Improving the Authentication Mechanism of Business to Consumer (B2C) Platform in a Cloud Computing Environment: Preliminary Findings

Dr. Feras Matarneh
Department of computer science / Duba University of Tabuk. Tabuk, Saudi Arabia

doi: 10.19044/esj.2017.v13n18p482 URL:http://dx.doi.org/10.19044/esj.2017.v13n18p482

Abstract

The reliance of e-commerce infrastructure on cloud computing environment has undoubtedly increased the security challenges in web-based e-commerce portals. This has necessitated the need for a built-in security feature, essentially to improve the authentication mechanism, during the execution of its dependent transactions. Comparative analysis of the existing works and studies on XML-based authentication and non-XML signature-based security mechanisms for authentication in Business to Consumer (B2C) e-commerce showed the advantage of using XML-based authentication, and its inherent weaknesses and limitations. It is against this background that this study, based on review and meta-analysis of previous works, proposes an improved XML digital signature with RSA algorithm, as a novel algorithmic framework that improves the authentication strength of XML digital signature in the B2C e-commerce in a cloud-based environment. Our future works include testing and validation, and simulation, of the proposed authentication framework in Cisco's XML Management Interface with inbuilt feature of NETCONF. The evaluation will be done in conformity to international standard and guideline –such as W3C and NIST.

Keywords: Authentication mechanism; e-commerce portal; business to customer (B2C); cloud computing; XML digital signature

Introduction

The success of a Business-to-Consumer (B2C) electronic commerce platform relies on the consumers' acceptance of the technologies involved as viable means (Cudjore, 2014; Pavlou, 2003). The internet and technology infrastructure serves as the enabler of the commercial online transactions between the consumers and the web retailers (Ayo, Adewoye, & Oni, 2011; Brynjolfsson & Smith, 2000), and this must engender transactional trust.

This trust is always engineered by the safety and less security vulnerabilities of the technology involved (Barcena, & Wueest, 2015; Lee, 1998). The experience of monetary loss, distorted transaction information, breach of privacy and confidentiality, among others, are instances of security issues confronting e-commerce platforms (Culnan & Armstrong, 1999; Federal Trade Commission, 1998), especially in the cloud computing environment.

Cloud computing, defined as a model for ubiquitous, convenient and on-demand network access to shared computing environment (Gamaleldin, 2013; NIST, 2011), is a supporting infrastructure for e-commerce platforms. Though cloud computing's deployment models can be private, community, public or hybrid, its service models are essentially Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (NIST, 2011). IaaS is the most prominent service rendered by the cloud computing architecture to e-commerce platforms. In this regard, the technology-backed commercial transaction platforms are deployed on an infrastructure given by a service company and expected to be paid for –as similar to utility companies. A close example of this is the Amazon EC2 IaaS technology (Gamaleldin, 2013).

In e-commerce platforms, where wide range of business activities that accommodate online products and services available for customers and business owners (Aulkemeier et al., 2015; Meziane & Kasiran, 2008; Ranganathan & Ganapathy, 2002) can be executed, deployment on cloud-based environment is economical and technologically reliable, but highly prone to security issues, especially the Business to Consumer (B2C) e-commerce model (Thaw, Mahmood, & Dominic, 2009; Pavlou, 2003). The B2C characterises e-commerce activities like purchasing, selling and exchange of goods and services via a computer network in an electronic form (Digitsmith, 2011; Markley, Barkley, & Lamie, 2007), and thus involve vast amount of confidential customers' information (Nyshadham & Ugbaja, 2006). The need for improved security mechanism for e-commerce platforms in a cloud-based environment had attracted significant researches (Nafi, Kar, Hossain, & Hashem, 2013; Rosado, Gomez, Mellado, & Fernandez-Medina, 2012; Juniper, 2012; Juncai & Shao, 2011; Zhu, 2010), and this is the core motivation of this study.

Authenticating the true identities of the receivers of associated transaction documents in a B2C e-commerce platforms, in a cloud-based environment, is still experiencing unresolved issues, owing to the deficiencies of the prominently-used XML signatures (Ramgovind et al., 2010; Siani & Charlesworth, 2009). Therefore, this study proposes an improved XML signature authentication mechanism based on RSA algorithm and elliptic curve. This proposed algorithm framework is billed to offer an improved authentication mechanism in terms of (a) smaller key size

and (b) faster response time, in the transfer and receipt of key between the sender and the receiver.

