산업융합연구 제21권 제9호 pp. 49-56, 2023
ISSN 2635-8875 / e-ISSN 2672-0124
DOI : https://doi.org/10.22678/JIC.2023.21.9.049

단수 계정에 다중 권한 부여가 가능한 다중 해시값 기반의 안전한 패스워드 인증 기법 설계

문형진*
성결대학교 정보통신공학과 조교수

The Secure Password Authentication Method based on Multiple Hash Values that can Grant Multi-Permission to a Single Account

Hyung-Jin Mun*
Assistant Professor, Dept. of Information & Communication Engineering, Sungkyul University

요 약 개인별 서비스를 위한 ID 기반 인증으로 ID가 식별정보로 활용되고, 패스워드가 사용자 인증에 사용된다. 안전한 사용자 인증을 위해 패스워드는 클라이언트에서 해시값으로 생성하여 서버에 전달되고 서버에 저장된 정보와 해시값을 비교하며 인증을 수행한다. 하지만 패스워드의 해시값은 패스워드에서 한 개라도 틀리면 전혀 다른 해시값이 생성되어 사용자 인증에 실패하여 패스워드에 의한 다양한 기능을 적용할 수 없다. 본 연구에서는 입력된 패스워드의 해시값을 허수를 포함하여 여러 개 생성하고 서버에 전송해서 인증을 수행한다. 또한 제안 기법에서는 여러 권한을 가진 사용자가 하나의 계정으로 다양한 권한을 부여받을 수 있도록 패스워드에 따라 권한을 차등적으로 부여할 수 있다. 제안 기법을 통해 허수 패스워드를 생성함으로써 엿보기 공격을 차단하고, 패스워드 기반으로 권한을 부여하므로 다양한 권한을 가진 사용자에게 편리성을 제공할 수 있다.

키워드 : 사용자 인증, 해시함수, 다중 해시, ID 인증, 접근 권한

Abstract ID is used as identifying information and password as user authentication for ID-based authentication. In order to have a secure user authentication, the password is generated as a hash value on the client and sent to the server, where it is compared with the stored information and authentication is performed. However, if even one character is incorrect, the different hash value is generated, authentication will be failed and cannot be performed and various functions cannot be applied to the password. In this study, we generate several hash value including imaginary number of entered password and transmit to server and perform authentcation. we propose a technique can grants the right differentially to give various rights to the user who have many rights by one account. This can defend shoulder surfing attack by imaginary password and provide convenience to users who have various rights by granting right based on password.

Key Words : User authentication, Hash function, Multiple hash, ID authentication, Access authority

*Corresponding Author : Hyung-Jin Mun(jinmun@gmail.com)
Received August 26, 2023 Revised September 20, 2023
Accepted September 20, 2023 Published September 28, 2023

1. 서론

ICT(Information and Communication Technology) 발달과 스마트 폰의 보급으로 다양한 통신 서비스가 가능하게 되었다. 스마트 폰 사용자 인증 기법은 2007년 LG의 터치 스크린 기반 스마트 폰의 출시로 인해 다양한 인증 기법에 제시되고 있다.

대표적인 사용자 인증으로 ID 기반 인증과 PIN 인증기법을 보편적으로 사용하고 있다. PIN(Personal Identification Number) 인증 기법은 짧은 길이의 숫자로 사용자인증하는 방식으로 은행 뱅킹서비스 등에서 비밀번호로 많이 사용하는 방식이다. ID 기반 인증은 패스워드 인증이라고도 부르는 데 ID로 사용자를 식별하고, 입력된 패스워드로 사용자를 인증하는 방식으로 대중화된 스마트 폰의 사용으로 많은 금융거래가 이를 이용하여 이루어지고 있다. 하지만 스마트 폰이 무선 통신으로 단말기의 스크린 기반으로 인증을 수행하지만 크기가 작아 패스워드나 PIN을 입력하는 과정에서 발생 가능한 보안 취약점이 존재한다. 스마트 폰을 이용한 금융거래을 위해 안전성이 높고, 편리한 인증 기술이 요구되고 있다.

