# An Innovative Two Factor Authentication Method: The QRLogin System

Soonduck Yoo*, Seung-jung Shin and Dae-hyun Ryu

*Dept. of IT, University of Hansei,*
*604-5 Dangjung-dong Gunpo city, Gyeonggi do, Korea,*
*harry-66@hanmail.net, expersin@hansei.ac.kr, dhryu@hansei.ac.kr*

## *Abstract*

*For over the past 10 years, the overwhelming majority of online login required only an ID and password, which classifies as one factor authentication. In response to rising cyber-security concerns, firms and banks have implemented several new forms of two factor authentication. This paper focuses on QRLogin, one of the leading two factor authentication programs, which successfully balances security with convenience. The system combines the traditional username and password with a time-sensitive, one time passcode. In contrast to this advanced security, users may conveniently login by scanning a code with their smartphone. Although the scanning feature of the QRLogin system is limited to smart phone owners, users may also login through the traditional ID and password method. The QRLogin system illustrates the modern development of two factor authentication, which substantially increases the security of online transactions. We encourage further research cyber-security to foster consumer confidence and growth in online markets.*

***Keywords:*** *Authentication, Account Control, Hacking, Telecommunication, Security*

## 1. Introduction

As information technologies develop, users store more personal information online, raising the importance of cyber-security. To motivate our research into authentication, we first explore different types of security risks. After identifying the threats, we analyze developments within the two factor authentication system. Specifically, we are interested in the use of smartphones to generate a One Time Password (OTP). Recent technological advances in telecommunications have inspired the replacement of tokens with smartphones, increasing the ease of use and accessibility of OTP systems. To empirically analyze these developments in depth, we perform a case study of the QRLogin, one of the leading forms of smart phone OTP systems. Within our case study we identify similarities and differences between the QRLogin systems and traditional OTP systems. For example, instead of entering a 6 to 8 digit code generated by a unique token, the QRLogin system allows users authenticate themselves by scanning a QR code on the website with their smart phone. These new developments within telecommunications and two factor identification systems are significantly increasing the application of security systems to protect personal information. We can expect innovative systems that connect smart phones and personal security such as the QRLogin system to play a major role in developing more secure user accounts and internet transactions.

## 2. A Motivation for authentication systems: Hacking

Most people use ten or more sites on average and remembering a unique password for each site is not easy. Before delving into alternatives to memorizing several strings of numbers, we will explore various security threats. The types may be loosely divided into 1) System hacking, 2) Network hacking, 3) Web hacking, 4) Wiretapping, and 5) Wireless lan hacking. System hacking, also known as memory hacking, is the most classic way to steal information from hardware and software. Memory hacking may be loosely defined as counterfeiting and tampering with stored data. Traditional hacking focuses on stealing an account password; however, memory hacking depends on installing an application such as a backdoor. These have been commonly used to steal passwords and money from bank accounts. The most prevalent type of memory hacking program is the key logger. However, the most well-known method is Network hacking, where attackers penetrate an entire network and steal information. Similarly, hackers web hack by installing foreign programs on targeted sites to steal client information. Despite these advanced techniques, one of the most effective ways for hackers to gain access to a user's PC is through viruses hidden in emails. All of these concerning security threats provide the motivation for our research in advances to cyber-security.

## 3. One Time Password (OTP) Service

### 3.1 Two Factor Authentications

There are three commonly classified levels of verification. The first and most common is a simple ID and password. The second level requires additional verification, such as a personal item (mobile phone, token, security card and *etc.*). The final level demands the use of the user's biological information, such as a finger print, face recognition and etc. Two factor authentication systems combine two of the three levels of verification. One typical example of two factor authentication is a combination of the first level, ID and password, and the second, an OTP (One Time Password) [2]. Currently, smart phones are the most common source of the OTP. In the next section, we will discuss one time passwords in detail.

### 3.2 OTP service

The development of the One Time Password (OTP) system significantly increases the security of websites and minimizes the potential of unauthorized access. To log in, users are required to first enter their user name and password. After the one factor identification, the second layer of security requires inputting an OTP. Although the username and password remains constant, the OTP systematically changes. The OTP algorithm creates a 6~8 digits (1,000,000 ~ 100,000,000) number to authorize each login. Even if the user's login and password leaks, the OTP will prevent any unauthorized access.

