JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 12 : 2289~2296 Dec. 2016

기본 패스워드와 회원 가입 정보를 이용한 사용자 인증 시스템

정종문[1] · 황민태[2*]

User Authentication System using Base Password and Member Registration Information

Jongmun Jeong[1] · Mintae Hwang[2*]

[1]Dept. of Eco-Friendly Offshore Plant FEED Engineering, Changwon National University, Changwon 51140, Korea
[2*]Dept. of Information and Communication Engineering, Changwon National University, Changwon 51140, Korea

요 약

사용자 계정 발급 시에 적용되는 패스워드 생성 규칙이 웹사이트 별로 다른 경우가 많아 사용자가 패스워드를 기억하기 힘들고 잦은 입력 오류로 인해 패스워드 재설정 단계를 거쳐야 하는 시간 낭비를 초래한다. 이러한 문제를 해결하기 위해 본 논문에서는 사용자 인증 단계에서 패스워드가 일치하지 않는 경우 패스워드 재설정 단계를 거치는 것이 아니라 회원 가입시에 부가적으로 등록한 기본 패스워드와 개인 정보 기반의 추가적인 인증을 거쳐 로그인할 수 있도록 하는 새로운 인증 방식을 제안하였다. 이 방식은 기존의 방식과 동등한 수준의 보안성을 제공하면서도 패스워드 재설정에 따르는 트랜잭션 수나 소요 시간이 절반 정도에 불과해 효율적인 방식으로 볼 수 있다.

ABSTRACT

The password rules to be applied for the user account creation are often different by websites. Thus we often forget the password to sign in website and it creates waste of time for frequent password reset. In order to solve this problem we propose a new authentication method in this paper. When user forget the password to sign in, the existing methods require a password reset step but our proposed method provides new sign in scheme through the additional authentication step with base password and personal information registered at the member sign up stage. From the result of performance comparison the proposed method is considered to be more efficient than others because it provides not only an equivalent level of security with others but also requires only a half of the number of transactions and the time required for password reset step.

키워드 : 기본 패스워드, 단방향 암호화, 사용자 인증, 추가 인증, 트랜잭션

Key word : Base Password, One-Way Encryption, User Authentication, Additional Authentication, Transaction

Received 18 July 2016, **Revised** 22 July 2016, **Accepted** 04 August 2016

* **Corresponding Author** Mintae Hwang(E-mail:professorhwang@gmail.com, Tel:+82-55-213-3832)
Department of Information and Communication Engineering, Changwon National University, Changwon 51140, Korea

Open Access http://doi.org/10.6109/jkiice.2016.20.12.2289 print ISSN: 2234-4772 online ISSN: 2288-4165

ⓒThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

Ⅰ. 서 론

온라인 쇼핑몰, 이메일, 블로그, 온라인 카페 등과 같은 웹사이트를 이용하려면 회원 가입이 필수적인 경우가 많다. 일반적으로 사용자는 가입하는 모든 사이트에 대해 하나의 아이디와 패스워드를 사용하고자 하나 표 1에서 보는 바와 같이 웹사이트마다 회원 가입시에 요구하는 패스워드 생성 규칙이 다르기 때문에 관리에 어려움을 겪기 마련이다.

Table. 1 Password creation rules of websites

Website	Password creation rules
Common	Uppercase, lowercase, numbers and special characters are allowed. Continuity of numbers, continuity of alphabets and similar to ID are not allowed.
NAVER	Not allowed to use numbers only. 6 or more characters but maximum 16 characters.
DAUM	Not allowed to use numbers only. 8 or more characters but maximum 32 characters.
AUCTION & GMARKET	Alphabets and numbers must be used. 6 or more characters but maximum 15 characters.
11STREET	Alphabets and numbers must be used. 6 or more characters but maximum 20 characters.
GOOGLE	8 or more characters.
Changwon National University	Alphabets and special characters must be used. 9 or more characters but maximum 20 characters.