스마트 폰의 사용자 인증에서 문자서비스를 통한 피싱(Phishing)이나 스미싱(Smishing) 공격, 엿보기 공격(Shoulder surfing attack)과 같은 사회공학기법이 스마트 폰이라는 단말기의 특성에 의한 공격에 취약하다. 사회공학기법을 이용한 다양한 방법으로 악성코드를 설치하도록 유도하여 키로깅 공격(Keylogging Attack)과 같은 공격이 빈번하게 발생하고 있다[1-4]. 다양한 공격으로부터 안전한 거래를 위해 많은 인증 기술이 제안되고 있다. PIN 및 패스워드 인증, SMS 문자 기반 인증, FIDO (Fast IDentity Online) 생체인증을 통해 인증을 수행한다[5].

스마트 폰의 스크린이 커짐에 따라 사용자가 스크린에 PIN을 입력하는 과정에서 공격자가 어깨 너머로 직접적인 관찰로 정보를 획득하는 기법인 엿보기 공격(Shoulder-Surfing Attack)이 가능하다[6-8].

레코딩 공격은 엿보기 공격과 비슷하지만 사용하는 도구에 차이가 있다[7]. 레코딩 공격은 스마트 폰의 카메라와 같이 광학의 영상기록장치를 통해 정보를 획득하는 방식이다. 취득한 영상을 반복 재생이나 확대 기능을 통해 입력한 정보를 취득할 수 있어 공격의 성공률이 높다. 레코딩 공격을 차단하기 위해서는 동일한 패스워드 사용에 대한 취약점을 극복해야 한다.

기존 ID인증 방식은 하나의 ID와 연결된 패스워드를 기반으로 사용자 인증 이외의 기능을 제공하지 않는다. 정보시스템의 데이터베이스에 있는 회원정보테이블에 등록된 ID가 어떤 권한이 결정되어 인증 후에 ID로 접속한 사용자에게 권한이 부여된다. 즉, 패스워드는 ID에 일대일로 종속된 방식이다. 본 연구는 ID 한 개에 여러 개의 패스워드를 생성하여 패스워드에 따른 다중 권한 부여가 가능한 방안을 제안하고자 한다. 제안기법에서는 패스워드를 허수로 입력하거나 여러 개 사용하므로 엿보기 및 레코딩 공격을 차단할 수 있다.

본 논문에서는 허수의 패스워드 입력과 다중 패스워드 해시값을 기반으로 권한 부여 방식을 통한 엿보기 공격을 차단하는 기법을 제안하고자 한다. 다중 패스워드 기반 인증을 위한 요구사항이 필요하다.

- 기존 인증 시스템에서 인증 기법의 적용이 가능하여야 한다.
- 다중 패스워드의 해시값 생성으로 인한 오버헤드가 발생하지 않아야 한다.
- 스마트 폰 등에서 엿보기나 레코딩 공격 등에 대한 안전성이 보장되어야 한다.
- 패스워드 인증을 통해 사용자 인증 이외의 추가적인 기능을 제공하여야 한다.

2. 관련 연구

2.1 사용자 인증

사용자가 정보의 접근 및 사용을 위해 정당한 사용자인지 확인하기 위해서는 사용자 인증이 필요하다. 사용자 인증 방식은 다양하게 존재한다. 인증 방식은 지식 기반 인증(what you know-패스워드), 소유기반 인증(what you have-신용카드, 핸드폰 인증), 객체 특성기반 인증(what you are-생체인증)으로 구분하는데 본 연구에서는 소유기반 인증과 객체특성 기반 인증을 살펴보고, 지식기반 인증의 새로운 접근으로 고찰해 본다,

2.1.1 소유기반 인증

소유기반 사용자 인증(what you have-신용카드, 핸드폰 인증)은 사용자가 가지고 있는 소유물을 확인하는 인증기법이다. 인증에 사용되는 소유물은 신분증, 암호화키, 스마트 폰, 신용카드, OTP 등이 활용될 수 있다. 패

스워드 기반으로 인증한 후 추가 인증 기법으로 소유기반 인증인 SMS 인증이나 OTP 인증을 요구한다.

2.1.2 객체 특성기반 인증

객체인 사용자의 특성 기반인증((what you are-생체인증)으로 대표적인 방법으로 생체인증이 있다. 지문, 홍채 등 다른 사용자와 다른 구별된 특성을 가지고 인증하는 방식이다. 최근에는 Face ID를 이용하여 스마트 폰에서 카메라로 사용자의 얼굴을 인식하여 소유자를 확인하고, 스마트폰 사용 및 접근을 허용하고 있다.

