INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 5)
Available online at: https://www.ijariit.com

A methodology towards securing a web portal using XML encryption

Abhijit Dnyaneshwarrao Shahane
shahanea02@gmail.com
P. R. Pote Patil Institute of Engineering and Research , Amravati, Maharashtra

ABSTRACT

An online shopping system permits a costumer to submit online orders for items from a store. A Web portal acts as a gateway to the Internet. Web portals provide a single point of access to a variety of content and core services, and offer a single sign-on point. The main challenge for online shopping portals is to provide security for the transactions involved. Customers usually need to enter their crucial information like credit card number, debit card number etc. to buy products. Today most of the shopping portals use Secured Socket Layer (SSL) to transfer crucial data. This system was capable of providing good end-to-end security. But, it is unable to encrypt only a small part of the stored information; so a large cipher text is generated. To overcome this issue, new system is proposed here, which makes use of XML Encryption to provide security for transactions by generating a compact cipher text, which is transferred over the net as an XML document file. In this paper work the development of secured web portal is undertaken. Online shopping portals are new way for marketing hence must be designed in a creative but simple manner so that it is easy for the users to transact from it. There is need to analyse this new player by applying XML encryption which provides end-to-end security for applications that require secure exchange of structured data.

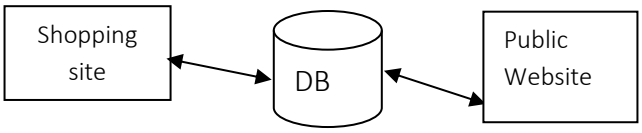
Keywords: *Crucial, Secured Socket Layer*

1. INTRODUCTION

1.1 E-Commerce

E-comerce encompasses three types of business transactions.

a) **B2C E-commerce Commerce** refers to the all activities surrounding the purchase or sale of goods or services. E-commemrce refers can occur to the process of buying or selling a product or service over an electronic network i.e.an Internet. This type between a business and consumer.
b) **B2B E-commerce:** This type can occur between one business and another business.
c) **C2C E-commerce:** This type can occur between two consumers.
d) **Database:** This acts as a storage container that holds information about the items that merchants sell.
e) **Shopping Website:** This is a website that enables to modify the information in the database.
f) **Public Web Site:** This is the website that displays and describes merchants products to the customers. From this website merchandise can be securely purchased by anyone in the world.



1.2 Trends In Online Shopping

Online shopping is a type of electronic commerce used for business to business (B2B) and business to consumer (B2C) transactions. It is a more effective way of getting products to people and spreading into different demographics. It offers some of the advantages such as Convenience, Information and Shipping cost, Online security etc.

2. LITERATURE SURVEY

2.1What is Portal?

Portal is a term, same as gateway, a WWW that is to be a major starting site for users when they get connected to the Web. A portal uses a consistent framework for presenting the information in a standard way. The services available through the portal are all designed to fit within a standard portal framework. A shopping portal is a page where buyers find links to a wide variety of products and services. A shopping portal offers convenience, saves time and makes it possible for customer to compare products and make selections.

2.2 A Brief History

Online shopping is important because it offers buyers convenience that has never before been achievable. The technology that is now available allows costumers to shop on Internet 24*7, without leaving their homes and offices. Shoppers are provided with an abundance of merchant sites where almost any goods can be bought. Consumers can also compare prices. It was invented in UK in 1979. In the 1990s these systems migrated to the Internet and WWW and became fully featured, fast and secure making. In the same year Netscape introduced SSL encryption to enable encryption over the data transferred online. This later became the necessity of online shopping. In 1995, Amazon started, which is the largest online shopping mall now.1998, witnessed use of electronic postage stamps where people can download and print postal stamps after paying nominal fee. In 1999 the first online shop was started in UK.

3. PRESENT THEORY AND PRACTICE

3.1 Existing system

As the popularity of online shopping increased the risks involved in the transactions grew exponentially. To address the issue of security Netscape introduced SSL encryption to provide security. SSL and TLS have been widely implemented in several open source software projects. Programmers may use the open SSL, NSS or Gnu TLS libraries for SSL/TLS functionality. Microsoft Windows include an implementation of SSL and TLS as part of its Secure Channel package. Delphi programmers may use a library called Indy. This standard is used for providing security by some browsers also such as the one listed. Mozilla Firefox supports TLS since version 2.2.2 featured in Opera 10, Opera supports TLS 1.2. Though, standards have been proposed and implemented for providing security for an internet transactions, the challenges in this field are never ending. Hence periodic development in the security standards and methodologies is the need of the online transaction process. The new methodologies developed should be the enhancement of current technology and not a completely new method, as global acceptance of a completely new system is beyond reach goal unless it requires minimum or no change in the ease of use, speed and other factors.

