International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp.79-86
http://dx.doi.org/10.14257/ijsia.2014.8.3.09

A Design of e-Healthcare Authentication Framework with QR Code

Non Thiranant[1] and HoonJae Lee[2]

1 Department of Ubiquitous IT, Graduate School of Dongseo University, Sasang-Gu, Busan 617-716, Korea
2 Division of Computer and Engineering Dongseo University Sasang-Gu, Busan 617-716, Korea
thiranant.non@gmail.com, hjlee@dongseo.ac.kr

Abstract

E-Healthcare is a term globally used for electronic healthcare, where a variety of services and systems provided include electronic healthcare records, prescriptions, patients' health records, healthcare information systems, etc. In this modern decade, a rising number of patients have taken e-Healthcare into consideration, as it provides the convenience of services and delivered at lower cost. The popularity and reputation have been increasing due to a wide range of services. From the system administrator's point of views, protecting privacy of patients and building trust of patients in e-Healthcare are two main issues. In this paper, an effective design of authentication framework that suits the modern e-Healthcare is proposed.

Keywords: *Privacy, E-Healthcare, Web authentication, Mobile authentication, Two-factor authentication, QR Code, Mobile device information*

1. Introduction

E-Healthcare has expanded its achievement and popularity from time to time, due to a wide range of services provided. In theoretical and practical, the system has to be secure and e-Healthcare service provider is entrusted with the responsibility to handle the sensitive information [1]. The e-Healthcare system encounters many threats such as patients' sensitive information are in wrong hands, unreliable authentication process, and confidentiality of patients. The factors mentioned above may result in a critical impact directly or indirectly to the patients, as well as the reputation of the service providers. Data integrity and availability are similarly of excessive importance; as a patient's life could depend upon the security of the e-Healthcare system. Patient's information should be well protected and ensured that it is always up-to-date, and will not be altered by those who have no right [1, 2].

It is well known that e-Healthcare involves a various types of users such as patients, doctors, nurses, etc. who can access electronic medical information. Each type of user has different assigned roles and tasks, perhaps having limitations to access some information. For example, doctors and nurses have right to access and modify the medical records of patients' diagnosis results, but this information shall not be accessed by patients.

In order to ensure the privacy of patients in e-Healthcare system, only insensitive information is revealed to all types of users. It can be easily achieved by having a clear separation line between each of user type. The sensitive information must be under control and permission to access and exchange data is based on their roles. A strong authentication process is the first step that each system should be aware of. A weak authentication system

ISSN: 1738-9976 IJSIA

may result in information leakage, and it is a possibility that patients will be the victim as the medical records are altered.

In this paper, a design of e-Healthcare authentication framework is proposed. The process includes the use of QR Code and smartphone, together with the web application and web services that can handle many transactions at a time and be able to detect the electronic device details. This authentication technique is not limited to e-Healthcare system, as it can as well be applied to other systems. At this point, the paper is focused on the design system for the authentication process in e-Healthcare. With the proposed technique and approach, e-Healthcare service is secure and cost-effective.

2. Background and Related Work

1. Web Authentication and Web Service

It is widely known that a number of people relying on internet, to accomplish their tasks are increasing. The authentication system should be developed in order to satisfy users from time to time. In the modern web applications, mutual authentication is provided. A pair of username and password is considered insufficient for a strong authentication process. Phone number, device detection, location detection, and keystroke behavior are now used together with username and password for the authentication process. A Web service a method of communication between electronic devices over internet. It is a software function provided at a network address over the web or the cloud. It is considered a software system designed to support interoperable machine-to-machine interaction over a network. Systems interact with the Web service by its description using SOAP messages, typically conveyed using HTTP with an XLM serialization in conjunction with other Web-related standards.

