International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 5, August 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Design and Implementation of Electronic Payment Gateway for Secure Online Payment System

Kyaw Zay Oo

Department of Information Technology, Technological University, Mandalay, Myanmar

How to cite this paper: Kyaw Zay Oo "Design and Implementation of Electronic Payment Gateway for Secure Online Payment System" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-5, August 2019, pp.1329-1334, **https://doi.org/10.31142/ijtsrd26635**

IJTSRD26635

Copyright © 2019 by author(s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

ABSTRACT

In e-commerce, main problem is to be more secure for payment systems and disputation between online merchant and customer. To solve this problem, this paper presents design and implementation of Electronics Payment Gateway for online payment system. In this system, a customer's financial information (credit or debit card information) is sent directly to a Payment Gateway also called Trusted Third Party, TTP instead of sending it through an online merchant. The Payment Gateway can support more secure for online payment system. In this system, Secure Socket Layer (SSL) with Rivest–Shamir–Adleman (RSA) is used to enhance more secure connection in payment process. In secure online payment system, end-to-end encryption is required to maintain the integrity of transactions carried out online. RSA is more secure because its factors are large integers and key size is large, which increases the security. The electronic payment gateway provides the confidentiality by using RSA for online payment transactions and trusted third party to recover the disputation between online merchant and customer.

KEYWORDS: *electronic payment gateway, e-commerce security, online payment system, RSA, cryptography*

I. INTRODUCTION

Electronic commerce (E-commerce) has presented a new way of doing business all over the world using internet.

Organizations such as online shopping have changed their way of doing business from a traditional approach to online payment processes. Electronic commerce and online business is trading in product or services conducted via open networks such as the Internet. It is considered to be the sales aspect of electronic business (e-business) consisting of the exchange of data to facilitate the financing, payment and security of business transactions. High degree of confidence needed in authenticity and privacy of such transactions can be difficult to maintain where they are exchanged over an unsecured public network such as the Internet [9].

In the both growth and development of e-commerce, the main problem is a greater need for secure payment systems and online authentication in both client side and server side. The main current concern of most internet users relates to the confidentiality of payment card information, since there is a growing realization that stolen card details can be used to make fraudulent transactions.

Although SSL and TLS are currently in use and provide secure transportation of information over the internet, e-commerce required a more reliable payment method or system to secure their customer's financial information. Frauds that occur on the internet today are mostly from hackers, fraud merchants, spammers, phishers, malware, spyware and data thieves who place attacks on networks and steal information [10].

In order to prevent these threats happening, the electronic payment services must consider the security requirements including the authentication of consumers [1], confidentiality of payment transactions [2], and non-repudiation of electronic payment [3]. To avoid the attacks from hackers, it is desirable not to send a customer's payment information to an online merchant at all [4], because it creates the possibilities of security breach and information leaks from the merchant's side.

Since customer's payment information such as the bank account, financing amount, identical account and password are sent to a merchant at all, there are many stolen payment data from hackers in online payment transaction because it creates the possibilities of security breach and information leaks from a merchant's side. So, a Payment Gateway (Trusted Third Party) is required instead of sending customer's payment information through a merchant.

This paper intends to design and implement an electronic payment gateway for secure online payment system with credit (or debit) card payment by using security mechanism based on secure exchange procedure. In this system, a customer's financial information is sent directly to a Payment Gateway (Trusted Third Party), instead of sending it through an online merchant.

II. RELATED WORK

Ailya, et al. [2] designed and implemented a new Secure Electronic Payment Gateway to provide authorization,

confidentiality, integrity and availability for transaction. They used Triple Data Encryption Standard (TDES) cryptosystem to secret the payment information and to achieve the more speed transaction time of payment gateway.

Chinedu, J. N. [1] implemented a RSA Ecommerce Security System (RSA-ESS), which provides the security and privacy problems of credit card information in ecommerce transaction. In his system, RSA was used to secret the payment information and achieve the comply speed in ecommerce transaction. His system was only used to security and privacy for payment information.

