A Novel Scan2Pass Architecture for Enhancing Security towards E Commerce

Hareth Zmezm[1]
[1]Computer Science Department, Faculty of Science,
University of Karbala, Iraq

Hamzah F. Zmezm*[2,3]
[2*]Academic Unit, Culture attaché, Embassy of Republic of Iraq in Kuala Lumpur, Malaysia
[3*]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, 76100, Melaka, Malaysia

Halizah Basiron[3]
[3*]Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, 76100, Melaka, Malaysia

Mustafa S.Khalefa[4]
[4]Computer Science Department, Faculty of education Pure Science, Basrah University, Iraq

Prof Dr. Hamid Ali Abed Alasadi[5]
[5]Computer Science Department, Faculty of Education Pure Science, Basrah University, Iraq

***Abstract*—Widely deployed web services facilitate and enrich several applications, such as e-commerce, social networks, and online banking. This study proposes an optical challenge-response user authentication system model based on the One Time Password (OTP) principle (Scan2Pass) that use multifactor authentication and leverage a camera equipped mobile phone of the legitimate user as a secure hardware token. The methodology which is designed and implemented to evaluate the proposed idea will be explored and explained throughout this paper. The chosen method presents a brief overview about the steps required to design an efficient and practical system. Also, the requirements will be discussed as well as our assumption to give a simple yet an adequate understanding about the security of our proposed system in general. Then, an overview about the basic architecture needed for the proposed system to explain the role of the shared secret and the challenge response protocol in order to complete authentication procedure and provide mutual authentication between the user and the server by adopting multi-factors such as time, OTP algorithm by describing the operation flows of users during each phase of this system.**

Keywords—Electronic commerce; authentication; one time password; performance and reliability

I. Introduction

Electronic commerce (e-commerce) uses electronic media for conducting commerce, which involves activities like setting up an electronic interface between service providers and target, namely, customer, streamlining the workflow in the organization to process the requests from the customer and ultimately deliver that was promised. The International Business Machines Corporation (IBM) has defined e-commerce to be "the transformation of key business processes through the use of Internet technologies" [1]. E-commerce is associated with the buying and selling of information, products and services via computer networks today and in the future via any one of the myriad of networks that make up the Information Superhighway. As e-commerce growth, it becomes more significant. Many countries must not only address and appreciate its potential for the growth of trade and industry but also as a means of survival in the new world of e-commerce-based trade and business. E-commerce is a global phenomenon providing markets and opportunities world-wide with a significantly reduced barrier to access as compared to global marketing in the 21th century [2]-[5]. This paper discusses on the background of study, the problem of the current system, research questions, objective to maintain this issues that leads to draw the conclusion and brief summary of approach that implemented in this research.

II. Research Design

This section introduces the research design to develop this research. As shown from Fig. 1 below, there are four main steps to complete this research. The first step is to work on the research gap from extensive reading on the literature. Study the literature about existing authentication method to find the research gap or weakness in the existing researches. Then, analyze the requirements for a new authentication system required to apply technology and solve the existing problems. The third step is to move in design stage [6], [7]. The process of defining the architecture, components, modules, interfaces and data for a system is to satisfy specified requirements. Then, begin to develop the new authentication system, called Scan2pass. Finally, after implementation Scan2Pas starts to evaluate the proposed LSB technique using PSNR measurement and compare the results with the previous existing system to show the performance of the new system. Fig. 1 shows the overall research design.

