Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 2 pp. 842-848, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.2.842

다중요소방식을 이용한 시스템 접근방안

진광윤[1*], 최신형[2], 서장원[3], 김영곤[4]
[1]강원대학교 컴퓨터공학과, [2]강원대학교 제어계측공학과
[3]동서울대학 컴퓨터소프트웨어과, [4]숭실대학교 컴퓨터학과

An Approach to Systems with Multi-Factor Method

Kwang-Youn Jin[1*], Shin-Hyeong Choi[2], Jang-Won Seo[3] and Young-Gon Kim[4]
[1]Dept. of Computer Engineering, Kangwon National University
[2]Dept. of Control & Instrumentation Engineering, Kangwon National University
[3]Dept. of Computer Software, Dong Seoul College
[4]Dept. of Computer, SoongSil University

요 약 본 논문에서는 스마트워크 환경에 적합한 인증 방법으로써, QR code를 이용하여 사전에 이동통신사로부터 인증 받은 단말을 이용하여 비 인가된 장비를 통해 접근을 하는 사용자를 인증할 수 있도록 하였다. 이를 위해, 기존의 사용자 인증 시스템보다 안전하고 복잡하지 않은 연산처리를 통해 상호간의 인증이 가능한 경량화 된 프로토콜을 설계하였다. 제안하는 사용자 인증 시스템은 외부 접근을 요청하는 클라이언트에 사용자의 어떠한 인증 정보도 입력하지 않고 사전에 인가된 단말을 사용하여 인증함으로써, PC에서 이루어지는 해킹 공격을 근본적으로 방지할 수 있다. 향후 연구에서는 일반 인터넷 환경의 사용자 인증에 사용하거나, 또는 단말 정보가 아닌 사용자 고유 정보를 사용하기 위한 연구가 가능하다.

Abstract In this paper, as a proper authentication method, we made it authenticate a user who has unauthorized device with using authorized device received from telecommunication company using QR code. We designed a better performance protocol which can authenticate mutually using safer and uncomplicated operations than existing user authentication system. Proposed user authentication system authenticates previously authorized mobile device without any information of client who is requesting to get access from outside, so we can basically prevent attack from hackers. In the future, we can possibly use it as user authentication method in common internet environment or we could study on user unique information instead of mobile device information.

Key Words : Smartwork, Authentication, Protocol

1. 서론

전 세계적으로 네트워크 환경과 IT 기술이 고도화되고, IT를 활용한 저탄소 녹색성장에 대한 관심이 높아지면서 주요 선진국을 중심으로 스마트워크 추진이 활발하게 이루어지고 있다. 최근 국내 기업에서도 스마트워크 도입에 많은 관심을 가지고 있으며 스마트워크 도입은 기업의 비용절감, 업무 생산성 향상 및 고객만족도 증가, 우수한 인재 확보 및 활용, 조직의 전문성 강화 등 기업에 긍정적인 영향을 기대할 수 있다. 하지만 긍정정인 영향만큼 처리해야 하는 보안적인 문제들이 수반된다.

스마트워크는 기존의 내부뿐만 아니라 외부에서도 사용자 접근이 가능하기 때문에 발생 할 수 있는 보안적인 문제점을 해결하기 위한 보안 기술이 있어야 하며, 특히, 다양한 기종을 통한 사용자의 서비스 접근의 문제를 해결하기 위한 사용자 인증 기술이 필수적으로 필요하다.

*교신저자 : 진광윤(kyjin@kangwon.ac.kr)
접수일 11년 12월 20일 수정일 12년 01월 17일 게재확정일 12년 02월 10일

본 논문에서는 스마트워크 환경에 적합하도록 QR code를 이용한 사용자 인증 시스템을 제안한다. 스마트워크는 다양한 기종을 통해 어떤 상황에서도 외부 접근이 가능하기 때문에 사용자와 서버간의 상호 인증이 필수적이다. 따라서 비 인가된 장비를 통해 사용자가 외부에서 접근을 할 경우 사전에 인가된 장비를 이용하여 사용자를 인증할 수 있는 방식을 제안하며 특히, 인증을 할 때 매번 인증서를 사용하지 않고 사용자와 서버간의 상호 인증이 가능한 방법을 제시하고 있다.