2.1.3 지식기반 인증

지식기반 인증은 사용자만 알고 있는 지식을 기반으로 인증하는 방식으로 PIN이나 ID/Password 인증 등이 있다. ID기반 인증은 ID와 짝이 되는 패스워드가 입력되었을 때 인증 성공여부가 결정되며, 패스워드 기반인증이라고 한다. ID기반 인증 기법은 Fig. 1과 같이 일반적으로 ICT 기반의 모바일 단말기 또는 PC의 웹 브라우저를 통해 인증을 시도한다. 사용자는 자신의 ID와 패스워드를 APP를 통해 입력한다. 입력된 패스워드의 해시값을 생성하여 ID와 함께 서버에 전달한다. 전송된 ID를 기반으로 사용자를 식별하고, 해당 ID에 연결된 패스워드의 해시값과 전송받은 패스워드 해시값과 비교하여 같으면 사용자 인증되고, 같지 않으면 인증 실패하는 방식이다[9].

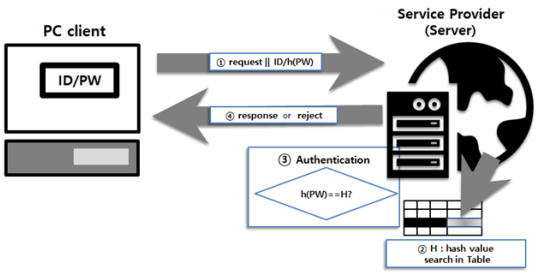

Fig. 1. Password based authentication method

패스워드 기반 인증의 안전성은 1차적으로 패스워드의 길이와 무작위성에 의존한다. 2차적으로는 패스워드가 저장된 테이블의 안전성에 좌우된다. DB 관리자나 내부자와 연계된 공격자가 회원정보가 담겨있는 DB 테이블을 유출하여 해시값으로부터 사용자의 패스워드를 유추하는 레인보우 테이블 공격(Rainbow Table Attack)을 수행할 수 있다. 사용자의 패스워드에 대한 레인보우 테이블 공격을 차단하기 위해 패스워드의 해시값 생성에 SHA-256이나 SHA-512 등 안전한 해시함수를 사용한다[10].

하지만 2차적 안정성을 보장하기 위해 안전한 해시함수를 사용하더라도 1차적으로 사용자가 패스워드를 입력할 때 어깨 너머로 훔쳐보기나 구글 글래스 등으로 패스워드를 입력할 때 녹화하는 방식으로 공격이 가능하기 때문에 사용자는 무작위의 패스워드를 길게 생성해야 한다[3,4]. 엿보기 공격이나 레인보우 테이블 공격을 차단하기 위해 패스워드 생성 시 복잡성을 요구하고 있다.

최근, 사용자의 스마트 폰을 이용한 SMS(문자서비스)나 OTP을 이용한 인증 기법, 큰 규모의 웹사이트나 포털 등을 이용한 3자 인증, 공동인증서나 I-PIN 등을 통한 인증하는 방법으로 발전하고 있다[9].

3. 제안 기법

3.1 허수가 반영된 다중 해시 생성 기반 인증

사용자가 패스워드를 입력할 때 공격자가 훔쳐볼 수 있기 때문에 시스템에서 패스워드의 길이를 8 또는 10 이상을 요구한다. 사용자가 시스템에서 지정한 임계치보다 패스워드의 길이가 길어질 때마다 해시값을 생성하여 서버에 전달하여 인증을 수행한다.

패스워드의 길이를 8 이상을 요구하는 시스템에서 ID는 “hong”이고, 패스워드가 “password1!” 인 사용자가 로그인할 때, 사용자는 ID를 입력하고, 패스워드 칸에 자신의 패스워드가 아닌 “password1!2”를 입력할 수 있다. 이 경우 클라이언트에서는 패스워드의 길이가 8이상부터 패스워드의 해시값을 생성한다. 즉, “password1!2”에 대한 해시값인 h(“password”), h(“password1”), h(“password1!”)와 h(“password1!2”) 같이 다수의 해시값을 생성하여 인증을 위해 서버에 ID와 함께 전송한다. Fig. 2는 클라이언트에서 사용자가 계정을 입력하고, 그 정보와 함께 추가적인 해시값이 생성되어 서버로 전달되고, 인증하는 과정을 보여주고 있다. 서버에서는 수신 받은 모든 해시값을 순서대로 비교하여 인증을 수행한다. Fig. 2에서는 입력된 패스워드의 길이가 11이므로 8일 때부터, 9, 10, 11까지 4개의 해시값을 생성하였다. Fig. 2 와 같이 사용자가 패스워드에 허수가 포함할 수 있기 때문에 공격자의 엿보기 공격으로부터 안전하게 패스워드를 입력할 수 있다.