표 1에서 보는 바와 같이 대부분의 웹사이트는 패스워드로 대소문자, 숫자, 특수문자를 사용 할 수 있으며, 알파벳 순서나 숫자 순서와 같이 연속적 이거나 아이디와 비슷해서는 안 된다는 공통적인 규칙이 있다. 하지만 세부 규칙은 제각각이다. 그래서 사용자들은 자신이 항상 기억하고 있는 기본 패스워드에 사이트 규칙에 맞춰 앞뒤에 숫자, 특수문자, 대소문자를 덧붙여서 패스워드를 생성한다. 하지만 가입하는 웹사이트가 한두 개가 아니고, 웹사이트 이외에도 통장 패스워드, 신용카드 패스워드와 같이 기억해야 할 패스워드가 다수 있어 사용자의 암기능력 범위를 초과하는 경우가 많다. 이처럼 웹사이트마다 다른 패스워드를 관리하는 애플리케이션이나 웹사이트도 개발되어 이용되고 있으나 이 또한 아이디와 패스워드를 만들어야 하는 아이러니한 상황이다. 이런 까닭에 웹사이트 방문시에 패스워드를 자주 틀리게 되고 심지어 일정 횟수 이상 틀려서 휴대폰 인증이나 이메일 인증을 통해 패스워드를 재설정 할 때도 많다. 이는 패스워드 관리 측면에서도 보안이 취약해지는 결과를 초래한다.

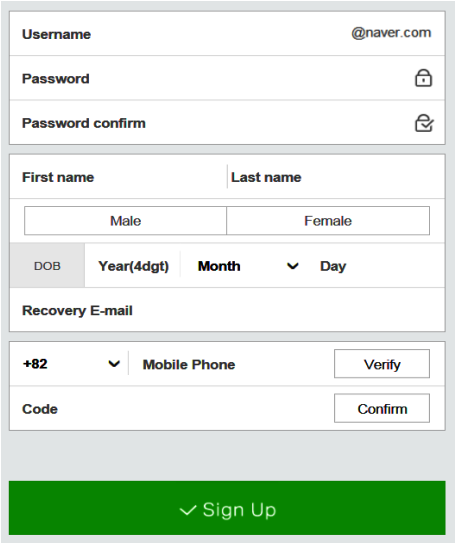

Fig. 1 Sign up procedure of NAVER

일반적으로 사이트에 회원가입시 위의 그림 1과 같이 아이디와 패스워드를 기본적으로 입력받고, 이메일 주소나 휴대폰 번호를 통해 사용자 확인을 하는 방식을 사용한다[1]. 여기서 다른 정보와 달리 패스워드는 MD5 혹은 SHA-2와 같은 단방향 암호화를 이용해 해시값으로 만들어서 DB에 보관하며, 사용자 인증시에 입력한 패스워드에 대한 해시값과 이를 이교해 일치 여부를 판정한다. 단방향 암호화는 사용자의 패스워드를 일정 길이의 해시값으로 암호화해 저장하나 이를 다시 복구할 수는 없는 암호화 방법을 말한다.

본 논문에서는 사용자 인증 단계에서 입력한 패스워드의 해시값이 DB에 저장된 해시값과 일치하지 않더라도 사용자가 지정한 기본 패스워드의 해시값과 일치하기만 한다면 추가적인 인증 단계을 거쳐 로그인할 수 있도록 하는 편리한 인증 메커니즘을 제안하고자 한다.

추가 인증 단계는 스마트폰 인증이나 OTP(One Time Password) 등 여러 종류가 있으나 본 논문에서는 회원 가입 시 입력한 주소, 전화번호, 이메일 등에 대한 간편한 개인 정보 확인을 거쳐 최종적으로 인증을 받도록 하는 시스템을 제안하고자 한다.

