International Journal of Engineering & Technology, 7 (4) (2018) 5434-5437

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.23802
Research paper

Secure login technique for online banking

Doaa Yaseen Khudhur[1]*, Belal Al-Khateeb[1], Hadeel Amjed Saeed[1]

[1]College of Computer Science and Information Technology, University of Anbar
**Corresponding author E-mail:duaa_82yaseen@yahoo.com*

Abstract

In recent years, there are many authentication protocols that are used in the accessing of the sensitive and private data. However most of those methods have many weaknesses by which data can be extracted and used by unauthorized people this due to the use of a one level authentication that may face many attacks. This paper presents an authentication method that involves three levels of user authentication; the first two levels use two level passwords authentication together with a Personal Identification Number (third level) for every operation in Electronic Banking system. Hash functions -Secure Hash Algorithms- and Cyclic Redundancy check (32) for the generations of Personal Identification Number are used. This system eliminates the problem that is related with single level password authentication system and improves the security by using Personal Identification Number.

Keywords:*Authentication; Online Banking; Two Level Passwords; Security; Personal Identification Number (PIN).*

1. Introduction

In recent decades, the internet become very important part in our life, and the number of people who anticipate being able to manage their banking operations anywhere, anytime is growing. Therefore, E- banking has become an effective component in the multi-channel enterprises strategy. The customer's information and transaction is very important and extremely sensitive in financial institutions, thus doing such business via a public network requires
challenges for security and trust. Any online banking system must meet three important conditions the first, that only authorized persons can enter a bank account, the second, that the information displayed is still special and cannot be modulated or altered by third parties, finally any commercial operation are tracked and verifiable, therefore the system must treat the issues of authentication, confidentiality, integrity, and non-repudiation[1][2].
In an E-Banking environment, emphasis must be placed on risk management related to authentication, and must review the risks and risk management controls of number of existing and emerging authentication tools necessary to new customers identity verification and verify existing customers that enters electronic banking services[3].
This paper presents three levels authentication system at which there are two levels password authentication together with a PIN authentication, those levels of authentication will be used in every online banking operation.

2. The proposed system

In this paper, a Security levels and layered system for enhancing login security on internet banking systems have been implemented. increase login security will help protect against online roguery by providing additional layers of protection for online user ID and password that users currently use to login.The implemented system aims to protect the banking system by using two level passwords authentication. In the first level, the first password is chosen by the user during the registration stage. The users enter the registration data (RD) which include full name (FN), username (UN), first password (F-PAS), address (ADD), email (E-M) and birthday (BIR).The second passwordresulting from combining the birthday with the following format (dd, mm, yy) with a randomly chosen 4-digit(X-X-X-X). So, this password is consisting of 10 digit numbers. Second password = (dd,mm,yy) & (x-x-x-x).
Also, the user must choose a PIN number at this stage.
The second level authentication will use the second password together with the selected PIN. User must enter the second password that appeared during the registration stage together with the selected PIN. Server will check second password and PIN are correct or not, if not the user cannot login to the system. This protocol helps preventing unauthorized access to banking system or to account numbers.

3. The Advantages of proposed system by compare with other works

In the previous many authentication protocols either have much weakness by using traditional password or using one level authentication, or have very complexity technique. We have proposed this system to improve on traditional methods and increase the security by using authentication for many levels. In addition, the system is smooth and characterized by its flexibility and Stay away from using some complex protocols by adding images or pixel coloras presented by Ashwini Deshpande et. al. [4] proposes an authentication methodology that involves three levels of user authentication which includes textual password, Image Authentication and Color Authentication.
On the other hand, most previous studies have merged between one-time password and image ordering or color pixel, the weakness of previous systems are when a user need to upload image or color pixel from other device or other serveras published by Abhishek Gandhi et. al.[5].

This is different from our proposal because the proposed system offer the flexibility, privacy, efficiency for any transaction need secure login. We use two levels of password, and on the third level we create a personal identification number (PIN) without restrictions such as opting in with a particular application as a QR code or using image authentication, color authentication that may reduce system speed and be reflected in system performance and flexibility if the desired application is not available.

