ISSN 2320 2629
Volume 9, No.6, November - December 2020
International Journal of Information Technology Infrastructure
Available Online at http://www.warse.org/IJITI/static/pdf/file/ijiti02962020.pdf
https://doi.org/10.30534/ijiti/2020/02962020

Two Factor Authentication by Using SMS for Web Based Application

Firkhan Ali Bin Hamid Ali, Mohammad Zaim Bin Mohammad Hanza,[1]
MohdKhairul Amin B. Mohd Sukri[1]
[1] Faculty of Information Technology and Computer Science,
UTHM, 86400 Parit Raja, Johor, Malaysia, email: firkhan@uthm.edu.my

ABSTRACT
Two factor authentications had two entry levels for authentication's mechanism. This study had used Short Messaging Service (SMS) technology as a second factor in doing authentication on the web application. It can minimize the problems that occur regarding to the illegal access over the user privacy information on the Internet. The system that uses two factor authentications is capable to give the priority and safety in aspect of user's privacy information from the web based applications.

Key words: *Two factor authentication, authentication, SMS, web, user privacy.*

1. INTRODUCTION

The study is focus on develop a web based system that will secure the user's data and information through online services. Authentication is an important aspect in any web based applications to ensure the user is a truly, valid and genuine user [1].

Authentication system in this study is use two factor authentication's technique. Two factor authentications are among the best technique to ensure the user's data and information are keep in safely from the frauds and cheating [2].

In accessing web application, the users need to use these two layers of authentication. Two layers of authentications are use web technology and SMS. Usually, web applications are use one layer of authentication only which is login and password. This technique will make any penetration to the system is become easier and simple. Two factor authentications are one technique that executed authentication over the things that we know and the things that we have. As an example is the use of authentication to withdraw the moneys from ATM machine at the bank which is we have the password that we know and use it within the ATM card that we have.

Today, the implementation of two factor authentication into web based system is not much use in Malaysia. Usually the systems use one factor authentication which is authenticating by login and password.

The study is more focus into the using of two factor authentication system which is first factor, it use the web authentication technology, login and password. Then, the second factor, it use secret word that will be sending through the SMS to the user's cell phone. Authentication code in this secret word is only will accepted by the register user's cell phone. The use of that mechanism will be secure more important data for users such as account bank number, card credit's number andothers from threats and frauds. If the first layer of this authentication had been penetrated, they only can get login and password but they need pass second authentication to access the account and they need the user's cell phone.

2. LIMITATION OF USING LOGIN AND PASSWORD

Basically, the usage of password for any application's authentication is never changes regularly and it will open to the threats. The organization procedure or policy must state that the password must be change at least on every 3 months.

Then, the owner will choose the password that easy for them to remember it. So, it's defiance within the security practice that the password must be difficult to guess such as by using a series of random characters for password.

Within this limitation aspects and more, the use of password only is vulnerable to many of possible threats such as Malware attack, guess the password, steal the password, shoulder surfing, phishing and others. However, it can minimize on the user part by using two factor authentication method.

3. METHOD AND DESIGN

First, one simple e-commerce web site had developed to implement this dual factor authentication's technique and concepts [3]. Then, One SMS software gateway had installed and connected to this e-commerce web site. This is to

make up the functionality of the dual-factor authentication system by using SMS.

The methodology of prototyping had used to develop this system as like in the Figure 1 as follow.

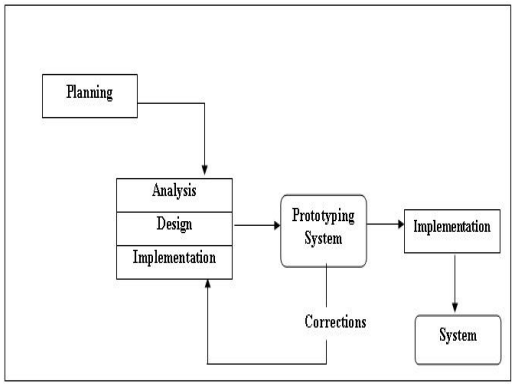

Figure 1: Methodology of prototyping (Source: [4])

Prototyping methodolgy is use to develop the system because of it's ability and capable to get the fast initial expectation result from the model of end system. The system had developed, test and redeveloped again till it become a functional system. Finally, the methodology is use because of the system was assume not complete at the early stage.

The study needs one web server within the database to implement the first authentication in this system. Then, its needs a SMS gateway server to perform a second authentication by using received secret word via SMS.

The following Figure 2 is show the hardware's architecture for the system.

