J Inf Process Syst, Vol.10, No.3, pp.483~490, September 2014
http://dx.doi.org/10.3745/JIPS.02.0005

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

Multifactor Authentication Using a QR Code and a One-Time Password

Jyoti Malik*, Dhiraj Girdhar**, Ratna Dahiya***, and G. Sainarayanan****

Abstract—In today's world, communication, the sharing of information, and money transactions are all possible to conduct via the Internet, but it is important that it these things are done by the actual person. It is possible via several means that an intruder can access user information. As such, several precautionary measures have to be taken to avoid such instances. The purpose of this paper is to introduce the idea of a one-time password (OTP), which makes unauthorized access difficult for unauthorized users. A OTP can be implemented using smart cards, time-based tokens, and short message service, but hardware based methodologies require maintenance costs and can be misplaced Therefore, the quick response code technique and personal assurance message has been added along with the OTP authentication.

Keywords—Authentication, One-Time Password, Personal Assurance Message, Quick Response Code

1. INTRODUCTION

Computer technology has come a long way in terms of communication, online banking, online shopping, etc., but it is very important that the actual/authorized individuals do the transactions. To prevent the confidential information from being accessed by unauthorized users, several schemes like using passwords, hardware devices, etc. are implemented. To ensure safe and secure remote authentications, multifactor authentication is used. Passwords, smart cards, tokens, etc. are difficult to manage. Due to advancements in mobile technology, we are proposing a quick response (QR) code with a one-time password (OTP) for remote authentication [1,2].

A QR code is a QR two-dimensional barcode. It can be read by using a smartphone. The large amount of data storage, readability in all the directions, and error correction capability are the advantages of using a QR code [3,4].

A OTP can be generated using 1) mathematical algorithm, 2) smart card, 3) time-based token, and 4) short message service (SMS). A one-way hash scheme is used in a mathematical algorithm based method. The maintenance and anti-theft/tampering measures of a password file cannot guarantee secure authentication. Smart cards are used in remote authentication due to being tamper-resistant and convenient to use. A user can forget to carry a smart card and it can

Manuscript received November 21, 2013; first revision October 03, 2013; accepted December 04, 2013.
Corresponding Author: Jyoti Malik (jyoti_reck@yahoo.com)
* Department of Electrical Engineering, National Institute of Technology, Kurukshetra, India (jyoti_reck@yahoo.com)
** Computer Associates, Bangalore, India (girdhar.dhiraj@gmail.com)
*** Department of Electrical Engineering, National Institute of Technology, Kurukshetra, India (ratna dahiya@yahoo.co.in)
**** HCL Technologies Pvt. Ltd., Chennai, India (sai.jgk@gmail.com)

be lost. Time based tokens are also hardware tokens that a user has to carry for authentication. They involve both a cost and inconvenience to the user. SMS can be more reliable for authentication as nowadays most everybody uses it. A service provider does not guarantee the delivery of SMS or that it will be delivered in a proper time span. As such there can be an issue with time limits for doing transactions. So the possibility of using SMS is also not the best way for doing what with authentication.

The best method to use is to integrate a Web-based application with mobile-based technology. As such, we are proposing a QR code, personal assurance message (PAM), and OTP in this paper [4,5]. The paper is organized as follows: the proposed QR code, PAM, and OTP are proposed in Section 2. Section 3 explains the security analysis and benefits of our proposed scheme. The paper is then concluded in Section 4.

2. PROPOSED SCHEME

The main aim of the proposed scheme is to use multifactor techniques like a QR code and a OTP to eliminate the drawbacks of single factor authentication. It is about combining Web applications and mobile devices for authentication. The authentication process involves the two stages of enrollment and verification.

2.1 Enrollment Stage

Authentication takes place between two parties of a server and a user. The various steps involved in the enrolment process are explained below.

Step 1: The server asks the user to send the customer ID (suppose on Web page), as shown in Fig. 1. The customer ID generated by the server is a unique identity.