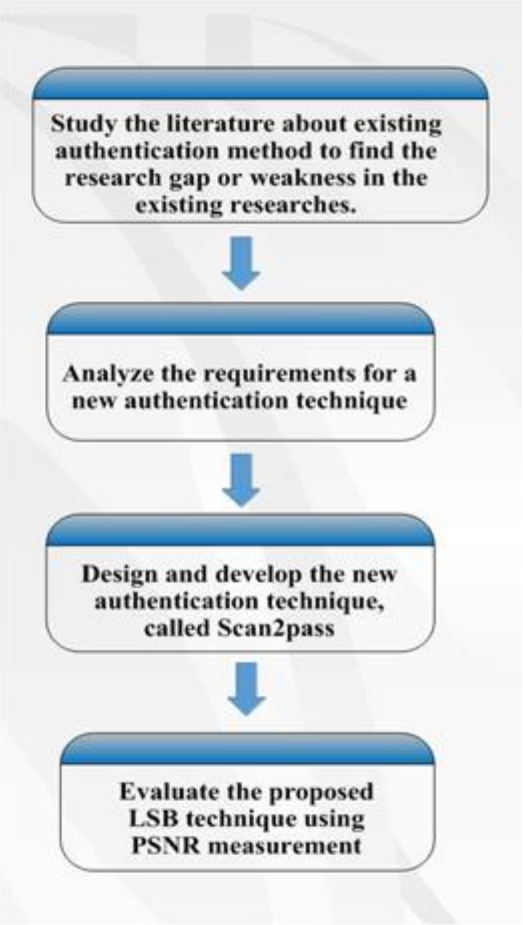
Study the literature about existing authentication method to find the research gap or weakness in the existing researches.
Analyze the requirements for a new authentication technique
Design and develop the new authentication technique, called Scan2pass
Evaluate the proposed LSB technique using PSNR measurement

Fig. 1. Overall research design.

III. PROPOSED SCAN2PASS ARCHITECHTURE

Until now, an internet user is continuously unsure about the security of his computer and his accounts. A typical internet user is in constant terror of dropping sensitive information while using Internet services such as e-commerce, on-line banking and email services, etc. This terror arises from the evolution and the advancement development in equipment and technology of cyber-attacks. These attacks are achieved with one purpose in attackers' mind: to bargain information from the victim's machine. This information, definitely, can be anything from user credentials and online banking information to email addresses and web surfing habits. Stolen credentials and banking information can be immediately sold in illegal-market. Therefore protecting user credentials and system resources are vital. Many suggestions and solutions to safeguard user credentials have been offered by scientists however, many of them have not been deployed due some limiting factors such as:

1) Additional hardware required on the client side.

2) High cost or inefficacy of solutions.

3) Hypotheses are far from ubiquity and reality.

In spite of these limitations and weaknesses in these solutions, several Internet services still use the combination of text usernames and passwords to validate one's identity of the remote user. This creates significant security vulnerability since the user's password can be captured and later reused by a hostile party, also it easy for cyber criminals to commit cyber theft. Another common case is computer malware. Without an up-to-date antivirus and a fully patched operating system, a computer could get easily infected with malware, and would not survive long in the wild [8]. Key logging and phishing attacks can extract user identity and sensitive account information for unauthorized access to users' financial accounts. Most existing or proposed solutions are vulnerable to session hijacking attacks [9].

JavaScript key loggers [10] are so far another problem. JavaScript key loggers are not like traditional key loggers. They do not record call back functions to obtain key strokes from lower levels. They, actually, append JavaScript functions to web pages in order to register keyboard actions sent to password or any other area on a web page, and after collection they are sent to attackers [11]-[15].

In an attempt to protect user credentials and to ward off the aforementioned attacks, this research proposes an efficient, practical and secure user authentication system model called Scan2Pass. To achieve this objective there are sub objectives need to be done. Therefore the proposed system model need to identify the weak factors of the authentication system and find solution for this weakness.

There are three main goals behind the proposal. First is finding a way to protect the sensitive data and the shared secret key exchange between user and web server during the registration and login phase by ensuring a secure communication between parties using SSL/TLS protocol. This task is done by adopting security policy mechanism called STS (strict-transport security) that certifies a web to client, so that the connection between user and server is upgrade to Hypertext Transport Protocol (HTTPS) and refuse to connect to any HTTP connection [16]. Second, protecting user's password by extending the key space length of password this operation is done by using a key derivation function which it is a part of RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, specifically PKCS #5 v2.0 specify in RFC 2898 [17] to extend the key space of the password to 256 bits to thwart brute force and dictionary attack. Encryption and hashing operations are applied on the sensitive information to provide privacy and integrity. Third, providing a mutual authentication between entities, this mutual authentication is achieved by combining a multi-factor elements, an appropriate technology represent in Quick Response Code (QR-Code) technique to compute a unified OTP code between user and server to verify each other through a the challenge response protocol that is play a vital role to provide mutual authentication between entities and prevent replay attack by generating a strong unpredictable challenge with the aid of secure cryptography pseudo random number generator called Fortuna.