These OTP systems are unique to each user. When a user registers to the system an OTP seed is embedded in the unit/device and the server system. Therefore users have unique OTP systems within their devices, guaranteeing their individual protection and connection to the system.

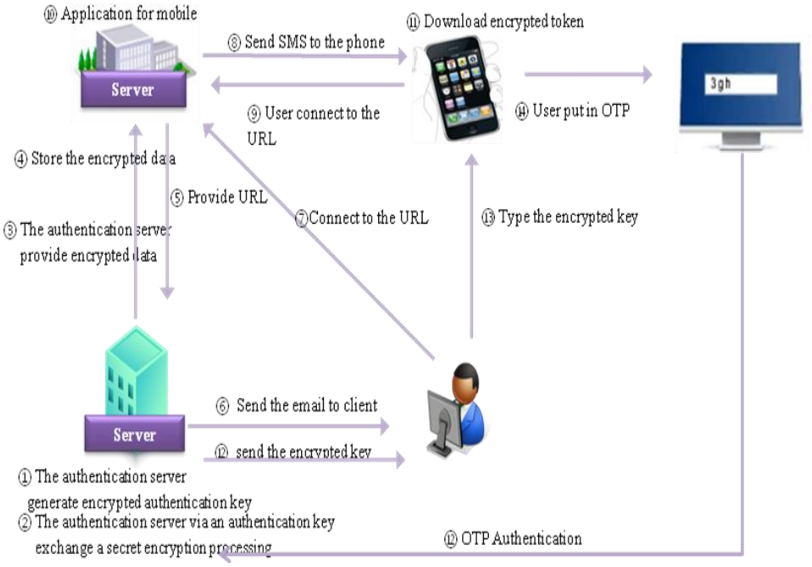
⑩ Application for mobile
Server
⑧ Send SMS to the phone
⑪ Download encrypted token
⑨ User connect to the URL
⑭ User put in OTP
3gh
④ Store the encrypted data
⑤ Provide URL
③ The authentication server provide encrypted data
⑦Connect to the URL
⑬ Type the encrypted key
Server
⑥ Send the email to client
⑫ send the encrypted key
① The authentication server generate encrypted authentication key
② The authentication server via an authentication key exchange a secret encryption processing
⑫ OTP Authentication

**Figure 1. OTP Login Process with Mobile Phone**

Despite the complexity of the system, the user's device may be as common as a mobile phone, token, card, or voice-activating. All of these devices may be designed to generate an OTP from the algorithm. In contrast the IC cards and voice-activating OTP generators are much safer, but cost money to set up and time to manage.

### 3.2 Account Verification through OTP

We have analyzed the details of generating an OTP and potential devices to house the OTP algorithm. Now we will relate this analysis to current market applications of OTP authentication systems.

First, common OTP formats consist of random numbers, images in conjunction with letters, QR code, and *etc*. However, the majority of OTP keys are 6~8 randomly generated numbers/letters.

Secondly, OTP keys serve two distinct purposes: verify access to a site and authenticate logins. OTP codes may be used to verify one's membership to a website before entering a unique username and password. In contrast, OTP codes may also be used after entering a username and password to provide an additional level of security. Both purposes are common within the marketplace.

Thirdly, most OTPs require users to manually code for authentication, but more advanced OTP devices immediately authenticate a user, once the device is connected to the system. For example, as soon as a mobile phone with an OTP algorithm is connected to a PC, the user may be verified automatically. Even though users have to carry the devices as well as connection cables for mobile verification, this automatic authentication protects users from key logger hacking. Since the user never types in any personal information, such malicious hacking is thwarted.

Fourthly, there are 2 common ways to exchange data between the system and users. One way is to issue the OTP key and deliver it by SMS (short messaging system) to user for each log in. The other, more sophisticate, method is to use synchronized data between the server and OTP generating device after setting up the initial connection. For example, the popular use of smart phones as devices allows for a costless synchronization between the server and device. The smart phone simply needs to install an application using smart phone as installing the application. This low cost and ease of use have propelled the smart phone method as the preferred market application.

Fifthly, although the common methods of OTP key generation require manual entry of the code, automatic verification systems do exist. These automatic systems may be generated by the PC or a mobile phone, allowing the user instant authentication. The benefits include convenience and additional protection from key logger hacking.