The next section, section II, presents the review of past related studies on securing e-commerce platforms in a cloud-based environment. Section III highlights the proposed algorithm framework for the authentication in a cloud-based e-commerce platform. Section IV presents the proof of concept and the preliminary findings. The future works and conclusion are presented in section V.

A Review of Past Studies on Securing E-Commerce Platforms in a Cloud-Based Environment

The security of e-commerce platforms in a cloud-based environment have attracted different researches (Wang, 2013; Nafi, Kar, Hossain, & Hashem, 2013; Rosado, Gomez, Mellado, & Fernandez-Medina, 2012; Juniper, 2012), and different techniques, especially for its authentication mechanism, have been proposed. Hyper Text Transfer Protocol Secure (HTTPS), XML digital signature, TCP/IP and End-to-End Web Security's Point to Point Tunneling Protocol (PPTP) are examples of these authentication mechanisms (Microsoft, 2016; Zhang et al., 2012; Al-Hamdani, 2010; Yue-sheng et al., 2010; Yue-sheng et al., 2009; Junxuan & Zhong, 2009; Jensen et al., 2009). In these, XML digital signature, defined as a security service with a set of W3C related designs for signing, key management and encryption (Coulouris et al., 2012) is remarked to be the most reliable in terms of confidentiality, integrity and availability (Federal Office for Information Security, 2017). XML digital signature is used for documents that require authentication or encryption so as to be prevented from manipulation or access by unauthorised persons. It helps in cooperative work transported over the internet (Homeland Security, 2016; Coulouris et al., 2012). The viability and reliability of XML digital signature as a security framework for B2C e-commerce can be best understood through a comparative analysis between XML signature-based authentication mechanism and other online transaction authentication mechanism as presented in the following sub-sections.

XML Digital Signature and Comparison with other Online Authentication methods

This comparative review is in view of highlighting the strength of XML digital signature in respect of its confidentiality, integrity and availability, over HTTPS, TCP/IP, and PPTP. This is presented as follows:

XML Signature vs. HTTPS

Hypertext Transfer Protocol (HTTP), or with a transport mechanism using TLS tunnelling (HTTPS), can only provide partial achievement in terms of data confidentiality, integrity and availability (NIST, 2008; Quasthoff et al., 2007). This is one of the reasons why XML becomes important to bridge the security gap inherent in HTML, as utilized in HTTP and HTTPs (Alkiviadis et al., 2016; Khaled et al., 2013). However, XML digital signature can be collectively utilized with XML management, XML encryption, Authentication and Authorization assertions (SAML), XML public key management and Security Assertion Markup Language (SAML) (Saravanaguru et al., 2013). Al-Hamdani (2010) utilised XML based on PHP and Oracle application with SOA for a combined functionality of the interoperable services and database, and affirmed that openness and ability to work with other security standard is unique to XML signature.

XML Signature vs. TCP/IP

TCP/IP, unlike XML Signature, could cover provision for integrity, authentication, availability and confidentiality for other web services based on the layer of implementation, but does not give the needed security for e-commerce (Niemi, 2009). The incompatibility of TCP/IP with e-commerce is a major drawback and a major reason why XML signature is preferred when securing e-commerce. XML digital signature, on the other hand, can be used to secure e-commerce webs, in fact it serves as basis for web services security technology in web-based transaction portals. It also possesses a high level of web server security administration, level of access control, web server backup, restrict remote authoring, Secure Socket Layer/ Transport Layer Security (SSL/TLS), symbolic links, CGI programs, mobile code, java servlet engines, SMTP, XML data encryption, collaboration servers, LDAP server security and classified web servers, which can all be further included as researches demand (Yue-sheng et al., 2009).