A. Requirements and Assumptions

Requirements are a significant factor when designing software solutions. They explain what the system should work and how it should act. Requirements must be measurable, testable and defined to a level of detail sufficient for system design. Requirements are divided into three types: functional requirements, non-functional requirements and security requirements.

B. Functional Requirements

Functional requirements keep the upcoming activities of the system [18]. In an authentication system the security functionality is the main objective. Below are the security functional requirements of the system:

1) Improve the security of Passwords against on-line guessing, such as dictionary attacks and brute force.

2) Providing a security mechanism to protect messages and authentication against replay attacks.

3) The authentication system should prevent eavesdropping.

4) An attacker is unable to retrieve or deduce the shared secret from any party involving in the authentication process.

5) The system should use multi-factor authentication.

6) The authentication system must be protected against session hijacking.

C. Non-Functional Requirements

Non-functional requirements explain limitations and qualities of a system [19]. The nonfunctional requirements are shown below.

1) Usability: Solutions must be simple and intuitive to use and must not scare users away with confusing or cumbersome technology impediments. They must not require special knowledge from the users, or demand expensive software or hardware on the user side.

2) Deployment cost: Cost includes setup costs (for example, specific hardware or software requirements), communication costs (how much information needs to be transmitted), delay costs (time authentication takes), scalability, and maintenance/support cost. The solutions must not be more expensive to deploy than existing solutions. They should not require any extra expenses for the users.

3) Availability and reliability: The authentication system must be available whenever the user needs to be authenticated. The error rate must not be higher than for existing systems.

4) Scalability: The system must scale easily when the number of users increases.

5) Performance: The authentication delay must be less or in the same range as that of existing solutions.

D. Security Requirements

Security requirements describe the conditions and capabilities need to be satisfied in order to achieve the security attributes.

1) Privacy: Privacy between the E-commerce site and user, user must be able to prove himself to the site that he is really was the right user. The user must trust that the e-commerce company is able to protect his/her secret information. Preventing who's in the firm itself from indicating which information here is very important.

2) Confidentiality: Encryption of sensitive information.

3) Verification: The system should check if the information is correct.

4) Authentication: Mutual authentication should be provided. User talk with the correct server, the server will talk to who he thinks talk or with the legitimate user.

5) System trust/person trust: Can user trust everyone who works at e-commerce site with his data.

6) Cryptographic: Cryptographic operations must be secure. However is very important to use it correctly in the larger system.

E. Assumption

The assumptions in our proposed system are as follows:

1) The web server possesses a unique phone number. Via the phone number, users can interact with the website through an SMS channel or direct call.

2) The users' cellphones are malware-free. Hence, users can safely input the shared secret key into cellphones.

3) User's cell phone equipped with a camera that can recognize QR code sent by the server.

4) The server side add a HSTS (Hodges et al. 2012) header and the user's machine has been notified of STS policy, therefore the browser will, by default, issue all requests to that domain under HTTPS only. Thus all data and sensitive information will transmitted in encryption form and only the entity that having matching key can decrypt the information also TLS/SSL provide identity assurance for both sides this will lead to achieve mutual authentication between both entities.

5) The clock is synchronized between client and server.