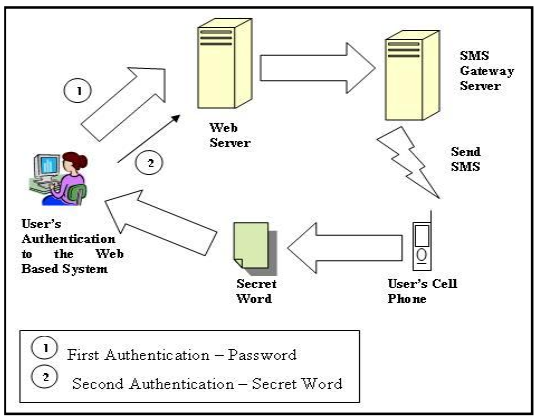

Figure 2: System Architecture

Users for this system must be register first through the web site and need to register too for their mobile phone's number. From the figure 2, it shows that the user must do first authentication by using login and password. Then, if the system had recognized the login and password is valid, one secret word will generate from this system. This secret word will send to the user's cell phone via SMS to perform second authentication on this system.

A context diagram in following Figure 3 is show how this system interacts with the end users and system administrator. The system itself is e-commerce website that uses two factor authentications.

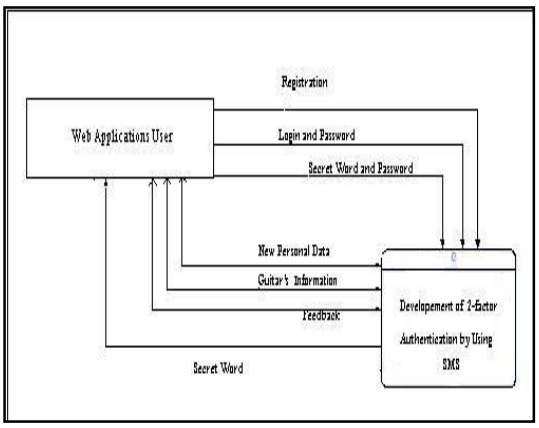

Figure 3: Context Diagram

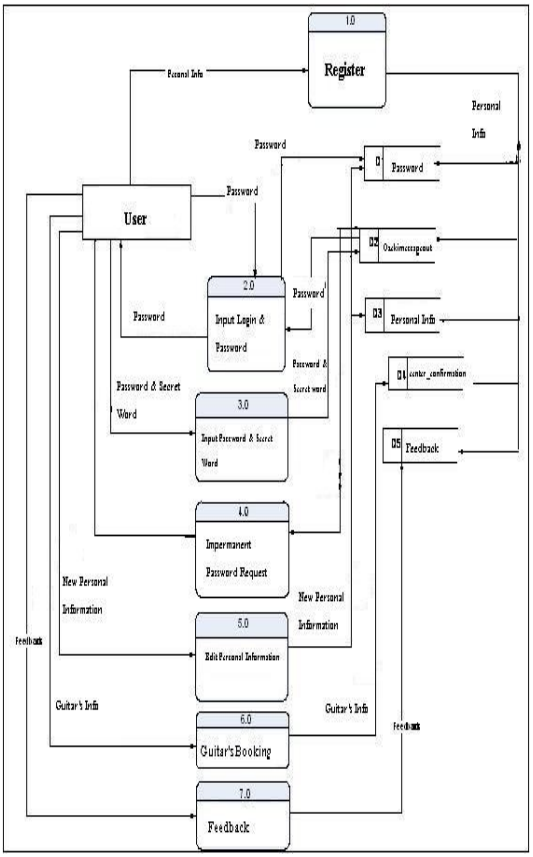

Figure 4: Diagram 0

In Figure 4 is show about Diagram 0 for the system. Diagram 0 will elaborate more details about the system's modules rather than in the Context Diagram.

3. RESULTS AND DISCUSSIONS

The main focus for developed this system is about to integrate it with method of two factor authentications. So, this paper will not discuss in detail about other e-commerce services or functions.

Table 1: System Modules

Index	System's Module	Description
1	Registration	Registration for new users.
2	First Authentication	First authentication by using login and password.
3	Second Authentication	Second authentication by using password and secret word.
4	Impermanent Password Request	User's request for the impermanent password.
5	E-Commerce Application	Information and application for the product.

There are five main modules that the system had as state in Table 1. In this system, firstly, the users need to register an account for using the system that had provided in New User Registration function. There is a form as state in Figure 5 that needs the user to fill it up with the personal information including cell phone number, password and others.

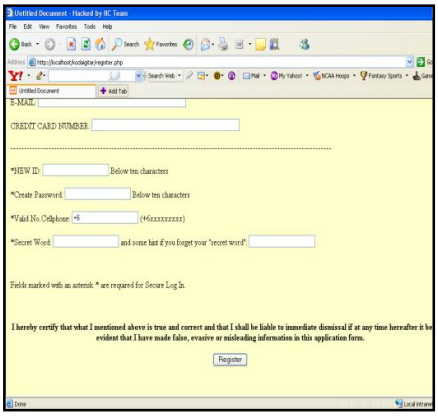

Figure 5: New User Registration Function

In first authentication function, users need to perform login and password to the system as state in following Figure 6.