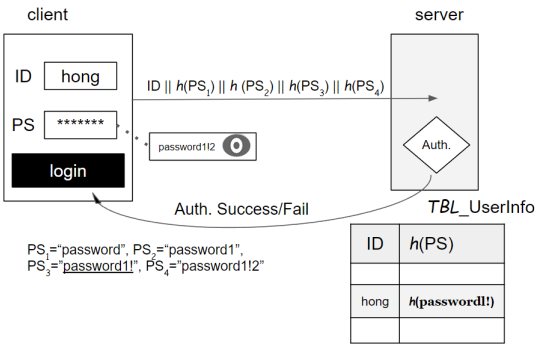

Fig. 2. Multi-password ID-based authentication

3.2 등록된 패스워드에 따른 권한 부여

정보서비스를 제공하는 시스템에는 많은 사용자와 각기 다른 권한과 역할이 부여된다. 사용자 별로 역할에 따라 정보 접근 권한의 차이가 존재한다. 정보시스템의 운영 및 관리 등 필요에 의해 한 사용자가 여러 권한과 역할을 갖는 경우가 있어 여러 개의 계정을 소유할 수밖에 없다. 특히, 관리자의 경우, 여러 가지 역할과 권한이 주어진다. 관리를 위해 관리자 권한에서 사용자 권한으로 변경할 필요가 있다. 이 경우 관리자는 현재 계정을 로그아웃하고 변경할 계정으로 ID와 패스워드를 입력하여 다시 로그인해야 하는 불편함이 존재한다.

제안 기법은 여러 권한을 가진 사용자가 같은 계정으로 사용자가 입력된 패스워드에 따라 권한을 차등적으로 부여할 수 있다. Fig. 3는 하나의 ID에 여러 개의 패스워드를 가지고 있고, 각 패스워드마다 권한이나 역할이 다름을 보여주고 있다. Fig. 3에서는 PSn이 가장 넓은 역할로 권한이 가장 큰 관리자 권한으로 부여되고, PS1는 가장 작은 접근 권한이 부여되어 있다. 일반 사용자 또는 준회원이 PS1이 부여된 사용자로 볼 수 있다. PS2와 PS3과 같이 경우에 따라 권한이 포함관계가 아닌 교차 권한로 정보 접근이 허용될 수 있다. 예를 들어 패스워드에 따라 사용자, 수퍼 사용자, 관라자로 권한을 부여할 수 있다.

Fig. 4는 사용자가 ID와 패스워드를 입력하여 패스워드에 맞는 권한을 부여하는 과정을 보여주고 있다. 사용자가 ID와 패스워드를 입력하면 입력된 패스워드의 해시값을 생성하고, 정보시스템인 서버에 전달한다. 서버는 전송받은 ID를 기준으로 패스워드가 사전에 등록된 패스워드 목록에 있는지 확인하는 과정을 수행한다. 서버는 사용자 등록하는 과정에서 사용자의 여러 권한 및 역할에 맞게 패스워드의 목록을 받아 저장이 되어 있다. 사용자 인증과정에서 입력된 패스워드(해시값)가 사전에 등록된 패스워드 목록(해시값)에 있는지 확인하는 과정은 Fig. 4와 같이 순서대로 비교한다. 입력된 패스워드가 i번째 패스워드와 같으면 i번째 권한이 부여되고, n번째까지 비교해서 없으면 인증에 실패한다.