2. QR Code

QR (Quick Response) Code is the trademark for a type of two-dimensional matrix barcode introduced by the Japanese company Denso-Wave in 1994. A barcode is an optically machine-readable label that is attached to the product with the information related to that item. The common information encoded into QR Code form is of the type string, number, bytes, and ASCII characters. QR Code has now been widely used in a variety of fields, such as URLs, business cards, sales wrapping, code payments, etc. A study by MRI shows that 90% of Japanese mobile phone users have a QR Code scanner. Figure 1 depicts the structure and components of QR Code [3, 4].

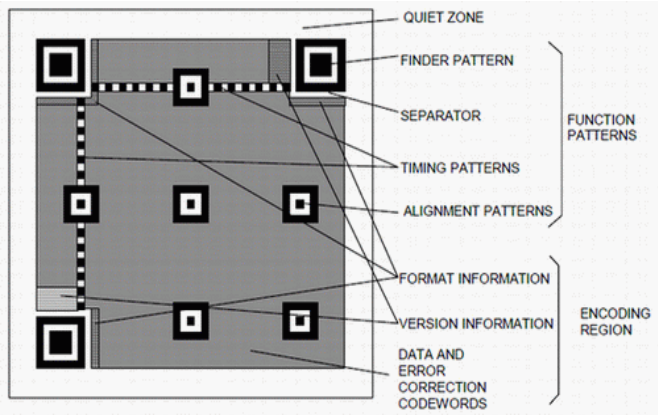

Figure 1. QR Code Structure

3. Mobile Device Information

Mobile devices such as smartphones and tablets have been popularly used all over the world. Each mobile device is unique in terms of the device serial embedded. This information of the device makes itself unique, which different from others, and managed by the product company. With mobile device information as a parameter for the authentication process, the risks can be effectively reduced. Motivated by this idea, a new approach is proposed by including the device information detection for the authentication process.

4. Authentication and Authorization Framework

S.Han, G. Skinner, V. Potdar, E. Chang proposed a technique for authentication and authorization for e-Healthcare is proposed. The work suggests that authorization and authentication are to be performed simultaneously and sequentially for the access control. The limitation is that design and implementation are not provided [6].

The previous work on an implementation of a simple two-factor authentication was proposed. It utilizes the usage of QR Code nowadays and a smartphone device for a secure login transaction. The system does not require users to type their password. The idea of this system is to leverage the mobile device as a personal identifier, and bring advantages in order to improve the security in authentication process in terms of the mobility, efficiency and flexibility of the system [7].

Mungyu Bae, Suk Kyu Lee, Seungho Yoo, and Hwangnam Kim proposed an idea of using one-time password scheme with QR Code based on mobile phone was proposed. The major concern of this scheme is to make use of the deployed widespread QR Code techniques. It is separated into two phases: Registration and Verification phases. The paper shows the security analysis which is proved to be safe from illegal users' attempt and man-in-the-middle attack [8].

3. Proposed Technique and Implementation

The proposed authentication technique essentially makes use of the existing QR Code technology, web application, web services, and mobile device. Mobile device is used as a personal unique identifier, where embedded serial of each device is parameter for the authentication process. The web application includes the normal authentication process, where a pair of username and password is used. Detecting device information and generating QR Code are two main features added to this scheme. A database is needed along with the web service to store user's identification information, registered device information, one-time QR Code, *etc*.

In the hospital system; doctors, nurses, and other related staffs have own mobile devices and registration is needed for a pair of username and password. They are only allowed to access the system using their registered device with username and password. In case the system is accessed from unregistered devices, an extended authentication process will be activated, where QR Code will be generated and shown on the screen. Users are required to use their registered devices with the QR Code scanner application to scan and transmit the one-time password back to the web server.

With this authentication method, the system relies on the web server, a mobile device, and web services which serve as the medium between mobile application and web server. Mobile devices with internet connection; says WiFi or 3G technology allows users to access the web server from anywhere. User has two ways to access the system. The first one, user can use his/her own registered mobile device together with their username and password pair. The second one, user uses any other devices to access the system; but in this case he/she has to use

his/her registered mobile device to snap the given QR Code and transmit back to the web server for the authentication.