Figure 6: First Authentication Function

In second authentication function, it has components like banner, user ID and cell phone number of the user and field for secret word and password (SMS code) input. So, the user need to fill up that registered password and SMS received secret word and click the button, Enter Your Page to process it as shown in Figure 7.

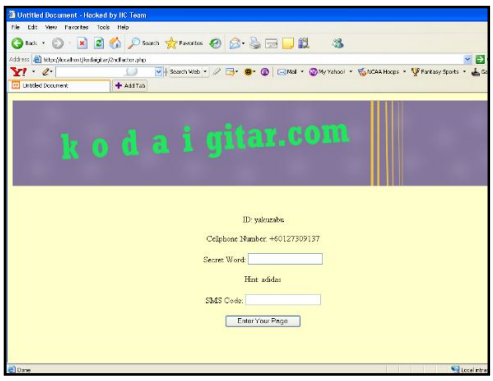

Figure 7: Second Authentication Function

Then, the users can have e-commerce application modules if the system recognizes password and secret word are valid. In this study, the module for e-commerce application is developed as simple and it had several components like banner, sell item for guitars in mode of button view, can list the buying item by clicking the item Cart and put it into the list in item View Cart and feedback button for the user to make any comments or suggestions. The users are also can have and change their personal information by clicking the button Personal. Background button is about information in history and background for the company. Log Out button is for the users to properly sign out from the system and all the functions in this module are shown in the Figure 8.

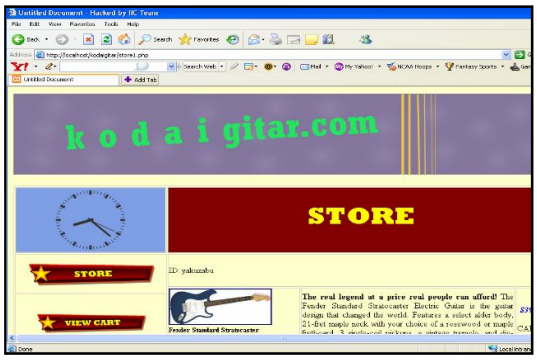

Figure 8 : E-commerce Application

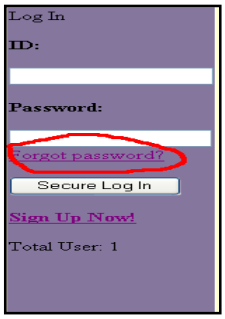

Figure 9: Impermanent Password Request Function

In the section of Impermanent Password Request, user can request impermanent password from the system and the system will generate and pass to the mobile phone user through the SMS.

5. CONCLUSIONS

Secure information and applications has become more important issues especially for the system or applications that had been online on the Internet [5]. The system that use single authentication by using password is more vulnerable rather than by using two factor authentication especially on the Internet. Usually by using password, it's always not to be changed and become statically. Implementation of strong password is also become vulnerable because it's not practice in reality by the many users [6].

Two factor authentications can be as alternative to minimize the problems that occur from single authentication by using password [7]. In this study, the second factor authentication for the system is using SMS and mobile phones.

REFERENCES

1. Victor D. Sawma, Robert L. Probert (2003). "E-Commerce Authentication, An Effective Countermeasures Design Model." University of Onawa. Ontario, Canada
2. RioDiNapoli (2005). "Two Factor Authentication Options." CIT/ATA.
3. Federal Financial Institutions Examination Council (2001). "Authentication in an Internet Banking Environment." Arlington, VA.
4. Art Conklin1, Glenn Dietrich2, Diane Walz3 (2004). "Password-Based Authentication: A System Perspective." The University of Texas at San Antonio, USA.
5. Rongsheng XU (2002). "Security Forensic on E-commerce." IHEP Computing Center. ChineseAcademy of Sciences.
6. Dario AnibalMarra (2005). "A Strong Authentication Mechanism for Consumer-Facing Online Transactions." MIT. Chisec Group.
7. Guomin Yang, Duncan S. Wong, Huaxiong Wang danXiaotie Deng (2006). "Formal Analysis and Systematic Construction of Two-factor Authentication Scheme." City University of Hong Kong, China.
8. Victor D. Sawma, Robert L. Probert (2003). "E-Commerce Authentication, An Effective Countermeasures Design Model." University of Onawa. Ontario, Canada
9. RioDiNapoli (2005). "Two Factor Authentication Options." CIT/ATA.
10. Federal Financial Institutions Examination Council (2001). "Authentication in an Internet Banking Environment." Arlington, VA.