Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
ISSN NO. 2320-5407

Article DOI: 10.21474/IJAR01/2340
DOI URL: http://dx.doi.org/10.21474/IJAR01/2340

RESEARCH ARTICLE

COMPARATIVE STUDY OF TESTING METHOD AND TOOLS FOR WEB SITES.

***Ms. Ami Shaileshkumar Desai[1] and Dr. Sanjay Buch[2].**

1. Phd Scholar of R. K. University, Rajkot.
2. Assistant Vice President Of Reliance Industries Ltd., Naroda.

Manuscript Info

Manuscript History

Received: 30 September 2016
Final Accepted: 30 October 2016
Published: November 2016

Abstract

Nowadays social networking/service sites are our daily habits and necessity. About 80% of transaction done through online web services, but it is not safe or reliable. Because People may unaware have fraud and crime happened online or they have less command on English language. So, threats are increasing day by day. SOA (service oriented architecture) provides based to online servicing, social interactions and communications without human interaction, but it is raises privacy and security concerns in web services. Generally Web services managed by more than one stake holders. In this review we discuss the security testing methods as well as model issues of web services. Development based on SOA is still required for providing the unique security or proper testing.

Introduction:-

With today’s many people are attached with each other using web technology. Many service providers deliver facilities to exchange of ideas, information, videos, pictures, and graphics based on SOA. It also allows easy sharing and distribution of existing content to others so that professional work can be shared through networks.

Using Social networking web sites maximum people are share or transfer images, video clips, text and personal details without any precautions and bothered about fraud. People also doing on-line transaction without any security check because of many people do not have awareness about on-line fraud and cyber crime. Thus hackers can easily hack and misuse of their information. The issues include privacy issues, identity theft, social networks spam, social networks malware, and physical threats. There are certain issues regarding on-line fraud occurs with people are describe as below,

- Hacking
- Theft
- Cyber Stalking
- Identity Theft
- Malicious Software
- Child soliciting and Abuse

These frauds are occurs because of some lacking in software designing, software coding, hardware, software, security protocols, methodology, network, web standards, Architecture, tools and technology. As per study and review major problems occurs due to proper testing model for the web services.

Corresponding Author:- Ms. Ami Shaileshkumar Desai.
Address:- Phd Scholar of R. K. University, Rajkot.

Generally for protection, all web site developers are testing their web sites using white box testing, black box testing and gray box testing. After web hosting some web automated tools are provided in SOA for automation performance, load and security testing like Soap, Apache jmeter, Curl, Jconsole, Jprofiler, Jira, Bugzilla, Mantic, Redmine, SET, SSL etc.
According to R. S. Pressman, Testing have own pros and cons.

In white box testing:-
White Box testers have access to the source code and are aware of the system architecture. A White Box tester typically analyzes source code, derives test cases from knowledge about the source code, and finally targets specific code paths to achieve a certain level of code coverage.

Advantages

- Increased Effectiveness
- Full Code Pathway Capable
- Pre Defect Identification
- Expose Hidden Code mistake

Disadvantages

- Difficult To Scale
- Difficult to Maintain
- Cultural Stress
- Highly intrusive

In Black box testing:-
Black Box testers do not have access to the source code and are oblivious of the system architecture. A Black Box tester typically interacts with a system through a user interface by providing inputs and examining outputs without knowing where and how the inputs were operated upon.
In traditional system input and output is check by in known and fixed interface so it is easy task. But in web services entire system work throw different interfaces, operating system, programming language and also dependent on 3rd party for on library (API), online payment(bank), shipping (currier services) etc so it is difficult to testing.

Advantages

- Efficient Testing
- Unbiased Testing
- Non intrusive
- Easy to execute

Disadvantages

- Localized Testing
- Inefficient Test Authoring
- Blind Coverage

In Gray box testing
Gray Box testing refers to the technique of testing a system with limited knowledge of the internals of the system. Gray Box testers have access to detailed design documents with information beyond requirement documents. Gray Box tests are generated based on information such as state-based models or architecture diagrams of the target system.

Advantages

- Offers Combined Benefits
- Non Intrusive
- Intelligent Test Authoring
- Unbiased **Testing**

Disadvantages

- Partial Code Coverage
- Defect Identification

According to Naik & Shivalingaiah (2008), Nowadays All service oriented web services based on web 2.0 standards and SOA. SOA is the architectural style that supports loosely coupled services to enable business flexibility in an interoperable, technology-agnostic manner. SOA consists of a composite set of business-aligned services that support a flexible and dynamically re-configurable end-to-end business processes realization using interface-based service descriptions.