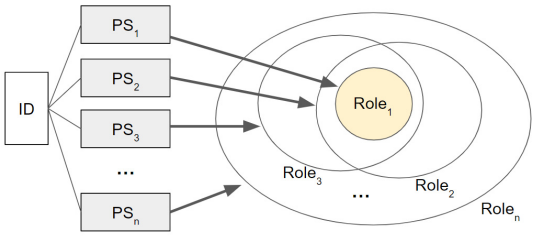

Fig. 3. Assign different roles based on passwords

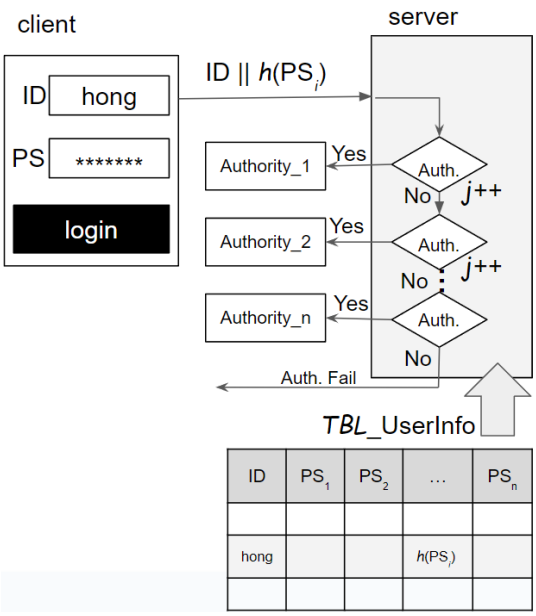

Fig. 4. The process of granting authorization based on passwords

4. 제안 기법 프로토콜

4.1 허수 기반 다중 해시 생성 프로토콜

ID을 인증할 때 사용자가 입력된 패스워드에서 여러 개의 패스워드를 추출하고, 그에 따른 해시값을 생성한다. 클라이언트에서 생성된 여러 개의 해시값을 서버에 전송하고, 서버에서는 인증을 수행하여 일치하는 해시값이 있는지 확인하여 인증을 수행한다. 여러 개의 패스워

드 중에서 하나의 패스워드의 해시값으로 인증이 된다. Fig. 5는 사용자가 허수를 포함한 패스워드를 입력하여 다중 해시값을 생성하여 인증하는 과정을 나타낸 순서도이다.

step 1. 사용자는 허수가 포함된 패스워드를 입력한다. 패스워드의 길이에 대한 임계치보다 큰 경우 임계치부터 계속적으로 패스워드의 해시값을 생성한다. 예를 들어 임계치가 10이고, 입력된 패스워드의 길이가 15라면 클라이언트에서는 6개의 해시값을 생성한다. 그 해시값 중에 사용자가 사전에 등록된 패스워드가 포함되어 있다.

step 2. ID와 여러 개의 패스워드의 해시값들을 서버로 전송한다. 시스템은 사용자의 ID를 통해 TBL_UserInfo 테이블에 저장된 패스워드의 해시값($h(PS^*)$)를 조회한다.

step 3. TBL_UserInfo 테이블로부터 받은 해시값을 클라이언트로부터 전송받은 해시값과 비교한다. 같으면 사용자 인증이 완료된다. 같지 않으면 클라이언트로부터 받은 다음 해시값을 다시 TBL_UserInfo로부터 받은 해시값과 비교한다. 클라이언트로부터 전송받은 해시값의 개수만큼 반복적으로 비교를 수행한다.

step 4. 클라이언트로부터 전송받은 모든 해시값과 비교하여 같지 않으면 인증이 실패된다.

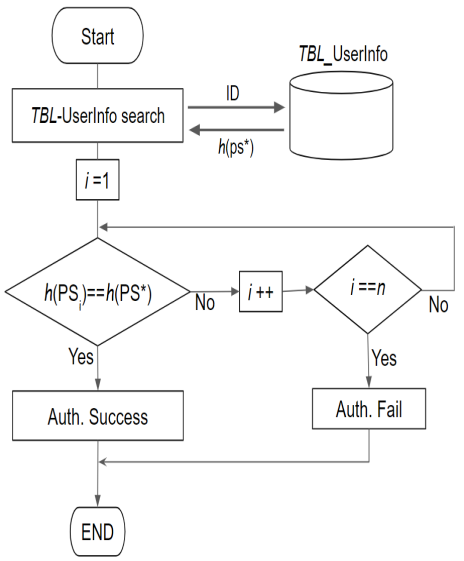

Fig. 5. The authentication process using multiple hashes

4.2 등록된 패스워드에 따른 권한 프로토콜

4.2.1 다중 패스워드 가입 과정

다중 패스워드를 이용한 권한을 차별적으로 부여하기 위해서는 사용자가 가입 시 추가 절차가 필요하다.

