스마트워크 환경에서 음성인식을 활용한 사용자 인증 기법에 관한 연구

위유경*, 곽 진*

요약

스마트워크는 사람들에게 좀 더 편리한 근무환경을 제공해주는 유연한 업무형태이다. 이미 국내·외 많은 국가에서는 편리한 근무환경 제공을 위해 스마트워크 도입을 추진하고 있다. 이렇게 스마트워크에 대한 관심이 높아지면서 보안 위협의 대응방안에 대한 중요도 또한 높아지게 되었다. 특히, 인증되지 않은 디바이스를 통해 서버로 불법 프로그램 및 악성코드가 전송되고 공격자가 기업의 기밀정보를 유출할 가능성이 있기 때문에 이를 해결하기 위한 대응방안의 필요성이 증가하고 있다. 따라서 본 논문에서는 사용자와 디바이스의 ID를 기반으로 XOR 연산과 해쉬연산을 이용한 경량화된 인증 프로토콜을 제안한다.

A Study on User Authentication using Speech Recognition in Smart Work Environment

Yoo-Kyeong Wi*, Jin Kwak**

ABSTRACT

Smartwork is flexible work type providing convenient work environment to people. Many countries are promoting introduction of smartwork provide for convenient work environment. As the importance of smartwork is increasing, countermeasure of security threats become more important. Especially, we found it necessary to countermeasure the problem, because illegal program and malicious code can be installed by unauthorized devices or the attacker can trying to leak confidential information. In this paper, we propose user and device based light-weight authentication protocol using XOR operation and hash operation.

Key Words : Smart Work, Speech Recognition, User Authentication, USIM, Smart Phone

* 순천향대학교 정보보호학과 정보보호응용및보증연구실(✉ykwi@sch.ac.kr)
** 순천향대학교 정보보호학과
· 제1저자(First Author) : 위유경 · 교신저자(Correspondent Author) : 곽 진
· 접수일(2011년 9월 19일), 수정일(1차 : 2011년 10월 27일), 게재확정일(2011년 10월 31일)

Ⅰ. 서 론

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 근무형태로써 출·퇴근 시간 감소로 인해 시간을 효율적으로 활용할 수 있고, 탄소배출량 감소, 기업의 예산절감 등의 효과를 제공하는 장점이 있다[1, 2].

최근 스마트워크는 세계적으로 많은 관심을 받고 있으며 다양한 나라에서 도입을 추진하고 있다. 국외 동향으로는 이미 미국, 일본, 네덜란드 등이 국가적인 차원에서 스마트워크를 추진하고 있다. 국내 동향으로는 정부에서 2010년에 스마트워크 센터 2곳을 설립하여 공무원을 대상으로 시범운영하고 있으며, 현재 정부청사와 제주도에 스마트워크 센터를 개소했다. 또한 2015년까지 50곳으로 확대하는 것을 목표로 적극적으로 추진하고 있다. 하지만 다양한 형태로 스마트워크 환경이 조성되고 여러 가지 IT 기술이 접목되어 있어 기존 기술들이 갖고 있는 취약점과 새롭게 발생되는 취약점에서 보안 통제가 완벽하게 이루어지지 않고 있다. 이러한 보안 취약점이 노출될 경우, 업무와 관련된 중요한 정보가 유출될 수 있기 때문에 정당한 사용자 인증이 되지 않는다면 많은 경제적 손실을 입을 수 있어 높은 보안성의 사용자 인증 수단이 필요하다[3, 4].

생체인증은 기존 사용자 인증 수단 중에서 비교적으로 높은 보안성을 지니고 있다. 사용자 본인이 갖고 있는 가장 정확하게 본인 인증을 할 수 있는 수단으로써 복제 및 악의적인 행위로부터 보다 안전하다. 하지만 현재 기기의 한계로 인해 지문, 홍채 등의 생체정보를 이용하기 위해서는 추가적인 기기가 필요하므로 스마트워크 모바일 서비스 환경에서는 활용하기 어렵다.

