Secured Webmail Authentication and Spam Filtering

Muhammad Azrulisham B. Mat Khair
University Kuala Lumpur
UniKL MIIT, Jalan Sultan Ismail.
Kuala Lumpur, Malaysia
azrulishamk@gmail.com

Han Lock Siew
University Kuala Lumpur
UnikL MIIT, Jalan Sultan Ismail
Kuala Lumpur, Malaysia
lshan@unikl.edu.my

***Abstract* — Webmail are one of the most popular platform for sending and receiving emails using a web browser. The webmail has the capability of sending messages or receive message via internet which makes it almost cost free for the users to communicate with each other. Unfortunately, like any other webmail, majority of these applications are vulnerable to brute force attacks and have junk email problem at their webmail. The motivation for this thesis is the need to identifying security services of a webmail and to design a secure webmail system for user. This research approach which provides a secure webmail design which protects its users with better integrity, confidentiality and privacy. To achieve this goal a research is conducted to investigate current security features of popular for webmail based on the latest solution. A list of requirements for good security is generated and based on those requirements an architecture is designed. A demo is also implemented and evaluated.**

Keywords—Webmail, Secured Authentication, Two-factor security, CAPTCHA, Spam Filtering

I. INTRODUCTION

Today's e-mail is a method of exchanging messages between people using electronics. Billions of email messages are sent daily in the world. But have some problems need to be faced if using email is a lack authentication and spam message. With the increasing number of software crackers available for free on the internet, authentication and spam for webmail continues to suffer from security vulnerabilities. With the current need for secured authentication and spam filtering of webmail, there need for solutions that will mitigate against threats in webmail. This project aims in developing a secure webmail authentication and spam filtering.

Email authentication is used as a way to verify that an email is from user. Email authentication is an important process in improving user deliverability score and can also help to prevent spoofing and phishing scams. Spam message is considered to be electronic junk mail or junk newsgroup postings we no need. Because of this problem we need spam filtering to filter unsolicited and unwanted email and prevent those messages from getting to a user's inbox. For this case we need spam filtering function to protect for company and individually who daily using email.

Hence, secured authentication and spam filtering indispensable for more provide prioritize security risk on email. By implementing this secured authentication and spam filtering, security of private and confidential data will be improved. The design system is not only meant for public use but it is also focus on banking and data commerce sectors where this system need to interact with each other. This webmail system will be targeting a user-friendly environment in where it will be very easy to handle and provides good security.

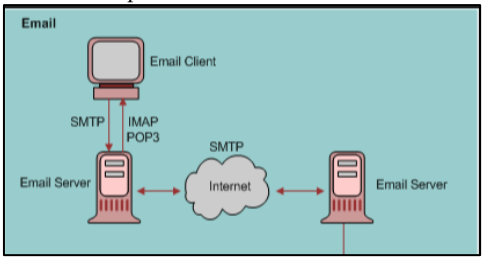
II. RELATED WORKS

A. Webmail provider Concept

A Webmail provider is a program that allows user to receive and send e-mail messages using a web browser. Users can simply enter the Webmail Web site URL in their browser's address or location field and use their Webmail account by typing in a username and password. To use a webmail such as Gmail or Yahoo user need to connect with the internet to access the webmail and user cannot open the message in offline. Different with Webmail client software such as Thunderbird and Roundcube user need to install the software on user computer and then use it to download and store e-mail messages to user computer. For this called an e-mail agent or an e-mail client[1].

According to researchers about webmail provider. Webmail's provider primary difference from Webmail client is how you access it. Webmail is accessed on the Internet through a Web browser while client-based email is accessed through a desktop program[2].

Fig. 1. Webmail Concept



e-ISSN: 2550-1550

B. Spam Filtering technique

A spam filter is a program that is used to detect unsolicited and unwanted email and prevent those messages from getting to a user's inbox. Like other types of filtering programs, a spam filter looks for certain criteria on which it bases judgments. For example, the simplest and earliest versions (such as the one available with Microsoft's Hotmail) can be set to watch for particular words in the subject line of messages and to exclude these from the user's inbox [3].

