.2 음성 등록 단계

- ① 사용자는 본인의 음성으로 임의의 한 단어를 선택하여 음성인증서버에 전송한다.
- ② 등록된 사용자의 음성 데이터는 음향 파장 각각의 최고점과 최저점의 특징점을 찾아 추출하고 이를 표본화하여 등록한다.

4.3 인증 단계

- ① 사용자는 USIM이 장착된 스마트폰을 사용하여 음성인증서버에 접속하여 음성을 인증시킨다.
- ② 스마트폰은 사용자의 음성 재배치를 할 임의의 수 n 값을 넣어 음성을 분할시킨 뒤 재배치한다.
- ③ 사용자의 USIM으로 음성인증서버의 공개키를 이용하여 재배치된 음성 $n(V)$ 과 함께 암호화한 뒤 음성인증서버로 전송한다.
- ④ 음성인증서버는 분할되어 재배치된 음성의 절단면과 미리 등록된 사용자 음성표본의 특징점을 찾아 매핑을 한다.
- ⑤ 등록된 음성표본과 확인 대조 후 스마트워크센터로 접속을 승인을 요청하고, 인증을 수행한다.

5. 효율성 분석

본 논문에서 제안한 음성기반 사용자 인증 기법을 통해 인증을 수행할 경우에는 스마트워크 모바일 서비스 업무를 수행함에 있어 다음과 같은 이점을 가져올 수 있다.

<표 2> 효율성 분석

분류	기존 방안	제안 방안
정당한 사용자 인증	<ul style="list-style-type: none"> · ID / PW 방식 · 별도의 추가적인 사용자 인증 없음 	<ul style="list-style-type: none"> · 사용자 음성 인증 · 미등록된 사용자 음성 접근 불가
악의적인 사용자의 접근 방지	<ul style="list-style-type: none"> · 사용자의 정보만 있다면 접근 가능 	<ul style="list-style-type: none"> · 사용자의 기본 정보만으로는 접근 불가능 · 사용자의 음성정보와 일치해야 접근 가능
중요 정보 노출 방지	<ul style="list-style-type: none"> · 사용자 정보의 노출 가능 	<ul style="list-style-type: none"> · 사용자 음성정보를 사용하므로 정보 노출 예방

참고문헌

- [1] 고용, 광진, “스마트워크 환경에 접근 가능한 안전한 디바이스 인증 기법 연구”, 제35회 한국정보처리학회 추계학술대회 논문집, 제 18권 1호, 2011
- [2] 강점자, 강병욱, 정호영, 정훈, 이윤근, “신성장동력산업용 대어휘 음성인식 기술 동향 및 응용”, 전자통신 동향분석, 제 23권 1호, 2008
- [3] 이윤근, 박준, 김상훈, “음성인터페이스 기술”, 전자통신 동향분석, 제 20권 5호, 2005
- [4] 정병근, “USIM 기반 무선 네트워크 연동 보안 인증 시스템에 관한 연구”, 한국정보과학회 가을 학술발표 논문집, 제 34권 2호, 2007
- [5] 이형찬, 이정현, 손기욱, “스마트워크 보안 위협과 대책”, 정보보호학회지, 제 21권 3호, 2011
- [6] 이재성, 김홍식, “스마트워크 현황과 활성화 방안 연구”, 한국지역정보학회지, 제 13권 4호, 2010
- [7] <http://www.smartwork.go.kr>

6. 결론

스마트워크는 스마트폰과 통신 인프라를 기반으로 하는 혁신적인 IT 서비스의 대표적인 기술이다. 기업은 생산성 향상과 편리성 증대를 위해 많은 비용과 노력을 투입하여 스마트워크를 환경을 구축하고 있다. 그러나 단말의 분실, 모바일 악성코드의 감염, 기업정보 및 기술의 무단 유출과 같은 보안 문제가 지적되고 있다. 이러한 보안 문제에 대한 개선 없이는 안전한 스마트워크 환경을 구축할 수 없다.

유·무선 디바이스를 이용하여 외부에서 기업 내부로 네트워크를 통해 접근을 수행하게 되는 스마트워크 환경에서는 사용자에 대한 정당한 인증 과정이 필수적으로 요구된다.

본 논문에서는 스마트워크 환경에 접근하는 다양한 사용자에게 대하여 사용자 본인의 음성데이터를 이용하여 보다 안전하고 정당한 인증을 수행하는 방안을 제안하였다.

이를 통해 스마트워크 환경을 구축하고 내부망에 접근하여 업무를 수행할 때 사용자 고유의 음성데이터를 이용하여 인증되지 않은 사용자에게 대한 원천적 차단이 가능하고 중요 정보 노출 차단이 가능할 것으로 기대할 수 있다. 이를 통해 스마트워크 환경 전반에 대한 보안성을 향상시킬 수 있을 것으로 기대된다.