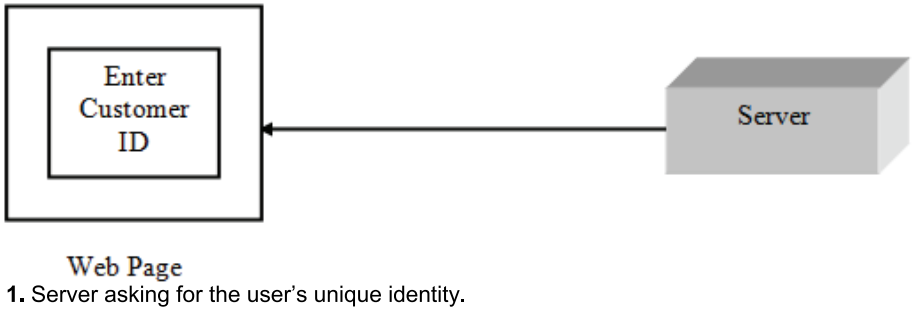

Fig. 1. Server asking for the user's unique identity.

Step 2: The user sends the server their unique customer ID as shown in Fig. 2. The server displays a set of PAM images and a PAM text message as shown in Fig. 3. The PAM image is chosen in the enrollment stage.

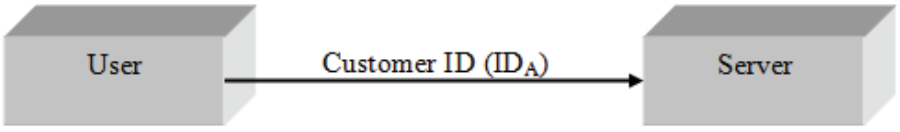

Fig. 2. User sending their identity to the server.

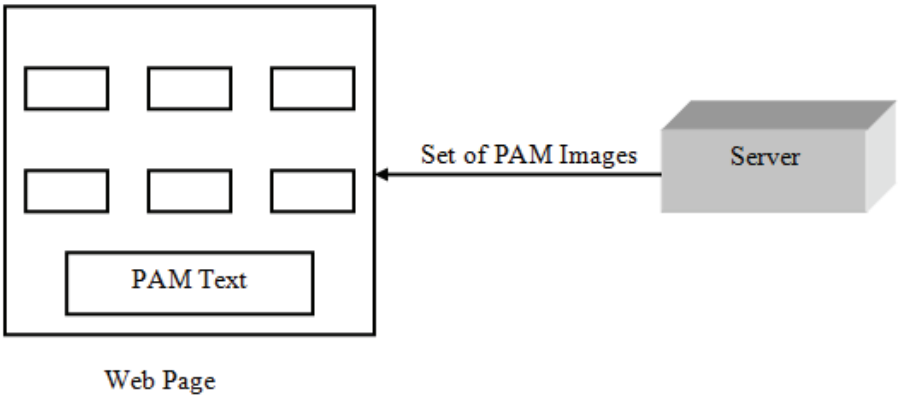

Fig. 3. Server displaying personal assurance message (PAM) images for the user.

Step 3: The user selects the PAM image from a set of PAM images and a PAM text message as shown in Fig. 4.

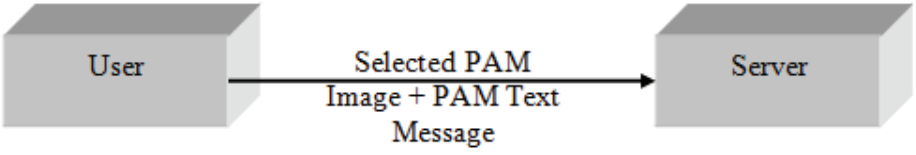

Fig. 4. User selecting personal assurance message (PAM) images from the list of images.