따라서 본 논문에서는 사용자의 음성 데이터와 모바일 기기에서 사용되는 USIM을 활용하여 스마트워크 환경에 적합한 음성인식을 활용한 사용자 인증 기법을 제안한다.

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

Ⅱ. 관련연구

2.1 스마트워크

스마트워크는 기존에 사무실이라는 한정된 공간에서 업무를 수행하는 개념과는 다르게 시간과 공간의 제약 없이 언제 어디서나 업무를 수행할 수 있는 업무 환경으로 스마트폰, 태블릿 PC 등의 모바일 기술, 광대역 통신, 클라우드 컴퓨팅 및 가상화 기술의 발달로 인해 등장하게 되었다[5, 6].

스마트워크는 근무 방식 및 근무 장소에 따라 스마트워크 센터 근무, 이동근무, 재택근무로 구분할 수 있다.

표 1. 스마트워크 근무 유형
Table 1. Type of smart work working

유형	근무형태
스마트워크 센터 근무	자택 인근의 정보통신기술 환경이 갖춰진 원격 사무실에서 근무
이동근무	모바일 오피스 환경을 이용하여 현장에서 직접 및 이동 중 근무
재택근무	자택에서 기업 내 네트워크에 접속하여 근무

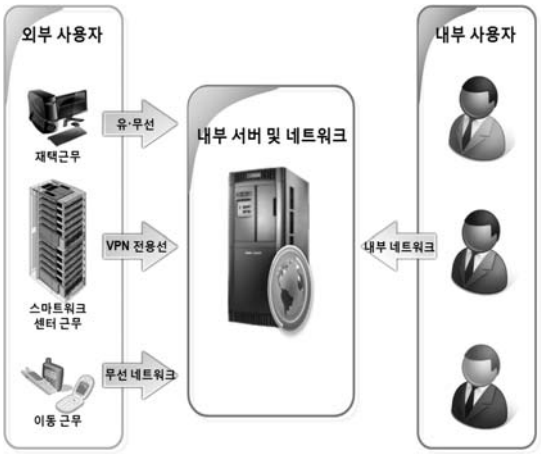

그림 1. 스마트워크 개념도
Fig. 1. Conceptual diagram of smart work

2.1.1 스마트워크 센터 근무

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

스마트워크 센터는 근태관리가 용이하고, 보안 인프라가 구축되어 있어 일반 인터넷망을 사용하는 재택근무, 무선통신망을 사용하는 이동근무의 근무유형보다 보안성이 보장되어 있으며, 기업 본사에서 직접 관리하여 육아 놀이시설, 편의시설 등이 마련되어 있어 업무집중도가 향상될 수 있어 업무의 효율성이 향상될 수 있다[6].

2.1.2 이동근무

스마트폰, 태블릿 PC 등을 활용하여 무선 네트워크 통신망을 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[6].

2.1.3 재택근무

자택에서 기업 내부의 네트워크에 접속하여 업무를 수행하는 유형으로 출·퇴근 시간을 소비하거나 교통비에 대한 부담을 감소시킬 수 있다. 또한 자택에 구축되어 있는 유·무선 네트워크 통신망을 사용하므로 업무를 수행할 수 있는 별도의 공간을 구축 할 필요가 없다[7]. 또한 사무실에서 근무하기 불편한 육아 휴직자 또는 장애인, 노약자 등에게 유용한 업무 환경이다.

2.2 음성인식 기술

음성인식은 전화, 마이크 등의 음성 입력장치를 통하여 컴퓨터 또는 음성인식 시스템으로 전송된 음성으로부터 특징을 추출하고 분석하여 미리 입력된 음성 데이터 목록에서 가장 유사한 결과를 찾아내는 기술이다[8, 9].

음성인식 기술은 그 분류기준에 따라 여러 종류로 나누어진다. 발성의 자연성에 따라 단어인식기술, 연속음성인식기술, 대화체인식기술로 분류되며 사용자의 범위에 따라 화자종속 인식기술, 화자독립 인식기술 그리고 인식대상 어휘수에 따라 소어휘 인식기술, 대어휘 인식기술 등으로 구분된다[9, 10, 11].