Other than, different style marker is employed on Enron-spam dataset to capture the nature of emails written by spam and ham email authors. Mainly, technique from five categories, consisting of character-based technique, word-based technique, tag based, structural technique, and Bag-of-Words technique. All these techniques look for some known pattern or features alone that usually appear in spam or ham message, to classify the emails.

character-based technique – include total number of character, ratio of total number of lowercase letter(a-z) and ratio of total number of uppercase character

word-based technique – consist of total number of word, average length per word

Function words – are words that express grammatical relationship with other words within a sentence.

Structural technique - represent the way author organizes the layout of the message

Bag-of-Words technique - all sentence in each email body are tokenized into a set of words and frequency of every term is counted within each file.

C. Captcha Authentication

CAPTCHA is the abbreviation of "Completely Automated Public Turing Test to Tell Computers and Humans Apart", which is a program algorithm for distinguishing between computers and humans. Common CAPTCHA generally contains symbols, text, pictures, and even videos, which is mainly used for human-computer verification. With the popularization of the Internet and its related applications, many malicious attacks against websites, systems and servers gradually appear. Therefore, the using of CAPTCHA is especially important for authentication[4].

With the popularization and development of information technology, the issue of information security has drawn more and more attention. Especially the importance of cyber security has become a hot issue in many countries. One of the many solutions to common cyber security problems is to provide protection against network attacks on the client side, of which the CAPTCHA technology is the most widely used.

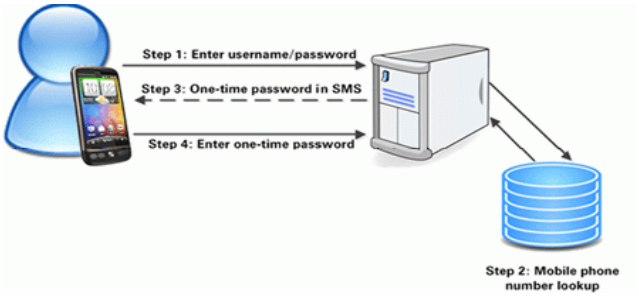
Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA) is a program that generates and evaluates solvable tests yet which exceed the capabilities of current computer programs. This technology is now almost a standard security mechanism for defense. A good human machine identification system must not only be humanized, but powerful enough to automatically pass the CAPTCHA test so as to prevent the computer program written by an attacker.

D. One Time password authentication with push notification for a security code

Password is use for authentication by all the Webmail. In addition, Static passwords have many weaknesses. Password can be hacked by any malicious hacker. Sometimes, Careless people might note down their own passwords some place, system with spared passwords might be use by different users or a malicious user may reset all passwords just to make destruction. Therefore, it is exceptionally useful to use dynamic password. By implementing one-time password, it is more secure when compared with static password[5].

There is no compelling reason to record these passwords and recollect these passwords. For each login session, every time the user wants to login into the system, another password has been produced and will be send it to the user. One-time passwords are more reliable and user friendly for authentication. OTP generation should be possible by different OTP generation algorithms for generating strings of passwords and OTP will guarantees security[6]. This prompt authenticating them repeatedly over the period for each login session. To maintain a strategic distance from the overhead we can use OTP for multi cloud environment. Figures bellow shows the picture about the process of one-time password.

Fig. 2. One-time password Process



E. Methods for Webmail

According to researchers email is an important part of our lives, whether it's for work or just to keep in touch with friends and family. IMAP and POP are two methods to access email. IMAP is the recommended method when you need to check your emails from several different devices, such as a phone, laptop, and tablet[7].

IMAP

IMAP allows you to access your email wherever you are, from any device. When you read an email message using IMAP, you aren't actually downloading or storing it on your computer; instead, you're reading it from the email service. As

a result, you can check your email from different devices, anywhere in the world: your phone, a computer, a friend's computer. IMAP only downloads a message when you click on it, and attachments aren't automatically downloaded. This way you're able to check your messages a lot more quickly than POP.

POP

POP works by contacting your email service and downloading all of your new messages from it. Once they are downloaded onto your PC or Mac, they are deleted from the email service. This means that after the email is downloaded, it can only be accessed using the same computer. If you try to access your email from a different device, the messages that have been previously downloaded won't be available to you.

