Adopting information system security services in online clothing marketing system using rup methodology under php

Lim Jin Long[1], Umapathy Eaganathan[2], Nor Afifah Binti Sabri[3]
[1]Student, BSc (Hons) in IT with Specialism ISS, Asia Pacific University
[2,3]Faculty in Computing, Asia Pacific University
E-mail: [1]TP034787@mail.apu.edu.my, [2]umapathy.eaganathan@apu.edu.my,
[3]afifah@apu.edu.my

Abstract: -In this sophisticated era of globalization, people are more preferring to shop through online easily. Online consumers are constantly presented with situations in various types of web security vulnerabilities. Eventually web applications not able to meet the expected target then business will become negative. However this paper dealt about Online Clothing Marketing System and it will be a standalone web application which allows users to securely purchase clothes online. The primary features of this website allowing users to securely purchase product online by validating the customer input with multiple layers of validation. Also, there will be data transaction between client and server taking place through encryption algorithm, secure socket layer, password hashing and captcha verification. The process followed in captcha will be implemented to encrypt the whole data transaction process to ensure the security level of the system. Hence, through this web application, problems will be reduced with a great quality and can able to reduce the attackers from stealing the information.

Index Terms— Captcha, Rational Unified Process (RUP),Security Services, Vulnerability, Web Application

1. Introduction

In this sophisticated era of globalization, people are more preferring to shop through online. Internet consumers are constantly presented with situations of various types of web security vulnerabilities. Basically, e-commerce sites record the important data of customer includes name, phone number, address, bank details and credit card number. Therefore, online shoppers should be aware to various kinds of scams that targeting to the online consumers. Based on the statistics, the Internet Crime Complaint Centre reported that online payment fraud complaints by consumers in 2007 had reached $239 million compared to $198 million in 2006 [1]. Hence, e-commerce sites should provide the best security measures such as encryption of data, implement of SSL (Secure Socket Layer) to protect the customer's information [2].

The proposed project will be able to deliver an e-commerce website to the users with security system that will able to secure customers confidential data that have entered to this e-commerce website through encryption and hashing. Also, the users can be assured to browse this website as the connection of this website established to the server is secured by secure socket layer (SSL). Besides, users able to operate this e-commerce website by using any browser in their devices such as Google Chrome, Internet Explorer, Opera, Mozilla Firefox and many more. The targeted users of this project are the e-commerce customers and admin of the system.

2. Related Work

2.1 Encryption Algorithms

Based on [3] the opinion suggested that encryption is a better solution to secure the information. It is better to encrypt the data at first before store the data to the cloud server. They suggested a data security model which comprises of authentication, data encryption, data integrity, data recovery and user protection can use to improve the data security over the cloud. Besides, before uploading the file or data to the cloud, users are suggested to verify that the data is stored on the backup drivers and the keywords is remained unchanged. Furthermore, network-based intrusion prevention can use to detect the threats in real-time. RSA based storage security can be used to compute large files in different sizes [3].

Based on the research, there are three security algorithms which includes Alternative Data Distribution (AD2), Secure Efficient Data Distributions (SED2) and Efficient Data Conflation (ED-Con) used to determine the data packet to be split or stored in the distributed cloud servers. In this proposed model, it is proved that the proposed model can defend the major threats from the cloud-side as compared with the AES Model due to the computation time and processing time were shorter. Not only that, other method such as FHE and ABE can prevent the data from information leakage by encryption. However, this type of data security cannot fulfil the current industrial demands due to lower efficiency level of operation. For the future work, securing data duplications can be addressed to increase the level of data availability [4].