표 2. 음성인식 기술의 구분
Table 2. Classification of speech recognition technology

구분	종류
발성의 자연성	단어인식기술, 연속음성인식기술, 대화체인식기술
사용자의 범위	화자종속 인식기술, 화자독립 인식기술
인식대상의 어휘수	소어휘 인식기술, 대어휘 인식기술

2.2.1 연속음성인식 기술

연속음성인식 기술은 문장을 인식하기 때문에 사용자가 단어 단위로 끊어 발음하지 않아도 된다. 이 시스

템은 종전까지 인식률이 95% 이하였고, 인식 어휘수에도 제약이 많았다. 그러나 최근에 알고리즘의 개선, 인간공학기술 사용 등으로 1,000~3,000 어휘의 95% 이상의 인식률을 보이고 있다[11].

2.2.2 화자종속 음성인식 기술

화자종속 음성인식은 화자독립 음성인식에 비해 인식률이 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[11].

2.2.3 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[10, 11].

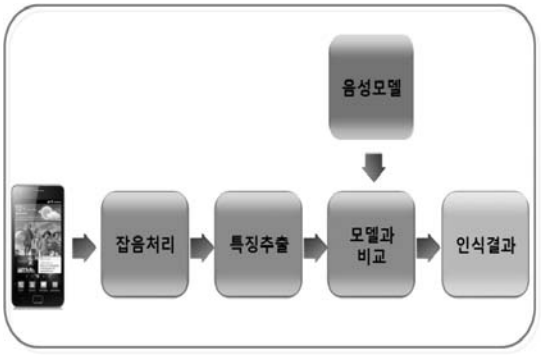

그림 2. 음성인식 시스템의 기본 구성도
Fig. 2. Schematic diagram of speech recognition system

2.3 USIM

USIM은 SIM(Subscriber Identity Module) 카드와 UICC(Universal IC Card)가 결합된 용어로써 사용자 인증과 글로벌 로밍, 전자상거래 등 여러 기능을 손톱 크기의 카드에 담은 것이다. 가입자 인증을 하는 SIM 카드와 교통카드 및 신용카드 등의 기능을 담을 수 있는 범용 IC카드의 역할을 한다. USIM은 소형 CPU와 메모리로 구성되는데 CPU는 암·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[12].

III . 보안 취약점 분석

스마트워크 환경은 기본적으로 유·무선기기를 사용하여 기업 외부에서 기업 내부의 네트워크에 통신망을 통해 접근하여 업무를 수행하기 때문에 사용자의 정당한 인증 과정이 필요하다.

스마트워크 환경에서는 기기가 다수의 기업에 접근하게 되며, 다루게 되는 정보 또한 기업의 기밀정보 등 높은 등급의 보안 수준을 요구하는 경우도 많다[13].

스마트워크 센터의 경우에는 일정한 보안 수준을 만족하기 위해 보안 인프라가 구축되어 있어 보다 안전한 수준의 접근이 가능하다. 그러나 이동근무 및 재택근무와 같은 경우 공공 통신망을 활용하므로 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[14, 15].

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

Ⅳ. 음성인식을 활용한 사용자 인증 기법

본 논문에서는 스마트워크 환경에서 안전한 모바일 서비스 환경을 구축하기 위하여 사용자와 스마트워크 사내망 간에 음성인식을 활용하여 안전성이 향상된 사용자 인증 기법을 제안한다.

4.1 제안방식

스마트워크 사내망에 안전하고 편리한 접속을 위해 사용자의 음성 데이터와 모바일 기기를 사용하여 보다 편리하고 안전한 사용자 인증을 제안하고자 한다. 본 논문에서 제안하는 방식은 데이터의 경량화를 위해 사용자의 음성 데이터를 분할하고, 안전성 향상을 위해 음성인증서버가 지정하는 임의의 분할값을 사용한다. 본 제안 방식은 음성 등록 단계, 인증 단계로 구분 된다.