3.2 Proposed System

With the ever-increasing popularity of internet, the population capable of participating in internet increased dramatically, increasing the security challenges. Also network traffic also became a prime issue. To make efficient use of the available bandwidth, the messages transferred over the internet should be of smaller size and also, to establish end-to-end security session handshake message passing if possible should be avoided as it substantially increases the network traffic which in extreme cases may lead to congestion. Existing system using TLS/SSL was capable of providing a very good end-to-end security for transactions involved. But it required long chatty signals for establishment of security session between two parties. Also, the whole file or whole message should be encrypted before sending over the internet. At a time not more than two parties could take part in the secured communication.

To, address the issues not addressed by the current system, a new system is proposed here, which makes use of XML encryption to provide security. XML Encryption provides end-to-end security for applications that require secure exchange of structured data. XML Encryption is the natural way to handle complex requirements for security in data interchange applications. Security provided to the Existing system:

Presently, Transport Layer Security (TLS) is the de facto standard for secure communication over the internet. TLS runs on layers beneath application protocols such as HTTP, FTP , SMTP, NNTP and XMPP and above a reliable transport protocol. TLS/SSL has a variety of security measures:

- SSL handshake with two way authentication with certificates.

A TLS client and server negotiate a stateful connection by using a handshaking procedure. During this handshake, the client and server agree on various parameters used to establish connection's security.

- The handshake begins when a client connects to a TLS-enabled server requesting a secure connection, and presents a list of supported cipher and hash functions.
- From this list, the server picks the strongest cipher and hash function that it also supports and notifies the client of the decision.
- The server sends back its identification in the form of digital certificate. The certificate usually contains the server name, the trusted certification authority (CA), and server's public encryption key.

The client may contact the server that issued the certificate and that the certificate is authentic before proceeding.

- In order to generate the session keys to used for the secure connection, the client encrypts a random number (RN) with server's public key (Pbk), and send the result to the server. Only the server can decrypt it with its private key (Pvk): this is the one fact that makes the keys hidden from the third parties, since only the server and client have access to this data. The client knows Pbk and RN, and the server knows Pvk and RN. A third party may only know Pbk, unless Pvk has been compromised
- From the random number, both parties generate key material for encryption and decryption.

This concludes the handshake and begins the secured connection, which is encrypted and decrypted with the key material until the connection closes. If any one of the above step fails, the TLS handshake fails, and connection is not created.

In other system, the client may use the certificate authority's (CA) public key to validate the CA's digital signature on the server certificate. If the digital signature can be verified, the client accepts the server certificate as the valid certificate issued by a trusted CA. If any one of the above step fails, the TLS handshake fails, and the connection is not created. Early implements of SSL used 40-bit symmetric key because of US government restrictions on the cryptographic technology. After several years of controversy, a series of lawsuits, and eventual US government recognition of cryptographic products with longer key sizes produced outside the US, the authorities relaxed some aspects of the export restrictions.

4. PROBLEM DEFINITION

4.1 Statement of problem

All the online shopping today makes use of TLS/SSL security, which is the de-facto standard used for providing secured transactions over the internet. But, this system has some limitations such as, it cannot establish secured session more than two parties and also it requires handshake signals to establish secured session which consumes considerable network bandwidth. This provided the motivation to develop the proposed system which by making use of XML encryption covers the limitations of current system.

To develop the proposed system XML encryption it requires development of different modules of various stages in which the above mentioned themes are common:

a) **Customer:** The customer plays very good role in this project. The registered customer is allowed for the shopping transaction only when he/she register with the name and password on the app, else what the new customer has to fill the registration form. Products purchased by customer will get stored in his/her cart, and he/she is able to make payment using credit or debit card.

b) **Merchant:** It will act as a data store. It sends the list products to the service provider for the display purpose on a portal.

c) **Bank:** It is a trusted agent. The credit card provided number Is sent to bank where it reads that number using UPI pin of bank to complete the transaction.

4.2 Developing portal

Portal provides information of all products and users in one place. The major task of it is to reduce the traffic in the network as the user need not make repeated requests to find related information.

