# Secure Architecture for E-commerce Websites

Tooba Ahmad[1], Tauseef Rana[2]

(Received May 22, 2018; Revised November 27, 2018; Accepted May 17, 2019)
DOI: 10.33317/SSURJ.V9I1.108

***Abstract*— With the rapid growth of Information Technology (IT), the current markets are being transformed into e-markets/e-commerce. This has created a need for a secure approach to implement e-commerce and to keep its security. To meet this need, Service Oriented Architecture (SOA), is one of the best proficiencies to opt to, because it is flexible and easy to use. However, together with the advantages of SOA, there is also a possibility of unauthorized access of data, and interfering with key data is also easy. It is therefore a challenge for some organizations to implement secure e-commerce. This paper will explore/highlight the significance of SOA for e-commerce and also the issues/faults in the current e-commerce systems. An implementation design of a secure architecture for an e-commerce system supported by SOA has also been suggested in this paper.**

***Index Terms*— Logical Security, Service Oriented Architecture (SOA), System Consolidation, E-Commerce, Web Services.**

## I. INTRODUCTION

Computing based on Component Object Model (COM) and Common Object Request Broker Architecture (CORBA) models are the ones which have been commonly used for e-commerce modeling [1]. These models are quite complex to implement because they are derived from distributed computing which has some requirements and rules which determine the format of transmission of data. They also are coupled tightly in nature and therefore it is required that the current system will be redeveloped to enable other businesses and organizations to cope with the codes. The CORBA and the COM models are also incompatible with the latest e-commerce systems; as for these systems it requires to be flexible, loose in coupling, and some more requirements of the active commercial endeavors environments. Some of these requirements of e-commerce like flexibility in services and loose coupling are fulfilled in Service Oriented Architecture (SOA). For this, the needs include preparation and putting up systems which are scalable, easy to adopt and pliable in order to support the active business environment [2].

This model will allow enterprises to design, bring up, deploy, and to incorporate the services which do not depend on the applications and the platforms where they function. The linking is done through business processes so as to form applications and complex services which fulfill the required affairs. Even though services are not affiliated to each other, they are all coupled with each other where between the services is controlled by standard protocols.

SOA is the overriding choice in the implementation of e-commerce because of its advantages, which includes flexibility, easy usage, scalability and reusability. However, the security implementation of e-commerce is very complex because with SOA it is easy to tamper or interfere with messages and it also provides unauthorized access. A SOA based e-commerce's implementation is aided in this paper.

Fig. 1 shows the complexity of implementing the SOA based e-commerce system.

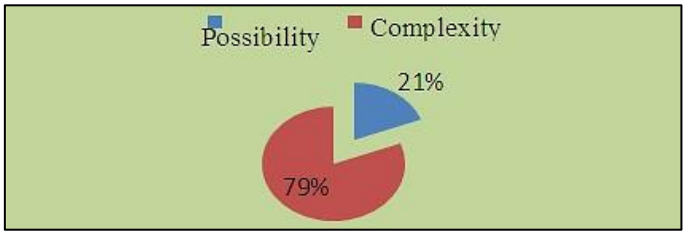


**Fig. 1: The Percentage Simplicity/Complexity of Implementing a SOA based E-commerce System**

In the rest of the paper, Section II highlights the previous related work present in the literature. A proposed solution is presented in Section III and in Section IV, methodology is being described. Lastly, Section V presents the conclusion and directions for the future work.

## II. LITERATURE REVIEW

### *A. Current Security Standards*

This section describes several security standards and technologies for e-commerce implementation:

i. Transport layer security (TLS); Secure Socket Layer (SSL):

These are non XML security models which have been mostly applied in the transportation of layer data communication. It is a security measure that ensures confidentiality of the messages being transmitted, their authenticity and integrity. SSL sustains the security of data communication using the public and significant secret cryptography. It is usable in several modes which depend on the security requirements, but the most common ones include, two way authentications, server authentication and/or no authentication. In no authentication, it is only the confidentiality which is used while in server authentication the server will authenticate itself and in the two way authentication, the server and the client authenticate to each other.