Mohammed, et al. [3] implemented a software tool to investigate Distributed Guessing Attack in payment transaction process. They analyzed that isolated online merchant and bank with their own security policies cannot be protected these attack. Therefore, the number of guessing attempt is limited to prevent repeated invalid attempts made within a certain time span and post code is verified to detect the invalid address information stored by the card issuing bank.

III. BACKGROUND THEORY

To make it secure between each element, especially between the customers (i.e., the card holder) and the online merchant or payment gateway, a number of methods have been suggested. Specifically, online shoppers need to feel completely confident that their credit card and banking details are secure and cannot be accessed by hackers. So, secure connection is required to essentially guarantee payment transactions.

A. Electronic Payment Gateway (Trusted Third Party)

A Payment Gateway is an e-commerce application service provider that provides tools to process a payment between a customer, merchant and banks over the World Wide Web (WWW). It helps secure a purchase and a customer's payment information in a transaction. A payment gateway protects payment information by encrypting sensitive information, such as credit/debit card details, to ensure that information is passed securely between a customer and, the payment processor. Besides encrypting the payment information, a payment gateway also helps in authorizing payments and protect against financial frauds. Many online merchants use payment gateways for its security, reliability and immediate authorization of payment.

B. Secure Socket Layer

SSL is internet standard protocol and used to protect sensitive information that end users send to web servers, such as passwords, credit card numbers, email content and private messaging. SSL creates a uniquely encrypted channel for private communication over public channels, and it checks the server's certificate for authenticity before any information is sent. Transporting sensitive data over SSL helped in achieving security [4]. SSL employs asymmetric key encryption to protect the transfer of information between customers and merchants or payment gateway. SSL provides server and client identification, data confidentiality, and data integrity using digital certificate.

If the server and client are capable of running SSL programs, then the client can use the Universal Resource Locater (URL) https://... instead of http://. Hyper Text Transfer Protocol Secure (HTTPS) appears in the URL when a website is secured by an SSL certificate. When SSL is used to secure HTTP, it assures a web user with intended web server and then sends or receives messages securely. So, SSL uses the RSA cryptosystem for authentication and encryption. SSL works to protect the internet communication by the following features.

- Server authentication
- Encryption
- Data/Message integrity

SSL certificates have a key pair: a public and a private key. These keys work together to establish an encrypted connection. The most important part of an SSL certificate is that it is digitally signed by a trusted Certificate Authority (CA). Browsers only trust certificates that come from an organization on their list of trusted CAs.

SSL use Secure Hash Algorithm 2 (SHA-2) to create the message digest and RSA to encryption/decryption data security between web server and client. SHA-2 is a cryptographic hash function which takes an input and produces a message digest. So, The SHA-2 hash function and RSA are implemented in SSL.

C. RSA Public Key Cryptosystem

RSA is an algorithm used by encryption and decryption messages [1], [6]. RSA is widely used for secure data transmission. In RSA, the encryption key is public and it is different from the decryption key which is kept secret (private). RSA includes three parts:

- Key generation,
- Encryption,
- Decryption.

RSA is a relatively slow algorithm and because using to directly encrypt and decrypt actual message. So it is useful for short messages. The following is the algorithm for RSA cryptosystem.

Key generation:
P and Q both Prime, $P \neq Q$
$\varnothing = (p-1)(q-1)$
$1 < e < \varnothing$
$\gcd(e, \varnothing) = 1$

Public Key = {e, n}

Private Key = {d, n}

Plaintext Encryption:
$M < n$
Cipher text: $C = M^e \bmod n$

Cipher text Decryption:
Plaintext: $M = C^d \bmod n$

IV. OVERVIEW OF THE SECURE ONLINE PAYMENT SYSTEM

The secure online payment system is composed of four elements: customer (card holder), online merchant, payment gateway and banks. The overview of the system is shown in Figure 1.