4. Mechanism level

Firstly, the system will check whether the user is registered or not. If not, then user will register himself by giving user name (UN) and first password and will give all the details like address, email and birthday. After that the system appears to user the second password and PIN. All the details and second password will be saved in the database.

First level consists of traditional login. The user will use his correct username and password. Then, He will be directed to second level and the session. In the second level, the user must enter the second password and PIN for login to banking system. These warranty the peace and safety even if a thief is guessing the first password or if user wastes or loss it. In addition, all corporation networks, bank accounts and other systems that contain important and sensitive data need some form of strong and effective authentication that we can achieve by using Second passwords and PIN.

a) First level

The First level will be the first password. Password based authentication is the most widely used method to verify the validity of a user. User must enter UN and provide their password to begin using a system. User authentication authorizes human-to-machine interactions in operating systems. The stepsofregistration phase is:-

The user should register him/her by introduce the personal details. If the user is a new user then he enters the RD (FN, UN, F-PAS, ADD, E-M, BIR) and gives all details to the system. The system generates the second password and PIN.

- User submits user name and first password to the server throughsecurechannel.
- Server will check either user name and first password iscorrect ornot,if not the user cannot login to the system.

If password is correct then direct to second level.

Show the first level in figure 1.

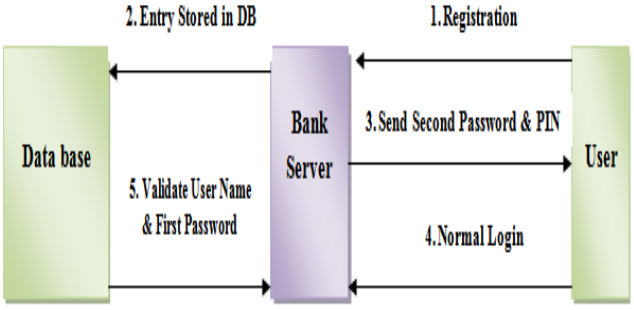

Fig. 1: Level One.

b) Second level

In the second level, each user has a unique PIN and second password and can uses it for every operation on banking system. This level strengthens the reliability of the user by using the PIN and additional password.

If the server validated the UN and F-PAS in fist level, the user should enter the second password in second level, shows figure 2.

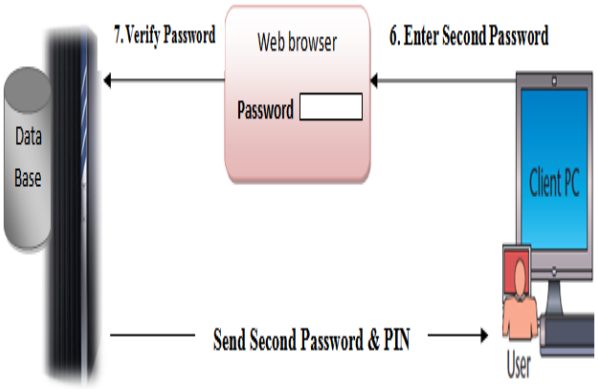

Fig. 2: Level Two (Second Password Verification).

5. PIN generation

After the user enters the second password and the server validate the user, the user can be introduced to the banking system web site and made any operation by enter the PIN, as shown in figure 3.

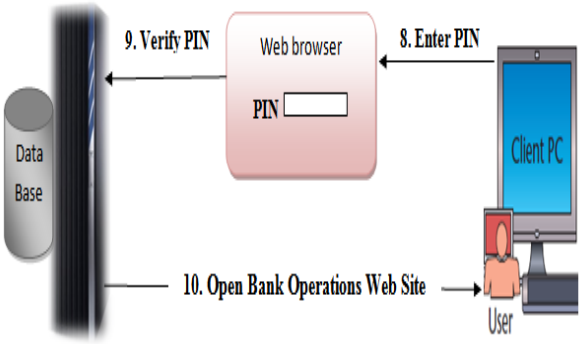

Fig. 3: Level Two (PIN Verification).

Each user has a unique PIN and must use it when he wants to transfer money, deposit money withdrawal money, etc., the server generates the PIN in registration phase, PIN is 4-digit numbers calculated by Three steps: The first step is enter a system time during registration phase TR (00.00) toSHA-1 hash function to generate text of charactersand numbers, the result is named T1. The second step is generate second text (T2)by add the last name (LN) of userto T1. The third step is compute CRC(32) to convert the T2 to digital number and took the four digits as a PIN, T1=(SHA-1(00:00)), T2=(T1&LN), PIN=CRC32(T2).Generation a PIN shows in figure 4.