Step 4: The server sends the customer ID (ID_A) digest and server secret key (S). The digest can be generated using a hash operation of the customer ID and server secret key as shown in Fig. 5. The digest is stored on the user's mobile device.

$$D_A = H(S, ID_A) \tag{1}$$

where, D_A is the digest sent to user A, H(.) is the one-way hash function, S is the server's secret key, and ID_A is the user's identity.

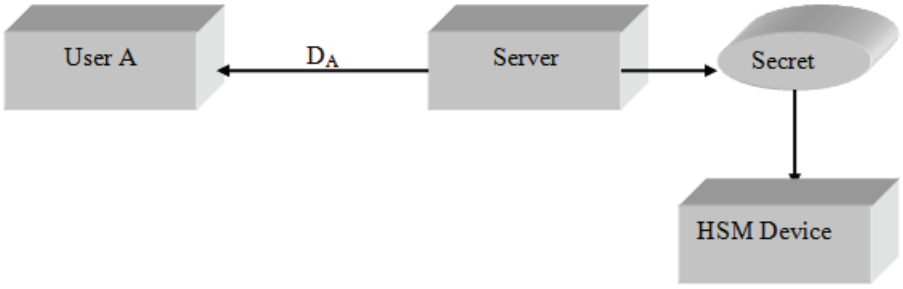

Fig. 5. Server sending the D_A digest to the user.

2.2 Verification Stage

The various steps involved in the verification process are explained below.

Step 1: The server asks the user to send the customer ID as shown in Fig. 6.

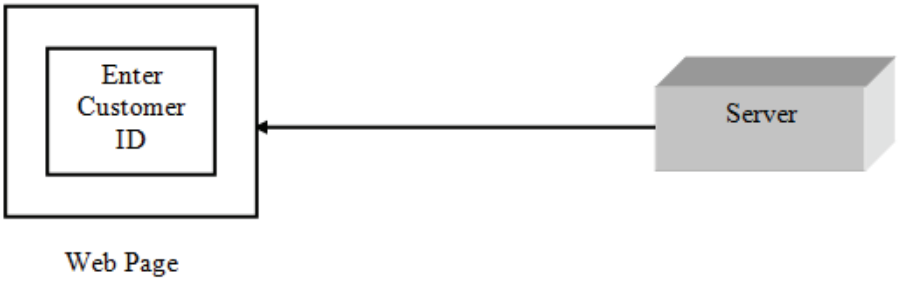

Fig. 6. Server asking for the user's unique identity.

Step 2: The user sends the server their unique customer ID as shown in Fig. 7. The server displays PAM images and a PAM text message as shown in Fig. 8.

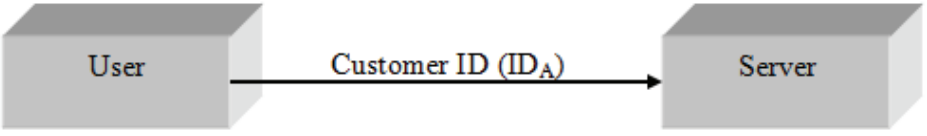

Fig. 7. User sending their identity to the server.

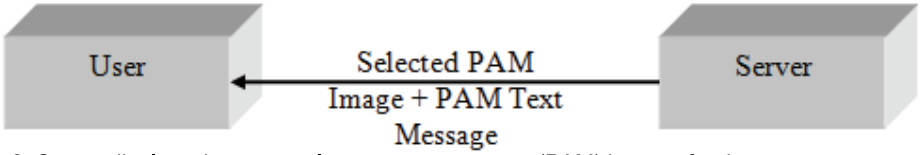

Fig. 8. Server displays the personal assurance message (PAM) images for the user.