1. System Requirements

Web service is implemented as an intermediary consumed by web application and mobile application. Any web-based programming language can be used to implement. A database is built along with the web service to store data when users interact via website interface. More emphasis should be placed on the mobile application that can handle QR Code, and transmit the decoded message to the web server.

2. System Overview

Figure 1 depicts the architecture of the proposed system, which shows the overall process. Users have two alternate ways to access the system. It is either by using the registered mobile device or personal computer. The information needed to access the system via the registered mobile device is username, password, and device serial number. When a user uses the mobile device to access the system, username and password will be checked accordingly; followed by the device information. In case a user requests to access from unregistered devices such as personal computer or laptop, he/she is required to use his/her registered mobile device to decode the one-time QR code for identification verification. This QR Code will be generated and displayed on the screen whenever the system is accessed from unregistered devices.

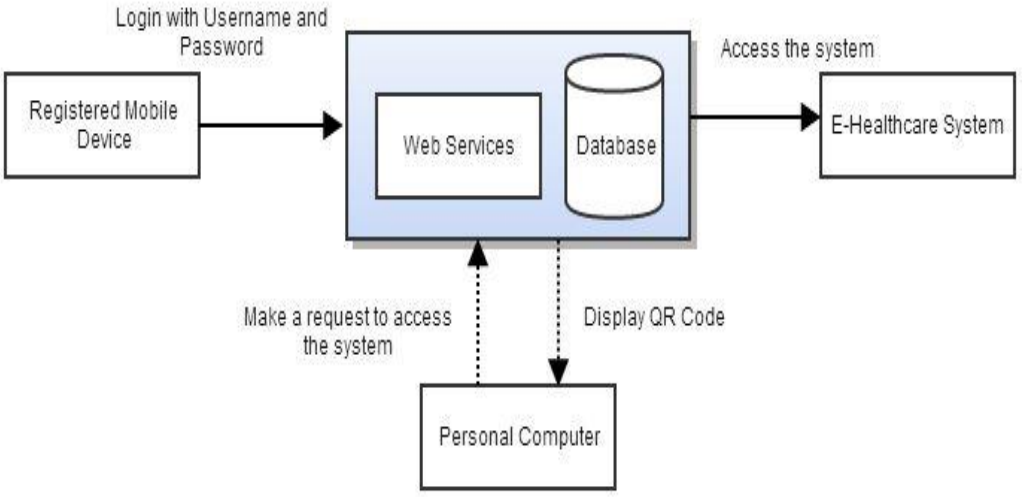

Figure 1. Architecture of the Proposed System

3. Registration Process

Figure 2 depicts the registration process which is the primary step for every type of user. When a user registers for an account, information has to be provided. The information includes a pair of username and password, device serial number, and mobile number. All the user information is encrypted and stored in the database of e-Healthcare system. These parameters shall be verified when an access is requested. All the registered information will be stored in the web server.