They are however accompanied by the following security attacks:

- Padding attacks.
- Renegotiation attacks.
- RC4 attacks.
- Version rolls back attacks.

[1] Masters Student, Department of Software Engineering, National University of Sciences & Technology (NUST), Islamabad, Pakistan. toobaahmad.developer@gmail.com
[2] Assistant Professor, Department of Software Engineering, National University of Sciences & Technology (NUST), Islamabad, Pakistan. tauseefrana@mcs.edu.pk

- Survey of websites.
- BEAST attacks.
- Truncation attacks.
- CRIME and BREACH Attacks.

ii. XML Encryption:

It is commonly used to encrypt and decode XML documents; however it is also usable to all other kinds of data and information. The XML encryption uses a different encryption algorithm in coding and decoding which includes:

- Triple Data Encryption Standard (3DES).
- Rivest Shamir Adleman (RSA).
- Advanced Encryption Standard (AES) [3].

It was developed in the year 2002 by World Wide Web Consortium (W3C) and it supports both symmetric cryptography and asymmetric cryptography. There are five various types of encryptions of XML. This kind of encryption is faced with a challenge of weak in chaining of cipher- text block. Therefore it is possible to decrypt data by modifying cipher texts and then you sent them together to an appropriate host where they will collect all the necessary data information from all the messages which had errors in them.

iii. XML Signature:

This works like a modern signature, where it is used as a policy to confirm the parentage of the information being transported. They can be used to secure all messages of XML Documents. It can also stop all text files, which can be accessed through Uniform Resource Allocator (URL). This signature was developed by a collaboration of Internet Engineering Task Force (IETF) and W3C and it supports integrity of information, authentication and non-renunciation. XML Signature can make several signatures at different sections of an XML document. These signatures are highly flexible when you compare them with all other kinds of signatures because this one does not utilize binary information but XML content.

The following are some security issues that are associated with the XML Signature:

- Complex and poor in performance.
- They don't apply to SOA application, which is very sensitive.
- Using XML signature in Web Service-security (WS-security) and Simple Object Access Protocol (SOAP), is susceptible to attacks, especially if it is not implemented properly.

iv. XML Key Management Specification (XKMS):

These are network services that provide Public Key Infrastructure (PKI) and average application of XML interface. It will to a great extent simplify the deployment of enterprise strength because it transfers the difficult tasks from clients to a trust service. The IETF collaborated with W3C and they developed XKMS for distribution of permanent keys and their enrollment.

Its design criteria included the following:

- It is supposed to be easy to implement and
- It should reduce or minimize the coding of the client and configuration.

The XKMS has two parts:

- XML Key Information Service Specification (X-KISS) and
- XML Key Registration Service Specification (X-KRSS).

They are used for processing and validation of public keys and registering of public keys where one can re-issue, recover, revoke and register.

Security issues in XKMS include:

- Recovery policy of the key,
- Replying of attacks and
- Denying of service attacks [4].

v. Security Assertions Markup Language (SAML):

It is a standard format, which is XML based and it authenticates and authorizes data between different parties which are conversing. Some components of SAML are:

- SAML Assertion, which contains safety data and for instance how to authentic or authorize.
- SAML Protocols, which explains the handling of requests and responses.

For SAML to operate it needs:

- XML signature,
- XML encryption,
- TLS and
- SSL.

vi. Kerberos:

It is normally used for the certification of where more than one user is passing messages to each other over a network which is not secure. It makes the environment very safe since the server and the customer both have to identify themselves,

It however has some drawbacks which include:

- Single point of failure.
- Requires user accounts.
- Restricted time requirement.

### *B. Security Analysis of SOA based E-commerce*

The supposed system gives several components of organization service, where users can call any time from online, some of which include but not limited to contract management services and trading information services.

