Development of A Secure Authentication Mechanism based on FIDO and OTP

Bing-Ruei Yang [#1], Takafumi Hayashi [#2], Neil Yuwen Yen [#3]

[#]*Computer Network Systems, The University of Aizu*
Aizu-Wakamatsu City, Fukushima-ken 965-8580, Japan

[1]yung.binray@gmail.com
[2]takafumi@u-aizu.ac.jp
[3]neilyyen@u-aizu.ac.jp

Abstract—**Our lives are changing from a wide range of online services over the Internet. Currently, the penetration of the Internet is high. However, the information technology was progress that makes the threshold of the attack skill of the network be reduced. The attackers are gradually increasing on the Internet, they creak accounts, passwords and especially confidential data from end users in order to obtain improper benefits. Using passwords to prevent such attacks is one of the solutions at present. But however, the longer the password is, it becomes more difficult for users to remember it. Therefore, this study comes up with an authentication mechanism based on the one-time passwords and biometric for the identity authentication. The mechanism improves the level of security of the authentication, and make the user quickly finish the authentication. The method captures the biometric of the user, and encrypt it by different codebook for each authentication for the concept of one-time passwords. Simultaneously, the codebook will be disassembled, the user need to get two combination key for the codebook. The combination key is encrypted by different symmetric key for that reducing the risk of the crack. Moreover, there use many hash function and symmetric-key encryption in the mechanism for the security, so the mechanism not only improve the level of the security, but also quickly finish the authentication.**

Keywords—**one-time passwords, biometric, information security, identity authentication, dynamic passwords**

1. INTRODUCTION

The development of the Internet is fast. There have many service on the Internet. The Internet makes convenient of the life, and affect our life so much. For example, Alphabet Inc. provides Google search engine, Gmail, Youtube [11-13]. Naver corporation provides communication service [16]. Dropbox Inc. provides the cloud service [14]. Facebook Inc. provides social service [15]. Those also are common online service which saves much information of the user. Therefore, it makes a convenient of our life, and generate many businesses.

The online service has a common characteristic, the service also needs an account, if the service need save the information of the user. Relatively, the user needs many accounts, if the user uses many services. And an account is cracked, other account will be cracked, if the password strong of the user is not enough, and other account and password is same. The user need to remember many passwords, if the user uses different passwords. Moreover, the attacker covets the information of the user, and try to steal the data, such as replay attack, man-in-the-middle attack, impersonation attack and etc., if the account save many data. The data are maliciously using. For example, unauthorized purchases on the credit card, personal data is trafficked or the user is counterfeited for the bilk.

Based on the reason, the study proposes a mechanism for that resolve weak passwords problem and multiple sets of password problem. The second section introduces related work. In the third section, we introduce our mechanism, and describe how to operate. We analysis the performance of the mechanism, and describe how to mutual authentication, the codebook has how many kinds of change in the fourth section. The fifth section is attack analysis. Finally, sixth section describes our contribution and improving direction in the future.

2. RELATED WORK

One-time passwords that have two characteristics, one is the timing, another one is the metering [2, 3, 4, 7, 10]. Due to the characteristics, so it is usually used for the identity authentication. For example, Chun-Ying Huang et al, they propose a mechanism through the instant messaging service to transfer one-time passwords in the limit time. The mechanism that has three roles, one is the user, one is the web site and another one is the instant messaging service. The mechanism that has two process, one is the registration process and another one is the login process.

(1) The registration process, as shown in Fig. 1.

Step 1a. The user login to his instant messaging account.

Step 1b. The web site login to his instant messaging account.

Step 2. The user send a login request to the web site.

Step 3. The web site send a message that the web site need the account of instant messaging of the user.

Step 4. The user sends his account of instant messaging to the web site.

Step 5. The web site sends what a challenge of CAPTCHA.

Step 6. The user is conducted for the challenge of CAPTCHA.

Step 7a. The web site shows what a login page for the one-time passwords.

Step 7b. The web site new the account of the user to his list of the user of the instant messaging service.

Step 8. The instant messaging service of the web site send a request to the user for new it to list.

Step 9. The user confirms the request.

Step 10. The instant messaging service of the web site show a message that the user has been new to your list.

Step 11. The the web site sends a one-time password to the user.

Step 12. The instant messaging service of the web site sends a one-time password to the user.

Step 13. The user input the one-time passwords at the login page.

Step 14. The web site shows the result of the verification.