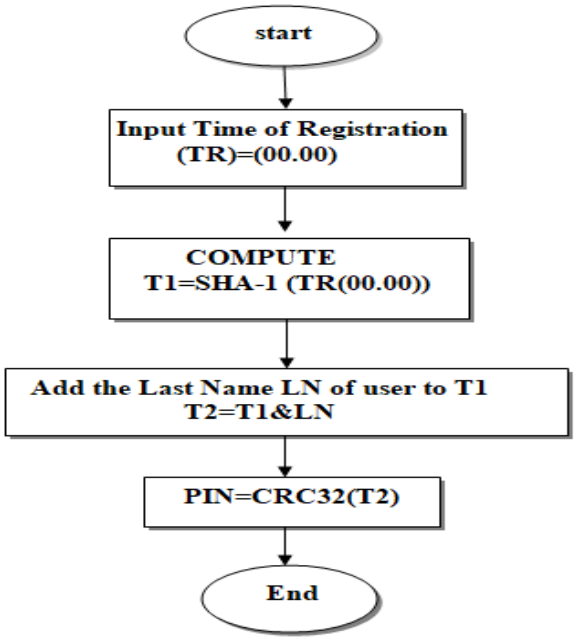

Fig. 4: Steps of A PIN Generation.

a) Secure Hash Function-1

SHA-1 is intricate algorithm that includes several operations multiples of 32-bit, data shifting, additions, logical functions, and repetition. The hash function MD4 was used to establish the SHA. SHA is secure hash function have several versionsSHA-0, SHA-1, SHA-256, SHA-384 and SHA-512[6].

The output of SHA-1 is 160 bits, message size is shorter than 2^{64}bit, block size is 512 bits [7].

The algorithm consists of the following steps:

1) Padding:Appending Bits by added n bits (1- 512).
2) Appending Length: appended to the end of the message 64-bit representation.
3) Initialization of buffer: H0, H1, H2, H3 and H4 are registers used during generate 160-bits hash, and every register be 32-bit.
4) Calculation of hash:

- The words are called W0, W1… W80 has 80x32-bit words a message schedule.
- A, B, C, D and E are Five working variables of 32-bits each.

H0+A ⟶ H0
H1+B ⟶ H1
H2+C ⟶ H2
H3+D ⟶ H3
H4+E ⟶ H4

5) Output: The output available in H0, H1, H2, H3 and H4 [6][8].

b) Cyclic Redundancy check (32)

CRC is defining an error-checking code that is used in DC data communication systems and DT data transmission systems. Polynomial manipulations are using to build CRC by modulo arithmetic. Cyclic Redundancy Check has many versions: CRC-8, CRC-12, CRC-16, CRC-32, and CRC-CCIT. The computation of CRC includes manipulating M(x) and G(x) using modulo arithmetic. The output of modulo arithmetic has the same result for addition and subtraction. Three operations namely addition, multiplication, and division are involving in polynomials [9].

Figure 5 shows CRC process, performed the addition, multiplication and division operations inmodulo-2here. The addition and subtraction have the same computations. Lets M is message and n is number of bits[10].

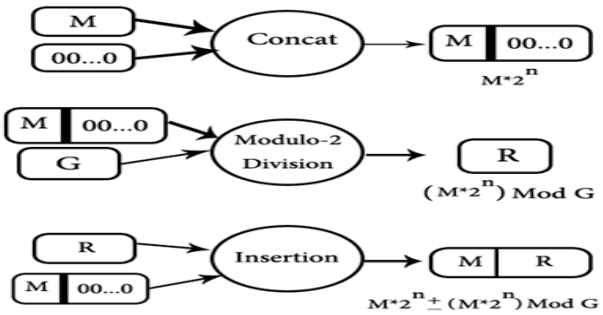

Fig. 5: CRC Process.