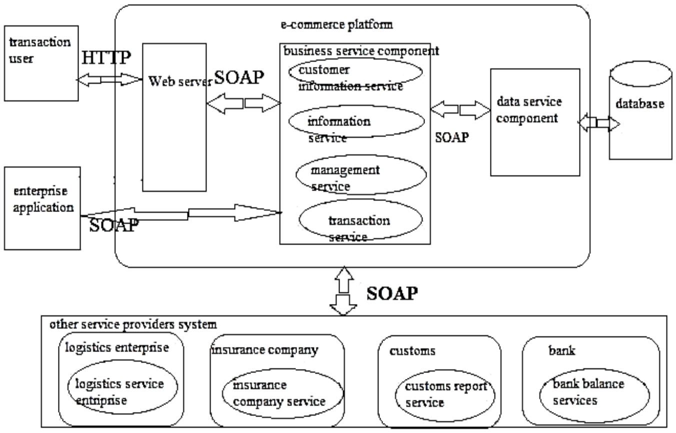


**Fig. 2: Basic Architecture for an E-Commerce System**

The users must be authenticated and passed before they access the management services by submitting their certification to a WWW host through an HTTP [5]. The current overall architecture system of an e-commerce system is illustrated in Fig. 2.

An e-commerce system confronts some safety factors which include but not limited to the following:

i. Certificate Duplicity:

The user is always supposed to deliver their certification through HTTP so as to be given a validation from a web host when it comes to business service components. User gets an authentication certificate from this process which is managed by Identity Management Service (IMS). This certificate can be easily be forged or a duplicate is unavoidable. Individuals, who were not really authenticated from the host, can easily access the system through these means.

ii. Unsecure Protocol:

HTTP is said be a safe system especially in dealing with some security threats and attacks for instance internal attacks in the systems. Attackers therefore interfere with the system and users keep on thinking that they are still using a system which is safe. They are then able to encode that communication easily.

iii. On the Application Level No Filters Mentioned:

In cases of no filters, which are mentioned in the application level, attackers may put some malicious codes through the web which may cause a very profound attack on the system.

iv. Unsecure Database:

When dealing with a malfunctioned database for instance, it may make an authorized person miss services and be denied.

v. Denial of Service Attacks:

It attempts to put in place for its users, the systems which are not found or unavailable. However, the current e-commerce model is prone to Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks since it is not protected.

## III. PROPOSED SOLUTION

### A. *Proposed Security Framework*

The proposed security framework provides solution to all risks and security problems discussed so far. The e-commerce makes accessible, some of the business components which may include online transaction services and transaction information services among others. The IMS (IP Multimedia Subsystems) is responsible for identification of users then making the business components available for the authorization and authentication.

There are two independent behaviors that can lead to achieving the business service components i.e., land access and remote access. A two-step verification mechanism is used here, which helps in ensuring that the certified users are the only ones to use the system and that there is no uncertified fellow be able to log in and use the networks. Fig. 3 represents the proposed security framework of a SOA based e-commerce system.

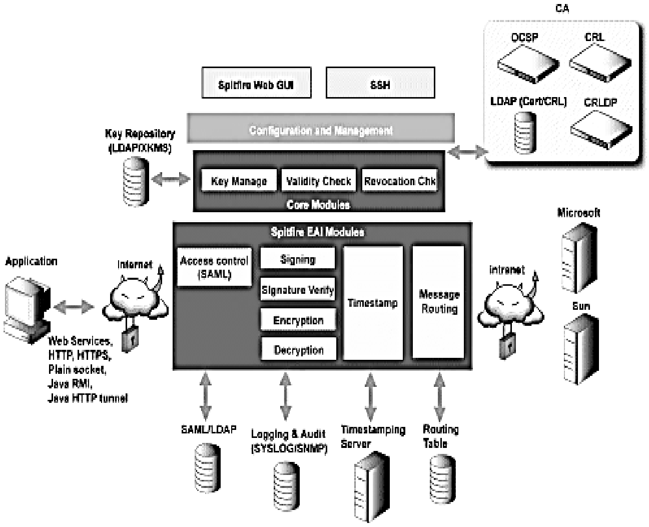


**Fig. 3: Proposed Security Framework Design [6]**

This kind of security can be accessed through the followings:

i. Input Sanitization:

The user should deliver an enquiry to the web server through a very safe protocol so that they may be given the opportunity to access the business service components. The information is checked again before passing it to the respective service component [7].

