International Journal of Economics, Commerce and Management
United Kingdom ISSN 2348 0386 Vol. VII, Issue 9, September 2019

http://ijecm.co.uk/

SECURITY IMPLEMENTATION OF E-COMMERCE SYSTEMS USING CRYPTOGRAPHIC METHODS IN THE TRANSACTION PROCESS

Yusuf Panorama Putra
Faculty of Technology and Engineering, Business Information System,
University of Gunadarma, Jakarta, Indonesia
panorama.putra@gmail.com

Rudi Trisno Yuwono
Faculty of Technology and Engineering, University of Gunadarma, Jakarta, Indonesia
rudity@staff.gunadarma.ac.id

Abstract

Security is the most important issue when we build a website specifically that supports e-commerce activities. However, many business owners are unaware of this because of limited information and often because of the lack of capabilities of the developers. In fact, if you want to order and purchase transactions on the e-commerce website, at least it must be equipped with data encryption facilities. One of the security methods is the use of Secure Socket Layer (SSL) technology. This can provide us with information about the security of an e-commerce system and threats that can occur during a transaction. This writing discusses the implementation of cryptographic methods in e-commerce. The method used is a literature study and case studies on e-commerce. Data obtained through observation on the website, along with other data obtained from the internet, journals, and other data from literature review.

Keywords: E-commerce, Security, Threats, Cryptographic, Secure Socket Layer, SSL

INTRODUCTION

The development of technology has made the marketing world also increasingly develop. As part of E-commerce business activities, online buying and selling is increasingly widespread. No need to leave the house and face traffic jams if you want to buy an item. By using the Internet and gadgets, buying and selling transactions have become very easy.

E-Commerce has a negative side, namely the existence of cybercrime (for example, lying to customers, credit card crime, phishing, hacking, sniffing, keylogging, and worms). This is directly proportional based on searches, a quarter of people who directly transact digital have felt the effects of fraud. While 1 in 2 users of digital transactions have experienced fraud on themselves or those around them. this will certainly complicate the growth of the digital economy industry in developing economies such as Indonesia because of the high number of fraud cases that occur, "said Managing Director of the Asia Pacific Experian, Dev Dhiman at Hotel Indonesia Kempinski, Jakarta (8/11). The threat will result in customers afraid of doing transaction and then return to traditional methods of doing business.

The standard data encryption facility used on the Internet today is SSL (Secure Socket Layer) issued by trusted issuers based on a recognized CA (Certificate Authority). In this case the HTTP protocol (Hypertext Transfer Protocol) is the standard protocol used on the web. In order to support the ease of communication between diverse devices, the HTTP protocol is designed to have an open platform. The simplicity of this design was apparently used by several individuals to steal information sent by users of a website.

LITERATURE REVIEW

E-Commerce Security

The system uses encryption method, or better known as cryptography, which is the method of presenting a message or data sent through a public network with certain keys. In cryptography there are four main things, namely:

1. Confidentiality is information only, for and understood by those who are entitled.
2. Integrity is information that cannot be changed in storage.
3. Non-Repudiation is information that can be ascertained who is the sender and recipient.
4. Authentication, ie the sender and recipient can confirm each other's identity and origin or destination of information.

Secure Socket Layer (SSL)

SSL is used to secure HTTP web communication between the browser and web browser. SSL uses three protocols namely the SSL Handshake Protocol (where the session takes place

between the client and SSL server), SSL Change Chiper Spec Protocol (gives approval to the Chippersuite while the session is in progress), SSL Alert Protocol (conveys an SSL error message between the SSL server and the client). SSL protocol is used to provide data integrity and reliability and has become part of the TLS (Transport Layer Security) protocol, which is an integrated security protocol (Stallings, 2003).

Public Key / Public Private key

Public key is a key that is known by the public, while private key is a key that is known by the owner. There are differences in the Private key and public key, namely the private key uses one key to do the encryption and description process, while the public key uses a different key. Private key has the advantage of being fast, while the public key has the disadvantage of requiring high computation and requiring key repositories.

Cryptographic Method

Cryptography is a technique to maintain the confidentiality of a message by encoding it so that it cannot be understood anymore. Cryptography has an algorithm in the coding process so that authenticity can be maintained. The scheme of the cryptographic system can be seen in the image below:

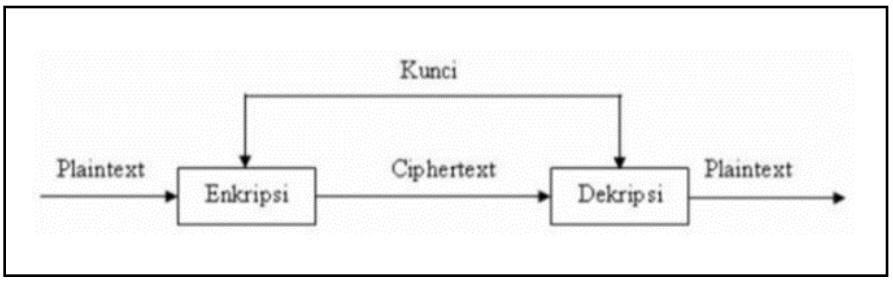

Figure 1 Scheme of the Cryptographic

RESULTS METHOD

Testing Method

Every software product can be tested through two testing approaches, the first is called black-box testing and the second is called white-box testing. White box testing is done by testing the program codes created in the application. Testing is done by checking all the code in the program has been executed at least one time. This test is carried out in the system development process, namely testing the program code (coding). In black-box testing, we will

observe the results of interface execution through test data and functional checking of applications that have been made.

Encryption System

At the beginning of the encryption process, the input that has been copied into the state will undergo an AddRoundKey byte transformation. After that, the state will undergo SubBytes, ShiftRows, MixColumns, and AddRoundKey transforms as many times as this process in the AES algorithm is called the round function. The last round is somewhat different from the previous rounds, where in the last round the state did not experience the MixColumns transformation. In Figure 2 is a flow diagram of the AES encryption algorithm.

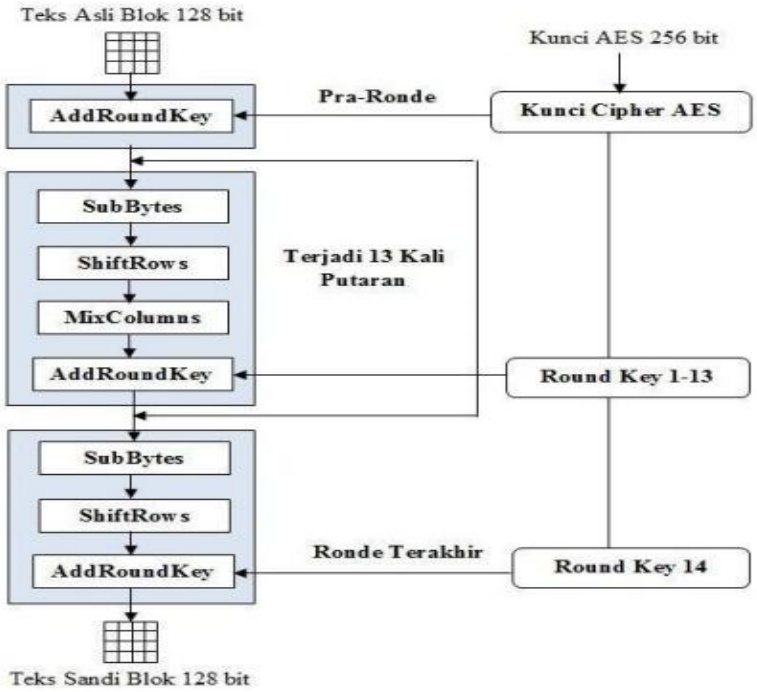

Figure 2 Encryption Flowchart

System Planning In Transactions

General system design procedures for adaptive E-Commerce development consist of several stages, including the design of program specifications, design of description and description, design of interfaces, and system testing.

Next in Figure 3; in the Use Case Diagram explains that the administrator has the right to do the entire data processing, and for customers can only log in, view and buy a list of products and can log out of the application.

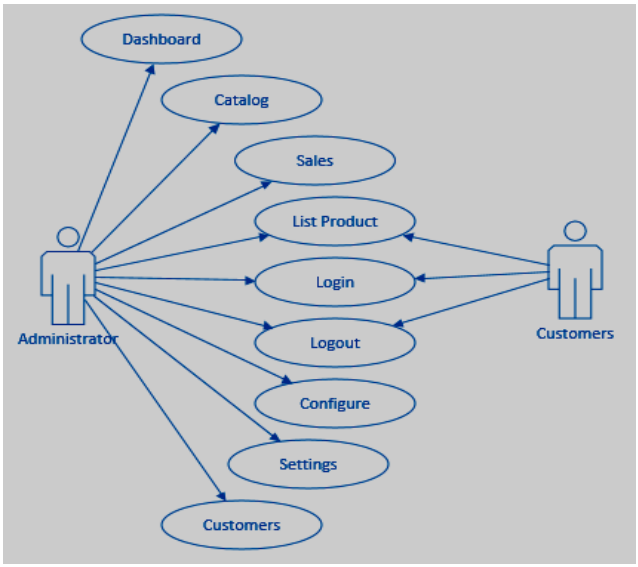

Figure 3 Use Case Diagram Administrator and Customers

RESULTS AND DISCUSSION

The Implementation encryption process is performed on a table contained in the database then a description is made to display the application page. This design consists of a list of fields to be encrypted, the conditions of the fields before they are encrypted, and the conditions after they are encrypted.