4.3 Providing Security

To secure the payment transactions the XML encryption technique is used. This provides the security to the whole program such as:

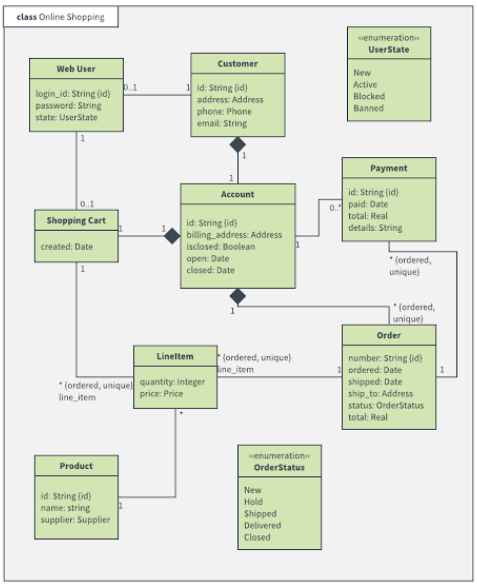
- **Authentication:** It confirms the identity of the user by checking it with the database
- **Confidentiality:** It secures the data like credit card number by encrypting it.
- **Data integrity:** It ensures that the data is not modified from source to destination.
- **Non repudiation:** It provides protection against denial by participating in all or part of the communication.

4.4 Developing Databases

Three different databases are need to be created:

- **Customer database:** This maintains all the basic information.
- **Merchant database:** It acts as a data bank of products available on portal
- **Bank database:** It contains account details of customer for the payment of purchase list.

5. SOFTWARE DESIGN



6. CONCEPTS USED

6.1 Cryptography

Cryptography is probably the most important aspect of communication security and is becoming increasing important as a basic building block for computer security. The increased use of computer and communication systems by industry has increased the risk of theft of proprietary information. This theft requires a variety of counter measures; encryption is a primary method of protecting valuable electronic information. The process of converting from plaintext to cipher text is known as enciphering or encryption. The many schemes used for enciphering constitute the area of study known as cryptography. Such a scheme is known as cryptographic system or cipher. Technique used for deciphering a message without any knowledge of enciphering details fall into the area of cryptanalysis. The area of cryptography and cryptanalysis are called cryptology. Types of cryptography:

1) Symmetric Key Cryptography
2) Public Key Cryptography

6.2 HTML (Hyper Text Markup Language)

- Hypertext is the method by which one can move around on the web by clicking on special text called hyperlinks which bring user to the next page.
- Markup is what HTML tags do the text inside them.
- HTML is a language as it has code words and syntax like any other language. This language is used for the creation of static pages.

6.3 XML (extensible Markup Language)

XML is a general purpose specification for creating custom markup languages. It is classified as an extensible language, because it allows user to define the markup elements. XML's purpose is to aid information systems in sharing structured data, especially via the internet, to encode documents, and to serialize data; in the last context, it compares with text based serialization languages such as JSON,

YAML, S-EXPRESSIONS.XML's set of tools help developers in creating web pages but its usefulness goes well beyond that. It makes it possible to define the content of a document separately from its formatting, making it easy to reuse that content in other applications or for other presentation environments. Most importantly, it provides a basic syntax that can be used to share information between different kinds of computers, different applications and different organization without needing to pass through many layers of conversion. XML document has two correctness levels:

Well formed & valid.
The basic syntax for one element is :

<element name attribute name="attribute value">Element Content</element name>.

The main goal of the project is to provide the security. The security is provided using the XML encryption. The entered credit card number is encrypted using RSA algorithm. The Encrypted credit card number is stored in the xml document which is called at the bank side for decryption.

6.4 Javascript

JavaScript is a scripting language used to enable programmatic access to objects within other applications. It is primarily used in the form of client-side JavaScript for the development of dynamic websites. JavaScript is a dialect of the ECMA Script standard and is characterized as a dynamic, weakly typed, prototype-based language with first-class functions. JavaScript was influenced by many languages and was designed to look like Java, but be easier for non-programmers to work with.

JavaScript, despite the name, is essentially unrelated to the Java programming language even though the two do have superficial similarities. Both languages use syntaxes influenced by that of C syntax, and JavaScript copies many Java names and naming conventions. The language's name is the result of a co-marketing deal between Netscape and Sun, in exchange for Netscape bundling Sun's Java runtime with their then-dominant browser. The key design principles within JavaScript are inherited from the Self and Scheme programming languages. JavaScript engine (also known as JavaScript

interpreter or JavaScript implementation) is an interpreter that interprets JavaScript source code and executes the script accordingly. For JavaScript a web browser is most common environment. The sample JavaScript can be written as,

```
<html><head>
<script>
document.write('Hello World!');
</script>
</head></html>
```

6.5 JSP

Java Server Pages (JSP) is a technology that mixes regular, static HTML with dynamically-generated HTML. The JSP page has .jsp extension. The code is written between the start of angular tag <%□ and end of angular tag %>□. Three main types of JSP constructs can be embed in a page they are scripting elements, directives, and actions.