XML Signature vs. End-to-End Web Security (Point to Point Tunneling Protocol (PPTP))

End-to-End Web Security using Point to Point Tunneling Protocol (PPTP) is a leading technique used in place of TCP/IP (Niemi, 2009). PPTP uses a point to point protocol being tunnelled via IP network with the data payload encrypted for confidentiality and authentication purposes. However, one major limitation of PPTP also is that it does not make a specific cryptographic algorithm used, it only provides the framework, and the negotiation for its workability depends on the PPP compression negotiation. This has made PPTP vulnerable to attack that compromises its authentication and confidentiality ability (Farooqi & North, 2011). In its stead, digital

signature technology in e-commerce systems, with preference to XML signature, is recommended because it allows being used with other standard security mechanism like public key cryptosystem. The functional mechanism of XML digital signature allows cryptographic algorithm (Junxuan & Zhong, 2009).

Comparative Advantage of Using XML Digital Signature as Authentication Mechanism in a Cloud-Based E-Commerce Platform

In sum, XML digital signature has been posited as a better alternative to other authentication mechanisms that are usable and implementable in a cloud-based e-commerce platforms. HTTPs has once been reported to be easily outsmarted by hackers' brute force (Murphey, 2004), TCP/IP is incompatible with e-commerce security (Niemi, 2009), and PPTP is vulnerable to attack that undermines authentication and confidentiality ability (Farooqi & North, 2011).

Comparatively, XML digital signature is preferred to others because, among others, it prevents authentication threat by defining XML syntax and processing rules for signing and verifying digital signatures over one or more data objects in an online business transaction (Zhang et al., 2012; Jensen et al., 2009). As explained by Coulouris et al. (2012), XML digital signature is a reliable web security services for e-commerce platforms due to its inclusion in the XML schema of web services and this makes it threat-resistant than others. XML signature and XML encryption can be integrated to achieve secure browser-based authentication, with a combination of Transport Layer Security (TLS) and Standard Operating Procedure (SOP), to enhance the security of Federated Identity Management (FIM) protocols (Jensen et al., 2009a; Jensen et al., 2009b).

Though XML cryptographic keys and algorithm achieve higher protection, and it is preferred over other authentication mechanisms (Jensen et al., 2009a; Yue-sheng, et al., 2009), there are still limitations in its working framework that need attention. For instance, Jensen et al. (2009b) used a naming scheme and an agreed API with its signature structure *<ds:Signature>*, but did not consider possible countermeasures against XML wrapping attacks despite XML wrapping attacks being caused by XML namespaces. In the example of XML signature wrapping attack given below (Fig. 1), the attacker leaks the message access by moving the original SOAP body to the SOAP header, and creates a SOAP body with a new *Id* as *"attack"* with an arbitrary function. The business logic is thus enforced to execute a function, giving the admin right to another person *"John Doe"*, then the newly defined SOAP body is taken as the input. Figure 1 shows the example of XML Signature Wrapping attack.

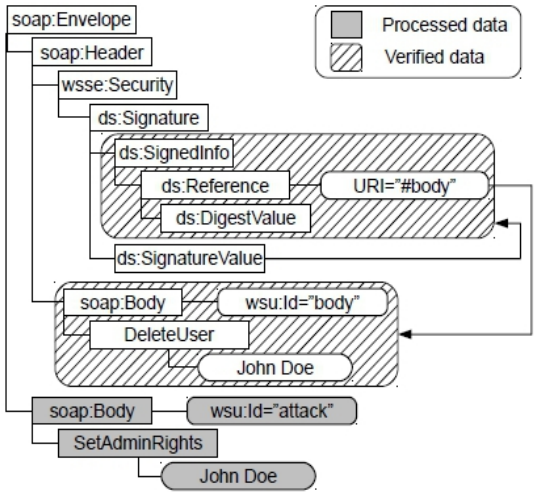

Fig. 1: XML Signature Wrapping Attack (Jensen et al., 2011).

Each of the signed data objects is given *ds:Reference* element that point to the URL containing a digest value calculated over the object. The referenced set is now grouped under the *ds:SignedInfo* element, and computed over the *ds:SignedInfo* element. This mechanism gives the data object protection against unauthorised persons, but can be improved by XPath extension with XML schema validation against wrap attack (Jensen et al., 2009a; Jensen et al., 2011).

In another study, Yue-sheng et al. (2010) formulated a XML signature and proposed its production and verification methods toward the improvement of XML digital signature, as an authentication mechanism. The encryption makes the data <*EncryptedData*> with <*EncryptedKey*> as the encryption key, with RSA as the most widespread application asymmetrical key algorithm at present. Al-Hamdani (2010) suggested a RSA-based elliptic curve in view of a lower key size and faster speed in achieving a more secured transaction.