Before Encrypting

In the Product_Grid Table the encryption in the name, quantity and price fields is all normal and has not been encrypted as shown in Figure 4.

id	name	description	sku	qty	weight	price	base_price	total	base_total	p
1	Asus ROG	(NULL)	12345-variant-1-8	1	0	150.000.0000	150.000.0000	150.000.0000	150.000.0000	
2	Asus ROG	(NULL)	12345-variant-1-8	1	0	150.000.0000	150.000.0000	150.000.0000	150.000.0000	

Figure 4 Table Products_Grid

After Encrypting

The Product_Grid Table After Encrypting the name field, the quantity and price have changed because encryption has been performed. as shown in Figure 5.

sku	type	name	quantity	price	status
00001	simple	eyA8EwDQMluS/Q+Dbhud7YfYXZvPSpGV8eVLuYMdU54=	eUbOyaHatE8z0+8EeZmf+w==	xo3484slIrOn0oFD41S8qg==	1
00002	simple	Ni7tWzqxbv+0a3gwhqrZyYYgTUlwLTlhj+yHf9m5jq6GT9S...	eUbOyaHatE8z0+8EeZmf+w==	shbyRRbrpdzjh5PxtavD1g==	1
00003	simple	paUw6WsRZDIzLPVZf7EjnxkZNt7GXG2H2m188kVqNADfj1...	eUbOyaHatE8z0+8EeZmf+w==	Yv1bPRHI+1fiw4I5Z1538A==	1
00004	simple	Gisy/aYDWqmZY8VH8izDZ+BxDLONm+vVvdugqIIuGVizQ...	eUbOyaHatE8z0+8EeZmf+w==	6K1HMhNpTRyoDT9FEwVYtg==	1
00006	simple	nIGKAJfdttJp/FFmVXQYq9Gu3lp/bEny27zAkGwEcsgWJg/...	2GN3FWsoyR9yRNrIrUTejA==	MMMlVpd+EHejJHJz7odVWQ==	1
00007	simple	R2f+rYBlsCiv9QF652pyCPC6JEX38WfFck/bujDVJAFldLqu...	+0IIir6UDoXHiBClAnfEUg==	/gsKrWXeB9xNg7mTQVEtQQ==	1

Figure 5 Table Products_Grid After Encryption

Implementation of SSL Certificate

The process of implementing SSL is done on the website throughout the application page to maintain the security of the application system and the identity of a website. The application page above the application of ssl has been done with the name url https://www.softrever.com/ and the application can run well, can be seen in Figure 6 below.

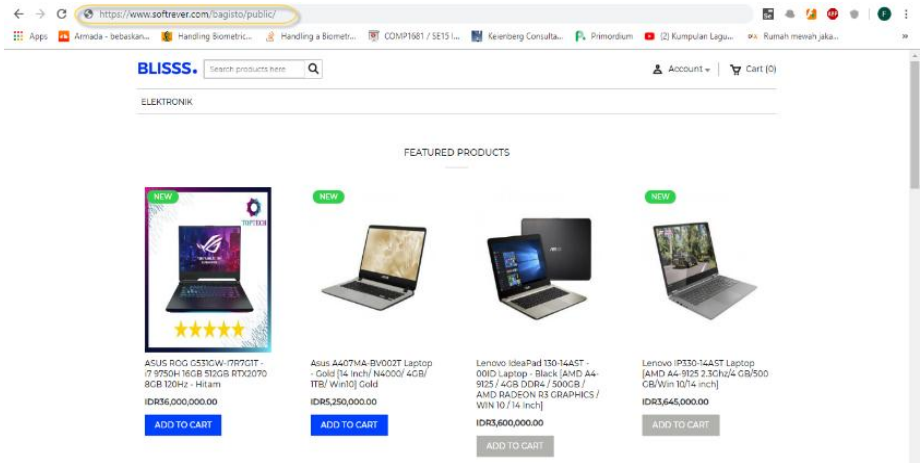

Figure 6 Application of SSL on the Website

Home Interface

This page is the first page that appears when E-commerce is accessed, on this page the customer can make an item transaction by looking at the details of the item that he wants to buy as shown in Figure 7 below.