본 논문의 구성은 다음과 같다. II장에서는 본 논문에서 제안하는 사용자 인증과 관련된 연구 동향을 소개하며, III장에서는 제안하는 사용자 인증 시스템의 동작 메커니즘을 설명한다. 그리고 IV장에서는 제안하는 사용자 인증 시스템을 구현한 결과를 소개하고, V장에서는 기존의 사용자 인증 메커니즘과의 성능 비교를 다룬다. 마지막으로 VI장에서는 결론을 기술한다.

Ⅱ. 관련 연구

“인터넷 뱅킹 환경에서 사용자 인증 보안을 위한 Two-Channel 인증 방식”은 PC와 모바일 기기에서 이중으로 인증을 받는 방식을 소개한다[2]. PC에서 인증한 거래정보를 모바일 디바이스에 전송하여 2차적으로 인증 받는 시스템으로 중간자공격, 메모리해킹 등에 안전하다. 하지만 모바일 디바이스를 필수적으로 가지고 있어야 한다는 단점이 있다.

“좋아하는 단어를 이용한 암기하지 않는 패스워드 시스템”은 사용자의 암기를 요구하지 않는 선호기호 패스워드 시스템을 제안한다[3]. 이는 선호하는 단어를 몇 단계에 걸쳐 선택하는 것으로 인증하는 시스템으로 기존의 생체정보나 키 스트로크, 마우스 패턴 등보다 설치비용과 사용 편리성면에서 우수함을 보인다. 하지만 무작위 공격에 상대적으로 취약하다는 단점이 있다.

“1Password”는 OS X, Windows, iOS, 안드로이드용 패스워드 관리 애플리케이션이다[4]. 사용자 ID 및 패스워드 정보를 통합 관리하는 기능을 가진 애플리케이션으로 사용자가 원하는 웹사이트의 로그인 정보를 입력해두면 원클릭으로 로그인 할 수 있다. 이 애플리케이션은 모든 정보가 AES 256비트로 저장되고, 다시 관리자 비밀번호로 이중 보안된다. 하지만 이 애플리케이션의 패스워드를 기억해야하고 이 사이트에 보관된 개인 정보가 유출된다면 막대한 피해가 발생 할 수 있다. 또한 이 애플리케이션에서 사용하는 암호화는 단방향 암호화가 아니라 키(Key) 값을 알면 복구가 가능하므로 완벽하게 안심할 수는 없다.

“이동통신단말기를 이용한 사용자 인증 시스템 및 사용자 인증방법”은 비밀번호를 직접 입력하지 않고 스마트폰과 같은 이동통신단말기를 이용해 로그인하는 방법에 대한 특허이다[5]. 인증절차의 간소화와 함께 보안성을 강화하여 개인정보 유출방지를 최소화하는 시스템이다. 하지만 이 방식은 스마트폰을 분실하거나 도난당했을 때의 위험성이 크다는 단점이 있다.

“SMS를 이용하는 개선된 이중 인증 기법”은 SMS를 이용한 양방향 이중 인증의 개선된 기법을 제안하고 있다[6]. 현재의 패스워드 인증 기법이 보안에 약하고 패스워드의 관리가 허술하다는 단점을 해결하기 위해 반응시간을 사용한 OTP 등으로 중간자 공격에서 안전한 새롭고 개선된 인증기법을 제안하였다. 하지만 이 방식 역시 스마트폰을 분실하거나 도난당했을 때의 위험성이 존재한다는 단점이 있다.

“이중 인증 로그인 시스템 및 방법”은 패스워드를 이용한 계정 기반의 기본 인증과 사용자 정보 입력에 의한 실사용자 기반의 인증을 이중으로 수행하는 방법에 대한 특허이다[5]. ID-Password 인증 방식의 취약성을 보안하고 실사용자 식별이 어려운 한계점을 극복할 수 있지만 패스워드를 잊어버렸을 때 여전히 시간 낭비가 크다는 단점이 있다.