From the review of past previous studies, as shown above, this study will employ XML digital signature, being a better authentication mechanism compared to the traditional digital signature. The XML encryption and decryption processes and XML schema validation included in the XML schema management will be used to counter possible XML wrapping attack that compromises the authentication integrity. However, even though XML digital signature is preferably better amongst its peers, there are certain limitations which can also be further improved. The next section describes the limitations of XML digital signature as an authentication mechanism in a

cloud-based e-commerce platform.

The Limitation of Using XML Digital Signature as Authentication Mechanism in a Cloud-Based E-Commerce Platform

Existing works have shown that XML signature provides authentication for the flow of information between the company and customers via the B2C e-commerce platform, but with bigger key size that delays decryption process (Ramgovind et al., 2010; Jensen et al., 2009). The improved works on XML digital signatures are with public key infrastructure (PKI), hence make the E-Commerce vulnerable to multiple PKI certifications and reduction of credibility (Medani et al., 2011; Wasef et al., 2010; Lee et al., 2007). It is against this background that this study, based on the presented review and meta-analysis of previous works, proposes an improved XML digital signature with RSA standard, using elliptic curve as a novel algorithmic framework that improves the authentication strength of XML digital signature in the B2C e-commerce in a cloud-based environment. The next section describes the proposed improved XML digital signature with RSA-based elliptic curve.

Proposed Improved XML Digital Signature

Proposed RSA-Based XML Digital Signature Algorithm

We proposed a RSA-based XML Digital signature algorithm, with the following key components:

a. Signature Assignment and Transport process,
b. Encryption and Decryption, and
c. XML Signature Schema Management.

At the signature assignment and transport process, the sender's identity is assigned and the document transported from its end. This is encrypted through the transport layer for confidentiality and identity integrity, and then decrypted accordingly when the receiver's identity is validated, and access granted. This proposed algorithm, with RSA elliptic curve, would be used as an alternative to the ordinary Public key cryptosystem of XML digital signature. Figure 2 presents the proposed algorithm framework. Notably, the implication of sender and receiver in a B2C e-commerce is as the Consumer and the Business owner, respectively, as the situation demands.

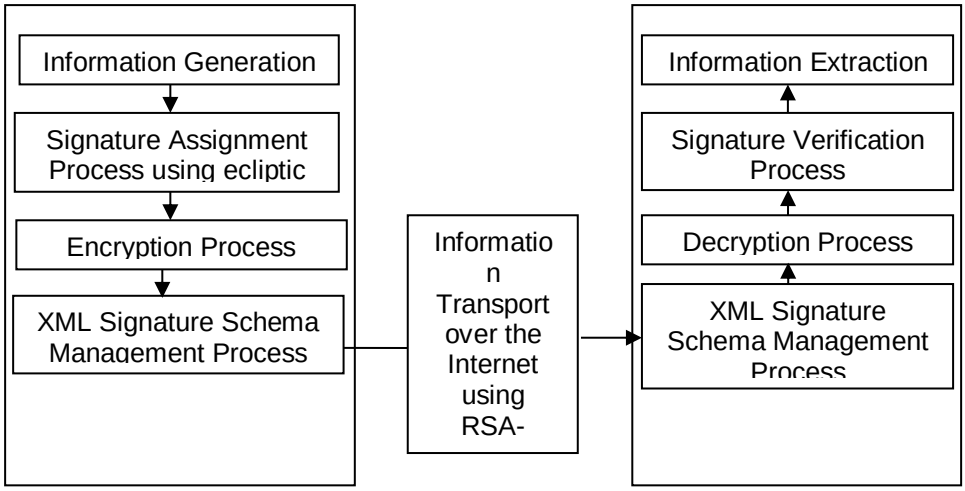

Fig. 2: Proposed Algorithm Framework

Proof of Concept and Preliminary Findings

First, an in-depth study of the attacks to the B2C online transaction in a cloud-based environment were studied, and this gives the theoretical background to the construction of new parameters. The proof of concept demonstrating how the XML wrapping attack work is then presented. It is on this basis that an improved XML signature with the RSA-based elliptic curve overcoming the XML wrapping attack is demonstrated. Secondly, a reverse engineering activities are carried out to prove the viability of XML digital signature, as a start, and finally, the code snippet for the improved XML digital signature is presented. The following sub-sections describe the reverse engineering an improved digital signature respectively.