According to Torry Harris, SOA divide into layers and all types of testing are done in these layers (which testing through customer, developer and provide view). Here testing is done on all layers but fraud occurs when multi stake holders web services, distributed data, different languages, multi ownership or anything else but still it is difficult to identify so below challenges are remain.

Challenges of web services:-

Functionality

- According to Asankav (2014), it is different from traditional software testing because in traditional testing GUIs, number of user, types of requirements and inputs are fixed. Mainly problem occurs for multiple types of GUIs and huge amount of various types of data.
- This multi functions are also managed by different service providers e.g. In Nokia token machine website some web pages or facilities are managed by other services providers/developers. So it is difficult for testing without testing rights and source code.

Publish, Find, and Bind

- According to Asankav (2014), before publishing and developing of web sites they needs to think as customer, developer, service provider and stakeholder point of view.
- It is also a major and important problem for binding and transportation because web services are manage by multi or distributed server and some time services are provides by third party like online payment services done by third party bank or PayPal.

Security

- Dolvara Gunatilaka mention that there are many types of SOA related issues from customer side like Privacy issues, Identity theft issues, Span issues, Malware issues, Physical issues, etc. because of improper architecture, technology or security method of SOA.
- As per report by US government (2013), online services provider collects many personal and bank information of customers. But it may be not secure because provider sells our private data to other provider for marketing without any intimation of customer which increased spamming, phishing, etc.
- Fake and same domain name (with minor change in domain name) also misguide the victim. Many web sites developed for collecting victim's personal information. These information will further use for fraud like spamming, spoofing, phishing etc by culprit.

Performance

- Asankav (2014) pointed that It is also a big challenge or nearly impossible to develop user friendly and error or bugs free system because after implementation it is difficult to do testing. Recently web sites data are managed in distributed server or third party server. These stored data also access by multi languages from multi platform. So, Huge and variety of data is difficult to manage load and performance testing. It needs automation needs to be done through programmatic interfaces.

Literature Review:-

(Hattangadi 2011) Author discussed phases of SOA life cycle. SOA challenges of implementation and solution. SOA testing model is divide in four steps: service level testing, Process testing, End-to–end testing, regression testing. Through generate automation testing tool. A modern SOA testing model is developed but it is difficult to implement in inaccessible system or per-user costs and repetitive steps for login and logout. SOA testing need development verification tool or testing methodology

(Asankav.wso2.com 2014) In this article they pointed what is SOA & SOA testing, Importance of SOA testing, Challenges of SOA testing, SOA testing lifecycle, SOA testing tools. Automation of SOA The ability to generate request messages automatically. The ability to validate responses using assertions .QoS-enabled service invocation, Service simulation, Support for multiple transport protocols, Multiple message support. In Future requirements are consideration for automation. Test environment setup/clustering, Unit/module testing, Product level feature automation and Integration scenario automation.

(Danchev 2013) Competition between internet browser on security protection. Especially author discussed anti-phishing facilities provided by internet browser. Through phishing sensitive information like username, password, and credit card detail will be misuse by culprit. In case of phishing comparative review of internet browser are: Opera internet 94.2%, Internet explorer: 82%,Google chrome: 72.4%,Apple safari: 65.6%, Mozilla Firefox: 54.8%.

(Ajeet, Singh and Shahazad 2012) Author specify which necessary and important security are require for online payment system like authentication, access control, data confidentiality (security), data integrity, non reputation. Attack on online payment system is basically done through network attack or cryptographic. So author prepare secure communication tunnel for protection. It provides secure transaction between customer, merchant and bank through cryptography and authentication check without install additional software.

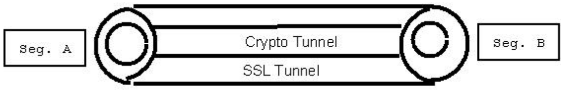

Fig 1

(Acharya and Pandya n.d.) Author pointed testing methods and their techniques. Also specify advantages and disadvantages of white box, black box and gray box testing.   Testing of web applications, web services, functional or business domain testing, security assessment, GUI, distributed, environments, etc. is done by gray-box testing.Without source code gray box testing will not work.