사용자 인증 관련 문헌이나 선행 특허 조사 결과 본 논문에서 제안하는 바와 같이 기본 패스워드 개념의 적용이나 추가 인증을 통한 사용자 인증을 제공하는 메커니즘은 소개된 바가 없음을 알 수 있다.

Ⅲ. 제안하는 사용자 인증 시스템

본 논문에서는 회원 가입시에 사이트에서 요구하는 패스워드 생성 규칙에 따라 패스워드를 지정하되, 사용자가 여러 사이트에 공통적으로 사용하는 기본 패스워드를 추가로 지정해 이를 활용한 새로운 사용자 인증 시스템을 제안하고 있다.

이 방식은 그림 2에서 제시한 흐름도에서 보는 바와 같이 웹사이트 인증시 아이디와 패스워드를 입력했을 때 웹사이트의 규칙에 맞는 정확한 패스워드를 입력했으면 바로 인증이 완료된다. 하지만 패스워드가 기억이 나지 않을 경우에는 여러 웹사이트에서 보편적으로 사

용하는 기본 패스워드를 입력한 다음 추가적인 인증을 통해서 인증을 완료하는 시스템이다.

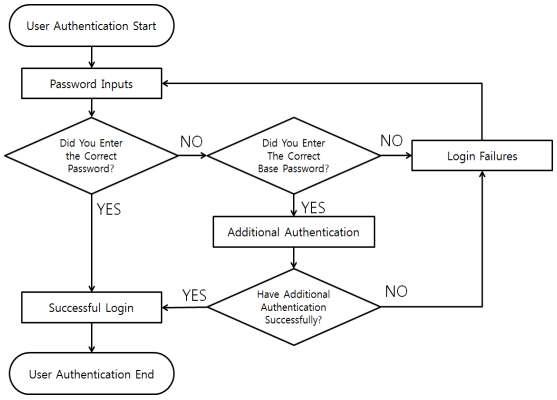

Fig. 2 Flowchart of proposed method

추가 인증은 패스워드 재설정보다는 훨씬 간편해야 할 것이며 사용자가 기억하기 위해 노력해야 할 필요가 없는 정보를 이용해야 할 것이다. 이러한 요구사항에 맞는 추가 인증 방식으로는 보안성이 높은 스마트폰을 통한 SMS 인증이나 OTP와 연동하는 방식이 있으며, 일반적인 방식으로 이메일, 선호 단어 연상 등의 방법이 있다.

본 논문에서는 기본 패스워드만으로도 일반적인 사이트에서 사용자 인증을 위해 사용되는 보안성이 우수한 패스워드라 판단되므로, 기본 패스워드가 일치하는 경우에 추가로 요구하는 인증은 비교적 사용하기 편리한 방식을 사용할 것을 제안한다. 즉, 사용자가 회원 가입시에 등록한 생년월일, 이메일 주소, 휴대폰 번호 등의 일부를 확인하는 방법을 사용할 수 있다.

Ⅳ. 제안 시스템의 프로토타입 구현

본 논문에서 제안하는 기본 패스워드와 추가 인증을 통한 사용자 인증 시스템을 APM(Apache2, PHP, MySQL5) 패키지 V7.0을 설치한 서버 환경에서 HTML, Java Script, CSS 및 PHP 언어를 이용한 웹 프로그래밍을 통해 구현하였다.

그림 3에 기본적인 회원 가입 화면을 보여주고 있다. 테스트용 웹사이트에서 요구하는 패스워드 이외에 기본 패스워드를 필수로 지정하도록 하였다. 이러한 기본 패스워드는 사용자가 여러 웹사이트에 걸쳐 보편적으로 사용하고 있는 패스워드를 지정하는 것으로서 본 웹사이트에서의 패스워드 생성 규칙을 따르지 않아도 되며, 기존의 회원 가입 폼에 하나의 필드 추가만으로 본 논문에서 제안하는 사용자 인증 시스템이 간단히 구현될 수 있음을 알 수 있다.