2.2 Secure Socket Layer (SSL)

SSL protocol is used to secure a connection establishes between two machines such as web server and client server by using a combination of public-key and symmetric-key encryption. SSL Certificates bind together with domain name and server name with a cryptographic key. It is installed to activate the https protocol that allow secure connections of web server and browser [5]. SSL protocol is available in two strengths, 40-bit and 128-bit. The length of the session key is generated of every encryption transaction. The longer the bit, the longer to break through the encryption code. Most of the browsers support 40-bit sessions, except Netscape Communicator 4.0 that support up to 128-bit sessions which is trillions of times stronger than 40-bit sessions. SSL using RSA, a public-key cryptosystem for encryption and authentication to encrypt and authenticate the data. RSA encryption requires 1024-bit to encrypt and decrypt the data. Hence, the web server that operates on 64-bit have to divide the 1024-bit data into 32-bit or 64-bit pieces before encryption and decryption can be done. It requires a significant amount of CPU processing power to carry out the process or else will result in poor performance [6].

2.3 Two-factor Authentication

Two-factor authentication is using two authentication methods (passport + Personal Identity Number (PIN) to increase the security of accessing secure systems. The example of the two-factor authentication can be the security token. It is used to prove identity of the users electronically before giving the authorization to the users. Two types of security token are available such as hardware token and software token. Software tokens are a type of security device use to authorize the usage of computer services. Two-factor authentication tools such as RSA SecurID can transfer the hardware of the users into a token device which can display a six-digit security codes that change every 30 seconds for authentication. The six-digit security code is strong and dynamic that can never be reused in the future logins [7].

Based on [8] agreed that (One Time Password (OTP) must be hard to guess by the hackers to secure the system. A secured cryptographic algorithm is proposed to generate complex passwords which are hard to guess. The factors can be used to generate the OTP can be IMSI number, ATM PIN, timestamp, date of birth and username. These information is retrieved from the user and concatenated with time stamp to generate valid OTP. The concatenated string is given to the input to Secured Hash Algorithm (SHA1). The algorithm converts the string by reducing from 20 bytes value to only 5 bytes. The 5-byte value is then right shifted of 4 digits and convert into hexadecimal value. Finally, the value is converted into ASCII character string and displayed as OTP to user [8]

3. Methodology

3.1 Development Phase

The system development methodology selected for the proposed project will be Rapid Application Development (RAD) Model. It is an iterative framework type methodology and aims to deliver a high-quality system at a very fast development with low investment cost. Besides that, RAD Model is an ideal methodology for this project because this methodology is appropriate for small to medium scale project to be done in short duration. RAD Model produces the system more quickly and likely to business focus which may produce system at a lower cost that suits this online clothing marketing system project. The usecase diagram for the implemented system shown in Figure.1