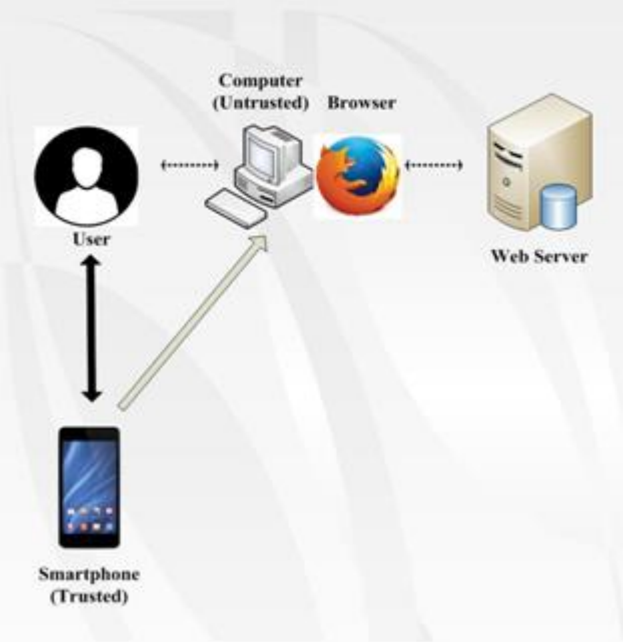

Fig. 2. Conceptual framework.

IV. Conceptual Framework

Little research has been focused on the balance between usability and security in authentication mechanisms when evaluating the effectiveness of system performance. Current authentication mechanisms rely on character-based passwords, with many alternatives which attempt to improve on certain usability aspects within the authentication mechanism concept. This research presents a framework of user authentication system model that use multi-factor authentication techniques for E-commerce application to provide seamless and efficient authentication mechanism in order to provide secure, simple, and fast authentication and achieve mutual authentication between user and the server (i.e. e-commerce companies).

Fig. 2 describes, the proposed solution takes advantage of features from previous work [20]-[22] to design a user authentication system model with a multi-factor authentication and which does not require any extra hardware devices by the user. By only using a mobile phone as a hardware token, strong authentication can be achieved with a system and a device that the user already has and knows how to use. On the other hand, the server needs a database that stores information about the user and his sensitive data. In addition, this framework needs to use a browser feature known as strict-transport security (HSTS).

HSTS is a web security policy that certifies a web to user. The user can access the web server via using HTTPS connection only. HSTS has many features. One of these features is that once there to make a mistake with this certificate, the browser will refuse to connect to the website. The user cannot ignore this warning. The proper set up a TLS/SSL web server therefore is highly desirable. For convenience and practicality purpose, the proposed solution uses RC4 as first choice in the cipher suite due to its efficiency, speedy and simplicity in implementation. With good implementation of a Pseudo Random Number Generator such as Fortuna, the challenge response protocol will generate a new challenge for every session and ensure that previous challenges are not reused. Challenge- response solves two problems. It makes sending the secret in plaintext unnecessary and prevents replay attacks, since challenges change every time. The confidentiality of the sensitive information at the application level will be considered by using key derivation function PBKDF2 and Bcrypt for the user password, preventing brute force and dictionary attacks.

The privilege factor of QR codes are part of a method to transmit information via visual channels in short-range communication, or using this technology in this framework to exchange sensitive data between server and the client without being captured by a kiosk or untrusted terminal which may be infected with malware or a keylogger. This will give proof to the authenticator that both devices (mobile and untrusted computer) are connected and controlled by the same person and prevent an attacker from snapping a picture of the QR code, because the attacker needs to be very close to the user to recognize the picture of QR code without being detected by the user. This leads to a number of difficulties for the attacker.

V. Operation Flow of the Proposed System - Scan2pass

This part presents operations flow for each phase of Scan2Pass. Scan2Pass consists of registration, login, and recovery phases. This research will introduce the details of these three phases, respectively. Unlike generic web login Scan2Pass will utilize a user's smartphone as a ubiquity authentication token and its ability to scan and recognize QR code delivered over https from the server to exchange sensitive information such as shared secret and challenge created by Fortuna.

A. Registration Phase

The aim of this phase is to create a user profile database to the legitimate user in the server and allow to the user and the server to negotiate the shared secret to authenticate succeeding login for this user. The details of registration phase are shown in Fig. 3. At the beginning the user will open the web browser and type the URL of the e-commerce web site since both browser and server adopted the strict transport security mechanism this policy will force the use of SSL/TLS in the communication between the web browser and the web server by upgrading the connection from HTTP to HTTPS, therefore both entities are protected because TLS provide identity assurance for both side in this way user and server are able to authenticate each other as well as all data encrypted will be encrypted inside TLS tunnel during the transition. Then user will choose registration button. During the setting up of an account, the user will provide personal information to the E-commerce site (via a web form). This information includes a user-selected password and personal details such as mobile phone number and his residence. To enhance the password on user's computer user sent PBKDF2 (password), the reason for doing this is to extend the user's password length to 256-bit then all information will be sent via secure channel SSL/TLS.