Reverse Engineering Process

To prove the viability of XML Digital signature as a reliable authentication mechanism and threat resistant algorithm, reverse engineering activities are carried out on a document using XML digital signature as its security mechanism. The proof of concept demonstrated here is only on the threat-resistant quality of XML digital signature from the existing work of Jensen et al. (2012). XML Schema Validation is used to counter XML Signature wrapping attack. A controlled laboratory experiment is set up virtually; an attack was carried out on the XML digital signature with XML wrapping attack to perform this testing, with both the static and dynamic analysis tools as given in table 1 below:

Table 1: Tools used In the Testing

Tool	Function
NSS	To support a cross platform development of secured client and server application

XML Digital signature tool	To process digital signature in XML documents
Notepad ++	To conduct the static analysis
CISCO Simulation Environment	To implement the XML code structure, and analyze the XML wrapping attack in the code.

Fig. 4: Demonstrating the XML Schema Validation

<soap:Envelope xmlns :soap=" . . . ">
<soap:Header>
<! Timestamp used by Signature Verification Logic >
<wsu:Timestamp xmlns:wsu=" . . . ">
<wsu:Created>2011□11□28T21:01:12.100Z</wsu:Created>
<wsu:Expires>2011□11□28T21:06:12.100Z</wsu:Expires>
</wsu:Timestamp>
<wsse : S e c u r i t y xmlns:wsse=" . . . ">
<!Attackers Payload for Timestamp Element: It is just updated>
<wsu:Timestamp>
<wsu:Created>2012□04□30T13:29:42.826Z</wsu:Created>
<wsu:Expires>2012□04□30T13:34:42.826Z</wsu:Expires>
</wsu:Timestamp>
<ds: S i g n a t u r e xmlns:ds=" . . . ">
<ds: S i g n e d I n f o>. . .</ds: S i g n e d I n f o>
<ds:SignatueValue>. . .</ds:SignatureValue>
<ds:KeyInfo>. . .
</ ds:KeyInfo>

Fig. 5: Code Snippet fending XML wrapping attack

```
<!The Object Element is created by analyzing the XML Schema >
<:wsatk=" . . . ">
<ds:Object>
<!Signed Body Element Wrapper >
<wsatk:wrapper xmlns
<ns1:payloadBody xmlns:ns1=" . . . ">
<ns1:signedElement>Original Content</ y
<ns1:signedElement>
</ns1:payloadBody>
</wsatk:wrapper>
</ds:Object>
</ ds: S i g n a t u r e>
</ wsse : S e c u r i t y>
</ soap:Header>
</:signedElement>
</ ns1:payloadBody>
</ soap:Body>

<soap:Body>
<ns1:payloadBody xmlns :ns1=" . . . ">
<! Attackers Payload i s placed here>
</ soap:Enve lope>

<ns1:signedElement>ATTACKERCONTENT</ns1
```

Schema validation as described is used to protect against nested <soap:Body> tags. It restricts valid elements at this position.

Figure 6: Output of XML wrapping attack

```
01 <xs:complexType name="Envelope">

02 <xs:sequence>

03 <xs:element ref="tns:Header" minOccurs="0"/>

04 <xs:element ref="tns:Body" minOccurs="1"/>

05 </xs:sequence>

06 <xs:anyAttribute namespace="##other"

processContents="lax"/>

07 </xs:complexType
```

The proof of concept is to practically demonstrate the authentication limitation in XML digital signature, and its vulnerability to XML wrapping attack. <! Timestamp used by Signature Verification Logic > gave the verification syntax used for authentication purpose, and <!The Object Element is created by analyzing the XML Schema > in the XML schema used as a counter attack measure. It is important to note that figure 3 gives the flow and show the stage when the attacker's message body is introduced. From figure 5, </processContents="lax"/> shows that XML Schema is too flexible to completely safeguard crafted attacks in XML Digital signature.