3.2 Use Case Diagram

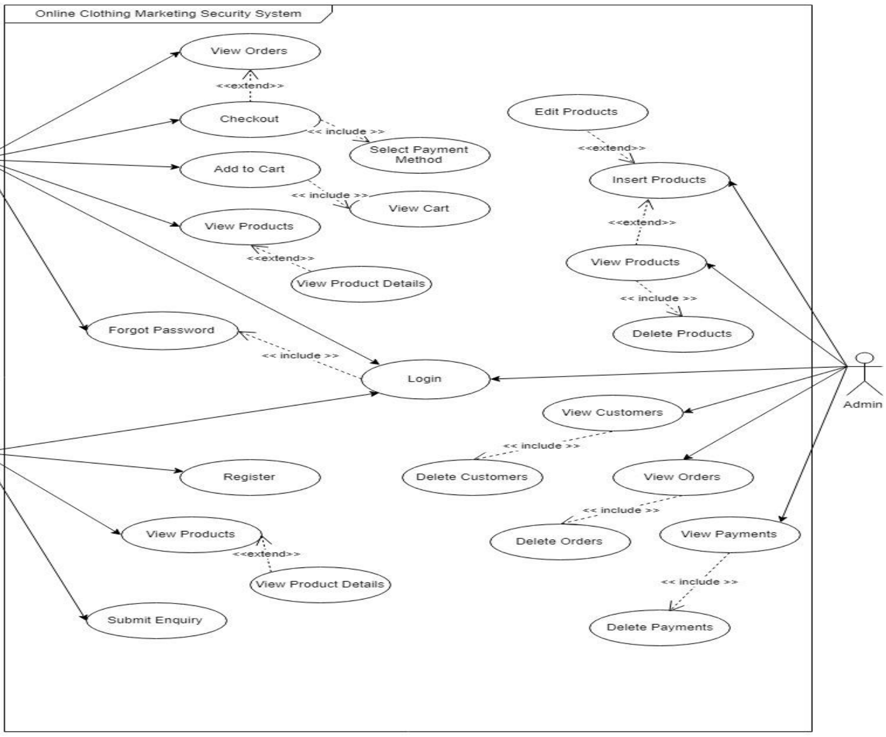


Figure.1 Usecase diagram

3.3 Security Features

3.3.1 SSL

SSL or known as Secure Sockets Layer is the standard technology for establishing a secure internet connection and protect any sensitive data that is sent between two systems by preventing hackers or attackers from reading and modifying the information transferred. Basically, SSL uses encryption algorithms to prevent the hackers from reading it as it is sent over the connection to the server. The sensitive information can include the password of the user or credit card numbers. In this proposed project, SSL is implemented to ensure the connection established from client to server is secured [9]

3.3.2 Password Hashing

Hashing is defined as a type of algorithm that takes any size of data and convert it into a fix-length of data. This is often used to ease the retrieval of data as large amounts of data can be shorten in a shorter string.

There are some modern hashing algorithms such as MD5, SHA (Secure Hashing Algorithm)-1, SHA2, SHA3 and many more. Because as compared to encryption algorithm, hashing is a non-reversible process which is infeasible for a hacker to modify the hash message without changing the hash value. Therefore, by hashing the password stored in the database, in the event of attackers get read access to the database, they cannot retrieve the password plain texts [10]. Bcrypt hashing algorithm is applied in this proposed system. It is an adaptive hash function that based on the Blowfish symmetric block cipher cryptographic algorithm [11]. Bcrypt hashing algorithm will generate salt which add a very long string of bytes to the password [12].

3.3.3 Encryption

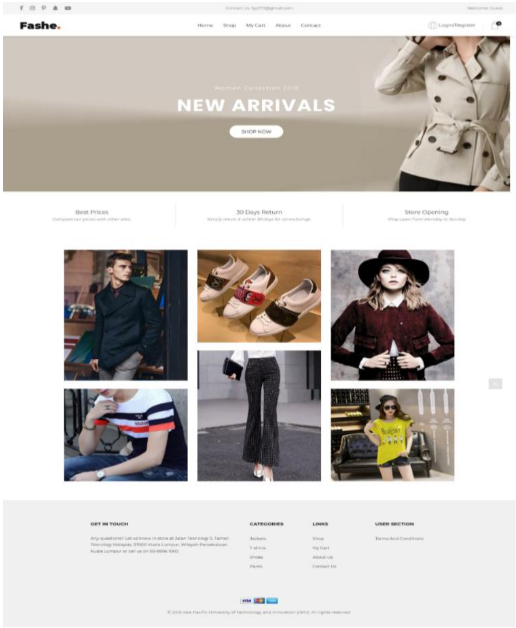
Data encryption translates data into another form with the access to a secret key or formally known as decryption key. Encrypted data is known as ciphertext while unencrypted data is called plaintext. Currently, encryption is one of the most popular and effective data security methods used by any organizations. The purpose of data encryption is to protect digital data confidentiality which stored in database and transmitted using the internet or other computer networks. In this system, data encryption is implemented to protect customer confidential data. The encryption algorithm applied in this project is AES_256 algorithm [13].