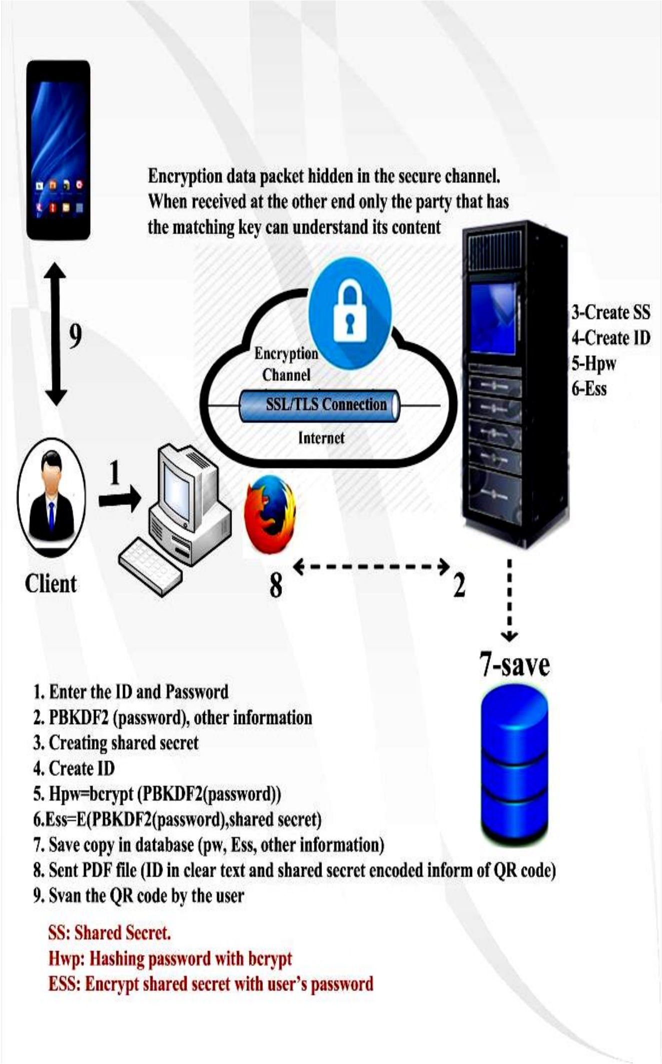
Encryption data packet hidden in the secure channel.
When received at the other end only the party that has
the matching key can understand its content
9
Encryption
Channel
SSL/TLS Connection
Internet
3-Create SS
4-Create ID
5-Hpw
6-Ess
1
Client
8
2
7-save
1. Enter the ID and Password
2. PBKDF2 (password), other information
3. Creating shared secret
4. Create ID
5. Hpw=bcrypt (PBKDF2(password))
6.Ess=E(PBKDF2(password),shared secret)
7. Save copy in database (pw, Ess, other information)
8. Sent PDF file (ID in clear text and shared secret encoded inform of QR code)
9. Svan the QR code by the user
SS: Shared Secret.
Hwp: Hashing password with bcrypt
ESS: Encrypt shared secret with user's password

Fig. 3. Registration phase.

After the server receiving these information it will create a shared secret key of 512-bit with Fortuna. The shared secret will store in the database together with other information. To protect user's credential the shared secret will be encrypted with the password that the server received with AES-256 (CBC).

Before storing the password of the user (output of PBKDF2) the password will be hashed with bcrypt to give the password a correct length to protect the hash password from cracking by rainbow table attack and brute force attack, this will prevent malicious insider from obtaining sensitive information on the registered user. This policy will prevent attack from inside the ecommerce company and provide privacy to the legitimate user.