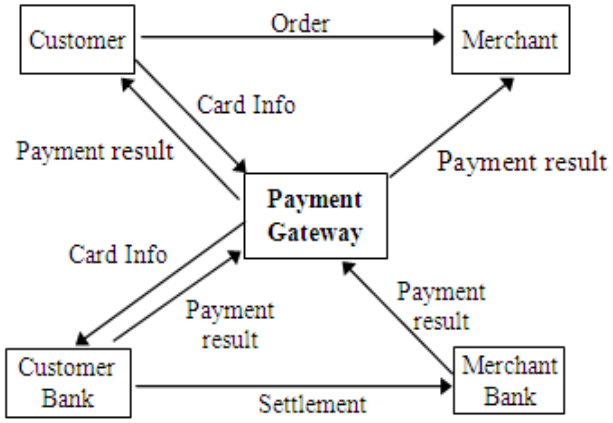

Figure1: Overview of the Secure Online Payment System

The processes that are performed at the customer site are as follows:

- Ordering process: Ordering operation perform to send the customer's order to the merchant.
- Message encryption process: After ordering, RSA encryption operation is performed to hide the customer's card information to obtain the cipher text.

The processes that are performed at the merchant site are as follows:

- Redirect process: After receiving the customer's order information, redirects to the payment gateway for encryption and decryption processes.

The processes that are performed at the payment gateway site are as follows:

- Key generation process: In this system, RSA key generation operation is firstly performed to generate the public key and private key for merchants and banks.
- Save key process: After key generation process, the keys are saved into the key database to distribute the customers.
- Message decryption process: After receiving cipher text from the customers, the cipher text is decrypted by RSA decryption operation to obtain the customer's card information.
- Validation card process: After the decryption the customer's card information, the payment gateway validate the card for payment process.

The processes that are performed at the bank site are as follows:

- Message decryption process: After receiving cipher text from the payment gateway, the cipher text is decrypted by RSA decryption operation to obtain the customer's card information.
- Validation account process: After the decryption the customer's card information, the bank validate the account for payment process.
- Settlement process: After the validation customer's account, settlement operation is performed between customer's account and merchant's account.
- Inform process: After the transaction process, the bank inform the payment confirmation to the customer and merchant.

V. DESIGN OF THE PAYMENT GATEWAY

The payment gateway must be responsible to provide the security function. At first, RSA algorithm is implemented in the payment gateway before the encryption and decryption processes. The payment gateway generates public key and private key for each online merchant and bank. And then, the generated keys are saved into the key database of the payment gateway. After receiving the encrypted customer's card information, the payment gateway decrypts the card information with merchant's private key. And then, the payment gateway must validate the card with card database. If the card is valid, the card information is again encrypted with bank's public key and the encrypted card information is sent to customer's card issuing bank. After validating and approving the customer's account for customer's order in the bank, the payment gateway informs the customer for the payment result (approved or rejected). The design of the payment gateway is illustrated in Figure 2.

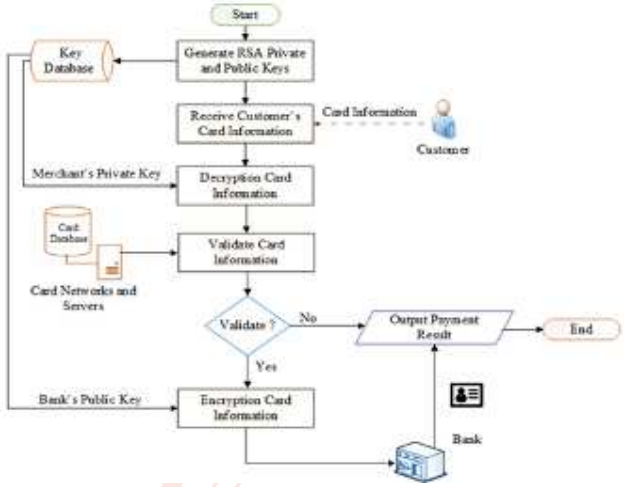

Figure2: Design of the Payment Gateway

VI. IMPLEMENTATION OF THE PAYMENT GATEWAY

The implementation results of the system are presented as a series of interfaces. To illustrate the system, online student admission system is implemented for Technological University (Mandalay) by using HTML, PHP and Java Script programming languages in web application. The university website is similar as online shopping website that acts as an online merchant. The student acts as an online customer. In addition, the TTP is Myanmar Payment Gateway and card issuing bank is TUM bank in the system. Besides, the customer's bank and merchant's bank are considered as the same bank in the system.