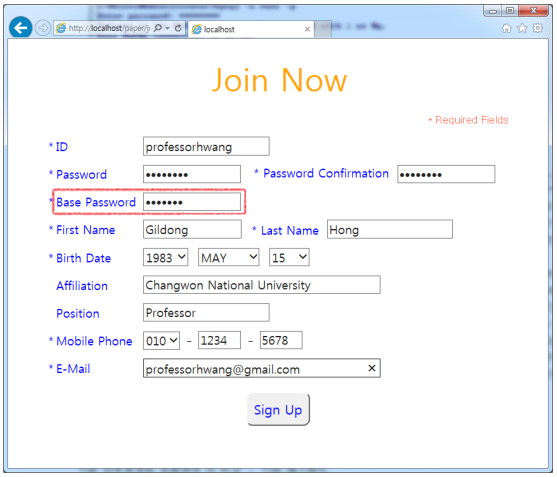

Fig. 3 Sign up including base password

그림 4는 회원 가입 절차를 통해 사용자 개인 정보가 데이터베이스 테이블에 저장되어 있는 모습이다. 웹사이트에서 요구하는 패스워드와 기본 패스워드가 모두 단방향 암호화 기술인 MD5 암호화 방식을 통해 해시값으로 저장되어 있음을 알 수 있다.

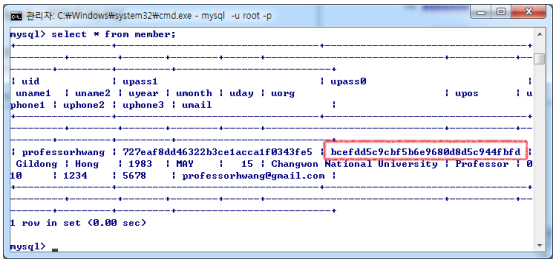

Fig. 4 Encryption of base password in DB

기본적으로 웹사이트의 사용자 인증은 어느 웹사이트와 마찬가지로 사용자 아이디와 패스워드의 입력으로 진행된다. 그림 5와 그림 6에서 보는 바와 같이 아이

디와 패스워드가 일치하는 경우에는 정상적인 로그인 과정이 이루어진다. 이는 사용자가 본 웹사이트에 대한 아이디와 패스워드를 정확히 기억하고 있다는 것을 의미한다.

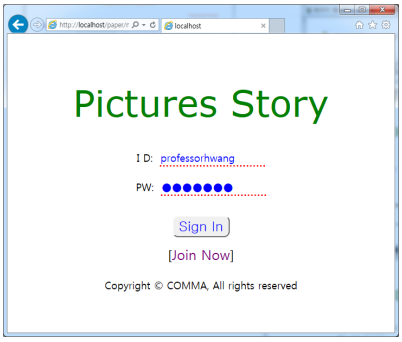

Fig. 5 Login Procedure

Fig. 6 In case of Successful login

일반적으로 사용자가 입력한 패스워드가 웹사이트의 패스워드와 일치하지 않는 경우에는 재입력을 하도록 요구한다. 패스워드 재입력이 성공하는 경우도 있겠지만 틀리는 경우도 다반사이므로 사용자는 불편함을 느끼게 된다.

그러나 본 논문에서는 사용자가 입력한 패스워드가 웹사이트의 패스워드와 일치하지 않더라도 기본 패스워드와의 일치 여부를 추가로 확인한다. 그림 7에서 보는 바와 같이 기본 패스워드와 일치하게 되는 경우에는 그림 8과 같이 사용자가 회원가입 시에 입력한 회원 정보(예: 생년월일, 전화번호, 이메일 주소 등)들 중에서 랜덤하게 선택한 항목을 이용한 추가 인증 단계를 진행하도록 한다.