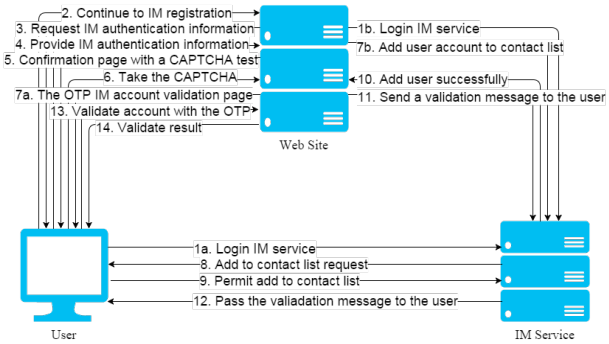

Fig. 1 The registration process of the mechanism of Chun-Ying Huang et al

(2) The login process, as shown in Fig. 2.

Step 1a. The user login to his instant messaging account.

Step 1b. The web site login to his instant messaging account.

Step 2. The user sends a login request to the web site.

Step 3. The web site shows what a login page.

Step 4. The user input his account and code of CPATCHA.

Step 5a. The web site shows what a page of the authentication for the one-time passwords.

Step 5b. The the web site sends a one-time password to the user.

Step 6. The instant messaging service of the web site sends a one-time password to the user.

Step 7. The user input the one-time passwords at the login page.

Step 8. The web site shows the result of the verification.

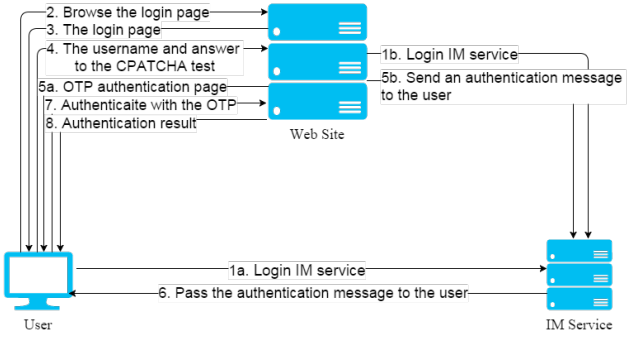

Fig. 2 The login process of the mechanism of Chun-Ying Huang et al

Mohsin Karovaliya et al [6], they propose a mechanism through short message service to transfer one-time passwords in the limit time. The mechanism that has two roles, one is the user and another one is the ATM (automated teller

machine), as shown in Fig. 3. This is the steps of the login:

Step 1. The user inserts the ATM card with the reader.

Step 2. ATM calculates the people is over one or not front ATM by the camera of ATM.

Step 3. ATM is comparison the user front and the user of card holder that is same or not.

Step 4. The server sends one-time passwords to the phone of the holder through SMS.

Step 5. The user input the passwords to ATM. ATM judge the one-time passwords is true or not. The user need to re-enter, if the one-time passwords is an error. And the card is blocked, and notifies the user, if the user over three errors.

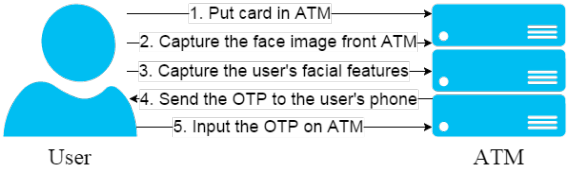

Fig. 3 Mechanism of Mohsin Karovaliya et al

Hyun-Chul Kim et al [2], they propose a mechanism through certificate and public key encryption [1, 2, 5, 6] verify the identity and protect the package. The mechanism that has four roles, they are the user, CA (certification authority), RA(registration authority) and the service provider. The mechanism that has four process, namely, "certificate issuance and registration", "user registration", "user authentication" and "password authentication".

(1) Certificate issuance and registration, as shown in Fig. 4.

Step 1. The user request certificate registration with RA.

Step 2. RA transfer user information to CA.

Step 3. CA save user information in the database.

Step 4. CA transfer reference number and approval code to RA.

Step 5. RA transfer reference number and approval code to the user.

Step 6. The user request certificate with CA.

Step 7. CA transfer certificate to the user.