회원 가입 시 1개의 자신의 권한을 가진 사용자라면 각 권한별 패스워드를 지정해야 한다. Table 1은 ID가 "hong"인 사용자가 가지고 있는 여러 계정을 보여주는 예시이다. 패스워드마다 해시값과 권한이 정보시스템의 회원정보테이블에 저장되어 있다. 예시 Table 1에서는 관리자, 슈퍼유저, 유저, 손님 계정으로 구분하였지만 시스템에 따라 복잡하고 다양한 권한을 부여할 수 있다.

Table 1. Examples of the relationship between passwords and permissions

ID	Password	h(Password)	Authority
hong	password1	E38A~~DA3D	root
hong	pass123!	8E45~~C904	super user
hong	pword123	747F~~2C74	user1
hong	pword1!	86EE~~6F76	user2
hong	pass1!2	6816~~F996	guest

4.2.2 로그인 화면에서 패스워드에 따른 권한 부여

여러 개의 권한을 가진 사용자가 권한에 따른 계정을 생성하는 방식은 계정 관리가 불편하다. 제안 기법에서는 여러 권한을 가진 사용자에게 패스워드 별로 권한을 차등적으로 부여하는 방식을 활용한다[11].

예를 들어, 시스템에서 관리자, 일반 사용자 등 여러 개의 권한에 대한 등급이 있고, 시스템에 접속한 사용자가 여러 개의 계정을 가지고 있는 현재 시스템에서 제안 기법을 통해 1개의 아이디에 여러 개의 패스워드를 기반으로 여러 개의 권한을 부여받아 수행할 수 있다. 사용자는 자신에게 필요한 권한에 맞는 패스워드를 기억하고 인증 시 해당 패스워드를 입력한다.

다음은 정보시스템의 인증 서버에 로그인하기 위해 회원정보테이블(TBL_UserInfo)에서 ID는 "hong"이고, 패스워드는 입력된 패스워드의 해시값("h(ps)") 인 레코드를 검색하는 SQL문이다.

```
select * from TBL_UserInfo ID="hong" and PS1=h(ps);
```

Fig. 6은 정보시스템의 사용자가 인증을 위해 로그인하는 화면을 보여주고 있다. 일반 사이트와 다르게 사용

자 역할을 선택하는 옵션이 존재한다. Fig. 6는 관리자 권한으로부터 일반 사용자 권한까지 제시되었고, 기본은 일반 사용자에 체크된 화면이다. 로그인할 때 역할을 선택한 후에 인증을 수행할 수 있다.

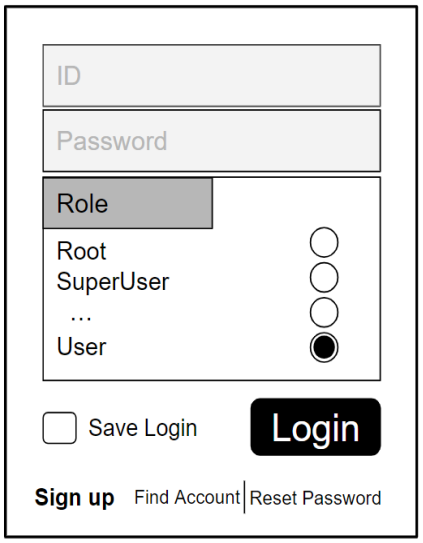

Fig. 6. The user log-in view

Fig. 6처럼 사용자는 ID와 패스워드를 입력하고, 역할은 선택한 후 로그인을 하면 서버로 ID와 함께, 패스워드, 역할(Role) 3가지 정보가 전달되고, ID와 역할을 기반으로 해당 해시값을 TBL_UserInfo 테이블에서 조회하여 입력된 해시값과 비교하여 인증을 하고, 역할에 맞는 접근 권한을 부여한다.

4.2.3 회원테이블에서 패스워드에 따른 권한 부여

패스워드에 따른 접근권한을 차등적으로 부여하는 시스템 구현 방법으로 다른 방법은 패스워드의 해시값을 일일이 비교하여 사용자의 권한 또는 역할을 찾아 접근권한을 부여하는 방식이 있다.