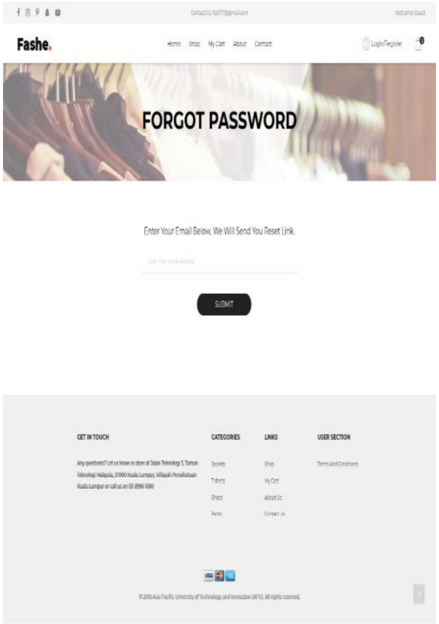
3.3.4 CAPTCHA

CAPTCHA can be considered as a type of challenge response system that used to differentiate humans' input from robotic software system. Generally, CAPTCHAs are used as security checker to prevent spammers or hackers from inject malicious code into the forms of web pages. In this proposed system, CAPTCHA is implemented to enhance the security of the system [14].

4. Implementation

Figure 2 shows the homepage of the system. The page includes the slider of new arrivals products, information of the shop and the latest product image. Figure 3 shows the login page of the system. Users should fill in their email and password in order to login to the system. Users can also click on "forgot password" link if they forgot their password. For users who do not have an account for the system, they can click on "register here" to register an account.





Enter Your Email Below, We Will Send You Reset Link.

Any questions? Let us know in store at Jalan Teknologi 5, Taman Teknologi Malaysia, 57000 Kuala Lumpur, Wilayah Persekutuan Kuala Lumpur or call us on 03-8996 1000

© 2018 Asia Pacific University of Technology and Innovation (APU). All rights reserved.

In the register page of the system users are required to enter their name, email, password and check on terms and conditions and perform captcha verification in order to register a new account. Also in the product page of the system. users able to filter the products based on their respective categories.

5. Testing

In this project, there are three types of testing will be carried which are unit testing, user acceptance testing and security testing. Unit testing will be performed during the implementation stage of single unit or function, user acceptance testing will be carried out after the final system is produced while security testing will be carried out from time to time to find out all the possible threats and vulnerabilities existed in the system [15].

5.1 Unit Testing

In unit testing, each part of the software is isolated from the whole application, only a small part of the individual component is performed the testing and demonstration to verify the part is fulfilling the requirements and the desired functionality. The individual component of the application may include the login page, product page, payment page etc. For instance, the register page is tested by verify the length of the password must contain at least one number and one uppercase and lowercase letter, and at least 8 or more characters. Usually, this type of testing is performed at the earliest stage of development. All the individual unit should go through this testing phase before it can integrate into a complete component.

5.2 User Acceptance Testing

User Acceptance Testing (UAT) or often known as End User Testing is one of the last stages to be performed during software development life cycle. It is performed by the end users after the whole software has been thoroughly tested for the approval of the production release. Basically, the testing involves multiple test case to determine the overall quality of a product by eliminating the errors and defects. In this project, user acceptance testing is conducted by three users for verifying whether the product is meeting with the user requirements and objective as stated during the early stage of development process. By performing UAT, the satisfaction level of the users can be identified which allow the developer to accomplish the successful of user acceptance [16].

5.3 Security Testing

Security Testing is a level of testing technique to determine where the information protects the data and sustain the functionality as intended by accomplish 6 basic principles include confidentiality, integrity, authentication, authorization, availability and non-repudiation [17]. Besides, security testing ensures that the system is free from loopholes, weakness or defects that may cause threats or vulnerabilities in the system. There are various types of security testing test cases such as password store in database must be in encrypted format, the application should not allow invalid users to login or the session time of the application [18].Based on the testing results retrieved from three types of testing carried out in this project which are unit testing, user acceptance testing and security testing, it seems that the system is developed to meet customer requirements and satisfaction. The results collected from unit testing shows that the functions of the system are working properly as expected and help to ensure the system is free from possible bugs occurred. Besides, based on the suggestion and feedback collected from user acceptance testing, the developer has taken the user's feedback into consideration and applied in the system. Lastly, the security testing ensures the system accomplish 6 basic principles include confidentiality, integrity, authentication, authorization, availability and non-repudiation.