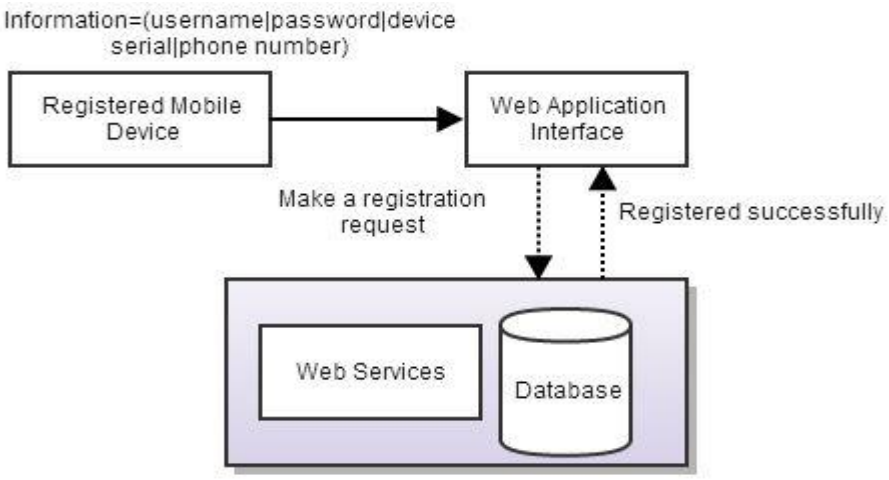

Figure 2. Registration Process

4. Verification Process

Figure 3 depicts the verification process which is required when a user request an access to the system. This figure shows the process when a user accesses the system using unregistered device; says personal computer. User inputs username and password normally via the web interface. The authentication server would detect that the device information is not in the list, and one-time password will be encoded into the form of QR Code and displayed on user's personal computer. The user is then required to use registered mobile device to decode the given QR Code and send to the web authentication server, using the specific mobile application. Lastly, the authentication server will verify the information including mobile device serial number, and mobile number. Once the verification process is completed, the access request will be granted.

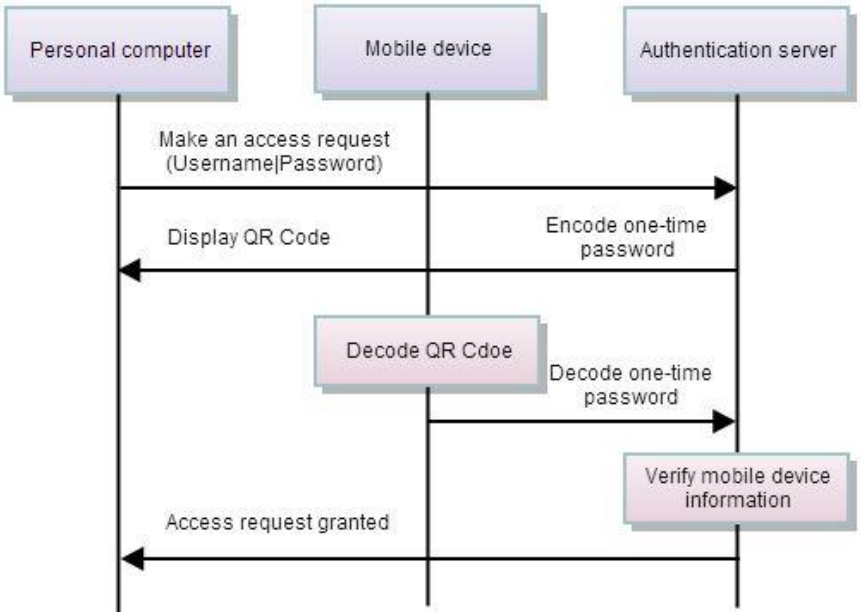

Figure 3. Verification Process

4. Security Analysis

1. Man-in-the-middle attack

Suppose an attacker manages to steal username and password pair from a user. It is still impossible to access the system without registered devices. In order to access the system, the attacker needs to have the registered mobile device together with the username and password.

2. Brute force attack

With the proposed system, it is impossible to perform the brute-force attack. The one-time password is encoded into the form of QR Code, and it is to be decoded by the unique mobile application designed for e-Healthcare system. Brute force attack can only be performed to get username and password, but it is meaningless unless the attacker has the registered device.

3. Phishing attack

Phishers cannot exploit a breach in the system since there is no use setting up a spoof of a website, since QR Code can only be decoded and mobile device is used as a unique identifier. Each mobile device is unique, which means each is different from others. Thus, threats from phishing and man-in-the-middle attack can be overcome.

4. Application security

The application is basically delivered via the internet through a web browser. The problem may arise if there are flaws involved in the web application, and this may produce various vulnerabilities for the software as a service application (SaaS). It has always been a problem, because traditional security solutions are not protecting effectively against recent threats nowadays. In this case, the web application should be carefully implemented. The strong authentication process is required for the safety of data.