(Fire, Goldschmidt and Elovici FOURTH QUARTER 2014) OSN users readily Expose personal and private details about themselves, such as Relationship status, Date of birth, School name, email address, Phone number, and even Home address. This information, if put into the wrong hands, can be used to harm users. So, author prepared review of the different security threats and privacy risks.   Author provide awareness of detection and prevention of online social network threats.

(gunatilaka n.d.) According to Authods a survey on different privacy and security issues include privacy issues, identity theft, social networks spam, social networks,malware, and physical threats. A Survey paper addressed different privacy and security issues, as well as the techniques that attackers use to overcome social network security mechanisms or to take advantage of some errors in social Networking site

(Naik and Shivalingaiah 2008) Author justified compare between web standards. All service oriented web sites based on web 2.0 standards and SOA. SOA is the architectural style that supports loosely coupled services to enable business flexibility in an interoperable, technology non supportive manner. Web 1.0 - read-only web. Web 2.0 - read-write. Web 3.0 - read-write-execute.

(Netmarcom 2009) As per author pointed working of online bank system protect from Trojan affected PC fraud. In this, during the fraud transaction detection system verify users authentication through 2FA(two factor authentication) means first verify by username & password and then check by automatic SMS (one time password) / voice call before transaction. Author protect transaction by unauthorized user and monitoring solution to block criminal acts attempted with stolen identities. Author provide 2FA protection to bank transaction. Hackers can hack our mobile accessibilities also at that time some protection mechanism/model is needed.

(Sultana, Sadiq and Ahmad 2014) Author discussed Need of testing.Types of testing and compare of testing techniques. Advantages and disadvantages of testing techniques.Author developed method for selection of testing techniques using AHP(ANALYTIC HIERARCHY PROCESS) Proposed method is a four step process, namely, (i) identify the criteria (ii) construct the hierarchical structure of Software Testing Techniques (iii) construct the decision matrix (iv) the selection of a technique. Proposed method selects the responsive methods for the testing of the project. A need to improve the agile methods by interlink of decision making approaches for the selection and prioritization of requirements.

(Torry 2007) Author explained What is SOA. Explain level of SOA. Which types of testing check in SOA of every level like component testing, services testing, workflow testing, system testing, integrated testing, link testing etc. but SOA is loosely coupled with complex independences of every level of SOA More testing effort will be required at the service level, security testing need to check every end to end module throughout life cycle of project. SOA need experts of domains within business. So, SOA test approach demands an appropriate tool strategy   SOA demands strong governance, well-defined standards, processes and disciplines for protection.

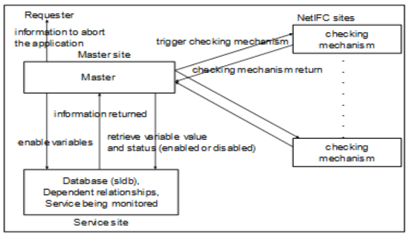
Requester
information to abort the application
Master site
Master
trigger checking mechanism
checking mechanism return
NetIFC sites
checking mechanism
checking mechanism
information returned
enable variables
retrieve variable value and status (enabled or disabled)
Database (sldb), Dependent relationships, Service being monitored
Service site

Fig 2

(Chou 2015) To specifies maximum data was leaked during the execution of net services. Author has developed NetIFC (net information control flow) for controlling leakage of information. NetIFC is not embedded with net services it is execute parallel with different web sites. Author develop architecture of NetIfc with its functions. Network overhead time calculation using t2-t1-t3 Where t1 is time of site when sender send message to receiver. t2 is time of site when receiver send message to sender. t3 is time for process and execution time in the receiver site. For each checking operation, the execution time includes: (1) the master execution time, (2) the checking mechanism execution time, and (3) five network overheads. Fig. 5 shows that the network overheads include: (1) that for master to retrieve variable value and status, (2) that for master to receive variable value and status, (3) that for master to trigger checking mechanism, (4) that for master to receive checking mechanism return, and (5) that for master to enable variables. If program is longer than execution time t3 is larger so NetIFC runtime overhead time is increase so, message transaction time is increase do to NetIFC. NetIFC mechanisume not exicute autometicaly for security cheching . Need to develop a model which protect from worms, virus and stop leaking information.

(Tan Phan 2010)Author provide end to end collaborative partner services in properly protecting each other’s data. In message handling mechanisms of Web Service engines dynamically gather protection requirements for a given outgoing message by collecting requirements from original owners of message data. Author encrypt data using binding method, encrypted algorithm and length of the key. It broadcast input and output data flow of data with protection. Provide approach for collaborative service partners to protect data in transit according to the requirements of parties who created and processed that data.