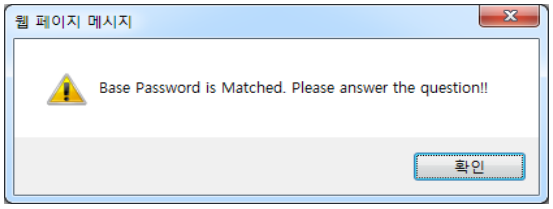

Fig. 7 Notification when base password is matched

Fig. 8 Additional authentication using personal information

그림 9에는 사용자 이름, 이메일 주소 등 다양한 회원가입 정보들 중에서 본인임을 확인할 수 있는 다양한 항목들이 추가 인증 단계에서 활용 가능함을 보여주고 있다. 이미 기본 패스워드만으로도 보편적인 웹사이트에서 이용 가능한 패스워드이기 때문에 추가 인증 단계에서는 사용자가 기억하기 쉬운 항목을 제시하는 것을 권장한다.

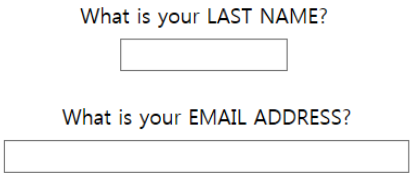

Fig. 9 The other usable personal informations

만약 추가 인증 단계에서 실패하는 경우에는 사용자 인증에 실패한 것으로 간주며, 그렇지 않은 경우에는 정상적인 로그인과 동일한 것으로 간주한다. 다만 구현 선택 사항으로서 그림 10에서 보는 바와 같이 사용자 개인 정보를 수정하는 화면으로 진행할 수가 있다.

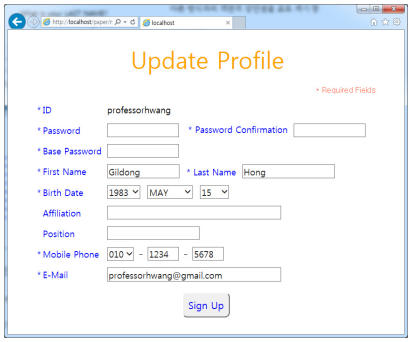

Fig. 10 User profile update procedure

Ⅴ. 제안 시스템의 성능 평가

본 논문에서 제안하는 기본 패스워드를 이용한 사용자 인증 시스템의 성능 평가를 위해 네이버(NAVER)와 다음(DAUM) 포털 사이트의 사용자 인증 시스템[1, 7]과 트랜잭션 수 및 평균 소요 시간 측면에서 비교를 하였다[8].

여기서 트랜잭션 수는 사용자 인증 단계와 인증 실패에 따른 패스워드 재설정 단계를 거치는 과정에서 사용자의 입력(키보드 입력 혹은 마우스 클릭)이 필요한 단계 수를 말하며, 그 예로는 ID 입력, 패스워드 입력, 인증번호요청, 이메일수신, SMS수신, 인증번호입력 등이 있다. 그리고 평균 소요 시간은 이러한 트랜잭션을 거쳐 새로운 사용자 인증에 성공하기 까지 걸리는 평균 소요 시간을 의미한다.

Table. 2 Average time and variance per transaction

Transaction	Average Time	Variance
Input ID and password & Input personal information	3.97s	$0.5s^2$
Input authentication code or CAPTCHA	6s	$1.24s^2$
Click buttons & switch pages	1.61s	$0.03s^2$
Receive SMS	9.27s	$10.69s^2$
Receive email	11.17s	$7.61s^2$

상기 표 2는 기존 포털 사이트의 사용자 인증 과정 및 인증 실패에 따른 패스워드 재설정 과정을 100회에 걸쳐 실시하고서 도출한 주요 트랜잭션별 평균 소요 시간과 분산값을 보여주고 있다. 일반적으로 사용자 인증에 실패하는 경우 대부분의 웹사이트는 패스워드를 재설정 단계를 거치도록 하는데, 이는 SMS를 이용하는 방법, 이메일을 이용하는 방법 그리고 개인정보를 이용하는 방법으로 나눌 수가 있다.