2. 관련연구

2.1 스마트워크의 정의

스마트워크는 종래의 지정된 업무공간인 사무실 개념이 아닌 다양한 장소와 이동환경에서도 업무를 효율적으로 처리할 수 있도록 하는 미래지향적인 업무 환경으로서, 현장에서 신속한 업무처리를 통해 업무속도와 생산성이 향상된다. 또한, 원격 협업을 통한 실시간 협업이 가능해져 신속한 의사결정과 빠른 문제해결이 가능해지며, 근무형태의 유연화로 인해 근로 취약계층의 취업기회 확대 등 긍정적인 효과를 기대할 수 있다[1, 3].

2.2 QR code

(1) QR code의 특징

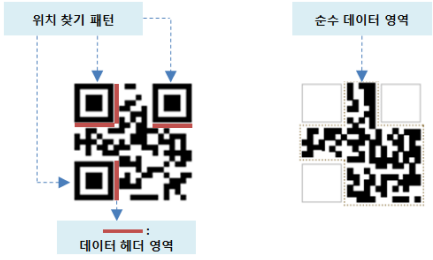
QR code는 그림 1과 같이 2차원 행렬의 구조로 데이터를 표현되며, 크기는 버전마다 다르다.

[그림 1] QR code
[Fig. 1] QR code

QR(Quick Response) code는 흑백 격자 무늬 패턴으로 정보를 나타내는 매트릭스 형식의 2차원 바코드이다. QR code는 종래에 많이 쓰이던 Bar code의 용량 제한을 극복하고 그 형식과 내용을 확장한 2차원의 Bar code로 종횡의 정보를 갖기 때문에 숫자 외에 문자의 데이터를 저장할 수 있으며, 디지털 카메라나 전용 스캐너로 읽어 들여 활용되고 있다.

(2) QR code의 구조

QR Code의 구조는 다음의 그림 2와 같다. 일반적으로, QR code는 위치 검출 패턴, 타이밍 패턴, 데이터 영역, 형식 정보 영역으로 구성된다. 위치 검출 패턴과 타이밍 패턴은 고정되어 있는 부분으로 코드 디코딩시 위치 감지 및 좌표 결정에 사용되며, 데이터 영역과 형식 정보 영역은 인코딩 된 데이터의 값에 따라 정해진다.

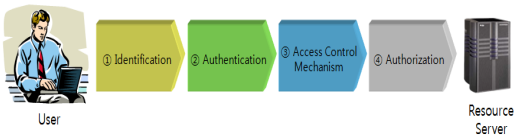


[그림 2] QR Code의 구조
[Fig. 2] Structure of QR code

2.3 사용자 인증 기술

인증 기술은 임의의 정보에 접근할 수 있는 주체의 능력이나 주체의 자격을 검증하는 것으로 시스템이 접근을 요청한 사용자가 그 본인이 맞다고 인정해 주는 모든 과정을 의미한다. 이러한 인증은 해당 서비스를 사용하고자 하는 사용자 인증과 전달되는 정보에 변경이 없음을 보장하는 메시지 인증으로 구분되며 패스워드, 공인인증서, 생체인증 등과 같은 기술의 안정성에 의존 한다. 기밀성은 권한이 없는 사람으로 하여금 해당 정보를 확인 할 수 없도록 하는 기술로서 대칭키 암호화 또는 공개키 암호화 알고리즘에 기반을 두고 있다. 무결성은 송수신 되는 정보에 대하여 변경됨이 없음을 보장하기 위한 기술이다[7]. 부인방지 기술은 송수신자 상에 전송된 정보에 대해 송신하거나 수신한 사실을 부인할 수 없도록 하는 것으로 전자서명을 통해 구현될 수 있다. 사용자 인증기술은 시스템이 본인임을 주장하는 요청자에 대해 해당 시스템에 등록되어 있는 정당한 사용자임을 인정해 주는 것으로 그림 3과 같다.

사용자가 인증서버에 자신이 누구임을 밝히는 식별(Identification), 인증 서버가 접근을 요청하는 사용자를 증명하는 인증(Authentication), 접근이 허용된 사용자에 대해 접근통제 메커니즘에 입각해 시스템 자원 사용을 허가하는 권한부여(Authoriz -ation)의 3단계로 이루어진다. 특히, 인증 과정은 접근 요청자가 서비스 제공자로부터 제공되는 서비스를 제공받기 위해서는 필수적인 요구조건이다.