Finally, as an additional precaution to OTP authentication, the system may send an SMS to check with the user before and after login. An example of such a failsafe verification message is "ooo site login is competed on a.m. 12:30." These messages are sent to verify both login and logout, providing the user with a sense of security and confirmation. This method allows the user to be actively involved in guaranteeing the strong security of his or her account. Furthermore, if unauthorized access does occur, then the user may quickly report the breach and reduce any potential damage. The following Figure 2 illustrates the safety of the system, but also the tradeoff with convenience. The balance between ease of use and security is essential for any such system.

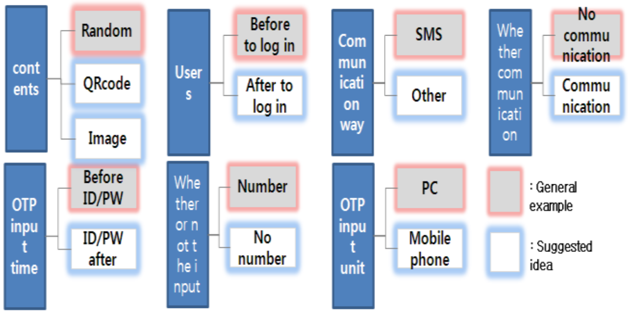

**Figure 2. Classification Authentication Form using OTP**

### 3.3 OTP Account Verification Advantages and Disadvantages

Security systems developed two factor authentication systems to solve the problem of hacking, which one factor authentication system was exceedingly susceptible to. The typical applied example of two factor authentication is the OTP system. Although the OTP provides strong security, the system is complicated and not easy to use. Even as a two factor authentication system, the OTP algorithm may be exposed to hacking, especially if users lose their OTP generating unit. In the specific case of the event synchronization method, the OTP may be leaked or exposed from memory hacking technologies that target the system. Despite the millions of combinations that would be required to brute force hack the OTP, the lack of a time limitation of many OTPs exposes the system to “fishing.” Hackers will attempt to exploit this open window of time to steal OTP codes. To address these issues, the modern market applies event and time specifications, which limits the login time. Even with these potential problems, the OTP system provides the strongest security for user authentication with current technologies. Thus, the OTP system is used throughout the online market.

## 4. QRlogin Service

### 4.1 Defining the QRLogin System

With the advent of smart phones, the accessibility and need of advanced authentication systems have increased. The currently prevalent OTP method is inconvenient to use and taxing on the memory. Individuals must keep track of personalized usernames, passwords, and devices. A developing alternative to the OTP is the QRLogin system. The uniqueness of the QRLogin stems from the QR code, which may be scanned by a user to verify membership. The traditional barcode contains information in only one direction, but the Quick Response Code (QR Code) contains two-way information (horizontal and vertical), allowing for increased security. With the prevalence of smart phones, users may easily scan a QR code through their mobile phone. The flexible QR Code may be used for online as well as offline markets. Furthermore, the use of such a unique image based code circumvents the common access points of hackers. This newly developed method presents an innovative way to maintain a high degree of security, without sacrificing ease of use.

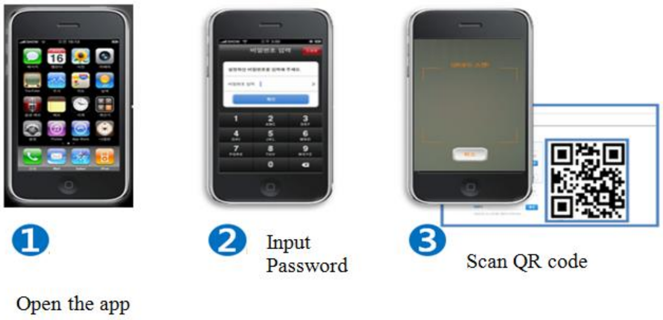

Figure 3. Login Window on the Web Site

### 4.2 How to Register and Use QRLogin

Here, we will discuss how to register and use the QRLogin system. When users register membership to a site, they must identify QRLogin as the preferred login method. In the registration process, each site will request unique information to register. Once the information is provided, click the QRLogin authentication button. In contrast to this manual method, users may conveniently download a QRLogin application, which performs a similar function. After supplying the necessary information, a link will open, providing an introduction of the QRLogin system with a QR code. Users need only scan the QR code with their mobile phone to access the QRLogin website where they may install the program. Upon finishing the registration process, the user will receive a confirmation SMS, verifying that the mobile phone is properly registered with the system. The QRLogin authentication procedure may be described as follows: (1) the server system displays the QR code containing the OTP value, (2) the user scans the QR code with a mobile phone, and (3) the user chooses from a list of accounts associated with the QR code. During the authentication process, the QRLogin system uses a secure communication protocol. As soon as users scan the QR code on the site, the OTP key, phone number and IP address are delivered to the server system through a wireless network, which are then compared with the generated OTP values. These OTP values are time sensitive, allowing the server to verify the user and immediately, but safely, log the user in. The phone number and IP address add more layers of security because the information serves as device specific identifiers. Despite all of these complicated security mechanisms, the QRlogin conveniently does not require the user to manually type an ID and password. To summarize the above-mentioned processes:

(1) Login request

(2) The website server recognizes the request

(3) An OTP is generated

(4) The server delivers the OTP Key through a QR code

(5) The user scans the QR code with a smart phone

(6) The user's information is transferred to the server

(7) The server authenticates the information

(8) After a successful authentication, the user is automatically logged in

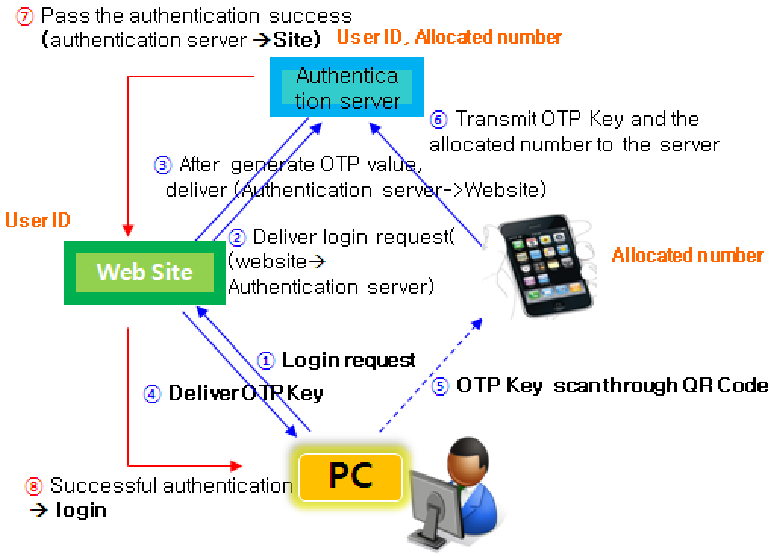
⑦ Pass the authentication success
(authentication server →Site)
User ID, Allocated number
Authentica tion server
⑥ Transmit OTP Key and the allocated number to the server
③ After generate OTP value, deliver (Authentication server->Website)
User ID
Web Site
② Deliver login request( (website→ Authentication server)
Allocated number
① Login request
④ Deliver OTP Key
⑤ OTP Key scan through QR Code
⑧ Successful authentication
→ login
PC

**Figure 4. QRLogin Authentication Process**

This system is one of two channels of authentication that users request to login and then it is allowed auto login by mobile verification with using 2 channels; the website and mobile phone.

Here, we delve into more detail about the data generating process of the QRLogin system (See Figure 5). When users open the website to login, they find the QRcode on the site, which contains the one time passcode (OTPx), server time (CTx,) serial number (SNx) and quick response code (QRCx). Upon accessing the website, the system registers the serial number, trial number (xth trial) and the site location information (PCx). When the user logins, the authentication server generates the necessary information: OTPx, CTx, SNx and PCx. By simply scanning the QRcode on the site, all of this information is delivered to the user's mobile phone. The phone responds with the user's mobile information, which includes the mobile product number (MPx) and the user's phone number (MIDx). As an added level of security, the authentication server checks the verification request time (RTx). To maintain security and user convenience, the delay time (DTx) between the verification request time and server time is less than 1 minute (1 > DTx = RTx – CTx). However, the delay time may be changed to meet the needs of various applications and institutions. This time-sensitive nature of the data substantially decreases the risk of security breaches. Consequently, the QRLogin system effectively employs two channel security, without sacrificing user convenience.