그림 3은 본 논문에서 제안하는 음성인식을 활용한 사용자 인증 모바일 서비스 방안의 전체적인 개념을 나타낸다.

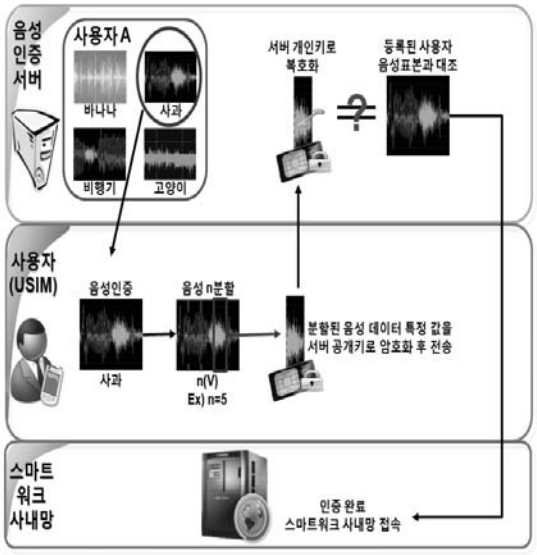

그림 3. 제안 방안 개념도
Fig. 3. Conceptual diagram of proposal system

4.2 음성 등록 단계

음성 등록 단계는 사용자 인증을 위해 음성인증서버에 사용자의 음성 데이터를 등록하는 단계이다.

사용자가 음성인증서버에 접속하면 서버는 임의로 N개의 단어를 생성하여 사용자에게 지정해주고, 사용자는 지정받은 해당 음성 데이터를 입력시켜 전송하면 음성인증서버는 해당 사용자의 음성 데이터를 표본으로 저장한다.

음성인식 기술은 일종의 패턴 인식 과정으로, 사람마다 목소리와 발음, 억양 등이 다르기 때문에 최대한 많은 사람들로부터 음성 데이터를 수집해 이로부터 공통된 특성을 추출하여 기준 패턴을 생성한다. 따라서 음성 데이터의 False Negative나 False Positive 등의 발생을 최소한으로 한다.

그림 4는 음성 등록 단계를 나타낸 것이며, 수행절차는 다음과 같다.

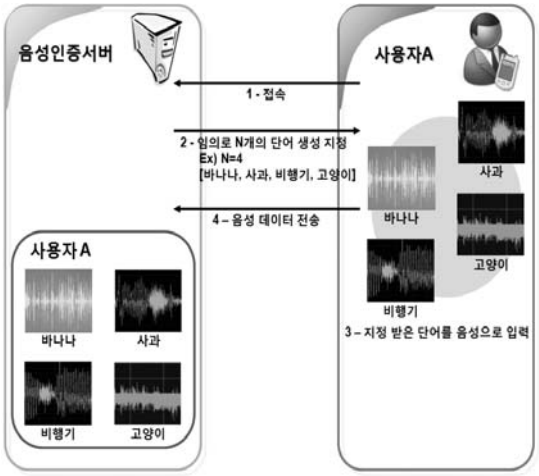

그림 4. 음성 등록 단계
Fig. 4. Voice registration phase

① 사용자는 모바일 기기를 사용하여 음성인증서버에 접속한다.
② 음성인증서버는 임의로 N개의 단어를 생성하여 해당 사용자에게 지정한다.

③ 사용자는 지정받은 단어를 음성으로 모두 입력한다.
④ 음성인증서버로 N개의 음성 데이터 값을 전송한다.
⑤ 음성인증서버는 음성 데이터를 표본으로 저장하여 서버에 등록한다.

4.3 인증단계

인증단계는 음성인증서버의 공개키와 사용자의 개인정보가 담긴 USIM칩이 장착된 모바일 기기를 사용한다.