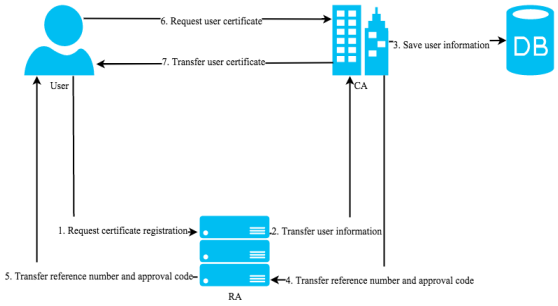

Fig. 4 Certificate issuance and registration of Hyun-Chul Kim et al

(2) User registration, as shown in Fig. 5.

Step 1. The user transfers ID and certificate to the service provider.

Step 2. The service provider request certificate status with CA.

Step 3. CA check the certificate status in the database.

Step 4. CA response certificate status with the service provider.

Step 5. The service provider register ID and certificate information in the database.

Step 6. The service provider response registration result with the user.

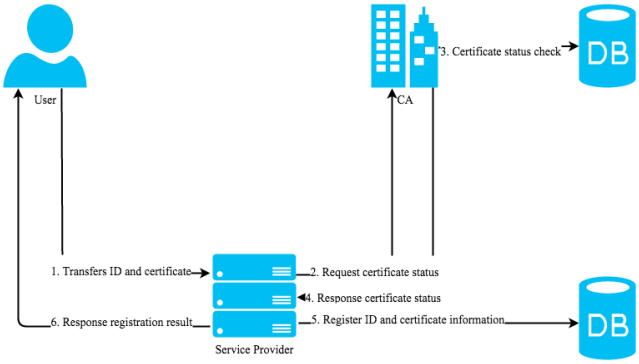

Fig. 5 User registration of Hyun-Chul Kim et al

(3) User authentication, as shown in Fig. 6.

Step 1. The user transfers its own ID to service provider and requests the information to generates one-time password.

Step 2. The service provider generates label L, random value R and symmetry key K.

Step 3. The service provider encrypts L, UII1 and K by the public key of CA, and transfer it to CA.

Step 4. CA decrypts it, and get L, UII1, K.

Step 5. The service provider generates HLU1.

Step 6. The service provider encrypts HLU1 by K, and transfer it to CA.

Step 7. CA decrypts it, and get HLU1.

Step 8. CA generates HLU2, and comparison HLU1 and HLU2.

Step 9. CA check the certificate status.
Step 10. CA encrypts CS and L by K, and transfer it to the service provider.
Step 11. The service provider decrypts it, and get CS and L.

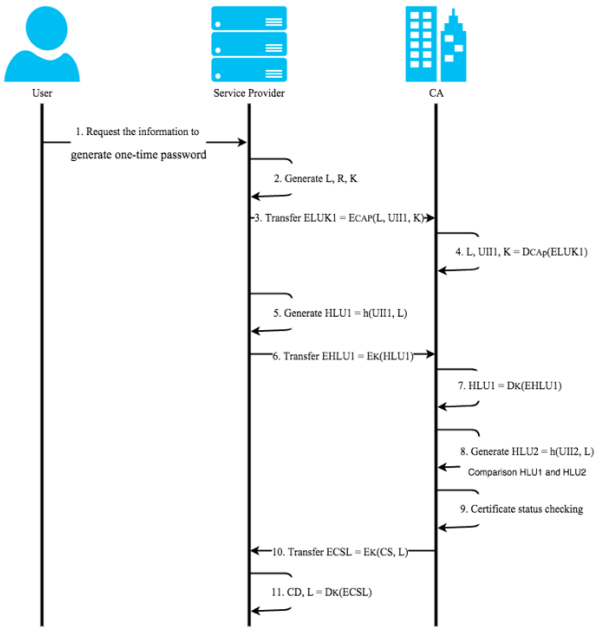

Fig. 6 User authentication of Hyun-Chul Kim et al

(4) Password authentication, as shown in Fig. 7.
Step 1. The service provider encrypts L and R by the public key of the user, and transfer it to the user.
Step 2. The user decrypts it, and get L, R.
Step 3. The user generates GP.
Step 4. The user encrypts GP by the private key of the user, and get DSGP.
Step 5. The user encrypts DSGP by the public key of the service provider, and get EDSGP.
Step 6. The user transfer EDSGP to the service provider.
Step 7. The service provider decrypts EDSGP, and get DSGP.
Step 8. The service provider decrypts DSGP, and get GP.
Step 9. The service provider generates GP1.
Step 10. The service provider comparison GP and GP1.
Step 11. The service provider response authentication result with the user.

