ENHANCED SECURITY APPROACH FOR ONLINE USER AUTHENTICATION

[1]Srinivasan Jayaraman, [2]Taru Tak, [3]Isha Patil, [4]Neeti Deshmukh, [5]K.V Deshpande
[1,2,3,4]Students, [5]Asst. Prof
[1]Computer Engineering, Rajarshi Shahu College of Engineering,
[1]Savitribai Phule Pune University, Pune, India

Abstract— In Quick Response (QR) codes can be used efficiently to store small data. They are two dimensional barcodes. Smartphones can be used as QR code scanners. As the market of smartphones is increasing day by day, the no of applications in which QR codes are used is increasing. Even though QR codes have many advantages because of which they are very popular, there are many security risks and issues associated with them. While the user is reading the QR code in the foreground, he may be subject to many security risks in the background like running malicious code, identity theft, violation of their privacy and loss of information. In this project, a security system for QR codes that guarantees both users and generators security concerns is implemented. The system is backward compatible with current standard used for encoding QR codes. The implementation of the system and its testing is done by using an Android-based smartphone application. It was found that the system introduces a little overhead in terms of the delay required for integrity verification and content validation.

Index Terms – QR codes, online privacy, mobile security, secured authentication, smartphone

I. INTRODUCTION

Today Internet is the most widely used medium for accessing the information. On the internet, many websites are available for providing the information and also most of the services are getting Online such cloud security, banking, insurance, shopping etc. These services providing websites requires the strong authentication. Multiple authentication methods have been developed such smart card based system, one time password, SMS based OTP system and some using biometric features. Some of these authentication systems require hardware devices, and this increases the cost. Users also have their accounts at many web sites, and they have to remember passwords of all these sites. To make the access easier, many websites support the concept of federated identity management, in which the user having a single account can log on to the other websites by authenticating themselves to a single identity provider. Android smart phones are getting more popular. In this paper, a system is proposed for secured authentication using Challenge Response, Quick Response Code, the identity provider and mobile phone, the most commonly used device. A Quick Response code is a two dimensional matrix code. It can store large amount of encrypted data, and it also has error correction ability.

II. RELATED WORK

[1]Kyeongwon Choi, Changbin Lee, Woongryul Jeon, Kwangwoo Lee and Dongho Won, "A Mobile based Anti-Phishing Authentication Scheme using QR code" ACM SIGMOD Record, vol. 39, no. 4, pp. 12–27, 2010.

Due to the development of information and communication technology, protecting the personal authentication information from infected computer or web phishing has become a crucial task to be achieved. Using a pair of username and password authentication scheme is no more secure since attacker can collect information from web phishing and computer infection. Various malwares or intended programs attempt to capture the sensitive information from personal computer. Therefore, secure authentication scheme is required. In this paper, we propose a anti phishing single sign-on (SSO) authentication model using QR code. This scheme is secure against phishing attack and even on the distrusted computer environment.

[2]Syamantak Mukhopadhyay, David Argles. "An Anti-Phishing mechanism for Single Sign-On based on QR-Code. International Journal of Video & Image Processing and Network Security IJVIPNS 10, no. 04.

Today internet users use a single identity to access multiple services. With single sign-on (SSO), users don't have to remember separate username and password for each service provider, which helps the user to browse through the web seamlessly. SSO is however susceptible to phishing attacks. This paper describes a new anti phishing SSO model based on mobile QR code. Apart from preventing phishing attacks this new model is also safe against man in the middle attack and reply attacks