사용자가 음성인증서버에 접속하게 되면, 음성인증서버로부터 해당 사용자의 미리 지정된 임의의 한 단어와 음성을 분할하기 위한 n값을 전송받는다. 사용자는 음성 데이터를 인증 후에 지정받은 n값을 입력하여 분할된 음성 데이터 $n(V)$을 생성하면, 서버로부터 $n(V)$의 특정 값을 요청받는다. 특정 값을 서버의 공개키로 암호화하여 전송하면, 서버는 개인키로 복호화한 후 등록된 음성 데이터와 매핑한다. 음성인증서버는 확인 대조 후 일치할 경우 스마트워크 사내망으로 접속승인을 요청한다.

그림 5는 인증 단계를 나타낸 것이며, 수행절차는 다음과 같다.

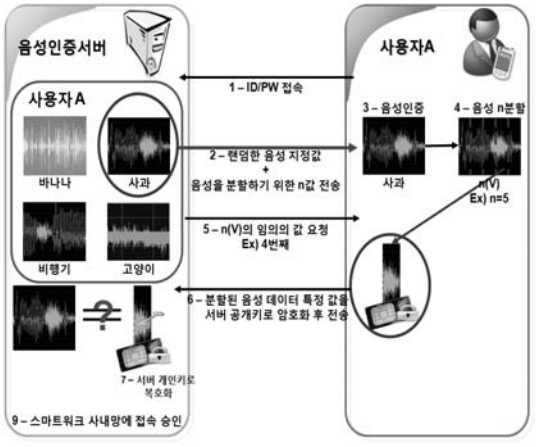

그림 5. 인증 단계
Fig. 5. Authentication phase

① 사용자는 ID/PW를 입력하여 1차 인증을 실시한다.
② 음성인증서버는 미리 지정된 해당 사용자의 음성 데이터 중 임의의 한 단어와 음성을 분할하기 위한 n값을 사용자에게 전송한다.
③ 사용자는 전송받은 단어를 음성 데이터로 인증한 뒤 음성을 분할하기 위해 지정받은 n값을 입력한다.
④ 모바일 기기는 음성을 임의대로 n번 분할시켜 $n(V)$를 생성한다.
⑤ 음성인증서버는 사용자에게 분할된 $n(V)$ 음성 데이터 중 특정 값을 요청한다.
⑥ 모바일 기기는 USIM에 저장된 음성인증서버의 공개키를 이용하여 해당되는 분할 음성 데이터의 특정 값을 암호화하여 음성인증서버로 전송한다.
⑦ 음성인증서버는 개인키를 사용하여 복호화한다.
⑧ 음성인증서버는 분할된 $n(V)$ 음성 데이터의 특정 값을 미리 등록되어 있는 사용자의 음성 데이터 표본의 절단면과 공통점을 찾아 매핑한다.
⑨ 음성인증서버는 사전에 등록된 음성표본과 확인 대조 후 일치할 경우에 스마트워크 사내망으로 접속승인을 요청한다.
⑩ 스마트워크 사내망은 음성인증서버의 승인요청을 확인 후 사용자의 접속을 허락한다.
⑪ 사용자는 스마트워크 사내망에 접속하여 인증을 마무리한다.

V. 안전성 및 효율성 분석

본 논문에서 제안한 음성인식을 활용한 사용자 인증 기법을 이용하여 인증을 수행할 경우에는 스마트워크 환경에서 모바일 서비스 업무를 수행할 때 다음과 같은 이점을 가져올 수 있다.

5.1 안전성 분석

표 3. 안전성 분석
Table 3. Security analysis

분류	기존 방안	제안 방안
정당한 사용자 인증	· ID / PW 방식 · 별도의 추가적인 사용자 인증 없음	· 사용자 음성 인증 · 미등록된 사용자는 음성 접근 불가
중요 정보 노출 방지	· 사용자의 정보가 노출될 경우 정보 노출 가능	· 사용자 음성 데이터를 사용하여 정보 노출 예방
악의적인 사용자의 접근 방지	· 사용자의 정보만으로 접근 가능	· 사용자의 기본 정보만으로는 접근 불가능 · 사용자의 음성 데이터와 일치해야 접근 가능
향상된 음성인식 인증	· 하나의 음성 데이터를 사용하여 안전성이 떨어짐	· N개 이상의 음성 데이터를 서버로부터 랜덤하게 받기 때문에 안전성을 향상시킴
음성 데이터 수	1	N

• 정당한 사용자 인증

기존의 ID와 Password 방식은 별도의 추가적인 사용자 인증 방법 없이 1차 인증정보만을 사용하여 보안에 다소 취약하지만, 제안하는 방식은 보안성이 높은 사용자 고유의 음성 데이터인 생체 인증을 사용하므로 미등록된 음성으로 인증을 수행할 시 접근 할 수 없다.