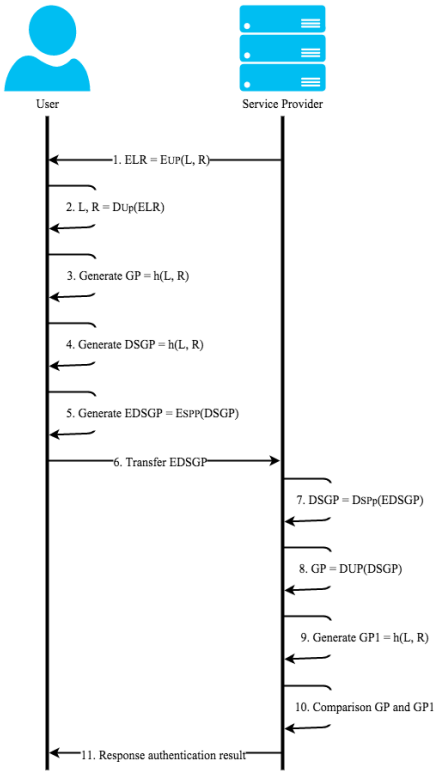

Fig. 7 Password authentication of Hyun-Chul Kim et al

Three scholars that each one proposed a secure authentication mechanism using one-time passwords. The mechanism of Chun-Ying Huang transfers the one-time passwords through instant messaging service. However, the one-time passwords are a plaintext, when the web site transfers the one-time passwords to the user. Therefore, the attacker can easily get the one-time passwords, when he knows which one is the transmission path. Mohsin Karovaliya et al proposed a mechanism that judge the user is true or not front ATM through one-time and biometric [8, 9]. The mechanism has high security, but it only can used on the closed network, so reducing the practicability. Hyun-Chul Kim et al also propose a mechanism through certificate and public key encryption verify the identity and protect the package for identity authentication. However, due to it often use the public key encryption, so the performance of the mechanism is not fast.

3. Our Mechanism

In this chapter, we describe the mechanism how to operation, and introduce our method that are how to generate a codebook, encrypt the plaintext and decrypt the ciphertext.

3.1. Scenario

The user generates a combination key 1, and send a login request and the combination key 1 to the server, when the user wants to login. The server generates a combination key 2, and send these data to the user, when it receives the login request from the user. Finally, the user generates a value R, then make the dynamic codebook by the combination key 1, 2 and value R, after the user receives these data. And the code of biometric of the user will be a dynamic code of biometric of the user using the dynamic codebook, and the user sends the value R and the dynamic code of biometric of the user to the server for that verify his identification, as shown in Fig. 8.

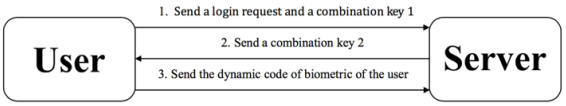

Fig. 8 Scenario

3.2. Mechanism

In the mechanism, we are using many hash functions and symmetric encryption function. The following describe that each variable means what, as shown in table 1.

TABLE 1
Variable Description

Variable	Description
U	User.
S	Server.
ID_i	ID of i, i= U.
K_i	The i of combination key, i=1, 2.
K_{U-S_i}	The i of symmetric-key between the user and the server, i=1, 2, 3
R	This is a random number for making the codebook, the length is same with the biometric of the user. The range of number is from 0 to 3.
T_i	The i of timestamp, i=1, 2, 3.
Tag_i	The i of hash value, i=1, 2, 3.
DCB_i	Dynamic code of biometric of i, i= U.
B_i	Code of biometric of i, i= U.
CB	Dynamic codebook.
X_i	Secret value of i, i= U. The value shared with the server.
$h(\cdot)$	Hash function.
$E_i(\cdot)$	Symmetric encryption function via i, $i = CB$, K_{U-S_1}, K_{U-S_2}, K_{U-S_3}.