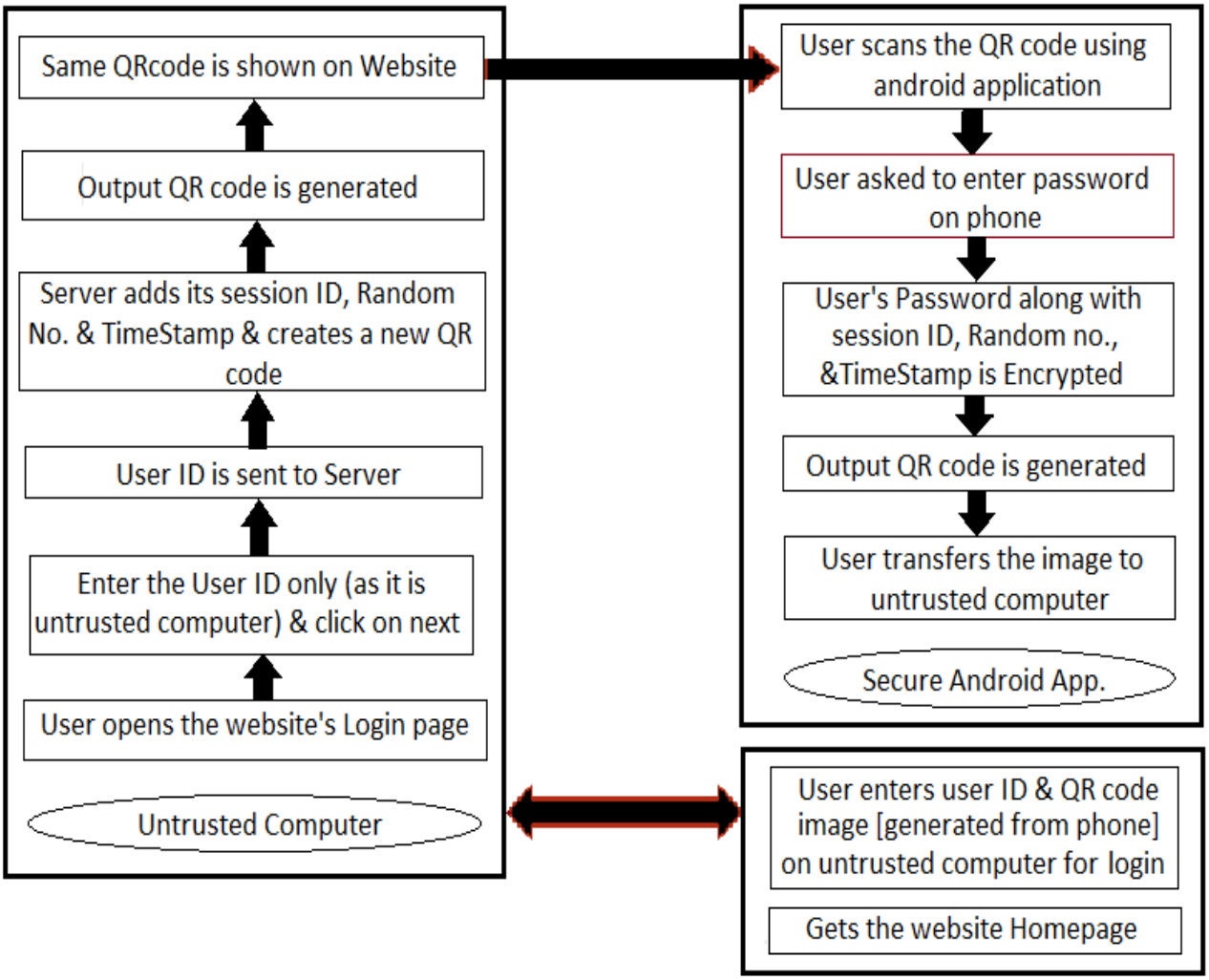
[3] "A Novel Approach for User Authentication to Industrial Components Using QR Codes." Alexander Borisov, Robert Bosch.

First, common requirements for a secured communication in an industrial environment will be presented. Second, the comparison of different authentication techniques with focus on one-time passwords will be given. Third, a new model for user authentication with QR codes will be presented. Additionally, a procedure for generating time based one-time passwords is shown. Finally, the presented approach is compared to other popular authentication techniques with an analysis in terms of security, deployability and usability.

III. PROBLEM DEFINITION

To create an application that will run on android based devices. Its primary purpose would be to make use of QR code for banking transaction. It would be consisting of three modules, QR code generation and scanning, AES encryption module and communication module. Two phase of System Registration phase and login phase. Firstly user will open the website's login page and will enter user ID and is sent to server. Output QR code is generated and displayed, user scans the QR code using android application and the generated QR code is sent to untrusted system.

IV. PROPOSED SYSTEM



The following are the points that mention the overall working of the proposed application:

- A mobile banking transaction on untrusted system.
- Server adds session id, random number and timestamp and creates QR code.
- Generates and scans QR code using android application.
- User's password along with generated session id, random number and timestamp is encrypted and a new QR code is generated.
- User transfers the image to the untrusted computer.
- The transferred QR code along with user id is entered on the website home page.
- If verified then transaction proceeds.

IV.CONCLUSION

Security has become extremely important in the digital society. Authentication methods should be seriously considered by services that store sensitive information. Most of the users have android smart phones. These Smart phones have good processing power and memory size.

As a mobile phone has become an indispensable accessory and carry-on device in real life, compared with the traditional key or access card, sending the authentication image by using mobile phones through MMS (Multimedia Messaging Service) allows the user to carry fewer objects and no extra specific hardware cost needed. So some security features can be deployed on them in order to identify a user to the service provider.

Using QR Code, successful authentication can be done. The use of QR code image for authentication makes it difficult to be accessed, modified and copied, and it can be applied to many services that require authentication.

V.REFERENCES

[1] Mukhopadhyay, S.; Argles, D., "An Anti-Phishing mechanism for single sign-on based on QR-code," Information Society (i-Society), 2011 International Conference on , vol., no., pp.505,508, 27-29 June 2011

[2] A.S. Narayanan. "QR Codes and security solutions," International Journal of Computer Science and Telecommunications Volume 3, Issue 7, July 2012

[3] Soon,TanJin.,"QR Code." ,Synthesis Journal: 59-78

[4] AvielD.Rubin. "Independent One-Time Passwords", June 1995. Website- http://avirubin.com/onetime.pdf6

[5] Azhar,Rizwan."Camera Based Authentication Methods". Website www. ida.liu.se/ TDDD17/old projects/2010/projects/ 011.pdf

[6] Open ID Foundation, "Get an Open ID". [Online]. Available:http://openid.net/get-an-openid