Fig. 7은 일반 사이트의 로그인 창을 통해 ID와 패스워드를 입력했을 때 패스워드로 역할을 찾는 방법을 순서도로 보여주고 있다. 즉, Fig. 7은 패스워드에 따른 정보 접근 권한을 부여하는 과정을 나타내고 있다.

step 1. 사용자는 권한에 맞는 패스워드와 함께 ID를 입력하여 로그인한다.

step 2. 서버에 전송된 ID를 TBL_UserInfo 테이블에서 조회하여 ID에 연결된 패스워드의 해시값들을 사용자에게 입력된 패스워드의 해시값과 비교한다.

step 3. 테이블에서 가지고 온 첫 번째 해시값을 사용자가 입력한 패스워드의 해시값과 비교하여 같으면 사용자 인증에 성공하고, 첫 번째 접근 권한을 부여한다.

step 4. 첫 번째 해시값과 같지 않으면 TBL_UserInfo에 저장된 두 번째 패스워드의 해시값을 사용자가 입력된 패스워드의 해시값과 비교하여 인증을 수행한다.

step 5. 인증에서 실패하면 step 4를 TBL_UserInfo에 저장된 패스워드의 해시값의 개수만큼 반복적으로 수행한다. 즉, 사용자의 접근 권한의 개수만큼 반복을 수행한다. 계속하여 인증을 수행하여 성공하면 해당 해시값에 맞는 접근권한을 부여하고, 입력된 패스워드의 해시값이 TBL_UserInfo의 모든 패스워드 해시값과 같지 않으면 사용자 인증에 실패한다.

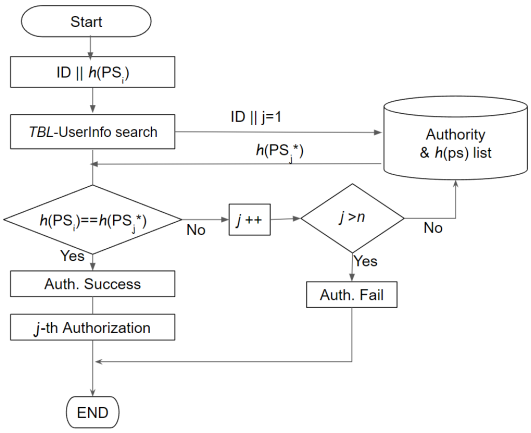

Fig. 7. The grant process based on multiple password

5. 분석 및 평가

패스워드 기반의 인증은 사용자 식별과 인증 이외에 기능이 존재하지 않고, 패스워드를 입력하는 과정에서 훔쳐보기 등의 공격에 취약할 수 밖에 없다. 기존의 패스워드 한 개를 이용하여 인증하고, 거기에 맞는 권한을 부여하는 방식에서 여러 개의 패스워드를 이용하여 식별 및 인증 이외의 기능을 제공할 수 있다. 제안 기법은 여러 개의 패스워드를 이용하여 2가지 기법을 제공하여 정보시스템의 기능과 요구사항에 따라 각기 다른 기능을 제공할 수 있다. 하나는 다양한 패스워드를 통해 패스워드 별로 다른 권한을 부여하여 사용자가 여러 권한을 가지도록 할

수 있다는 점이고, 또 하나는 패스워드를 입력하는 과정에서 엿보기 공격으로 안전하게 정확한 패스워드의 노출 없이 인증할 수는 점이다.

본 논문에서는 다중 패스워드를 기반으로 권한 부여 및 엿보기 공격을 차단하는 기법으로 서론에서 제시된 요구사항을 만족한다. 첫째, 기존 인증 시스템에서 인증 기법의 적용이 가능하다. 본 제안 기법은 클라이언트에서만 해시값을 생성하는 과정이 수행되고, 하나의 인증코드가 전송되는 것이 아니라 여러 개의 패스워드 해시값이 전송된다.

둘째, 제안 기법에서는 하나의 ID에 여러 개의 패스워드에 대한 해시값을 생성하지만 N번의 해시값 생성에 따른 속도는 평균 시간복작도가 O(1)을 유지한다. 셋째, 진짜 패스워드가 무엇인지 서버에서 확인하기 때문에 어깨너머로 엿보기나 스마트폰으로 녹화하는 레코딩 공격 등으로부터 안전하다.

6. 결론

스마트 폰의 보편적인 사용으로 핀테크 환경에 다양한 서비스를 위해 사용자 인증 기술이 다양하게 제안되어 사용되고 있다[12].