Workflow:

Step 1. The user generates K_1, timestamp and verify value, when the user login. And these data will be encrypted by symmetric encryption, and send to the server.

$$Tag_1 = h(ID_U, K_1, T_1, X_U) \quad (1)$$

Step 2. The server generates a timestamp and computes the time difference by the timestamp of the packet, and check that the data are correct or not by the verify value, when the server received data from the user. Then the server generates K_2, new timestamp and verify value, if those are not tampering. And encrypt these data by formula (2), then send to the user.

$$K_{U-S_2} = h(K_{U-S_1}, Tag_1, X_U) \quad (2)$$

$$Tag_2 = h(K_2, T_2, X_U) \quad (3)$$

Step 3. The user generates a timestamp and computes the time difference by the timestamp of the packet, and check that the data are correct or not by the verify value, when the user received data from the server. Then the user scans his biometric by the scanner, and generates a value R, and make a dynamic biometric by the dynamic codebook. And then generate a timestamp, verify value, and encrypt these data by formula (4), then send to the server. The user will get access right, if his dynamic biometric, the time difference and the verify value also are correct, as shown in Fig. 9.

$$K_{U-S_3} = h(K_{U-S_2}, Tag_2, X_U) \quad (4)$$

$$DCB_U = E_{CB}(B_U) \quad (5)$$

$$Tag_3 = h(DCB_U, R, T_3, X_U) \quad (6)$$

$$new\ K_{U-S_1} = h(K_{U-S_3}, R, Tag_3, X_U) \quad (7)$$

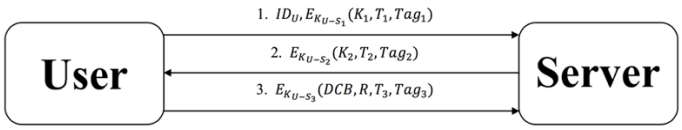

Fig. 9 Mechanism

4. OUR CODEBOOK

The section describes how to generate codebook, and introduces combination key, include the format, and the method of generation.

4.1. Combination Key and Value R

K_1 is a random string consists of 32 zeros and 32 ones. K_2 is a random string consists of 'A' to 'Z', 'a' to 'z', '0' to '9' and two special characters. Each character of the K_2 is not repeated. Value R is a random number for making the codebook, the length is same with the biometric of the user. The range of number is from 0 to 3.

4.2. Generation Method of Codebook

When the user wants to generate the codebook, he has to compare K_1 with K_2. Each character of K_2 has to be divided by 2, and get the remainder, and then find the corresponding value of K_1. For example, the first code of K_2 is 9, so the remainder is 1 on the figure 10. Therefore, we need to find the corresponding value of K_1, and we will get that the value of the positions of the corresponding code of the codebook is 9.

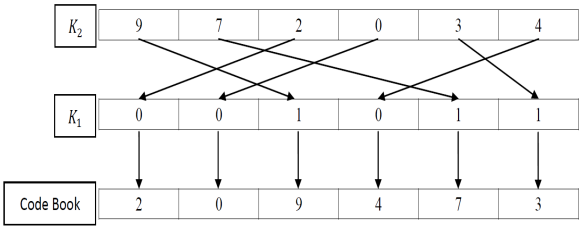

Fig. 10 Generation method of codebook exemplary diagram

5. ENCRYPTION, DECRYPTION AND DYNAMIC CHANGE

The section describes how to encryption, decryption, and how to change the codebook.

5.1. Encryption and Decryption

We have to assume the string of the codebook is a cube that are four to the power of three. The encryption method and decryption function is done by the three-dimensional coordinates, as shown in figure 11. We find the coordinates of 'H', if the character 'H' will be an encrypted character, and the coordinate will be the ciphertext. For example, the ciphertext of 'H' is '230', and we only find the coordinate, then we will get the plaintext, when we want to decrypt the ciphertext.

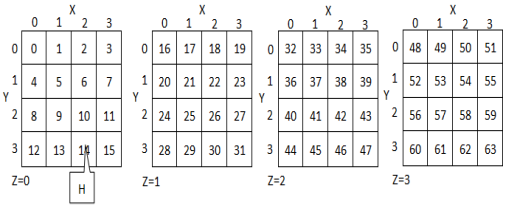

Fig. 11 Decryption method exemplary diagram

5.2. Dynamic Changing

Each character is encrypted by the different codebook. The codebook is auto-conversion, when the last character was encrypted. The conversion method has three stages, namely is X stage, Y stage and Z stage. When conducting the X stage, the codebook will cut into four pieces on X-axis, and the first value of each piece (x, 0, 0) decide the new position. The order of shift that compute the new position of the codebook from small to large by X-axis. The computing method is that the first value of each piece (x, 0, 0) divided by four, and take the remainder. The first value has to plus the corresponding values of the value R, and then divide by four, and take the remainder, the other three values don't need to do it. The remainder decides that the shifting steps of the piece. The remainder plus one, until the new position is not occupied, if the new position has been occupied. And the remainder will be zero, if the value over three. Y stage and Z stage similar X stage, but the conversion axis are different. When the Z stage is finished, the new codebook is generated, as shown in Fig. 12 to Fig. 14.