The request of the user can therefore be cleaned in cases whereby it could have contained some extra qualities e.g., $, #, &, *, and abc, where the information will only be treated as ABC having included sanitization rules to be in the system. It will also prevent those who will want to bypass authentication process. The problem of duplication of certificate can be solved by this method of input sanitization.

ii. Rule Based Plug-in for Additional Protection:

This will permit covering other layer of protection around the web server so that in case the sterilization is passed from the attackers, they would be choked in the next layer of security. The new level will function like an external security to enhance security and therefore in turn increasing the protection. For example in detecting and preventing attackers before the attacker will be able to access the control system of the business. For this layer to be created, Mod-Security is configured on Apache. Mod-Security can be used because it gives one, the authority to create rules and directives which will control the host. For this reason if dangerous request will be allowed to get to the business point, they will be detected. They will then be barred to access and logged out of these systems.

iii. Predefined Action Filter:

In this framework, filters are used. When users visit certain service component and they correspond an activity from a database, then the petition is forwarded to the respective service component and petition discharged. In the other case when an action is not available in the database, then the petition will not be given to the service component and an error message will be displayed [8]. In order to acquire spare security to business components and those related to database, Intrusion Protection System (IPS) and Intrusion detection system (IDS) are employed. In this security framework, the business service components and the database are connected and kept on different hosts. The connection between these two hosts should be monitored by firewall which should break down in case of any interference.

### *B. Implementation Benefits of Proposed Security Framework*

There are a number of benefits associated with the implementation of this proposed security framework:

i. Database Encryption:

The database is kept by two independent hosts which are all encrypted and they are monitored by IDS and IPS. The IPS and IDS disconnects communication between A and B in case an attack is sensed and encryption will protect any other data and information from the wrong use by attackers.

ii. Indirect Access to Enterprise Applications:

There is no permission for enterprise application to pass directly to the business but it is connected through a web host. This application provides another user interface and prevents most attacks, maintaining safety [9].

iii. Prevention Against DoS and DDoS:

The IDS and IPS will look at all the incoming information and it will therefore prevent all the DoS attacks. They can be easily configured to block all IP addresses.

iv. Post-Exploitation Prevention:

Post exploitation prevention should be enabled to prevent danger in cases where the intruders could have managed to log in to the system. Fig. 4 shows the process of identity management service.

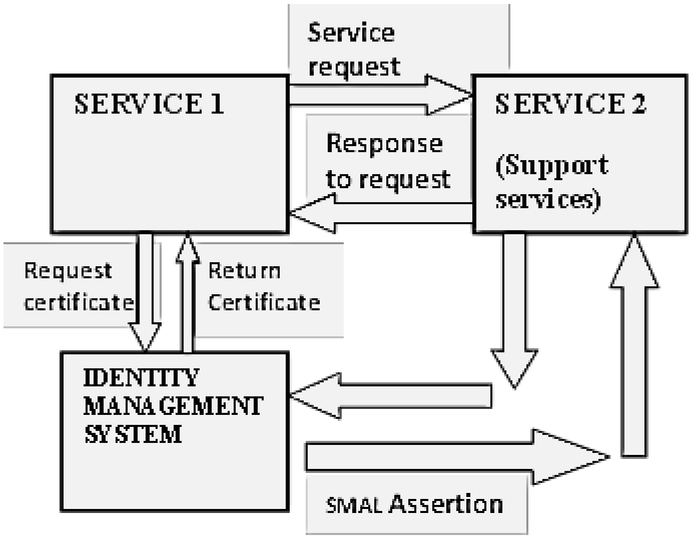
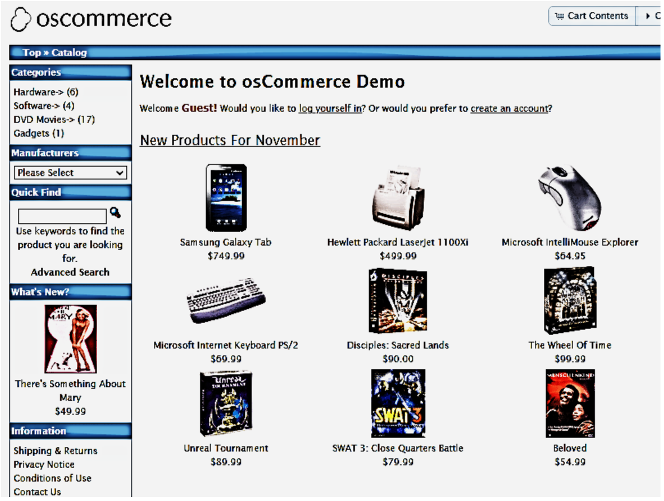