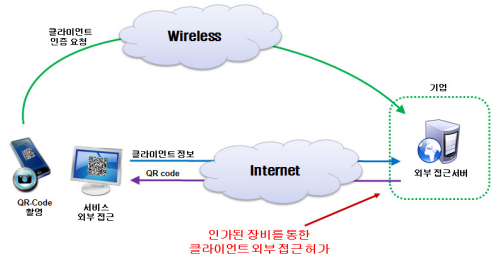
[그림 3] 사용자 인증 절차
[Fig. 3] User Authentication Process

사용자 인증 기법은 형태에 따라, 사용자가 알고 있는 것을 인증 요소로 사용하는 Type-I 인증, 사용자가 소유하고 있는 물건을 인증 요소로 사용하는 Type-II 인증, 사용자의 신체적 특징을 이용하는 Type-III 인증, 사용자의 행동적 특징을 이용하는 Type-IV 인증으로 분류할 수 있다[5].

3. 사용자 인증 제안 시스템

3.1 제안 시스템 모델

본 논문에서 제안하는 시스템은 스마트워크 환경에서 발생하는 보안 위협을 방지하기 위해 기존의 사용자 인증 기술을 사용하지 않는 다중요소 방식의 사용자 상호 인증 기술이다. 이 인증 기술은 접근하려 하는 인가되지 않은 기기에 어떤 입력 값도 주지 않고 사전에 인가된 기기를 통해서만 인증이 가능한 방식이다. 다음의 그림 4는 제안 시스템의 구조도를 나타낸 것이다. 제안하는 시스템은 스마트워크 환경에서 서비스 외부접근이 진행 될 때 클라이언트에서 인증정보를 입력하는 것이 아니라, 사전에 인가된 단말을 통해 클라이언트를 대신 인증 하는 방식으로서, 비 인가된 클라이언트에 인증을 위해 필요한 어떤 정보도 입력하지 않기 때문에 기존의 인증시스템에서 발생할 수 있는 보안 문제점을 해결하여 안전하게 사용자 인증을 할 수 있다.



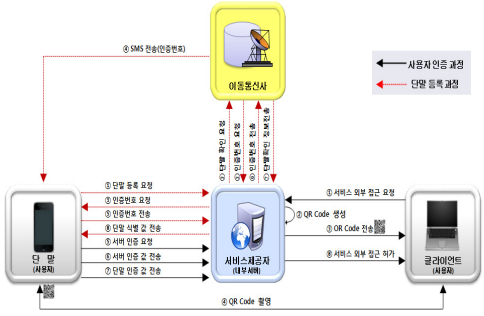
[그림 4] 제안 시스템 구조도
[Fig. 4] System Structure

제안하는 시스템은 다음과 같은 조건들을 만족해야 한다.

① 사용자는 QR code를 촬영하기 위해 카메라 기능이 내재된 단말을 소지하고 있어야 한다.
② 사용자의 단말은 사전에 인증되어 기업 서버에 단말의 정보가 등록되어 있어야 한다.
③ 기업 서버에 등록되어 있는 사용자의 단말기 번호는 오프라인을 통해서만 변경이 가능하다.
④ 단말기에는 단말 인증 에이전트가 설치되어 있어야 한다.
⑤ 모바일 기기는 암·복호화 및 연산을 위하여 SHA-1 해시함수와 AES 알고리즘을 수행할 수 있는 연산 능력을 가지고 있어야 한다.

그림 5는 본 논문에서 제안하는 사용자 인증 기법의 전체 구성도를 나타낸 것이다. 이 구성도는 크게 단말등록과정과 인증과정으로 구성하였으며, 단말등록과정의 단계별 설명은 다음과 같다.