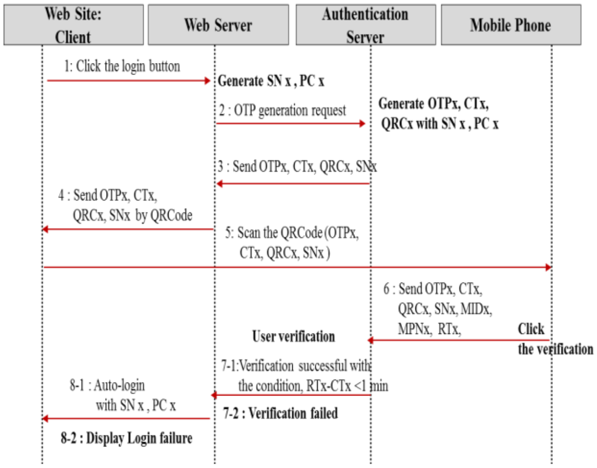
Web Site: Client
Web Server
Authentication Server
Mobile Phone
1: Click the login button
Generate SN x , PC x
2 : OTP generation request
Generate OTPx, CTx, QRCx with SN x , PC x
3 : Send OTPx, CTx, QRCx, SNx
4 : Send OTPx, CTx, QRCx, SNx by QRCode
5: Scan the QRCode (OTPx, CTx, QRCx, SNx )
6 : Send OTPx, CTx, QRCx, SNx, MIDx, MPNx, RTx,
Click the verification
User verification
7-1:Verification successful with the condition, RTx-CTx <1 min
8-1 : Auto-login with SN x , PC x
7-2 : Verification failed
8-2 : Display Login failure

**Figure 5. QRLogin Authentication Data Process**

### 4.3 QRLogin Platform

The QRLogin platform effectively extends the security of 2 factor authentication, while incorporating user friendly features. The platform works off of two systems, the mobile application and the server system. The mobile application system consists of a PIN (Personal Identity Number, application login password here we consider MID, MPN), a validation module, a communication system to connect the mobile and the server system, and a scanning system to recognize the QR code. The QRLogin system connects with the mobile by joining the mobile's information management module. Through this connection a QR code is transmitted to the mobile device. However, much of the work occurs within the server system of QRLogin. For example, a membership module manages the users' information, an authentication module verifies the users, an OTP generating module creates the OTP code, a website module stores site information, and a QR Code generates the image to be scanned. Of these modules, the OTP generator module is most important because this module generates the security codes. These codes are essential for secure authentication and safe logins. The QR code module simply transforms the information into an easy to use, scan-able image for the user. Thus the security of the QRLogin system depends on the OTP generator module.

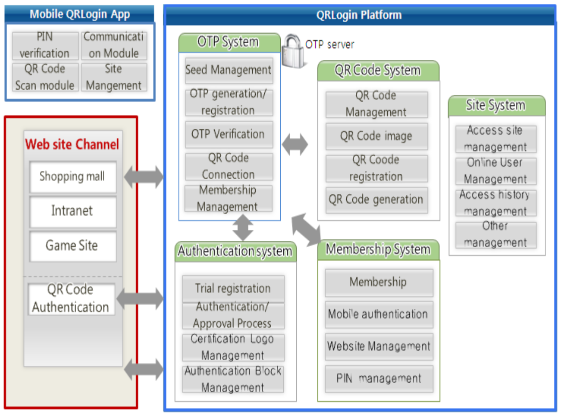

**Figure 6. QRLogin System Configuration, PIN: Personnel Identification Number (MID:Mobile Number, MPN:Mobile Product Number)**

### 4.4 A Comparative Feature Analysis of QRLogin

To illustrate the strengths of the QRLogin system relative to other cyber-security systems, we comparatively assess its features. Many commercial websites use one channel authentication, which verifies users through one measure. Although this verification may use an OTP, the login occurs only through the website. However, the QRLogin system utilizes a two channel authentication method: the user requests login at the web site, but the verification occurs in a secure system. This multilayered security is a focal point of our research (See Figure 7). Table 1 compares the strengths and weaknesses the QRLogin system.

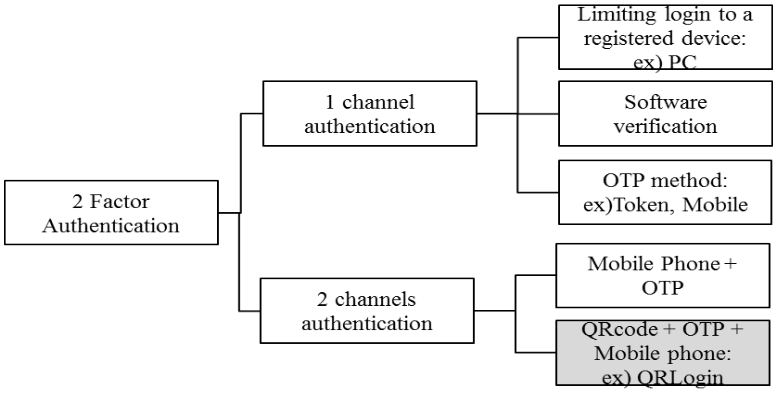
2 Factor Authentication
1 channel authentication
2 channels authentication
Limiting login to a registered device: ex) PC
Software verification
OTP method: ex)Token, Mobile
Mobile Phone + OTP
QRcode + OTP + Mobile phone: ex) QRLogin