- Scripting elements specify Java code that will become part of the resultant servlet.
- Directives control the overall structure of the servlet.
- Actions specify existing components should be used to perform the operations.

6.6 JCA

The Java platform strongly emphasizes security, including language safety, cryptography, public key infrastructure, authentication secure communication, and access control. The JCA is a major piece of platform and contains provider architecture and a set of APIs for digital signatures, message digest, certificates, certificate validation, encryption, key generation and management and generation of random numbers etc. These APIs allow the developer easily integrate the security into their code. The architecture was designed around the following things.1. Implementation independence and Interoperability. 2. Algorithm extensibility

6.6.1 Client Side Encryption Using Javascript: JavaScript is used in the project to validate the entered card number entered by the user when making a purchase order and also to encrypt the card number before sending it over the network to provide additional security. Usually the java script is used at the client side for providing the security.

6.6.2 Server Side Encryption using JSP: To send crucial information such as credit card number, in an encrypted form to the bank for validation, the service provider makes use of JSP along with the functionalities of JCA to provide security.
Two methodologies have been used here for encryption and decryption.

a. TLS/SSL security
b. XML Encryption

TLS/SSL security: Transport Layer Security along with Secured Socket Layer is the default standard used for providing security over the Internet. In the project, RSA algorithm is used. Public key generated in the RSA is used for encrypting the data and Private Key is used for decryption. The pair of the keys are generated at the bank the bank then send this public key to the customer for making the encryption that is, using this public key the credit card number is encrypted and perform the transactions.

XML Encryption: XML makes use of asymmetric encryption. Asymmetric encryption is used for encryption of the credit card number by making use of a public key bank. The resulted encrypted data is placed in the nodes of XML and a XML file is generated which is sent over the network. At the recipient Bank uses its private key to decrypt the credit card number. Parsing of XML file is needed at the recipient. In the project, RSA is used as public key algorithm.

6.7 System Testing

System testing is concerned with finding errors that result from unanticipated interactions between components and component interface problems. It is also concerned with validating that the system meets its functional and non-functional requirements and testing the emergent system properties. For large systems, this may be a multi stage process where components are integrated to form the final system. In the project the all three personal terminals are connected to one another for the secure transaction from the customer to the bank and then to the merchant. The connection from one terminal to the other is checked that is subsystem checking. Then the overall system is checked for the error correction and provides the major security measures.

6.8 XML Document Page

The main goal of the project is to provide the security. The security is provided using the XML encryption. The entered credit card number is encrypted using RSA algorithm. The Encrypted credit card number is stored in the xml document which is called at the bank side for decryption.

7. CONCLUSION AND FUTURE SCOPE

The main principle of this project is to provide security for online transactions. This project makes use of XML Encryption to secure the transactions. XML encryption tries to overcome the limitations of earlier system. It can encrypt only a part of the file. Only the crucial information such as credit card number is encrypted leaving the rest of the file as it is. Hence, it is a combination of secure and non-secure encryption. It effectively reduces the overhead involved in encrypting the whole file. The encryption and decryption here is performed using the functionalities provided by java and XML language is used for transferring the encrypted data. Properties of XML and java allow full compatibility with large installed base of secure web servers, extensibility and flexibility.

Currently the system treats the entered credit card numbers if they are in the right format as valid and proceeds further. But, a list of invalid and fraudulent credit card lists should be maintained to avoid misuse of the crucial information.
The encrypted XML may be compressed to further reduce the size of the cipher text which makes efficient use of the network bandwidth. The compression of encrypted XML can be added as the future scope.

8. REFERENCES

[1] Cryptography and Network Security–By William Stallings, Pearson Education Publication, Third edition-2004.
[2] HTML Introduction to Web Page Design– By David Mercer, Tata McGraw Hill- Edition 2004.
[3] The Complete Reference–By, HarbertSchildt, The Tata MC Edition,Seventh edition 2005 for java concepts.
[4] Software Engineering-By Ian Sommerville, Pearson Education Publication, Seventh Edition-2004.

Declaration of interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