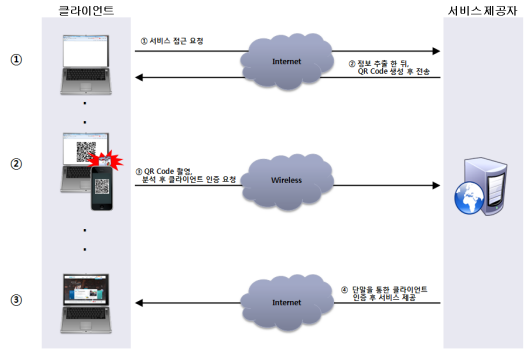
① 단말을 Wireless를 통해 서버에 접근하여 단말등록 요청을 한다.
② 서비스 제공자는 이동통신사에 단말 사용자에 대한 정보와 번호를 보내 단말확인 요청을 한다.
③-⑥ 이동통신사는 서비스 제공자에게 인증번호를 요청하고 단말에게 SMS를 통해 인증번호를 전송해 준다. 단말에게 인증번호를 전송 받은 서비스 제공자는 이동통신사에게 다시 전송한다.
⑦ 인증번호를 확인 한 뒤 이동통신사는 서비스 제공자에게 단말을 확인 할 수 있는 값을 생성하여 전송한다.
⑧ 서비스 제공자는 단말 확인 값과 매칭 되는 단말 식별 값을 생성하여 단말에게 전송한다.



[그림 5] 제안하는 사용자 인증 기법의 전체 구성도
[Fig. 5] The Entire Configuration

위의 단계를 거쳐 단말은 서비스 제공자에게 등록되게 된다. 그런 후에, 등록된 단말을 통해 사용자 인증 과정을

거치게 된다. 사용자 인증과정을 간략하게 살펴보면 그림 6과 같다.



[그림 6] 사용자 인증 과정
[Fig. 6] The Process of User Authentication

사용자 인증과정의 단계별 설명은 다음과 같다.

① 사용자가 외부에서 인가되지 않은 클라이언트를 통해 서비스 제공자에게 서비스 접근 요청을 하면, 서비스 제공자는 외부 접근 요청을 한 클라이언트의 정보를 추출한 뒤, QR code를 생성한 후 전송한다.

② 클라이언트 화면에 QR code가 나타나면 사용자는 사전에 단말 등록과정을 통하여 등록된 단말로 QR code를 촬영하여 분석한 후, 서비스 제공자에게 클라이언트 인증을 요청한다.

③ 클라이언트 인증을 요청 받은 서비스 제공자는 단말을 인증 후 클라이언트를 인증하여 서비스를 제공한다.

4. 성능 분석 및 평가

여기서는 3.1절에서 제안한 QR code를 이용한 사용자 인증 시스템을 구현한 결과를 바탕으로 효율성과 성능을 알아보고, 기존의 사용자 인증 시스템과의 비교 분석을 수행함으로써 보안의 우수성을 알아본다.

4.1 구현 환경

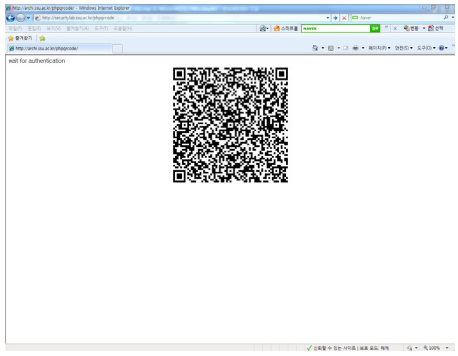
본 논문에서 구현 된 시스템은 Microsoft Windows 7 Enterprise 32bit 운영체제에서 웹 서버인 Apache와 개발 도구로 데이터베이스는 mysql을 사용하였고 PHP를 이용하여 구현하였다. 하드웨어는 Intel(R) Core(TM)2 Quad CPU 2.66GHz, RAM 4GB 환경에서 구현하였다.

제안하는 시스템은 데이터 암·복호화를 위해 대칭키 알고리즘인 AES 암호화 알고리즘을 사용하였고, 데이터의 일방향성을 위해 SHA-1 해시 함수를 사용하였다.

4.2 구현 결과

본 논문의 제안 기법은 사용자가 사전에 등록된 단말을 이용하여 인증을 하는 방식으로 구현에서는 사용자가 단말을 통해 서비스 제공자에게 인증을 받아 홈페이지에 접근 하는 시나리오로 구현 결과를 설명한다.