(Karumanchi and Squicciarini 2015) A web services are classified the services into 6 types based on their provisioned service: Business (eg., quote retrieval), Location (eg., weather), Communication and Entertainment (eg., email, travel, holiday), Scientific/Security (eg., gene variations, encryption), Search (eg., search for university data), and Others. they discussed various vulnerabilities associated with Web Services. They provide comprehensive solution to prevent the exploitation of these vulnerabilities. We suggest the adoption of a proxy-based solution to counter these vulnerabilities. As part of the future work, they plan to complete the deployment and testing of the proposed proxy-based solution. It provide security between client and server system but it not workable in multi stake holder or multi environment system (Choudhary, Aaseri and Roberts 2013) as author per develop Web service security model based on HTTPI protocol over SOAP, with the security goal: client/server authentication and integrity on message, without confidentiality. They use Username/Password Tokens, Binary Authentication Tokens (X.509 certificates) for Authentication, XML Digital Signature for Message Integrity. To secure the communication between two web services. The secured web services based on HTTPI can be used in non-confidential open applications (like: Social Networking, Blogging and News sites) in future.

(Yunus 2012) Author discussed that SOA testing done by IT professional using automated tools for check. Functional testing, first transport protocol for transferring services or communication on internet by http/https protocol. Public key infrastructure is managed by SSL and HTTP for secure functional testing. Services require client authentication and authorization for before the request is accepted and a response is returned through identity token in encrypted form Performance testing is testing by SOA tool by calculating time stamps, latency time, and transaction per second. Security testing for data base security SQL injection, SOAP and XML protect database information. It also protected from virus and malware. SOA testing provide functional, transportation, message, security testing for simple web sites SOA testing requires demanding domain skill, tools and processes for simple web sites. SOA lifecycle testing framework is crucial for ensuring a successful SOA deployment.

(Casado, Tuyaa and Younasb 2012)Author pointed that three dimensions of testing WS transactions (level, feature, depth) according to some basic test concepts (test unit, test conditions, test coverage items) Its check Flow dependencies, data dependencies and control dependencies. Author said this model need to evaluate because it not work for security purpose it just control and testing transaction during the web services

(Sharma, Hellmann and Maure 2012) Authors are provided an overview of the current state of research into testing of web services. To understand this subject, conducted a systematic mapping. The results suggest that research into testing web services is still in its early stages. They provide recommendations about holes in existing research that need to be addressed and directions for future research that will have maximum novelty and potential for impact on the field. Work is done in systematic mappiing flowchart: 1) Check past and current status of “prepared reserch questions” 2) check reserch question in IEEE and ACM library. 3) check testing methods and web services keywords combinly provide overview of testing method use for testing of web services. Many methods of testing is same which differenceate by name only But we cannot identify because of proper terminology. So need to develop proper terminology for detection of testing techniques and which types of web services are testing by them.

(Nontarak and T 2012) To developing and evaluating securely web-based application for construction material testing using object-oriented technology and parameterized queries for SQL command queries. Several techniques attacking the web application; 1) cross-site scripting (XSS).2) SQL injection 3) parameter tampering 4) hidden manipulation 5) plain text attack 6) cookie poisoning were reported SQL injection break through 1) authorization bypass 2)execute commands of the web application being tested. It cover bellowed area 1) injection flaw 2) information leakage 3) improper error handing 4) insecure cryptographic storage 5)broken authentication 6) session management insecure communication. Whereas two web scanning tools detected that the SQL injection vulnerability was significantly reduced to 62 and 84%, compared to the web-based application using non-parameterized queries Protection from sql injection need to more proper tool

(Mohammada and Mcheickb 2011) several numbers of successful methods for automatic Cloud service composition, the main issue with that is the lack of test environment with some standards to compare and evaluate these methods. short survey to explore Cloud Services testing methods. compares several software testing researches and pose questions for further research work to find Cloud suited testing techniques for the software testers. The Cloud service design and development as well as testing of available services have shown considerable diversity from the traditional in-house system development for an internet enabled monotonous application. The list of questions given is not complete and extensive, exactly as the testing of a software can never go extensive, to save both time and cost to the end-user.