When the server receives this information, it firstly checks whether the password is correct by using bcrypt and compare the result with the password stored in the database. If the verification successes, the server can verify that the received password is sent from the legitimate user or not (malicious attacker) by identifying the value of password with bcrypt before trying to decrypt the shared secret key, the original password (the output of PBKDF2 of the user stored previously in the database) must be used to decrypt the shared secret in the database, in this way the server can validate the user because the user deliver the correct password. For the rest of the session a plaintext version of shared secret will be available on the server. At this moment both user and the server have the clear text of the shared secret.

The detailed processes are depicted as follows:

1. User enter the ID and Password
2. PBKDF2 (password)
3. b = bcrypt (PBKDF2 (password)).
4. b' = password in database
5. Verify that b = b'
6. Decrypting the shared secret with password (output of PBKDF2).
7. Create a random 8 bytes challenge with Fortuna and encoded this challenge as QR code.

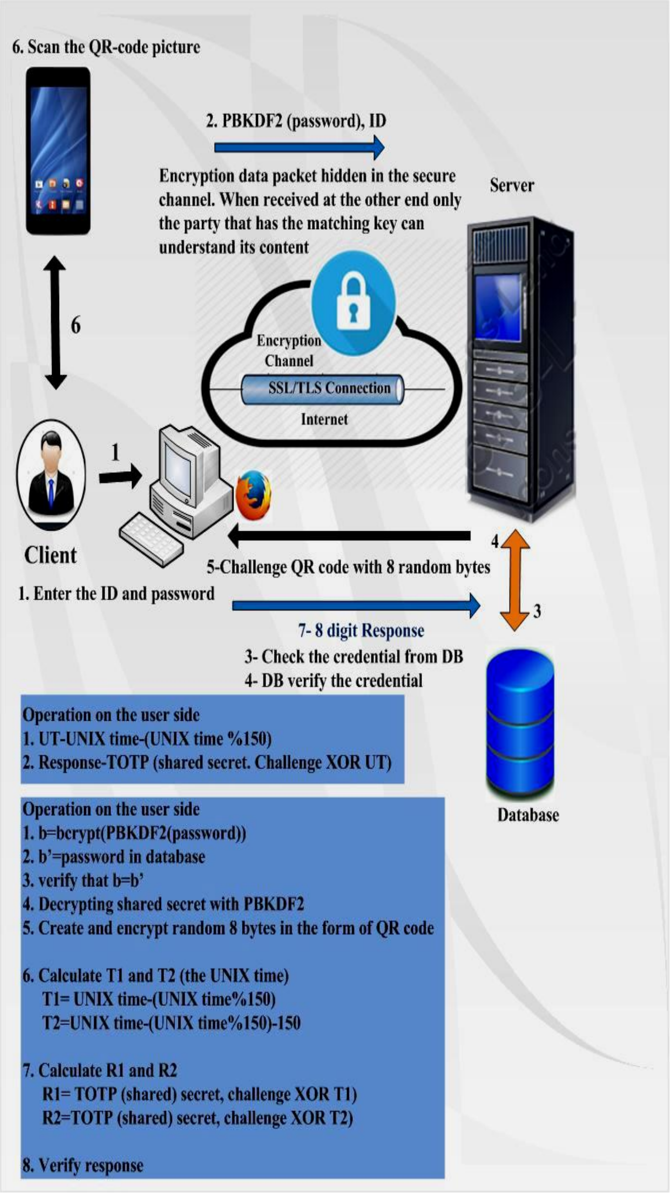
6. Scan the QR-code picture
2. PBKDF2 (password), ID
Encryption data packet hidden in the secure channel. When received at the other end only the party that has the matching key can understand its content
Server
6
Encryption
Channel
SSL/TLS Connection
Internet
1
Client
4
5-Challenge QR code with 8 random bytes
1. Enter the ID and password
3
7- 8 digit Response
3- Check the credential from DB
4- DB verify the credential
Operation on the user side
1. UT-UNIX time-(UNIX time %150)
2. Response-TOTP (shared secret. Challenge XOR UT)
Operation on the user side
1. b=bcrypt(PBKDF2(password))
2. b'=password in database
3. verify that b=b'
4. Decrypting shared secret with PBKDF2
5. Create and encrypt random 8 bytes in the form of QR code
6. Calculate T1 and T2 (the UNIX time)
T1= UNIX time-(UNIX time%150)
T2=UNIX time-(UNIX time%150)-150
7. Calculate R1 and R2
R1= TOTP (shared) secret, challenge XOR T1)
R2=TOTP (shared) secret, challenge XOR T2)
8. Verify response
Database