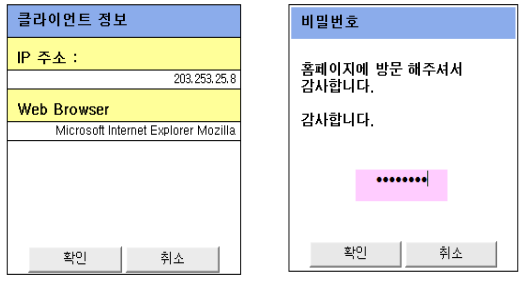
다음의 그림 7은 사용자의 초기 접근 화면을 나타낸 것이다.



[그림 7] 초기 접근 화면
[Fig. 7] Early Access Screen

사용자가 서비스 제공자에게 접근을 하면 서비스 제공자는 사용자 클라이언트의 정보와 RSN (Random Serial Number), KEY(AES 128bits Key) 값을 이용하여 QR code를 생성한 후, 화면에 출력한다.

화면에 있는 QR code를 촬영하면 다음의 그림 8과 같은 순서로 인증이 진행 된다.



[그림 8] 인증 시스템 구현
[Fig. 8] Authentication System

먼저, QR code를 촬영하면 첫 번째 화면과 같이 IP 주소, Web Browser와 같은 기본적인 클라이언트 정보를 출

력하여 사용자 확인을 한 뒤, QR code의 무결성을 확인하기 위해 서비스 제공자와 통신을 한 뒤 QR code의 검증이 완료가 되면, 두 번째 화면과 같이 패스워드 입력창이 나타난다. 이 때, 패스워드를 입력하면 인증에 필요한 정보와 함께 연산 처리되어 서비스 제공자에게 전송이 되고, 서비스 제공자가 단말을 인증하게 되면 QR code의 데이터와 매칭 되는 클라이언트의 외부 접근을 허가 하게 되어, 그림 8에서 QR code가 사라지고 정상적인 서비스 화면이 나타나게 된다.

4.3 비교 분석

(1) 안전성 분석

제안한 시스템의 보안 요소를 검토하여 안전성을 분석하고, 사용자 인증 시스템의 보안 위협에 대한 문제점에 대하여 분석한다. 제안하는 사용자 인증 시스템의 안전성은 다음 두 가지 상황 중 한 가지만 발생할 경우에 안전성을 보장한다.

① 사용자의 패스워드가 노출된다.

사용자의 패스워드가 노출이 되더라도 사전에 등록된 단말을 소유하고 있지 못하면, 단말 정보를 생성할 수 없기 때문에, 안전성을 보장한다.

② 사용자의 단말이 분실된다.

사전에 등록된 단말을 분실 하더라도, 사용자의 패스워드를 알 수 없기 때문에 안정성을 보장한다.

제안한 사용자 인증시스템의 안전성 분석을 위한 보안 요소에 대해 검토한다.

① 인증(Authentication)

사용자는 서비스 제공자가 생성한 QR code의 무결성을 RSN과 KEY 값을 통해 검증하고, 서버는 사용자가 이동통신사를 통해 사전에 등록한 단말의 정보를 검증하여 인증하기 때문에 정당한 사용자만 서비스를 이용할 수 있다.

② 기밀성(Confidentiality)

송수신 되는 데이터는 노출에 대한 위험이 없는 데이터를 제외하고는 송수신 측에서 연산처리가 가능한 데이터를 생성하여, 여러 데이터를 연접하여 해시 절차를 통해 데이터가 전송되기 때문에 도청 및 개인정보 유출로부터 비교적 안전하다.

③ 무결성(Integrity)

기밀성과 비슷하게 실질적으로 전송되는 데이터는 모두 해시 절차를 통해서 전송되기 때문에 중간자로부터 데이터가 변조되는 공격을 방지할 수 있다. QR code의 무결성 검증은 RSN과 KEY 값을 통해 검증이 가능하여 더욱 신뢰성을 높일 수 있다.

④ 가용성(Availability)

복잡한 연산을 통해 여러 인증기관을 경유하는 시스템이 아니며, 연산 처리가 복잡하지 않은 해시 연산과 AES 연산만 사용하여 처리속도가 빠르다. 또한, 재전송이나 서비스 거부 공격 등에 대해서도 RSN과 KEY 값의 유효시간을 통해 해결 가능하여 가용성이 뛰어나다.