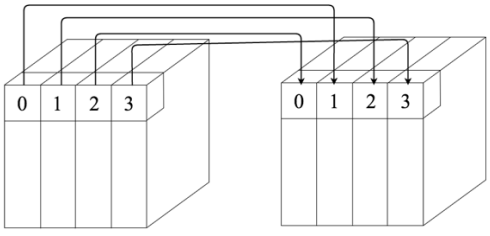

Fig. 12 X stage

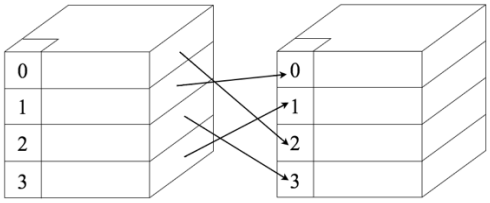

Fig. 13 Y stage

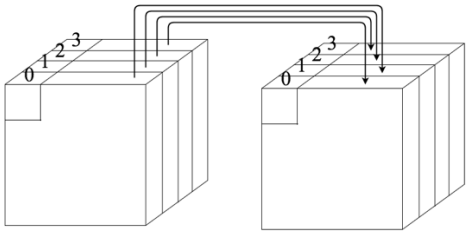

Fig. 14 Z stage

6. PERFORMANCE ANALYSIS

The section describes how to mutual authentication for each unit, and describes the security of the codebook. Finally, shown as performance analysis of the mechanism.

6.1. Mutual Authentication

Mutual authentication [3, 10] means each unit can prove their identity on the Internet between each unit. The receiver can check the identity of the other side by the data of the other side. When the both sides can check the identity of the other side, the goal of mutual authentication is achieved. Usually, hash function and public key encryption are used for mutual authentication.

In the study, the user and the server have a same secret data 'X'. The secret data 'X' is a private data, only the user and the server have it. And the hash value is used in each step in the mechanism for the verification, the hash value can check the packet is tampered or not. Therefore, the hash value can check the identity of the other side is correct or not, because the hash value consists of secret data 'X' and other data.

6.2. Security of the Codebook

The codebook is a string of 64 characters that consists of 0 to 9, lowercase a to z, uppercase A to Z as well as two special characters. The codebook is one-time, so the user will get different codebook for each login request. The change rate of the codebook is 64!, thus the user gets same codebook that the probability is small. When the biometric of the user is encrypted by the codebook, each character is encrypted by the different codebook. Therefore, the change rate of dynamic biometric is that 64! multiplied by the length of the biometric of the user. The attacker can't crack the password without short password.

6.3. Performance

In the mechanism, the user uses the symmetric encryption in the step 1, step 3, the total is three times. The server only uses once in step 2. About the hash function, the user and the server need to verify the verify value is true or not, and produce new symmetric key encryption, so the total is six times, as shown in table 2. The symmetric key encryption and hash function does not take up too much computing resources, so the mechanism has a good performance.

TABLE 2
Performance Analysis

Unit: Times

	Symmetric-key Cryptography	Hash Function
User	3	6
Server	1	6

7. ATTACK ANALYSIS

The section analysis the security of mechanism via that simulate replay attack, man-in-the-middle attack and impersonation attack.

7.1. Replay Attack

Replay attack [10] can take the access right of the user via that the attacker intercept the packet of the user, and send it to the server. Due to the verify data all in the packet, so the attacker doesn't need to know that the account, the password and other verify data, the attacker only intercepts and send the packet, it will get the access right of the user.

In the mechanism, each data always different without the ID of the user in each step. Therefore, no matter what the attacker intercepts any packet and replay attack, finally always be fail.

7.2. Man-in-the-middle Attack

Man-in-the-middle (MITM) attack [3, 4] mean the attacker intercepts the packet for tapping and modifying, when the units are communicating. Normal status is that the units are communicating directly. However, when the user is attacked, the transfer mode will be that the user A conveys to the attacker, and the attacker conveys to the user B. And the users don't know that their packet is stolen, modified.

The attacker only can get the ID of the user and the ciphertext, if the attacker attack by MITM. Because each packet is encrypted before the user send packet to the server in the mechanism. Therefore, no matter what the attacker intercepts

any packet, it also can't get useful information, as the packet always is ciphertext.