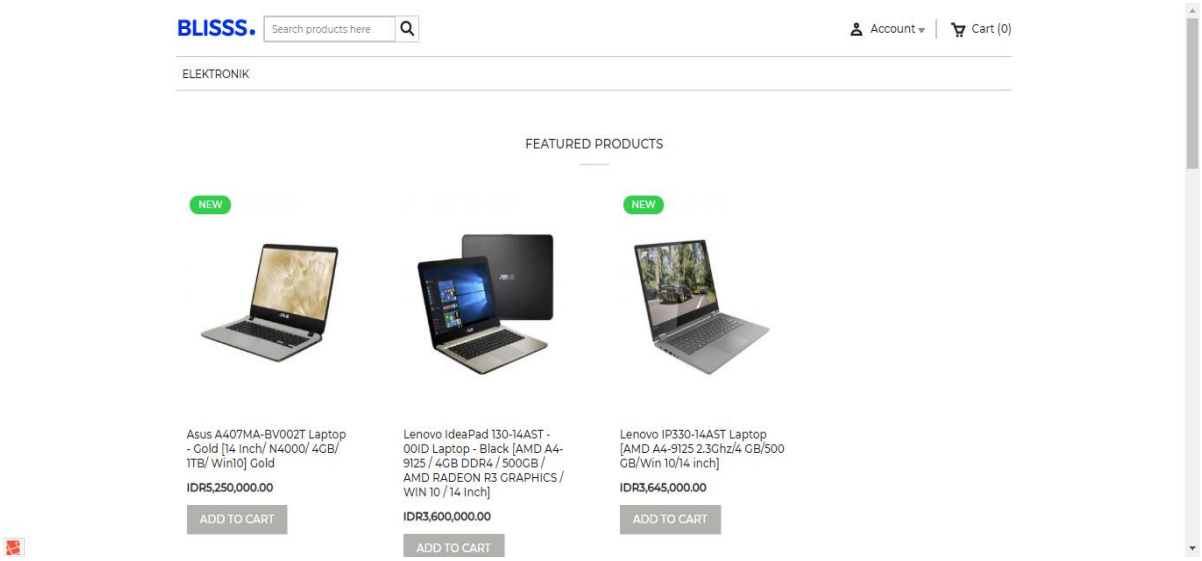

Figure 7 Home Interface Page

Blackbox Testing Interface

Blackbox Testing is a testing phase where the emphasis is on the interface.

Table 1 Blackbox Testing Interface

No	Testing	Expected result	Test result
1.	Interface halaman List Product	Halaman menu List Product	Corresponding
2.	Interface halaman Login	Halaman menu Login	Corresponding
3.	Interface halaman Logout	Halaman menu Logout	Corresponding

CONCLUSION

From the results of the research and discussion it can be concluded that:

1. The process of encrypting and describing product data and transaction data in e-commerce applications is successfully carried out and can maintain data in the database with the results of encryption so as to avoid data theft from the database directly.

2. Can strengthen the security system in e-commerce applications, so it can be assumed that the cryptographic method using AES encryption can be applied to this e-commerce application.

3. With the implementation of security methods using SSL can keep the security system of e-commerce applications from attacks carried out through computer networks.

RECOMMENDATIONS

Suggestions that can be used for developing this application are as follows:

1. The application still needs to add a certification authority / digital signature which functions to verify the identity of the sender and recipient so as to minimize fraud committed by people whose identities are unknown.

2. Applications can be combined with other cryptographic algorithms by following the development of data security science.

3. Ciphertext can be combined with data compression algorithms, so the results of encryption are not too long.

REFERENCES

Andre. M, Carolina. (2010). Keamanan Dalam Electronic Commerce, Bina Nusantara University Jakarta.

Asri Prameshwari, Nyoman Putra. (2018). Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen. Universitas Udayana.

Chey. C (2004). Cryptography For Dummies. Indianapolis, Canada.

Kartika Imam Santoso. (2015). Metode Keamanan E-commerce. STMIK Bina Patria Magelang.

Mateus, (2013). Tinjauan Keamanan Sistem Transaksi dan Pembayaran Pada E-commerce Studi Kasus Toko Online www.buahonline.com.

Pradnya B. Rane, B. B. Meshram . (2012). Application-Level and Database Security for E-Commerce Application. Veermata Jijabai Technological Institute, Matunga, Mumbai.

Revi Fajar Marta. (2013). Impementasi Kriptografi Pada E-commerce. Institut Teknologi Bandung.

Yanti Rusli Neti (2018). Implementasi Algoritma Data Encryption Standard Pada Penyandian Record Database, Teknik Informatika STMIK Budidarma Medan.

Harold Situmorang. (2016). Keamanan Basis Data Dengan Teknik Enkripsi, Universitas Sari Mutiara Indonesia.

https://epolebusiness.wordpress.com/2008/06/04/keamanan-e-commerce.

Voni Yuniati , Gani Indriyanta. (2009). Enkripsi dan Dekripsi Denngan Algoritma AES 256 Untuk Semua Jenis File. Universitas Kristen Duta Wacana Yogyakarta.