SMTP

The SMTP (Simple Mail Transfer Protocol) protocol is used by the Mail Transfer Agent (MTA) to deliver your eMail to the recipient's mail server. The SMTP protocol can only be used to send emails, not to receive them. Depending on your network / ISP settings, you may only be able to use the SMTP protocol under certain conditions

HTTP Protocol

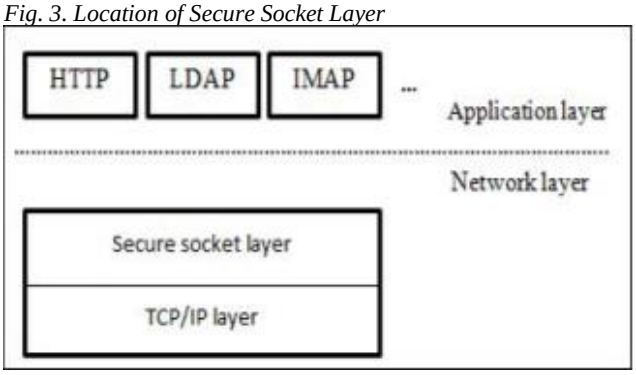
The HTTP protocol is not a protocol dedicated for email communications, but it can be used for accessing your mailbox. Also called web based email, this protocol can be used to compose or retrieve emails from user account. Hotmail is a good example of using HTTP as an email protocol.

F. Secure Socket Layer(SSL)

According to researchers the Secure Sockets Layer (SSL) protocol is the most popular protocol used in the Internet for facilitating secure communications through authentication, encryption, and decryption. One of the most important components of webmail provider is creating such an environment where potential user feels confident send and receive the privacy message from others. The SSL (Secure Socket Layer) protocol is used for this purpose. Thus, Secure Socket Layer is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server for communication, so that any information exchanged is protected within the secured tunnel. It uses s TCP to provide end –to-end secure services[8].

SSL protocol uses a combination of public-key and symmetric-key encryption to secure a connection between two machines that can be a Web or mail server and a client machine, communicating over the Internet or an internal network. SSL runs on the transport layer and the network layer. These layers are responsible for the transportation of data between the processes and the routing of network traffic between the processes and the routing of network traffic[9].

Fig. 3. Location of Secure Socket Layer



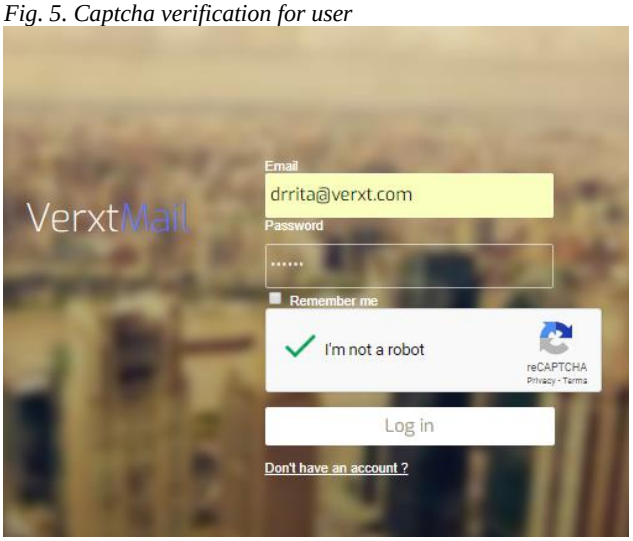
III. PROTOTYPE SYSTEM

The development of this project started with the login page. For new user need to sign up before use this webmail. After already have the account the user can login normally.

Fig. 4. Login Page(www.Verxt.com)

After the user fill in username and password the user need to verify the first security authentication that is CAPTCHA. Main objective for Captcha make sure the user is a human and not robot or program try to login the webmail.

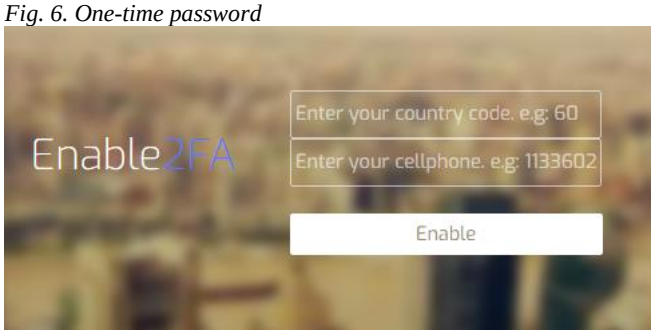
Fig. 5. Captcha verification for user



After user pass the verify first level authentication security. User must be proceeded the second level