6. Conclusion

Throughout the development process of this project, there are some limitations of the system which are listed as follows:

- The file upload function for the product image does not validate the file format of the file uploaded.
- Admin not able to confirm the order placed by the client.

Based on the evaluation of the final version of the system, there are some functionalities and specifications identified by the developer may be improved in the future in order to deliver more desirable functions to the target users.

- Implementing the intelligent recommendation system that filter the products of the website according the preference of the users. By implementing an intelligent recommendation system able to help the consumer to discover the products that they love easily [19]. It required the knowledge of data mining that identify the patterns and establish relationships to solve problems through data analysis.
- Integrate the system with real credit card payment gateway which allow the users to make payment of the orders with credit card.

Enhance the level of presentation of customer order in their profile. Currently, the orders of the customers are showing line by line in their profile. For the enhancement, the developer should integrate the different products into a same order with the presentation of order report.

The credit card payment of the system is a dummy function which the data processed does not go through back-end database. As the development of the proposed system proceed further, the types of recommendation system and encryption algorithms for secured data will be focused to provide recommendation to the users based on their needs and encrypt the data stored in the database. The further research for the proposed system will proceed more detailed into the types of recommendation system such as knowledge-based recommendation system and content-based recommendation system.

Acknowledgments

Authors would like to thank Asia Pacific University, Malaysia for the international conference opportunity also for journal publication

REFERENCES

[1] Kuriachan J K. 2014 Online shopping problems and solutions *New Media and Mass Communication* ,**Volume 23** pp. 1-4.

[2] Mittal T 2017*Common problems faced by customers while shopping online*

[3] RaoR V & Selvamani K. 2015 Data Security Challenges and Its Solutions in Cloud Computing. *International Conference on Intelligent Computing, Communication & Convergence* **Issue 48** pp. 204-209

[4] Li Y et al 2017 Intelligent cryptography approach for secure distributed big. *Information Sciences* **Issue 387** pp. 103-115.

[5] Kaur E P 2017 Review of Role of SSL in Cyber Security. *International Journal of Advanced Research in Computer Science,* **8(4)** pp. 187-190.
[6] Alnatheer, M. A., 2014. Secure Socket Layer (SSL) Impact on Web Server. *Journal of Advances in Computer Networks,* **2(3)** pp. 211-217.
[7] Singhal, M. & Tapaswi, S., 2012. Software Tokens Based Two Factor Authentication. *International Journal of Information and Electronics Engineering,* **2(3)** pp. 383-386.
[8] Amin, A., Haq, I. u. & Nazir, M., 2017. TWO FACTOR AUTHENTICATION. *International Journal of Computer Science and Mobile Computing,* **6(7**) pp. 5-8.
[9] DigiCert, Inc., 2018. *What is an SSL Certificate?*
[10] lucaskauffman, 2013. *About Secure Password Hashing.*
[11] The Hacker News, 2014. *Securing Passwords with Bcrypt Hashing Function.*
[12] Boterhoven, D., 2016. *Why you should use BCrypt to hash passwords*
[13] Lord, N., 2018. *What Is Data Encryption?.*
[14] TechTarget 2018 *CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Humans Apart).*
[15] Bennett, Coleman & Co. Ltd., 2018. *Definition of 'Software Testing'.*
[16] Bennett, Coleman & Co. Ltd., 2018. *Definition of 'User Acceptance Testing'.*
[17] tutorialspoint, 2018. *Security Testing.*
[18] Guru99 2018*What is Security Testing: Complete Tutorial.*
[19] *Editor Guided Selling Blog* 2014