Step 3: The server chooses a random number (R_N) and computes $D_A = H(S, ID_A)$ as used in Eq. (1).

$$\alpha_1 = D_A \oplus PAM\ Image \tag{2}$$

$$\alpha_2 = D_A \oplus PAM\ Text \tag{3}$$

$$\alpha_3 = D_A \oplus R_N \tag{4}$$

$$\alpha = E_{QR}\left(\alpha_1,\ \alpha_2,\ \alpha_3\right) \tag{5}$$

where, $E_{QR}( )$ is a function to encode the PAM image, PAM text, and R_N into the QR code image.

$$H_1 = H\ \left(PAM\ Image, PAM\ Text, T_1, R_N\right) \tag{6}$$

where, H(.) is the one way hash function, T_1 is time stamp attached by the server, and R_N is a random number. The server sends T_1, α, and H_1 to user A.

Step 4: The validity of the server is checked by the time stamp T_1, which is sent by the server in Step 3. If it is valid, the user derives the information from α sent by the server as shown by the equations below.

$$D_{QR}(\alpha) = \left(\alpha_1,\ \alpha_2,\ \alpha_3\right) \tag{7}$$

The user decodes α using the key available on their mobile phone sent by server (in step 3). Using D_A, various components in information can be extracted, like the PAM image, PAM text and a Random number.

$$D_A \oplus \alpha_1 = PAM\ Image \tag{8}$$

$$D_A \oplus \alpha_2 = PAM\ Text \tag{9}$$

$$D_A \oplus \alpha_3 = R_N \tag{10}$$

T_1 is the time stamp attached by the server.

In this step, the user verified the data integrity by using the hash value sent by the server and a time stamp also verifies it. In this way, the user verified the server on the basis of PAM images, a PAM text, a random number, and a time stamp. The next step is the verification of the user by the server.

Step 5: The validity of the user is checked by the server using time stamp T_2, which is sent by the user. The user key that is stored on the mobile phone and the time stamp T_2 generates a OTP using the OATH algorithm as shown in Eq. (11).

$$OATH\left(D_A,\ T_2\right) = OTP \tag{11}$$

$$H\left(OTP,\ R_N\right) = \beta \tag{12}$$

T_2 is the time stamp attached by user

User A sends T_2 and β to the server.

Step 6: The server checks the validity of time stamp T_2. If it is invalid, the server refuses the access request. Otherwise, it will verify whether β is the hash value of OTP and R_N. If the server found the information to be correct, the user is validated.

3. PERFORMANCE AND SECURITY ANALYSIS

We tested the performance of this Web application is on a laptop (Intel i5, 1.80 GHz processor, 4 GB RAM) and a mobile phone (2 GB RAM, quad-core 1.5 GHz processor). There were no performance related issues with the configurations for either the user (mobile) or the laptop. The proposed approach to achieve two-factor authentication is very robust, secure, reliable, and very hard for illegitimate users to crack.

We analyzed the proposed scheme under the possibilities of the types of attacks listed below.

1) Attempt to get the server's secret key

If the intruder tries to find the secret key S from Eq. (1), then it can access the user. But it is impossible to get S from Eq. (1) as it is a one-way hash function that generates the D_A digest and S cannot be derived from it.

$$D_A = H\left(S, ID_A\right)$$

2) Repeat/copy

The user information cannot be repeated/copied/reused, as it expires after the user is authenticated. T_1, T_2 and OTP will expire after authentication.

3) Attempt to get a user's secret key

It is impossible to know α_1, α_2 and α_3 from Eqs. (2)-(4), (8)-(10) without knowing the PAM image, PAM text, and random number.

$$\alpha_1 = D_A \oplus PAM\ Image$$

$$\alpha_2 = D_A \oplus PAM\ Text$$

$$\alpha_3 = D_A \oplus R_N$$

$$D_A \oplus \alpha_1 = PAM\ Image$$

$$D_A \oplus \alpha_2 = PAM\ Text$$

$$D_A \oplus \alpha_3 = R_N$$

4) Man-in-the-middle attack

The OTP generated on the mobile of user and the server using D_A is not traveling on network and all the communication between the user's phone and server are always encrypted. Therefore, it cannot be accessed by the man-in-the-middle.