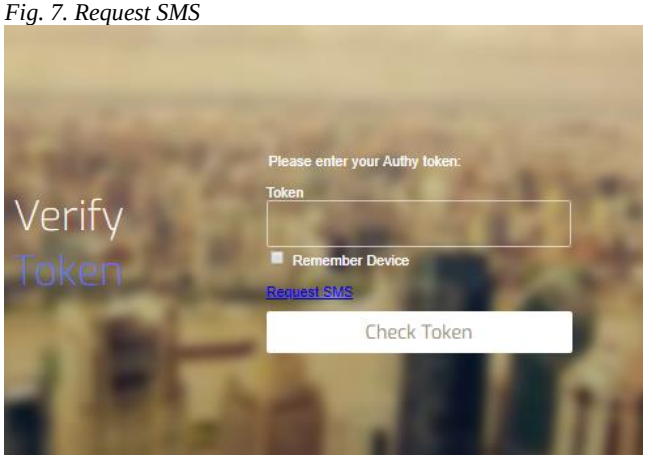
authentication security that is One-time password. User need to fill in the phone number for receive the token. After that user must be click the enable button to process the next step.

Fig. 6. One-time password



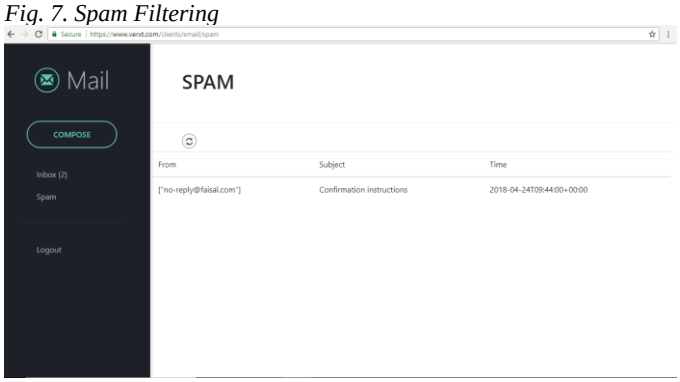
After that, user need to request the token then user will receive a notification token thru the phone. User need to fill in the same token to the box and click the check token for next process.

Fig. 7. Request SMS



After user pass all the security authentication. User ready can using the webmail for their platform send email and receive email from other email provider. For this webmail have spam filtering folder to filter junk mail and any bad word from others.

Fig. 7. Spam Filtering



IV. TESTING AND RESULT

Functional testing is a software testing process used within software development in which software is tested to ensure that it conforms with all requirements. Functional testing is a way of checking software to ensure that it has all the required functionality that's specified within its functional requirements. The testing is divided into several modules to test based on specific scenario and requirements. The result of functional and security testing has been summaries into table below:

Table 1 Test case for User to authentication

Test Case Field	**Detail**
Test Case ID	M_S_A_01
Test Case Name	Testing for User to authentication module
Purpose	To test the module if able to authenticate the user credential and toast message based on the response it receives from the server.
Initiation Criteria	1. The user must already register
Executions Step	1. Open the Webmail (www. Verxt.com) 2. Insert username and password in the given field and press login
Expected result	Webmail system able to authenticate the user credential based on the response it receives from the server

Table 1 shows that the user is able to login the system using a default credential username and password. This function is well working and Table 2 shows that the user is able to verify the CAPTCHA authentication.

Table 2 Test case for User to Captcha Verification

Test Case Field	**Detail**
Test Case ID	M_S_A_02
Test Case Name	Testing for User to check the respond Captcha Verification
Purpose	To test the Captcha verification for user it's a human
Initiation Criteria	1. The user must already register
Executions Step	1. Open the Webmail (www. Verxt.com) 2. Insert username and password in the given field and press login
Expected result	The Captcha Verification able to check a user it's a human.

Table 3 Test case for User to One-time password

Test Case Field	**Detail**
Test Case ID	M_S_A_03
Test Case Name	Testing for User to receive TAC Number module.
Purpose	To test the module if able to receive TAC Number to their phone number via SMS.
Initiation Criteria	1. The user must already register
Executions Step	1. Open the Webmail (www. Verxt.com) 2. Insert username and password in the given field and press login
Expected result	Webmail able to receive TAC Number that send to the user's phone number via SMS.