5. Data security and Accessibility

Data security is a common concern in the proposed scheme. From the proposed idea, the data processed should be transmitted in the proper encrypted form. Despite the fact above, it is still a big challenge because users have to rely on the service providers for the appropriate security. In addition, accessing the web application over the internet makes access from any device; information stealing in the intermediate state with the modern technology is still a problem.

5. Conclusion

In this paper, multi-factor authentication system for e-Healthcare system is proposed. The system utilizes the popular usage of QR Code and smartphone device for a secure authentication process. Multi-factor authentication includes mobile device information detection, username and password pair, and maybe as well mobile number. With the proposed system, the vulnerability of a traditional authentication process can be overcome. In addition, the registration and verification processes are explained. The core idea of this system is to leverage the mobile device as a personal and unique identifier for each user. The system brings many advantages in enhancing the security of the secure authentication process in terms of mobility, efficiency, and flexibility.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology. (Grant number: 2013-071188. And it was also supported by the BB21 project of Busan Metropolitan City

References

[1] R. Agrawal, A. Kini, K. LeFevre, A. Wang, Y. Xu and D. Zhou, "Managing Healthcare Data Hippocratically", Proc. Of ACM SIGMOD International Conference on Management of Data, Paris, France, **(2004)** June.
[2] A. Boonyarattaphan, Y. Bai and S. Chung, "A Security Framework for e-Health Service Authentication and e-Health Data Transmission", Institute of Technology, University of Washington, Tacoma, **(2009)**.
[3] K. Choi, C. Lee, W. Jeon, K. Lee and D. Won, "A Mobile based Anti-Phishing Authentication Scheme using QR code", Information Security Group Sungkyunkwan University, **(2011)**.
[4] D. Pintor Maestre, "QRP: An improved secure authentication method using QR code", Universitat Oberta de Catalunya, **(2012)**.
[5] K.-C. Liao, M. Hsuan Sung, W.-H. Lee and T.-C. Lin, "One-Time Password Scheme with QR Code Based on Mobile Phone", Fifth International Joint Conference on INC, IMS and IDC, **(2009)**.
[6] S. Han, G. Skinner, V. Potdar and E. Chang, "A Framework of Authentication and Authorization for e-Health Services", Proc. Of the 3rd ACM workshop on secure web services, **(2006)** November, pp. 105-106.
[7] N. Thiranant, Y. Tan Ying Hui, T. Y. Kim and H. J. Lee, "Challenge-Response Authentication with a Smartphone", Dongseo University, Dept. Information & Comm. Eng., **(2012)**.
[8] M. Bae, S. Kyu Lee, S. Yoo and H. Kim, "FASE: Fast Authentication System for E-health", Ubiquitous and Future Networks (ICUFN), Fifth International Conference, **(2013)**.
[9] A. Sun, Y. Sun and C. Liu, "The QR-code reorganization in illegible snapshots taken by mobile phones", In Computational Science and its Applications, 2007. ICCSA 2007. International Conference, IEEE, **(2007)** August, pp. 532-538.
[10] Y. Liu, J. Yang and M. Liu, "Recognition of QR code with mobile phones", Control and Decision Conference, 2008. CCDC 2008. Chinese, IEEE, **(2008)** July, pp. 203-206.
[11] Y. H. Chang, C. H. Chu and M. S. Chen, "A General Scheme for Extracting QR Code from a non-uniform background in Camera Phones and Applications", Multimedia, 2007, ISM 2007, Ninth IEEE International Symposium, IEEE, **(2007)** December, pp. 123-130.
[12] K. Choi, C. Lee, W. Jeon, K. Lee and D. Won, "A mobile based anti-phishing authentication scheme using QR code", Mobile IT Convergence (ICMIC), 2011 International Conference, IEEE, **(2011)** September, pp. 109-113.