• 중요 정보의 노출 방지

기존의 사용자 인증 방식에서 ID와 Password가 악의적인 공격에 의해 노출될 경우에 사용자의 중요한 정보들이 노출될 가능성이 높다. 하지만 제안하는 방식은 사용자 고유의 음성 데이터를 사용하기 때문에 악의적인 공격에 보다 안전하여 중요 정보에 대한 노출을 예방할 수 있다.

• 악의적인 사용자의 접근 방지

기존의 사용자 인증 방식에서는 사용자의 정보를 탈취할 경우 정보에 접근을 허용할 가능성이 크지만 제안하는 방식은 사용자의 음성 데이터를 인증시켜야 하기 때문에 기본 1차 정보만으로는 접근이 불가능하고 미리 등록된 2차 생체인증인 음성 데이터와 일치해야 하기 때문에 보안성이 향상되었다.

• 향상된 음성인식 인증

기존의 하나의 음성 데이터 인증으로는 보안성이 다소 떨어지는데 비해 N개 이상의 음성 데이터를 서버로부터 랜덤하게 받기 때문에 보안성을 높였다.

5.2 효율성 분석

표 4. 효율성 분석
Table 4. Efficiency analysis

분류	기존 방안	제안 방안
USIM칩 활용	· 별도의 보안카드를 소지해야 하므로 번거로움	· 모바일 기기의 USIM칩을 활용하여 번거로움을 줄임
처리속도 향상	· 음성 데이터의 재배치 후 암호화로 인해 처리속도가 저하됨 · $S\left(\frac{R}{n(V)}\right)$	· 재배치 없이 분할된 음성중 지정하는 값만 암호화하여 처리속도가 향상됨 · $\frac{R}{n(V)}$

- USIM칩 활용

기존의 보안카드 인증은 카드를 별도로 소지해야 하는 번거로움이 생기는데 비해 제안하는 방식은 기존 모바일 기기의 USIM칩을 활용하기 때문에 번거로움을 줄였다.

- 처리속도 향상

기존의 음성 데이터 인증은 음성 데이터 값을 분할한 후 재배치하기 때문에 처리속도가 저하된다($S\left(\frac{R}{n(V)}\right)$). 하지만 제안하는 방식은 재배치 없이 분할된 음성 중에서 지정한 값만 암호화하기 때문에 처리속도가 향상된다($\frac{R}{n(V)}$).

Ⅵ. 결 론

스마트워크는 모바일 기기와 통신 인프라를 기반으로 하는 혁신적인 IT 서비스의 대표적인 기술이다. 기업은 생산성 향상과 편리성 증대를 위해 많은 비용과 노력을 투입하여 스마트워크를 환경을 구축하고 있다. 그러나 기기의 분실, 모바일 악성코드의 감염, 기업정보 및 기밀의 무단 유출과 같은 보안 문제가 지적되고 있다. 또한 유·무선 디바이스를 이용하여 기업 외부에서 기업 내부로 네트워크를 통해 접근을 수행하게 되는 스마트워크 환경에서는 사용자에 대한 정당한 인증 과정이 필수적으로 요구된다. 이러한 보안 문제에 대한 개선 없이는 안전한 스마트워크 환경을 구축할 수 없다[16].

본 논문에서는 스마트워크 환경에 접근하는 다양한 사용자에 대해 사용자 본인의 음성 데이터를 이용하여 안전하고 정당한 인증을 수행하는 방안을 제안하였다.