Table 3 show the user pass using one-time password and user will receive the TAC number that send to the user phone.

Table 4 Test case for User send email to other webmail provider

Test Case Field	**Detail**
Test Case ID	M_S_A_04
Test Case Name	Testing for User to send email to other email.
Purpose	To test the module if able to send email to other email provider
Initiation Criteria	1. The user must already register
Executions Step	1. Open the Webmail (www. Verxt.com) 2. Insert username and password in the given field and press login
Expected result	Webmail able to send email to other email provider.

Table 4 show that user can send email message to other webmail provider.

Table 5 Test case for User receive email from other email provider

Test Case Field	**Detail**
Test Case ID	M_S_A_05
Test Case Name	Testing for User to receive email from other email provider.
Purpose	To test the module if able to receive email message from other email.
Initiation Criteria	1. The user must already register
Executions Step	1. Open the Webmail (www. Verxt.com) 2. Insert username and password in the given field and press login
Expected result	Webmail able to receive email message from other email provider.

Table 5 show that user can receive email message from other webmail provider.

Table 6 Test case for User not receive the junk email and spam message

Test Case Field	**Detail**
Test Case ID	M_S_A_06
Test Case Name	Testing for User not receive the junk email and spam message.
Purpose	To test the module if able not to receive junk email and spam message from other email.
Initiation Criteria	1. The user must already register
Executions Step	1. Open the Webmail (www. Verxt.com) 2.Insert username and password in the given field and press login
Expected result	Webmail able not to receive junk email and spam message from other email provider.

Table 6 show all the junk message and spam message will be separated in the spam folder.

Table 7 Test case for Password user in database will be encrypted

Test Case Field	**Detail**
Test Case ID	M_S_A_07
Test Case Name	Testing for Database to encrypt password user.
Purpose	To test the module if password user will be encrypted or not in database
Initiation Criteria	1. The user must already register
Executions Step	1.Open the Webmail (www. Verxt.com) 2.Insert username and password in the given field and press login
Expected result	The database can encrypt the password user.

Table 7 show the password in the database will be encrypted with salt

V. CONCLUSION

After a lot of development, and research, the objectives of this project have finally completed successfully and achieved the entire project plan. This project development gives useful experience and knowledge on many things such as how to plan and start the project, how to handle the process timeline, how to solve problem occur during development and the most important thing is to learn programming language better than before. The proposed architecture for a secured webmail authentication and spam filtering provides confidentiality, integrity and privacy for users who want use a webmail as a platform to send email to each other. Users can be confident that nobody, even not the provider of the service, can open their webmail. During the implementation of the architecture, several difficulties were encountered. Some of these challenges have been solved after extensive trials and workarounds and some of them remain. Some of the difficulties were regarding configuration of separated software.

.

VI. REFERENCES

[1] Crispin, M. (2016). Distributed Electronic Mail Models in IMAP4. RFC1733, University of Washington, U.S.; 2014.

[2] reed, N. and Borenstein, N. (2014). Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies. RFC2045, Network Working Group, U.S.; 2014

[3] Postel, J.B. (2016). Simple Mail Transfer Protocol. RFC821, University of Southern California, U.S.; 2016.

[4] K. Butler, W. Enck, J. Plasterr, P. Traynor, and P. McDaniel. Privacy Preserving Web-based Email. Technical report, Technical Report NAS-TR-0009-2005,

[5] R. Dingledine, M. J. Freedman, and D. Molnar. The Free Haven Project: Distributed Anonymous Storage Service. In International workshop on Designing privacy enhancing technologies, pages 67–95, New York, NY, USA, 2001. Springer Verlag New York, Inc

[6] B. Costales and E. Allman. Sendmail(2nd ed.). O'Reilly & Associates, Inc., Sebastopol, CA, USA, 2011.

[7] C. M. Ellison and B. Schneier. Ten Risks of PKI: What You're Not Being Told About Public-Key Infrastructure. Computer Security Journal, 16(1):1–7, 2013

[8] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. Mitchell. Stronger Password Authentication Using Browser Extensions. In Proceedings of the 14th USENIX Security Symposium, 2005

[9] R. L. Rivest. Chaffing and Winnowing: Confidentiality without Encryption. RSA CryptoBytes, 4(1), Summer 2012