(Satoh and Tokuda 2011) Composite method supports two approaches for composite web services : topdown and bottom-up. Using A security policy for an atomic service is classified as a Message Protection Policy (MPP) of an Access Control Policy (ACP). In MPP message will pass through XML encryption and XML signature. ACP check authentication through (access ermission, rights) Composite process/policy use MPP and ACP further transform in logical representation. There are some possible options to extend our approach, such as 1) supporting a specific access control representation 2) implementation for generating the valid composite policies

(Mary-Luz Sánchez-Gordóna 2014) To accessibility and testing should be integrated from the beginning of the product development cycle, when the application or product is in the planning or design phase Combine model of testing and accessibility of web site will be develop by that person who has knowledge of Domain management. But it is still necessary that Researchers clearly and explicitly set the testing processes for better support practitioners because a well-defined test process is necessary to assure required quality and accessibility within any development lifecycle.

(Reisa, Gülseçenb and Bay 2011) Author discuss, Secure Internet Banking Education System (it is named as GIBES), which is designed for internet banking users and prepared as a module for Computer Supported Education (CSE). Author survey on threats done through ATM, Call center and Internet Banking. Prepare model using UML. Explain steps how to work with this model. Using GIBES model author identify the most common theft are as follows: □ Keylogger □ Screenlogger □ Phishing □ Spyware □ Social Engineering. Using GIBES model awareness possible to single user and multi user system. GIBES is still a study in Progress. Improvements on the product are planned in such like adding sign language and plug-in description for the deaf and adding subtitles under the videos for the blind are intended to be put in the system,

(Decker 2007) SNSs usually offer the same basic functionalities: network of friends listings, person surfing, private messaging, discussion forums or communities, events management, blogging, commenting, and media uploading. SNS connect people with different ways but.Yet, fundamental problems with today's SNSs block their possible to access the full range of content and networked people online. A possible solution is to build semantic social networking into the framework of the next-generation which, Internet itself interconnecting both content and people in meaningful ways. This social networking stack require transfer data with (1) personal authentication and authorization layer.(2) social network layer for centrally manage data.(3) The content object access layer for make data secure use, connect, access and reuse data with verification. To deployment will progress toward object centered networks and driven by the need to develop information assessment methods direct integration into the technology stack of clients (the desktop)
and the Internet itself.

(Mike Ter Louw 2009) Here authors found solution in browser's default configuration and settings, without modifying browser's base code or through plug-ins. This approach enforces browser to understand content of web. This approach is called Blueprint i.e. based on two main steps: application server-site parse tree of untrusted HTML is generated in form of DOM, without including script nodes in tree or plug-ins and is converted to encoded form called model. Model is embedded in HTML-in original location of untrusted HTML- by enclosing <code>….</code> and is never visible because its display property is set. Second step is using client-site. This parse tree directly transfers to browser's document generator. It needs script library that included in every web page output by linking to external JavaScript. But here if DOM API contains methods like document.write(), eval(), innerHTML property than it may recursively points to parsing path of HTML and JavaScript that gives unsafe behavior. To avoid this, authors encoded raw untrusted data that contains characters (a-z) only and are syntactically inactive. It bypasses JavaScript parser and decode to Java Runtime that regenerate parse tree and then to DOM API to document so that it will not result in unauthorized script. DOM API uses whitelist as argument for style object. CSS and URI parser is not required. However, this approach takes much time for standard arguments and need to perform changes in browser.

(E. Gal´an 2010) This proposed system scan web site automatically to detected stored XSS attack. In this system, web page parser agent finds input points of application that can be vulnerable. Script injector agent injects selected attack vectors at this point. Verificator agent inspects whole flow path of web application in order to identify success of attack. Report regarding scanning process is evaluated and stored. Here, proposed system only detects attacks using predefine attack vector. It does not provide any kind of prevention.

(Zulkernine 2011) In this paper, authors produced acceptable data set using mutation based testing technique to find out cross-site scripting vulnerabilities. This technique injected malicious script to create mutants. This contains 11 such mutant operators. If mutant creates different output than original output, then test module destroy this mutant based on two criteria. These two criteria are: 1. Number of HTML tags presented in DOM tree and 2. HTML contents of browser. This technique is time consuming i.e. for creation of mutants.

(Lars Hermerschmidt 2015) Here, authors stated various problems that occur with correct unparsing and encoding. Authors allow web developer to create and maintain encoding table which contains encoding tokens defined for grammar. This table also contains encoding rules which converts to escape sequence. They follows Monti Core framework which creates parsers, unparsers, encoder and decoder of context-free grammar. Here, encoded data tokens are verify by regular expression and encoding of input data is perform at time of document creation.