이를 통해 스마트워크 환경을 구축하고 기업 내부망에 접근하여 업무를 수행할 때 사용자 고유의 음성 데이터를 이용하기 때문에 인증되지 않은 사용자에 대한 원천적 차단이 가능하고, 중요한 정보 노출에 대한 차단이 가능할 것으로 기대할 수 있다. 따라서 스마트워크 환경 전반에 대한 보안성을 향상시킬 수 있을 것으로 기대된다.

참고문헌

[1] OPM, "*Status of Telework in the Federal Government*", 2011.

[2] Robin Simpson. *"How to Keep Mobile & Remote Workers Happy in 2010"*, 2010.

[3] 행정안전부, "스마트워크 추진계획", 2010.

[4] 방송통신위원회, "스마트워크 활성화 추진계획", 2011.

[5] 고웅, 곽진, "스마트워크 환경에 접근 가능한 안전한 디바이스 인증 기법 연구", *제35회 한국정보처리학회 춘계학술대회 논문집*, 제 18권 1호, 2011.

[6] 데이코산업연구소, "스마트워크 실태와 모바일오피스 추진전략", 2011.

[7] 박승권, 이주한, "스마트워크 기술과 표준화 동향", *표준기술동향*, 2011.

[8] 길연희, 정윤수 외 3명, "다중 생체인식 기술 동향", *전자통신동향분석*, 제 20권 제 1호, 2005.

[9] L. R. Rabiner and B. H. Juang, Fundamentals of Speech Recognition, Pretice-Hall, 1933.

[10] 강점자, 강병옥, 정호영, 정훈, 이윤근, "신성장동력산업용 대어휘 음성인식 기술 동향 및 응용", *전자통신동향분석*, 제 23권 1호, 2008.

[11] 이윤근, 박준, 김상훈, "음성인터페이스 기술", *전자통신동향분석*, 제 20권 5호, 2005.

[12] 정병근, "USIM 기반 무선 네트워크 연동 보안 인증 시스템에 관한 연구", *한국정보과학회 가을 학술발표논문집*, 제 34권 2호, 2007.

[13] 김꽃마음, "스마트워크 활성화 정책방향", *방송통신위원회*

[14] 이재성, 김홍식, "스마트워크 현황과 활성화 방안 연구", *한국지역정보학회지*, 제 13권 4호, 2010.

[15] 이형찬, 이정현, 손기욱, “스마트워크 보안 위협과 대책”, *한국정보보호학회지*, 제 21권 3호, 2011.
[16] 스마트워크센터, *http://www.smartwork.go.kr*

감사의 글

본 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원에 의해 연구되었음 (No.2011-0007755).

저자소개

위유경(Yoo-Kyeong Wi)

2006년~현재 순천향대학교 정보보호학과 재학
※ 관심분야 : 정보보호, 스마트워크

곽진(Jin Kwak)

2003년 성균관대학교 컴퓨터공학과 (공학석사)
2006년 성균관대학교 컴퓨터공학과 (공학박사)
2006~2006년 : 일본 큐슈대학교 방문연구원
2006~2006년 : 일본 큐슈시스템 정보기술연구소 특별연구원
2006~2007년 : 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관
2007~ 현 재 : 순천향대학교 정보보호학과 교수
2007~2009년 : 정보통신연구진흥원 집필위원
2009~2009년 : 순천향대학교 공과대학 교학부장
2009~2010년 : 순천향대학교 정보보호학과 학과장
2010~2010년 : 교육과학기술부 국가기술수준평가 전문위원
현재 : 정보통신산업진흥원 기술평가위원, 사)국제정보능력평가원 쇼핑몰 플래너 자격 검정 출제 및 채점위원, 한국과학기술정보연구원 충남 과학기술 정보협의회 전문위원, 지식경제부 지식경제기술혁신평가단 평가위원, 순천향BIT 창업보육센터 센터장, 순천향대학교 중소기업산학협력센터 센터장
※ 관심분야 : 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅 보안, 스마트워크 등