기존의 사용자 인증 시스템과 제안한 사용자 인증 시스템간의 안전성 비교는 다음의 표 1과 같다. 즉, 기존의 사용자 인증 방식은 대부분 사용자만 인증하는 단방향성 인증으로 피싱 공격 등 위협이 있지만, 제안하는 방식은 양방향으로 상호 인증을 하기 때문에 보안 위협에서 벗어날 수 있다.

[표 1] 안전성 비교 분석
[Table 1] Comparative Analysis of Safety

	id/ password	공인 인증서	제안 시스템
사용자 인증 방향	단방향	양방향	양방향
패스워드 추측 공격	가능	불가능	불가능
패킷 스니핑	가능	불가능	가능
중간자 공격	가능	가능	불가능
재전송 공격	가능	가능	불가능
위조 공격	가능	불가능	불가능
키보드 해킹	가능	가능	불가능
웹사이트 해킹	가능	가능	불가능

(2) 효율성 분석

기존의 사용자 인증 시스템과 제안한 사용자 인증 시스템간의 효율성을 비교 분석하기 위해 처리시간을 비교 분석하였다. 테스트 환경인 PC가 스마트폰의 사양보다 훨씬 높기 때문에 한 번의 동작으로는 차이가 미세하다. 따라서 정확한 효율성 분석을 위해 기존 시스템의 동작 횟수와 제안 시스템의 동작 횟수를 늘리게 되면 차이를 알 수 있다. 다음의 표 2는 기존의 사용자 인증 시스템과 제안한 사용자 인증 시스템의 동작 횟수에 따른 시간차를 표로 나타낸 것이다.

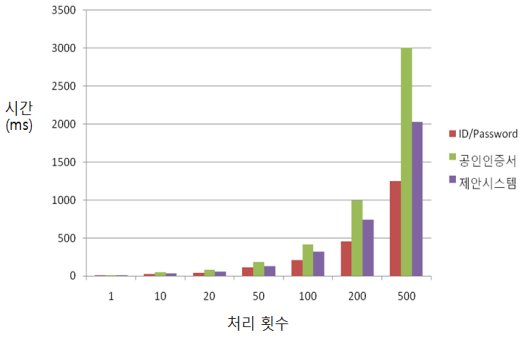
[표 2] 효율성 비교 분석
[Table 2] Comparative Analysis of Efficiency

구분	ID/Password	공인인증서	제안시스템
1회	2.7 ms	5.5 ms	3.4 ms
10회	24.2 ms	52.7 ms	31.6 ms
20회	43.3 ms	84.3 ms	60.4 ms
50회	114.2 ms	184.9 ms	132.1 ms
100회	205.6 ms	415.7 ms	321.8 ms
200회	454.9 ms	994.5 ms	742.4 ms
500회	1251.3 ms	3005.4 ms	2026.9 ms

표 2에서 보면, 안전성이 낮은 인증 시스템인 ID/Password 방식과 비교해서는 제안한 사용자 인증 시스템이 속도가 느리지만, 서비스 외부접근이 진행 될 때 클라이언트에서 인증정보를 입력하는 것이 아니라, 사전에 인가된 단말을 통해 클라이언트를 대신 인증 하는 방식이므로 비 인가된 클라이언트에 인증을 위해 필요한 어떤 정보도 입력하지 않기 때문에 비슷한 보안 강도를 가진 공인인증서 인증 시스템 보다는 처리시간 측면에서 성능이 뛰어남을 알 수 있다.

그림 9에서, 횟수가 적을 때는 성능의 차이가 크게 보이지 않지만, 횟수가 많아질수록 성능의 차이가 크게 나타나는 것으로 볼 때, 제안한 사용자 인증 시스템의 우수성을 증명할 수 있다. 테스트 환경이 스마트폰 환경 보다 성능이 훨씬 뛰어나기 때문에 스마트폰 환경일 경우에는 시간차는 더욱 많이 날 것이다.

다음의 그림 9는 테스트 결과를 보기 쉽게 그래프로 표현 한 것이다.



[그림 9] 비교분석 그래프
[Fig. 9] Comparison Graph

5. 결 론

본 논문에서는 QR code를 이용하여 비 인가된 장비를 통해 기업 서버에 접근 하는 사용자에 대해 사전에 인가된 단말을 통해 안전하게 사용자 인증을 할 수 있는 방안을 제시하였다.