The Improved XML Digital Signature with RSA Cryptographic Key

Introducing a better authentication mechanism in XML digital signature is therefore necessary. A XML signature structure with asymmetric cryptographic key using RSA is therefore introduced. This code snippet given below is an example of the XML digital signature structure for authentication.

```
<Signature>
  <SignedInfo>
       <SignatureMethod />
       <RSA-ECC 'Algorithm……'/>
    <Reference 'URI'>
      <Transforms>
      <DigestMethod>
      <DigestValue>
    </Reference>
    <Reference /> etc.
  </SignedInfo>
  <SignatureValue />
  <KeyInfo />
  <Object />
</Signature>
```

An excerpt of code snippet using RSA key is given below. Computational geometry using the elliptic curve is expected to be used in achieving a smaller key size.

```
KeyInfo>
<KeyValue>
<RSAKeyValue>
<Modulus>
      ---------
</Modulus>
<Exponent>AQAB</Exponent>
```

</RSAKeyValue>

Future Works and Conclusion

Our future work, beyond the reverse engineering of the XML wrapping attack demonstrated in this study, is to implement and evaluate an algorithmic framework of XML digital signature based on the improved RSA cryptosystem. This, as proposed, would improve the authentication mechanism in the B2C e-commerce platform using elliptic curve. Cisco's XML Management Interface with inbuilt feature of NETCONF will be the simulation environment for the experimentation, and its cryptanalysis. The evaluation is to be done using the W3C[3] and NIST Guidelines[4] on Cryptography and Web services security.

This paper focusses on the authentication problem affecting cloud-based Business to Consumer (B2C) e-commerce platforms. A XML digital signature, among HTTPS, TCP/IP, PPTP, is the preferred authentications mechanism because it provides full achievement in data confidentiality, integrity and availability; suitable for e-commerce security; and compatible with universal cryptographic algorithm. The authentication algorithmic framework proposed by this study is XML digital signature-based, improved by RSA algorithm, to protect the cloud-based B2C e-commerce against authentication threats caused by XML wrapping attack.

The improvement entails provision of secured senders' and receivers' keys identification and subsequent transmission over the internet. This study delivers the improved algorithm of XML digital signature through an extension of similar previous study. It is thus expected that the authentication problem associated with receivers' identities in a B2C e-commerce platform, while sending information from consumers to business owners, is better improved.

References:

1. Al-Hamdani, W. A. (2010). XML security in healthcare web systems, *2010 Information Security Curriculum Development Conference*, Kennesaw, Georgia.
2. Alkiviadis, G. (2016). Cloud computing security: protecting cloud-based smart city applications Cloud computing security: protecting cloud-based smart city applications. *Journal of Smart Cities*, 2 (1), 66–77. http://dx.doi.org/10.18063/JSC.2016.01.007.

[3] http://www.w3.org/standards/xml/
[4] Cisco NX-OS XML Interface User Guide, 2013.

3. Aulkemeier, F., Paramartha, M. A., Iacob, M-E., van Hillergersberg, J. (2015). A pluggable service platform architecture for e-commerce. *Inf Syste E-Bus Management*. DOI 10.1007/s10257-015-0291-6
4. Ayo, C. K., Adewoye, J. O., & Oni, A. A. (2011). Business-to-consumer e-commerce in Nigeria: Prospects and Challenges, *African Journal of Business Management*, 5 (13), 5109-5117.
5. Barcenna, M. B., & Wueest, C. (2015). *Insecurity in the Internet of Things*. A White paper publication of Symantec, Inc. Retrieved from https://www.symantec.com/content/en/us/enterprise/fact_sheets/b-insecurity-in-the-internet-of-things-ds.pdf at 25th May, 2015.
6. Brynjolfsson, E., & Smith, M. (2000). Frictionless commerce? A comparison of Internet and conventional retailers. *Management Science, 46* (4), 563 –585.
7. Coulouris, G., Dollimore, J., Kindberg, T., & Blair, G. (2012). *Distributed Systems: Concepts and Design*, 5th ed. UK: Pearson Education, Inc.
8. Cudjoe, D. (2014). Consumer-To-Consumer (C2C) Electronic Commerce: The Recent Picture, *International Journal of Networks and Communications*, 4 (2), 29-32. doi: 10.5923/j.ijnc.20140402.01.
9. Culnan, M.J., & Armstrong, P.K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10* (1), 104–115.
10. DigitSmith. (2011). *Ecommerce definition and types of ecommerce*. Available: http://www.digitsmith.com/ecommerce-definition.html
11. Farooqi, N., & North, S. (2011). Trust-based access control for XML databases, 2011 International Conference for Internet Technology and Secured Transactions (ICITST).
12. Federal Office for Information Security- Germany (2017). Cryptographic Mechanisms: Recommendations and Key Lengths – BSI Technical Guideline. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=6 on 27th May, 2017
13. Federal Trade Commission. Fraud Could Slow Growth of Electronic Commerce. June 25, 1998, FTC File No. P97–4406.
14. Gamaleldin, A. M. (2013). An Introduction to Cloud Computing Concepts: Practical Steps for Using Amazon EC2 IaaS Technology, Software Engineering Competence Centre Publication
15. Gaofeng, Z., Yun, Y., Xiao, L., & Jinjun, C. (2012). A Time-Series Pattern Based Noise Generation Strategy for Privacy Protection in Cloud Computing, *2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid)*, pp. 458-465