7.3. Impersonation Attack

Impersonation attack [3, 10] mean the attacker counterfeit some unit in the mechanism for the information of the user. The attack mode usually is used in the phishing, such as the counterfeit web login page of Facebook, Google, Yahoo, etc. for getting the account, the password of the user. It will cause a problem that the data of the user is leaked.

In the mechanism, the attacker has not the secret value and symmetric key, so the attack will be failing, if the attacker disguises the user, and send the ID of the user and fake packet to the server. The attacker can't make correct key and verify value, then the attack will be failing, if the attacker disguises the server.

8. CONCLUSION

The study proposes a secure authentication mechanism through the integration of FIDO and OTP. The user doesn't need to remember any password, and it can verify his identity safely. The biometric of the user be the dynamic biometric by the concept of OTP for that avoid data leakage. The mechanism does not take up too much computing resources, so the user can verify his identity quickly, as shown in table 1.

About the codebook, the study proposes a codebook that the codebook is generated by two combination keys. Two combination keys are generated by different unit for reducing the risk of stealing. The amount of change of the codebook depends on the length of the password. Therefore, each character of the password is encrypted by different codebook, the characteristic make that the attacker is hard for counterfeit the user.

However, the encryption function has a shortcoming. Due to the encryption function is by three-dimensional coordinates, so the ciphertext is three times as long as the plaintext. The problem can be a goal of improved in the future.

REFERENCES

[1] Saad M. Darwish and Ahmed M. Hassan, "A model to authenticate requests for online banking transactions," *Alexandria Engineering Journal*, Vol. 51, Issue 3, pp. 185-191, September 2012.

[2] Hyun-Chul Kim, Hong-Woo Lee, Kyung-Seok Lee and Moon-Seog Jun, "A Design of One-Time Password Mechanism using Public Key Infrastructure," *Fourth International Conference on Networked Computing and Advanced Information Management*, Vol. 1, pp. 18-24, September 2008.

[3] A. Hiltgen, T. Kramp and T. Weigold, "Secure internet banking authentication," *IEEE Security and Privacy*, Vol. 4, Issue 2, pp. 21-29, March-April 2006.

[4] Chun-Ying Huang, Shang-Pin Ma and Kuan-Ta Chen, "Using one-time passwords to prevent password phishing attacks," *Journal of Network and Computer Applications*, Vol. 34, Issue 4, pp. 1292-1301, July 2011.

[5] Yadigar Imamverdiyeva, Andrew Beng Jin Teoha and Jaihie Kima," Biometric cryptosystem based on discretized fingerprint texture descriptors," *Expert Systems with Applications*, Vol. 40, Issue 5, pp. 1888-1901, April 2013.

[6] Wen-Shenq Juang, "Efficient password authenticated key agreement using smart cards," *Computers and Security*, Vol. 23, Issue 2, pp. 167-173, March 2004.

[7] Mohsin Karovaliya, Saifali Karedia, Sharad Oza and Dr.D.R.Kalbande, "Enhanced security for ATM machine with OTP and facial recognition feature," *Proceedings of the International Conference on Advanced Computing Technologies and Applications (ICACTA)*, Vol. 45, pp. 390-396, 2015.

[8] Heng Fui Liau and Dino Isa, "Feature selection for support vector machine-based face-iris multimodal biometric system," *Expert Systems with Applications*, Vol. 38, Issue 9, pp. 11105-11111, September 2011.

[9] Vijay Bhaskar Semwal, Manish Raj and G. C. Nandi, "Biometric gait identification based on a multilayer perceptron," *Robotics and Autonomous Systems*, Vol. 65, pp. 65-75, March 2015.

[10] Ronggong Song, "Advanced smart card based password authentication protocol," *Computer Standards and Interfaces*, Vol. 32, Issues 5-6, pp. 321-325, October 2010.

[11] Alphabet Inc., "Gmail," 2016/01/13, https://www.gmail.com/

[12] Alphabet Inc., "Google," 2016/01/13, https://www.google.com/

[13] Alphabet Inc., "Youtube," 2016/01/13, https://www.youtube.com/

[14] Dropbox Inc., “Dropbox,” 2016/01/13, https://www.dropbox.com/
[15] Facebook Inc., “Facebook - Log In or Sign Up,” 2016/01/13, https://www.facebook.com/
[16] Naver corporation, “LINE : Free Calls & Messages,” 2016/01/13, http://line.me/zh-hant/