기존의 인증 방식은 해킹의 위협이나 분실 시 발생하는 위험도가 높은 취약성이 존재하지만, 제안하는 시스템은 비 인가된 클라이언트에서는 아무런 입력을 하지 않고 사전에 인가된 단말을 통해 사용자를 인증 할 수 있는 값을 생성해 내기 때문에 기존의 인증 방식 보다 안정성이 뛰어남을 확인하였다.

또한, 기존의 사용자 인증 방식은 대부분 사용자만 인증하는 단방향성 인증으로 피싱 공격 등 위협이 있지만, 제안하는 방식은 양방향으로 상호 인증을 하기 때문에 보안 위협에서 벗어날 수 있다.

효율성 부분 역시 비교 분석에서 보는 바와 같이 기존의 인증기술보다 빠르거나 뒤처지지 않음을 확인 할 수 있다. 따라서 처리 연산 부분이 빨라 효율성이 더욱 높거나, 비슷한 처리속도를 보인 인증기술 보다 안정성 측면에서 이점을 갖고 있다.

향후 QR code를 더욱 확장하여 스마트 워크 환경이 아닌 일반적인 인터넷 환경에서도 사용 가능한 사용자 인증 시스템 개발이 과제이다. 또한, IT 컨버전스를 통해 단말 정보가 아닌 사용자의 고유한 정보로 인증 데이터를 대체 할 수 있는 연구가 필요하다.

References

[1] Deyiko Industrial Research Institute, “Status and Strategies for Smart Work Mobile Office”, 2011
[2] YunGyeong Lee, “Anonymous Authentication Technology & Trends”, Trend analysis of electronic communications, Vol.23, No.4, 2008
[3] Korea Communications Commission, “Smart Work for a Company Operating Guides introduced", 2011
[4] Korea Information Security Institute, “Certificate for the Security Problem Diagnosis and Preparedness Forum", 2010
[5] Forouzan, "Cryptography and Network Security, McGraw-Hill, 2007
[6] J. Daemen, V. Rijmen, “The Design of Rijndael: AES - The Advanced Encryption Standard”, Springer-Verlag, 2002.
[7] Sung,J Park, "Copyrights Protection Techniques",

Proceedings International Digital Content Conference, 2000.
[8] Radia Perlman, "An Overview of PKI Trust Models, IEEE Network," Vol.13, No.6, pp.38-43, November/ December 1999
[9] Ronald Leenes, "PRIME Whitepaper v2 : Privacy En-hanced Identity Management", 2007

진 광 윤(Kwang-Youn Jin) **[정회원]**

- 1984년 2월 : 서울산업대학교 전자계산학과 (공학사)
- 1987년 2월 : 건국대학교 전자계산학과 (공학석사)
- 2004년 2월 : 경남대학교 컴퓨터공학과 (공학박사)
- 1990년 3월 ~ 현재 : 강원대학교 컴퓨터공학과 교수

<관심분야>
정보보안, 임베디드시스템

최 신 형(Shin-Hyeong Choi) **[종신회원]**

- 1993년 2월 : 울산대학교 전자계산학과 (공학사)
- 1995년 2월 : 경남대학교 전자계산학과 (공학석사)
- 2002년 8월 : 경남대학교 컴퓨터공학과 (공학박사)
- 2003년 9월 ~ 현재 : 강원대학교 제어계측공학과 부교수

<관심분야>
정보보안, USN, 임베디드시스템

서 장 원(Jang-Won Seo) **[정회원]**

- 1992년 2월 : 서울산업대학교 컴퓨터공학과(공학사)
- 1996년 2월 : 숭실대학교 대학원 전산공학과(공학석사)
- 2000년 2월 : 숭실대학교 대학원 컴퓨터학과(공학박사)
- 2001년 9월 ~ 현재 : 동서울대학 컴퓨터소프트웨어과 교수

<관심분야>
정보보안, 디지털신호처리

김 영 곤(Young-Gon Kim) **[정회원]**

- 2011년 8월 : 숭실대학교 대학원 컴퓨터학과(공학석사)
- 2011년 9월 ~ 현재 : 숭실대학교 대학원 컴퓨터학과 박사과정

<관심분야>
정보보호, 네트워크 보안, 인증