There are three portions of implementation in the system: implementation of student admission for student registration, implementation of payment gateway for secure payment information and implementation of card issuing bank for payment transaction.

A. Implementation of Student Admission

After the student admission in university website, the customer as student is check out and ordering. This is shown in Figure 3.

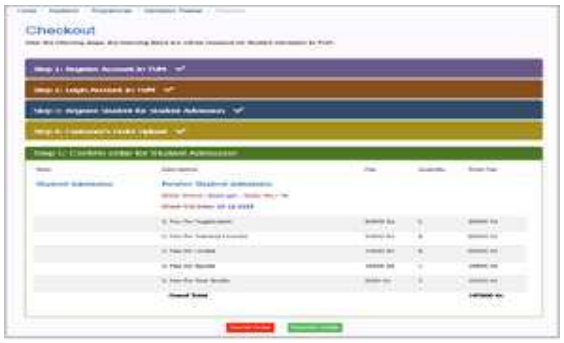

Figure3: Student Admission Order for Checkout

B. Implementation of Payment Gateway

To implement the security for payment information in payment gateway, RSA algorithm generates public key for encryption process to create cipher text for the student's important payment information and private key for decryption process to recover the original payment information. The key generation process is illustrated in Figure 4. In key generation process, the authorized user of payment gateway must choose a suitable length of key–2048 bits. After generating the keys, the keys must be stored into the payment gateway for any online universities and banks. Any online student can obtain the public key of their university from payment gateway before encrypting the card information. So, the payment gateway must be responsible to share the university's public key to online students.

Figure4: Key Generation of the Payment Gateway

The payment gateway must responsible to make secure payment transaction. Since the university and the payment gateway have been collaborated together, the order detail can be loaded in payment gateway and believe that this payment gateway is trust third party for online payment process. So, the credit card data (card number, expire date, security code, card holder name, email, and name of card issuing bank, etc.) are filled and encrypted with the university's public key by using RSA as shown in Figure 5.

Figure5: Encryption Card Information in Payment Gateway

In order to decrypt the student's cipher text, the payment gateway receive the cipher text and decrypt it with the university's private key to produce the original student's

card information as shown in Figure 6. And then, the payment gateway validate the card for payment transaction.

Figure6: Decryption Student Card Information in Payment Gateway

C. Implementation of Card Issuing Bank

After the card validating, the payment gateway send the card information to the customer card issuing bank. The bank make the payment transaction between customer's account and merchant's account. In payment transaction process, the online customer's bank account is also verified before transaction process. It is shown in Figure 7.

Figure7: Customer Account Information in Bank

VII. PERFORMANCE EVALUATE OF RESULTS

The secure online payment system is actually based on the public-key RSA cryptosystem, since the student's card information are transmitted over the insecure network to apply the confidentiality, cryptographic service, on the student credit card information. The experimental results for RSA key generation, RSA encryption and RSA decryption are shown in Table 1.

Table1. Experimental Results for RSA Algorithm

Description	Plain Text Size	Cipher Text Size	RSA Algorithm	
			Key Size	Execution Time (Millisecond)
Key generation	-	-	256 bits	43
Encryption	128 bits	-		1
Decryption	-	512 bits		4
Key generation	-	-	512 bits	57
Encryption	408 bits	-		1
Decryption	-	1056 bits		4
Key generation	-	-	1024 bits	146
Encryption	888 bits	-		1
Decryption	-	2064 bits		8
Key generation	-	-	2048 bits	658
Encryption	1960 bits	-		2
Decryption	-	4208 bits		35
Key generation	-	-	3072 bits	14977
Encryption	2984 bits	-		5
Decryption	-	6336 bits		127
Key generation	-	-	4096 bits	26280
Encryption	4008 bits	-		11
Decryption	-	8437 bits		311

The algorithm is coded in Java Script, and run on a computer with Intel Pentium Dual Core processor (3.30 GHZ) and RAM (4.00 GB). The implementation for RSA algorithm shows that RSA performs high level of security at a low cost. This experimental result is the average calculation of duration (millisecond) based on different key sizes and different plain text that represents the customer payment information.