SMS를 이용하는 방법과 이메일을 이용하는 방법은 사용자의 휴대폰 번호나 이메일주소로 인증 번호를 전송한 다음 이를 정상적으로 입력하는 경우 패스워드 재설정 단계를 거치도록 하는 방법이다. 그리고 개인정보를 이용한 방법은 회원 가입시에 입력한 개인정보(본명, 생년월일, 성별 등)를 확인한 후 패스워드 재설정 단계를 거치도록 하는 방법이다.

이러한 세 가지의 사용자 인증 방법과 본 논문에서 제안하는 기본 패스워드를 이용한 사용자 인증 방법과의 트랜잭션 비교 결과는 표 3과 같다.

Table. 3 Transactions of user authentication methods

Transactions \ methods	SMS	Email	Personal Information	Base Password
Input ID	O	O	O	O
Input password (5 times)	O	O	O	O
Click password forgot button	O	O	O	
Input ID again	O	O	O	
Input base password				O
Input personal Information	O	O	O	O
Input phone number	O			
Input email address		O		
Request authentication code	O	O		
Receive SMS	O			
Receive email		O		
Input authentication code	O	O		
Input new password	O	O	O	
Input new password confirm	O	O	O	
Input CAPTCHA	O	O	O	
Input ID again	O	O	O	
Input password again	O	O	O	

여기서 동일한 조건에서 성능 비교를 위해 네 가지 방식 모두 처음 사용자 인증시에 패스워드를 5회 연속 틀린 경우 패스워드 재설정 단계를 밟는 것을 기준으로 하였다. 그리고 이들 네 가지 방식 이외에 패스워드 재설정 단계에서 랜덤한 패스워드를 SMS나 이메일로 사용자에게 제공하는 방식도 있으나 이는 랜덤 패스워드를 사용자가 원하는 패스워드로 수정하는 트랜잭션까지 추가가 되는 방식이라 비교 대상에서 제외하였다.

이러한 네 가지 사용자 인증 방식별 트랜잭션에 대해 앞서 표 2에서 도출한 트랜잭션별 평균 소요 시간값을 대입시켜 표 4와 같은 성능 비교표를 얻어냈다. 여기서 트랜잭션 단계별 화면 전환에 따른 소요 시간은 성능 평가 과정에서 컴퓨터 성능이나 네트워크 상황에 따라 달라지므로 이는 고려 대상에서 제외하였다.

Table. 4 Comparison of authentication methods

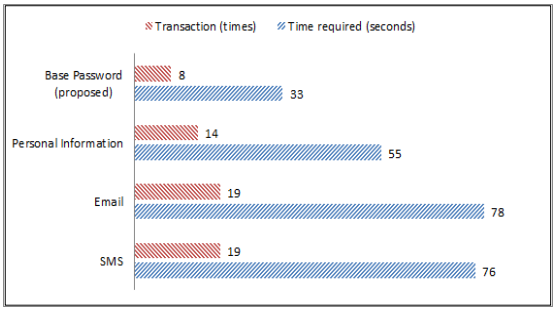

표 3 및 표 4에서 살펴보는 바와 같이 본 논문에서 제안하는 기본 패스워드를 이용한 사용자 인증 방식은 네이버(NAVER)나 다음(DAUM)과 같은 포털 사이트에서 주로 사용하는 SMS나 이메일을 사용하는 방식에 비해 패스워드 재설정에 따르는 트랜잭션 수나 소요 시간이 1/3 정도에 불과함을 알 수 있다. 아울러 개인정보를 이용하는 방식에 비해서도 1/2 정도에 불과해 효율적인 사용자 인증 방식이라 평가할 수가 있다.

그렇다고 해서 다른 세 가지 방식에 비해 보안성이 떨어지는 것은 아니다. 왜냐하면 기본 패스워드는 현재 사이트에서의 패스워드 생성 규칙에 맞지 않을 뿐이지 실제로는 사용자가 대부분의 웹사이트에서 사용자 인증을 위해 사용하고 있는 패스워드이기 때문이다.