본 논문에서는 PC 환경 뿐만 아니라 스마트 폰에서 안전한 사용자 인증을 효율적으로 수행하고 또한, 인증과정에서 다양한 기능을 제공할 수 있는 다중 해시값을 이용한 ID 및 패스워드 인증기법을 제안하였다.

인증을 위해 입력한 패스워드의 다중 해시값으로 2가지 기능을 제공한다. 다양한 패스워드를 통해 패스워드별로 다른 권한을 부여하여 사용자가 여러 권한을 가진 경우 사용할 수 있는 기능이다. 또한 패스워드를 입력하는 과정에서 엿보기 공격으로 안전하게 정확한 패스워드의 노출 없이 인증할 수 있다.

향후에는, 제안 기법을 통해 시스템 구현 및 안전성과 효율성에 최적의 패스워드 길이 및 다중 해시 생성에 대한 연구가 필요하다.

REFERENCES

[1] B. S. Yu & S. H. Yun. (2011). The Design and Implementation of Messenger Authentication Protocol to Prevent Smartphone Phishing. *Journal of the Korea Convergence Society,* 2(4), 9-14. DOI : 10.15207/JKCS.2011.2.4.009

[2] D. Y. Kim & S. M. Cho (2015). A Proposal of Smart Phone App for Preventing Smishing Attack. *Journal of Security Engineering,* 12(3), 207-220.

[3] S. H. Kim, M. S. Park. & S. J. Kim. (2014). Shoulder Surfing Attack Modeling and Security Analysis on Commercial Keypad Schemes. *Journal of the Korea Institute of Information Security & Cryptology,* 24(6), 1159-1174. DOI : 10.13089/JKIISC.2014.24.6.1159

[4] I. Y. Choi, J. H. Choi & W.Y. Lee. (2014). A Design and Implementation of a Solution for Real Detection of Information Leakage by Keylogging Attack. *Journal of Korea Multimedia Society,* 17(10), 1198-1204. DOI : 10.9717/KMMS.2014.17.10.1198

[5] C. J. Chae, H. J. Cho & H. M. Jung. (2018). Authentication Method using Multiple Biometric Information in FIDO Environment. *Journal of Digital Convergence,* 16(1), 159-164. DOI : 10.14400/JDC.2018.16.1.159

[6] Y. S. Jeoung & D. M. Choi (2017). D-PASS: A Study on User Authentication Method for Smart Devices. *The Journal of the Korea Institute of Electronic Communication Sciences*, 12(5), 915-922. DOI : 10.13067/JKIECS.2017.12.5.915

[7] D. M, Choi.(2021). A Study on User Authentication Method for Foldable Screen-Based Devices. *Journal of Korea Multimedia Society,* 24(3), 440-447. DOI : 10.9717/kmms.2022.25.7.932

[8] D. M, Choi. (2022). Design of Smartphone Secure Keypad Using Indirect Pattern. *Journal of Korea Multimedia Society*, 25(7), 932-944. DOI : 10.9717/kmms.2022.25.7.932

[9] H. -J. Mun & M. -H. Lee.(2022). Design for Visitor Authentication Based on Face Recognition Technology Using CCTV. *IEEE Access,* 10, 124604-124618. DOI : 10.1109/ACCESS.2022.3223374.

[10] H. J. Mun, S. H Hong & J. P. Shin.(2018). A novel secure and efficient hash function with extra padding against rainbow table attacks, *Cluster Computing,* 21(1), 1161-1173. DOI : 10.1007/s10586-017-0886-4.

[11] H. J. Mun.(2016). Apparatus and Method for

Allocating Role and Permission based on Password, Patent. DOI : 10.8080/1020150001799

[12] H. J. Mun. (2023). Analysis on the trends of PIN Input Method of Mobile Device in Fintech Environment. *Quality of Life Research,* 1(1), 33-38.

문 형 진(Hyung-Jin Mun) [종신회원]

- 1996년 2월 : 충남대학교 수학과
- 2008년 2월 : 충북대학교 전자계산학(이학박사)
- 2009년 3월~2012년 8월 : 중국 연변과학기술대학교 컴퓨터전자통신학부 조교수, 부교수
- 2017년 3월~현재 : 성결대학교 정보통신공학과 조교수
- 관심분야 : 정보보호, Fintech 보안, 사용자 인증, 보안키패드
- E-Mail : jinmun@gmail.com