In the system, the length of payment information (card data) of online customer is 142 characters (1136 bits/142 bytes) and the payment information must be encrypted before the transmission over the insecure network. In this case, 256 bits, 512 bits and 1024 bits key size in the RSA algorithm are not suitable for encrypting the customer payment information since the plain text size in the system is larger than the key sizes. So, 2048 bits, 3072 bits and 4096 bits key sizes have availability to encrypt the payment information in the system. According to the experimental results, processing time of 2048 key size in the secure online payment system is resonable time for the system and more suitable for security level and it can encrypt the student card information.

VIII. CONCLUSIONS

The proposed payment system protect a customer's financial information from being compromised by sending it directly to a payment gateway rather than sending through a merchant. Hence, public key of university must be shared from the payment gateway and private key must be secrete into the payment gateway. So, the payment gateway is used as TTP between payment parties in the system and provide the confidential for customer's card information.

So, the system provides secure payment transaction in online shopping and e-commerce since the suitable payment flow mechanisms with payment gateway are used in the system. Moreover, using large key size in RSA cryptosystem also protects the many attacks and time consumption is also suitable for payment process. In addition, the system is also efficient for online customer because there are no complex processes in payment transaction.

In the system, RSA algorithm generates pubic key and private key within 256 bits to 4096 bits key size. So, the maximum 4096 bits key size has availability to encrypt the (4008 bits/501 bytes) plain text size and the overall execution time include the key generation, the encryption and the decryption process is 26602 millisecond. So, larger 501 bytes plain text size cannot be encrypted in the proposed system.

As further extension, payment gateway should implement some method to secure a customer's payment that depends on the customer's personal information, like address. Moreover, the payment gateway should protect the stolen payment data from Distributed Guessing Attack by using filter guessing attempt number to detect repeated invalid attempts made within a certain time span and detect post code.

ACKNOWLEDGEMENTS

The author is deeply grateful to Dr. Moe Moe Aye, Professor and Head of Department of Information Technology, Technological University (Mandalay) for her willingness to share her ideas helpful suggestions and all teachers for providing the opportunity to embark on this paper writing.

REFERENCES

[1] Chinedu J. Nwoye, "Design and Development of and E-Commerce Security Using RSA Cryptosystem," International Journal of Innovative Research in Information Security (IJIRIS), Volume (6), Issue (2), 2015.

[2] Ailya Izhar, Aihab Khan, Malik Sikandar Hayat Khiyal, Wajeeh Javed, Shiraz Baig, "Designing and Implementation of Electronic Payment Gateway for Developing Countries," Journal of Theoretical and Applied Information Technology, Volume (26) No. 2 2011.

[3] Mohammed Aamir Ali, Budi Arief, Martin Emms, and Aad van Moorsel, "Does the online card payment landscape unwittingly facilitate fraud?," IEEE Security & Privacy 2017.

[4] Shristi Pant, "A Secure Online Payment System," *University of Kentucky*, 2011.

[5] Muzhir Shaban Al-Ani, Rabah Noory, and Dua'a Yaseen Al-Ani, "Billing System Design Based on Internet Environment," *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 9, 2012*.

[6] "Online Payment Process," Kathleen Kaye Acosta, E-Business Technologies – SS2008.

[7] Din Islam, "Secure Electronic Payment System through RSA algorithm," M. Eng. thesis, Rajshahi University of Engineering & Technology, Bangladesh, 20th December, 2014.

[8] Muzhir Shaban Al-Ani, Rabah Noory, and Dua'a Yaseen Al-Ani, "Billing System Design Based on Internet Environment," *(IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 9, 2012*.

[9] Kyaw Zay Oo, Moe Moe Aye, Mya Thidar Myo Win, "Development of Secure Online Payment System," (NCSE) National Conference on Science and Engineering, Mandalay Technological University, Mandalay, Myanmar, 28th-29th June, 2018.

[10] Kyaw Zay Oo, "Development of Secure Online Payment System Based on RSA," Master of Thesis, Department of Information Technology, Technological University (Mandalay), Mandalay, Myanmar, December, 2018.

International Journal of Trend in Scientific Research and Development
IJTSRD
International Journal of Trend in Scientific Research and Development
ISSN: 2456-6470