16. Homeland Security –United States of America (2016). DHS Sensitive Systems Policy Directive 4300A. Retrieved from https://www.dhs.gov/sites/default/files/publications/4300A%20Sensitive%20Systems%20Policy%20v12%2001.pdf on 27th May, 2017.
17. Jensen, M., Liao, L., & Schwenk, J. (2009). The curse of namespaces in the domain of XML signature, *Proceedings of the 2009 ACM workshop on Secure web services*, Chicago, Illinois, USA, 2009.
18. Jensen, M., Meyer, C., Somorovsky, J., & Schwenk, J. (2011). On the effectiveness of XML Schema validation for countering XML Signature Wrapping attacks, *2011 1st International Workshop on Securing Services on the Cloud (IWSSC)*, pp. 7-13.
19. Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009). On Technical Security Issues in Cloud Computing, in, *2009. CLOUD '09. IEEE International Conference Cloud Computing*, pp. 109-116.
20. Juncai, S., & Shao, Q. (2011). Based on Cloud Computing E-commerce Models and Its Security, *International Journal of e-Education, e-Business, e-Management and e-Learning*, 1 (2), 175 – 180
21. Juniper Networks, Inc. (2012). *Securing Multi-tenancy and Cloud Computing: Security That Ensures Tenants Do Not Pose a Risk to One Another In Terms of Data Loss, Misuse or Privacy Violation*, A White Paper Publication. Retrieved from https://www.juniper.net/us/en/local/pdf/whitepapers/2000381-en.pdf on 25th May, 2017.
22. Lee, H.G. (1998). Do electronic marketplaces lower the price of goods? *Communications of the ACM, 41* (1), 73–80.
23. Lee, Y, Lee, J, & Song, J. (2007). Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce, *Comput. Commun.*, 30, 893-903
24. Markley, D., Barkley, D. L. & Lamie, R. D. (2007). *Case Studies of E-Commerce Activity in Rural and Small Town Businesses*. Retrieved from http://ageconsearch.umn.edu/bitstream/112894/2/E-Commerce%20Project.pdf on 25th May, 2017.
25. McIntos, M., & Austel, P. (2005). XML signature element wrapping attacks and countermeasures, *Proceedings of the 2005 workshop on Secure web services*, Fairfax, VA, USA, 2005.
26. Medani, A., Gani, A., Zakaria, O., Zaidan, A. A., & Zaidan, B. B. (2011). Review of mobile short message service security issues and techniques towards the solution, *Scientific Research and Essays*, 6 (6), pp. 1147-1165