Fig. 4. Login Phase

The server performs challenge – response protocol to verify that the user has the correct shared secret. The server generates a random 8 bytes using Fortuna. These 8 random bytes are present in the form of QR-code to the user. The user launch the application in his smartphone to scan these 8 random bytes in the following way, The application take UNIX time and launch a time window of 30 seconds. Then XOR 8 random bytes with the UNIX time after that the application performs the TOTP algorithm described in RFC 6238. The parameter of TOTP is the shared secret and the 8 bytes XOR with the Unix Time as a time factor, the user sent the response as 8 bytes digit (the result is a token of eight long digits which is depended on the server challenge, time factor and shared secret). The detailed processes are depicted as follows:

8. The user launches his mobile app and scans the QR-code picture.
9. The app take UNIX time UT= UNIX time - (UNIX time % 150).
10. Response = TOTP (shared secret, challenge XOR UT).
The server receives 8-digit response and check the response, the detailed of server processes are depicted as follows:
11. The server calculates T1 and T2 (the UNIX time). T1 = UNIX time - (UNIX time % 150),
T2 = UNIX time - (UNIX time % 150) -150
12. Calculate response R1 and R2
R1= TOTP (shared secret, challenge XOR T1) R2= TOTP (shared secret, challenge XOR T2)
13. Verify the response.

If the server have the same information at the exact time following the mutual authentication is confirm and the login phase successfully done otherwise it will reject the login request. Therefore, every time when the server will generate its own verification OTP code will adjust its timestamp in order to match the timestamp from the phone. The last verification is used by the server to check the response code that it is falls either in the in the current period time or the period time before. Upon successful verification the server send back successful message through internet to the user's PC and the server will forward the user to the next page of E-commerce site. The system also keeps track of who has already logged in, so that a second login attempt for a session that is in progress will be seen as an attack attempt.

B. *Recovery Phase*

Inevitably, users will lose or break their cellphones, when this happens, the user must revoke the old key and establish a new key with a new cellphone. In the case of a lost cellphone, revocation prevents an attacker from accessing the user's accounts. Standard policies for password reset and account loss seems the best option. The user can contact the website to block his account and obtain a new shared secret the user calls the company via telephone. This is a well-established, familiar process today.

C. *Account Security Assets*

Login consists of two phases: the offering of the ID and password, and the execution of the challenge and response procedure (Fig. 4). The system will only give a message that the login was incorrect after the user has entered a response code, even though the combination of ID and password incorrect. This is to view leak information or to show which part of the login procedure is incorrect. If there are three incorrect login attempts, the user must contact to the E-commerce company to reset his account. This means that a new shared secret will need to be created.

VI. Conclusion

This paper illustrated method of the proposal authentication system named Scan2Pass. At the beginning of this paper, it introduced the functional, non- functional and security requirements of the system. In addition the assumption needed to be held in the proposed system. After that, explanation in details of the conceptual framework of Scan2Pass system and show all the parts that involved the system. The fundamental operations flow of the proposed system was described in details. Scan2Pass consist of three phases which are registration, login, and recovery phases. Scan2Pass describe in detail the registration process, and operation of exchange the shared secret between the user and server over secure connection with the help of visual communication channel represented as a QR code technique with a camera of user's smartphone. The login phase explained the authentication process and shows the vital role of the shared secret with challenge response protocol which is important for providing a secure login and mutual authentication between user and the server. Scan2Pass system model is based on the assumption of combining multifactor authentication to provide a seamless and secure authentication process. Furthermore it gives an important functionality about one time password that ensures independence between each login session attempt.