Ⅵ. 결 론

본 논문에서는 웹사이트의 사용자 인증 단계에서 패스워드가 일치하지 않는 경우 패스워드 재설정 단계를 거치는 것이 아니라 회원 가입시에 부가적으로 등록한 기본 패스워드와 개인 정보 기반의 추가적인 인증 단계를 거쳐 로그인할 수 있도록 하는 새로운 인증 방식을 제안하였다.

제안하는 방식을 PHP와 MySQL을 이용한 웹 프로그래밍을 이용해 구현하고서 동작 확인을 하였으며, 패스워드 재설정에 따른 트랜잭션 수와 소요 시간 측면에서 기존의 방식과의 성능 평가를 실시하였다.

성능 평가 결과 SMS나 이메일을 사용하는 방식에 비해 패스워드 재설정에 따르는 트랜잭션 수나 소요 시간이 1/3 정도에 불과했으며, 개인정보를 이용하는 방식에 비해서도 1/2 정도에 불과해 효율적인 사용자 인증 방식이라 평가할 수 있었다.

본 논문에서 제안하는 기본 패스워드 이용하는 사용자 인증 방식은 보안성과 편리성을 모두 제공하는 방식이라고 볼 수 있으며, 기존 웹사이트에서도 회원가입 폼을 간단히 수정한 다음 기본 패스워드 처리 알고리즘만 추가함으로써 손쉽게 활용 가능함을 알 수 있다.

ACKNOWLEDGMENTS

This research is financially supported by Changwon National University in 2015~2016.

REFERENCES

[1] NAVER [Internet]. Available: http://www.naver.com/.

[2] H. N. You, J. S. Lee, J. J. Kim, J. P. Park, M. S. Jun, “A Study on the Two-channel Authentication Method which Provides Two-way Authentication using Mobile Certificate in the Internet Banking Environment,” *Journal of the Korean Institute of Communications and Information Sciences*, vol. 36, no. 8, pp. 939-946, Aug. 2011.

[3] K. C. Rim, D. H. Kim, “Non-memorizing authentication system using the preference words,” *Journal of the Korea Institute of Information and Communication Engineering*, vol.

20, no. 3, pp. 565-570, Mar. 2016.
[4] AgileBits [Internet]. Available: https://agilebits.com/.
[5] KIPRIS [Ineternet]. Available: http://www.kipris.or.kr/.
[6] S. S. Ji, "The Improved-Scheme of Two Factor Authentication using SMS," *Journal of the Korea Industrial Information Systems Research*, vol. 17, no. 6, pp. 25-30, Dec. 2012.
[7] DAUM [Internet]. Available: http://www.daum.com/.
[8] D. S. Choi, S. H. Kim, S. H. Jin, "Smart Channel : A Method for Processing Transactions in Smartphone for Authentication, Payment and Digital Signature in N-Device Environment," *Journal of Korean Institute of Information Scientists and Engineers*, vol. 39, no. 6, pp. 506-513, Dec. 2012.

정종문(Jongmun Jeong)

2014 창원대학교 정보통신공학과 공학사
2016 창원대학교 친환경해양플랜트FEED공학전공 공학석사
현재 창원대학교 친환경해양플랜트FEED공학전공 대학원 박사과정
※ 관심분야 : 네트워크 보안, 사용자 인증, 안드로이드 응용

황민태(Mintae Hwang)

1990 부산대학교 컴퓨터공학과 공학사
1992 부산대학교 컴퓨터공학과 공학석사
1996 부산대학교 컴퓨터공학과 공학박사
1996 한국전자통신연구원 표준연구센터 선임연구원
1999 인제대학교 정보컴퓨터공학부 교수
현재 창원대학교 정보통신공학과 교수
※ 관심분야 : 안드로이드 응용, 매체접속제어 프로토콜, 사물인터넷 응용 기술