**Figure 7. The classification diagram of 2 factor authentication**

**Table 1. The strength and weakness of QRLogin**

| Strengths of QRLogin | Weaknesses of QRLogin |
|---|---|
| - Easy to use and user friendly interface<br>- Enhances security by applying OTP and QRCode through a registered smartphone<br>- Utilizes 2 channel verification<br>- Prevents advanced hacking techniques<br>- Easy to implement with any system because of a flexible module<br>- Easily accessed and joined by users | - Requires a smartphone<br>- User need to install the application on their phone. |

The three major factors to the success of such applications are ease of use, security and cost effectiveness. However, there are significant tradeoffs between the three. In this paper, we emphasize the QRLogin method, which innovatively uses smart phone technology to scan QR codes and grant automatic authentication. Therefore the QRLogin system combines the convenience of a smart phone with the security of a two factor OTP system. Furthermore, the cost-effective system does not require users to purchase separate verification devices. Table 1 shows the similarities and differences between OTP and QRLogin systems.

**Table 2. A comparison of mobile OTP and QRlogin authentication methods**

| Classification | | OTP | QRLogin |
|---|---|---|---|
| Process | Type ID/PW | Yes | No |
| | Process on the mobile | Open OTP application<br>OTP Key generation | - Run QR scanning application<br>- Scanning QR code<br>- Choose the account |
| | Type the key | Yes | No |
| Security | Use ID/PW | Yes | No |
| | Key | Random number | Random QR Code |
| | Input value on PC | Type the OTP key | No |
| Easy to use | | | Easy to login by scanning |
| Mobile | Units | 3G and smart phone | Only smart phone |
| Cost | | SMS type-Charged<br>Application type-free | Application type-free |

## 5. Conclusion

As information technologies such as smart phones develop, the threat of hacking grows in conjunction. More specifically, online account verification is a growing hot issue because of several well publicized hacking incidents of large Korean firms. In this paper, we discussed account authentication methods and the related hardware/software. Outdated and unsecure methods of authentication include the static one factor ID and password. In contrast, modern methods involve dynamic components such OTP (One Time Password) systems, which are commonly used in the market. Although dynamic OTP systems provide much more security than one factor authentication, the complexity renders the system a hassle to use. For example, a user needs to install the application and type the OTP key for every verification. Today people want an authentication method with both security and as ease of use. To address this demand, we suggest the QRLogin system. The unique aspect of the QRLogin system is that it allows automatic login through the scanning of a QR code by a smart phone. Within the QR code developed by the secure website is an OTP key. By scanning the code, the smart phone stores the QR code and transmits the mobile phone number, IP address and the OTP Key to the server system. Upon verification of this information, the server automatically logs the user in. Thus, the QRLogin system provides easy of use as well as strong security. Even though the QRLogin method requires a smart phone, the market applications for the system are immense. We encourage further research into the development of user verification technologies within internet security systems, especially since online security systems play a significant role in the growth of online markets.

## References

[1] S. Park, “Mobile Authentication System and It's Application based on 2-Dimensional Barcode and OTP”, Hanyang University in Korea, **(2009)**.

[2] S. -i. Cho, “Stream Cipher-based OTP Authentication Protocols using Clock-Counter”, Dongseo University in Korea, **(2010)**.

[3] Y.-s. Kim, “Memory hacking Countermeasures Utilized OTP for Secure E-banking Transaction”, Soonsil University in Korea, **(2008)**.

[4] S. Yoo and J. -I. Kim, “Open markets and FDS(Fraud Detection System)”, The Institute of webcasting internet and telecommunication, vol. 11, no. 5, **(2011)**, pp. 113~130.

[5] J. Jang, “A study on Security Management of Payment System in Internet commerce”, Konkuk University in Korea, **(2007)**.