27. Meziane, F., & Kasiran, M.K. (2008). Evaluating Trust in electronic commerce: a study based on the information provided on merchants' website, *Journal of Operational Research Society*, 59, 464-472
28. Microsoft Corporation (2016). Hypertext Transfer Protocol Version 2 (HTTP/2) Extension, document *[MS-HTTP2E] - v20160714, pp. 1 – 18*
29. Murphey, L. (2004). Secure Web-Based Authentication: Secure Methods for Authenticating Users on Web Applications, Available at: http://lukemurphey.net/ on 24th May, 2017.
30. Nafi, K. W., Kar, S.T., Hossain, M. A., & Hashem, M. M. A. (2013). A New Trusted and Secured E-commerce Architecture for Cloud Computing
31. National Institute of Standards and Technology (NIST) (2011). The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standard and Technology, in Mell, P., & Grance, T. (eds). Computer Security Special Publication 800 – 145.
32. Niemi, A. (2007). *End-to-end web security — protocols overview.* Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.114.5988&rep=rep1&type=pdf
33. NIST (2008). Guide to SSL and VPNs. Frankel, S., Hoffman, P., Orebaugh, A., & Parl, R. (eds.) US Department of Commerce, Special Publication 800-113.
34. Nyshadha, E. A., & Ugbaja, M. (2006). A Study of Ecommerce Risk Perceptions among B2C Consumers: A Two Country Study, *19th Bled eConference eValues*, pp.1 – 18.
35. Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model, *International Journal of Electronic Commerce*, 7 (3), 69–103
36. Pearson, S., & Charlesworth, A. (2009). Accountability as a Way Forward for Privacy Protection in the Cloud, in *Cloud Computing*. vol. 5931, M. Jaatun, G. Zhao, and C. Rong, Eds., ed: Springer Berlin Heidelberg, pp. 131-144.
37. Quasthoff, M., Sack, H., & Meinel, C. (2007). Why HTTPS Is Not Enough -- A Signature-Based Architecture for Trusted Content on the Social Web, *Web Intelligence, IEEE/WIC/ACM International Conference on Web Intelligence*, pp. 820-824.
38. Ramgovind, S., Eloff, M., & Smith, E. (2010). The management of security in Cloud computing, *Information Security for South Africa (ISSA)*, pp. 1-7.

39. Ranganathan, C., & Ganapathy, S. (2002). Key Dimensions of business-to-consumer websites, *Information & Management*, 39, 457-461
40. Rosado, D. G., Gomez, R., Mellado, D., & Fernandez-Medina, E. (2012). Security Analysis in the Migration to Cloud Environments, *Future Internet*, *4*, 469-487; doi: 10.3390/fi4020469
41. Saravanaguru, R. A., Abraham, G., Ventakasubramanian, K., Borasia, K. (2013). Securing Web Services Using XML Signature and XML Encryption. arXiv preprint arXiv:1303.0910. 2013
42. Sawesi, K. G. A., Mohd Saudi, M., & Jali, M-Z. (2013). Designing a New E-Commerce Authentication Framework for a Cloud-Based Environment, *2013 IEEE 4th Control and System Graduate Research Colloquium*, 19 - 20 Aug. 2013, Shah Alam, Malaysia
43. Stone, B. (2007). Study Finds Web Antifraud Measure Ineffective, Retrieved from http://www.nytimes.com/2007/02/05/technology/05secure.html?_r=0 on 24th May, 2017
44. Thaw, Y. Y., Mahmood, A.K., & Dominic, P. D. D. (2009). A Study on the Factors That Influence the Consumers' Trust on E-commerce Adoption, *International Journal of Computer Science and Information Security*, 4, 1 & 2, 153 – 159
45. Wang, D. (2013). Influences of Cloud Computing on E-Commerce Businesses and Industry, *Journal of Software Engineering and Applications*, 6, 313-318, http://dx.doi.org/10.4236/jsea.2013.66039
46. Wasef, A., Rongxing, L., Xiaodong, L., & Xuemin, S. (2010). Complementing public key infrastructure to secure vehicular ad hoc networks [Security and Privacy in Emerging Wireless Networks], *IEEE Wireless Communications*, 17, 22-28. \
47. Yue-Sheng, G., Bao-Jian, Z., & Wu, X. (2009). Research and Realization of Web Services Security Based on XML Signature, *International Conference on Networking and Digital Society, ICNDS '09.*, pp. 116-118.
48. Yue-Sheng, G., Meng-Tao, Y., & Yong, G. (2010). Web Services Security Based on XML Signature and XML Encryption, *Journal of Networks*, 5 (9), 1092-1097
49. Zhu, J. (2010). Cloud Computing Technologies and Applications, Furht, B., & Escalante, A. (eds.), *Handbook of Cloud Computing*, pp. 21 – 45. DOI 10.1007/978-1-4419-6524-0_2