**Fig. 4: Process of Identity Management Service**

## IV. METHODOLOGY

The proposed security framework is implemented on an open source e-commerce system and it will be evaluated by the character of security threats.

The user should deliver an enquiry to the web server through a very safe protocol so that they may be given the opportunity to access the business service components. The information is checked again before passing it to the respective service component. The request of the user can therefore be cleaned in cases whereby it could have contained some extra qualities e.g., $, #, &, *, and abc, where the information will only be treated as ABC having included sanitization rules to be in the system. It will also prevent those who will want to bypass authentication process. The problem of duplication of certificate can be solved by this method of input sanitization as illustrated in Fig. 5.



Welcome to osCommerce Demo

Welcome **Guest!** Would you like to log yourself in? Or would you prefer to create an account?

New Products For November

**Fig. 5: Illustration** of **Users Infected Input [5]**

## V. CONCLUSION

This paper discussed the security issues of e-commerce and proposed a secure framework for this system which is based on SOA. It will give a secure e-commerce system that is implemented on an open source e-commerce system. The main distinction of this research is that it will help to align the benefits of SOA with e-commerce system. To examine this security framework, it should be tested for all threats. The proposed system will help to protect SOA based e-commerce system.

## REFERENCES

[1] Huang, M., Zhao, Y., & Zhu, L. (2011, October). Research for e-commerce platform security framework based on SOA. In *2011 4th International Conference on Biomedical Engineering and Informatics (BMEI)* (Vol. 4, pp. 2171-2174). IEEE.

[2] Ezenwoke, A., Misra, S., & Adigun, M. O. (2013). An approach for e-commerce on-demand service-oriented product line development. *Acta Polytechnica Hungarica*, *10*(2), 69-87.

[3] Luhach, A. K., & Dwivedi, D. S. (2011). Service-Oriented Architecture and Web Services Concepts, Technologies, and Tools. In *2011 IEEE International Conference on Computational Intelligence and Computing Research*.

[4] Farshchi, S. M. R., Gharib, F., & Ziyaeef, R. (2011). Study of security issues on traditional and new generation of e-commerce model. In *International Conference on Software and Computer Applications-IPCSIT* 9(1), 24-31.

[5] Yan, P., & Guo, J. (2010, May). Researching and Designing the Architecture of E-government Based on SOA. In *2010 International Conference on E-Business and E-Government* (pp. 512-515). IEEE.

[6] Luhach, A. K., Dwivedi, S. K., & Jha, C. K. (2014). Desiging a logical security framework for e-commerce system based on soa. *arXiv preprint arXiv:1407.2423.*

[7] Baby, A. S., Raveendran, D. & Joe, A. J. (2012, June). A study on secure and efficient access control framework for SOA *International Journal of Computer Science and Telecommunications, 3(*6),71-76.

[8] Saeed, M. A., Zaidi, S. A., & Nasir, M. M. (2016). SSUET Parking Facility, A Case Study; Current Scenario, Future Needs and Proposed Solution. *Sir Syed Research Journal of Engineering & Technology*, *1*(1), 11-11.

[9] Danesh, M. H., Raahemi, B., Kamali, S. A., & Richards, G. (2013). A framework for process and performance management in service oriented virtual organisations. *International Journal of Computer Information Systems and Industrial Management Applications*, *5*, 203-215.