Below is an example for results(registration data, traditional login, second password and results of SHA and CRC functions)

-RD= (FN, UN, PAS, E-M, ADD, BIR)
= (Ali Maher Ahmad, AMA, 2D3A426, ali--ahmed22@gmail.com, Baghdad,22-05-1988)

-TL= (UN, PAS)
=(ALI, 2D3A26)

-SEC-PAS (10 digs) = (dd,mm,yy) & (x-x-x-x).
=(2205882176)

-T1=(SHA-1(00:00))

=6d43jdutre36902dhjllf87dsaqwkjgfds987f6d5s4a3f5g6j8k0l8b7v6c5x4s4z2x3c5v6b7n9m99j7g5f4s43fdj9i0t9g5d8u7t5e4w2q6u8i9o9j8u

- T2=(T1&LN)
=6d43jdutre36902dhjllf87dsaqwkjgfds987f6d5s4a3f5g6j8k0l8b7v6c5x4s4z2x3c5v6b7n9m99j7g5f4s43fdj9i0t9g5d8u7t5e4w2q6u8i9o9j8uAhmad

-PIN=FOUR DIGIT (CRC32 (T2))
=478276498
=4782

6. Conclusion and future work

In three levels authentication system at which there are two levels password authentication together with a PIN authentication is overcoming the various attacks, to eliminate menaces, to validate from identity of user and is also easy for user to access, those levels of authentication will be used in every online banking operation and can be executed by many of electronic technologies. The online banking login security is improved by using three levels authentication system.

The new authentication system that proposed for online banking achieved increase security, safety and convenience by using three level authentications that can be used by any user. Using the second and third level of authentication, the user became more secure during banking operations, the second level repeats the use of the second password and the third level uses algorithms to generate the PIN, all of this increases security and provides users with comfort ability and reassurance during banking transactions. The proposed work can be enhanced by using user's image to increase the levels of authentication, or using iris identification and thumbprint to ensure the validity for user.

References

[1] Janardan Choubey and Bhaskar Choubey," Secure User Authentication in Internet Banking: A Qualitative Survey", International Journal of Innovation, Management and Technology, Vol. 4, No. 2, April 2013.

[2] Rajpreet Kaur Jassal, Dr. Ravinder Kumar Sehgal,"Comparitive Study of Online Banking Security System of various Banks in India", International Journal of Engineering, Business and Enterprise Applications, IJEBEA, 6(1), September-November 2013, pp. 90-96.
[3] Jeffrey M. Kopchik, Matthew Biliouris, John Carlson and Michael Wallas, "Authentication in an Electronic Banking Environment August "8, 2001,2000 K Street,NW,suite 310,Washington DC 2006,(202)872-7500.FAX(202) 872-7501.
[4] Ashwini Deshpande,Suchita Singh, Amrita Kharga,Dr.LataRagha,"SESSION PASSWORDS USING THREE LEVEL AUTHENTICATION SYSTEM, International Journal of Technical Research and Applications ,e-ISSN: 2320-8163, www.ijtra.com Special Issue 41 (AVALON) (March 2016), PP. 26-29.
[5] Abhishek Gandhi, Bhagwat Salunke, SnehalIthape, Varsha Gawade and Prof.SwapnilChaudhari,"Advanced Online Banking Authentication System Using One Time Passwords Embedded in Q-R Code", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014, 1327-1329.
[6] Nalini C. Iyer and Sagarika Mandal,"Implementation of Secure Hash Algorithm-1 using FPGA",International Journal of Information and Computation Technology.ISSN 0974-2239 Volume 3, Number 8 (2013), pp. 757-764.
[7] William Stallings,"Cryptography and Network Security Principles and Practices, Fourth Edition", Prentice Hall, November 16, 2005.
[8] Yogendra Singh Solanki, "Performance Based Design and Implementation of a SHA-1 HashModule on FPGA",International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 12, December 2012.
[9] Chris Borrelli, "Cyclic Redundancy Check", IEEE 802.3, XAPP209 (v1.0) March23, 2001.
[10] Hamed Sheidaeian and Behrouz Zolfaghari,"PARALLEL COMPUTATION OF CRC USING SPECIALGENERATOR POLYNOMIALS",International Journal of Computer Networks & Communications (IJCNC) Vol.4, No.1, January 2012.