5) Replay attack

Suppose the intruder knows the random number (R_N) and tries to replay the request as in Eqs. (11) and (12) with time stamp T_2. The server checks at what time interval (T_2'') the request is received. If the time stamp T_2 and T_2'' are not within the time interval, the server will reject the intruder's attempt to access the online service because the random number keeps changing as time passes.

$$OATH\left(D_A,\ T_2\right) = OTP$$

$$H\left(OTP,\ R_N\right) = \beta$$

T_2 is the time stamp attached by user

6) Phishing attack via the web

If the intruder knows the user ID and can get the D_A digest from the server by replacing the actual web page with a similar one, it would be difficult to get the PAM image and PAM text because it is displayed in the form of a set of PAM images and a PAM text. It has to be chosen within a specified time stamp.

4. CONCLUSION

Nowadays, the majority of the population has smartphones that are able to access various applications, like scanning QR-codes and doing online transactions etc. The purpose of the paper is to integrate a web based application with mobile-based applications to make it more secure than the general authentication methods. The integration of web and mobile-based applications is a two-factor authentication approach that is better than the general username and password approach. In this paper, a QR code, PAM, OTP, and random number are used together to create safe access across the web via the usage of mobile devices. By using combinations of various entities like QR code, PAM etc, this method is safe and very reliable for online transactions and other applications [4].

REFERENCES

[1] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Computers & Security*, vol. 21, no. 4, pp. 372- 375, Aug. 2002.

[2] Y. Liu and M. Y. Liu, "Research on data encoding of two-dimensional QR code barcode," *Journal of Beijing Institute of Technology*, vol. 25, no. 4, pp. 352-355, Apr. 2005.

[3] R. Zhang, H. Zhu, T. Zhang, and X. Shen, "A pre-processing method on QR code two dimensional code image", *Computer Science*, vol. 35, no. A, pp. 146-148, 2008.

[4] H. W. Liu and Y. Yan, "Recognition and decoding of QR code", *Computer Engineering* and *Design*,

vol. 26, no. 6, pp. 1560-1562, Jun. 2005.
[5] H. J. Liu, "Omnidirectional recognition of quick response code image", *Chinese* Journal *of Scientific Instrument*, vol. 27, no. 4, pp. 376-379, Apr. 2006.

Jyoti Malik

She received her B.Tech in 2002 from R.E.C, Kurukshetra University, Haryana, and M.Tech in 2004 from NIT, Kurukshetra, Deemed University, Haryana. Presently, she is pursuing her Ph.D. in the area of biometric authentication from NIT, Kurukshetra. Her research interests are Image processing, Pattern recognition and Signal processing.

Dhiraj Girdhar

He received his B.E. (gold medalist) in 2003 from Sant Longowal Institute of Engineering and Technology (SLIET), Sangrur, Punjab Technical University, Punjab. M.S. in 2007 from BITS, Pilani. Presently, he is working with Computer Associates, Bangalore. His research interests are image processing, pattern recognition, multimedia and cryptography.

Ratna Dahiya

She received her B.Tech from GBU, Pant Nagar and M.Tech and Ph.D. degree in Electrical Engineering from R.E.C, Kurukshetra, Kurukshetra University, Haryana, India. Currently, she is working as Assist. Professor in Electrical Engineering Department with the NIT, Kurukshetra (Deemed University), Haryana, India. Her research interests include image processing, pattern recognition, SMES, induction machines, power quality, motor drives and renewable energy.

G. Sainarayanan

He is currently working in HCL Technologies Pvt. Ltd. He received his B.E., M.E., and Ph.D. degrees, respectively, from Annamali University, India, Bharathiar University, India, and University Malaysia Sabah, Malaysia, in 1998, 2000, and 2002. His research interests are in the areas of vision rehabilitation, medical imaging and intelligent control.