References

[1] Abbadi, L. 2012. Multi-factor Authentication Techniques for Video Applications over the Untrusted Internet, Doctoral dissertation, University Of Ottawa. Chicago.

[2] Abukeshipa, A. S., & Barhoom, T. S. 2014. Implementation and Comparison of OTP Techniques (TOTP, HOTP, CROTP) to Prevent Replay Attack in RADIUS Protocol.

[3] Bickford, J., O'Hare, R., Baliga, A., Ganapathy, V., & Iftode, L. 2010. Rootkits on smart phones: attacks, implications and opportunities. In Proceedings of the eleventh workshop on mobile computing systems & applications: 49-54. ACM.

[4] Blaze, M., Diffie, W., Rivest, R. L., Schneier, B., & Shimomura, T. 1996. Minimal key lengths for symmetric ciphers to provide adequate commercial security.

[5] Common Criteria. 2012. Introduction and general model. Common Criteria for Information Technology Security Evaluation. National Security Agency.

[6] Dacosta, I., Chakradeo, S., Ahamad, M., & Traynor, P. 2012. One-time cookies: Preventing session hijacking attacks with stateless authentication tokens. ACM Transactions on Internet Technology (TOIT), 12(1):1.

[7] Dierks, T., Allen, C. 1999. The TLS Protocol Version 1.0. https://www.ietf.org/rfc2246[June 23rd 2015].

[8] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., Stewart, L. 1999. HTTP Authentication: Basic and Digest Access Authentication. https://www.ietf.org/rfc2617[June 23rd 2015].

[9] Freier, A., Karlton, P., Kocher, P. 2011. The Secure Sockets Layer (SSL) Protocol Version 3.0. https://tools.ietf.org/html/rfc6101[June 23rd 2015].

[10] Gaw, S., & Felten, E. W. 2006, July. Password management strategies for online accounts. In Proceedings of the second symposium on Usable privacy and Security: 44-55. ACM.

[11] Gehringer, E. F. 2002. Choosing passwords: security and human factors. InTechnology and Society, 2002. (ISTAS'02). 2002 International Symposium: 369-373.

[12] Hodges, J., Jackson, C., Barth, A. 2012. HTTP Strict Transport Security (HSTS).

[13] Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. Communications of the ACM, 47(4): 75-78.

[14] Jain, A. K., Ross, A., & Pankanti, S. 2006. Biometrics: a tool for information security. Information Forensics and Security, IEEE Transactions on, 1(2): 125- 143.

[15] Jennings, C., Fischl, J. 2011. Certificate Management Service for the Session Initiation Protocol (SIP). http://tools.ietf.org/html/rfc6072[June 23rd 2015].

[16] Kainda, R., Flechais, I., & Roscoe, A. W. 2009, July. Usability and security of out-of- band channels in secure device pairing protocols. In Proceedings of the 5th Symposium on Usable Privacy and Security: 11. ACM.

[17] Maitra, S., & Paul, G. 2008. Analysis of RC4 and proposal of additional layers for better security margin. In Progress in Cryptology-INDOCRYPT 2008: 27-39. Springer Berlin Heidelberg.

[18] Percival, C. Stronger key derivation via sequential memory-hard functions. 2009.

[19] Primmer, R., & D'Halluin, C. 2013. Collision and preimage resistance of the Centera content address. arXiv preprint arXiv:1306.6020.

[20] Van Do, T., Nachef, A., & Aussel, J. D. 2006. Offering SIM Strong Authentication to Internet Services. In White Paper, 3GSM World Congress, Barcelona.

[21] Wu, M., Garfinkel, S., & Miller, R. 2004. Secure web authentication with mobile phones. In DIMACS workshop on usable privacy and security software, Vol. 2010.

[22] Zhang, B., Ren, K., Xing, G., Fu, X., & Wang, C. 2014. SBVLC: Secure barcode-based visible light communication for smartphones. In INFOCOM, 2014 Proceedings IEEE: 2661-2669. IEEE.F