(Adam Kie˙zun 2009) Authors used PHP based tool namely ARDILLA that generates SQL injection and cross-site scripting attacks. This application tool recognized 68 unknown vulnerabilities from five different web applications. This tool follows dynamic taint analysis technique. It monitors path flow of malicious input and observes its runtime behavior. If injected code get succeed to reach inside any MySQL function or function which creates HTML output, it will results in SQL injection or XSS attack. To do so, authors also developed attack creation technique which helps to create vulnerable input and observes whole resulting procedure as describe before. This procedure can be followed by four components i.e. input generator, executor/taint propagator, attack generator/checker and concrete+ symbolic database. This model only works with web application which is developed using PHP language

Conclusion:-

Generally developer provides user-friendly and secure web services but due to lack of proper testing model some bugs are there. Web Services based on SOA plays an important role in facilitating the integration of different applications from various departments or trading partners and thus increasing business productivity. Multi stakeholder web service will further need to enhance for security testing/prevention from fraud at the time of online transactions without considering the rights of stakeholders.

References:-

1. Acharya, Shivani, and Vidhi Pandya. "Bridge between Black Box and White Box – Gray Box Testing Technique." *International Journal of Electronics and Computer Science Engineering* 2: 175-184.
2. Adam Kie˙zun, Philip J. Guo,Karthick Jayaraman,Michael D. Ernst. "Automatic Creation of SQL Injection and Cross-Site Scripting Attacks." *Software Engineering, 2009. ICSE 2009. IEEE 31st International Conference* (IEEE), May 2009: 199 - 209.

3. Ajeet, Singh, Karan Singh, and Shahazad. "A Review: Secure Payment System for Electonic Transaction." *IJARCSSE* 2, no. 3 (march 2012).
4. Asankav.wso2.com. "How to Efficiently Test Service Oriented Architecture." *WSO2.* 4 11, 2014.
5. Casado, Rubén, Javier Tuyaa, and Muhammad Younasb. "A Family of Test Criteria for Web Services Transactions." *The International Symposium on Advances in Transaction Processing* (Elsevier), 2012: 880-887.
6. Casadoa, Ruben; Tuya, Javier; Younas, Muhammad. "A Family of Test Criteria for Web Services Transactions." *The International Symposium on Advances in Transaction Processing.* ELSEVIER, 2012. 880 – 887.
7. Chou, Shih-Chien. "Controlling Information Flows in Net Services with Low Runtime Overhead." *I.J. Computer Network and Information Security* (http://www.mecs-press.org), Feb 2015: 1-9.
8. Choudhary, Pankaj, Rajendra Aaseri, and Nirmal Roberts. "HTTPI BASED WEB SERVICE SECURITY OVER SOAP." *IJNSA* 5, no. 3 (MAY 2013).
9. Danchev, Dancho. *Comparative review: Opera leads in browser anti-phishing protection.* 2013. http://www.zdnet.com/article/comparative-review-opera-leads-in-browser-anti-phishing-protection/.
10. Decker, John Breslin and Stefan. "The Future of Social netwroks on internet." (IEEE) 11, no. 7 (nov-dec 2007): 86-90.
11. E. Gal´an, A. Alcaide, A. Orfila, J. Blasco. "A Multi–agent Scanner to Detect Stored–XSS Vulnerabilities." *Internet Technology and Secured Transactions (ICITST), 2010 International Conference for* (IEEE), Nov 2010: 1-6.
12. Fire, Michael, Roy Goldschmidt, and Yuval Elovici. "Online Social Networks: Threats and Solutions." *IEEE COMMUNICATION SURVEYS & TUTORIALS,* 16, no. 4 (FOURTH QUARTER 2014): 2019-2036.
13. gunatilaka, Dolvara. *A survey of privacy and security issues in social networks.* http://www.cse.wustly.edu/~jain/cse571-11/ftp/social/index.html.
14. Hattangadi, Gaurish. "Modern SOA testing." july 2011.
15. *Information resellers.* the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate, United States: Government office, 2013.
16. Karumanchi, Sushama, and Anna Squicciarini. "A Large Scale Study of Web Service Vulnerabilities." *Internet Services and Information Security* 5, no. 1 (FEB 2015): 53-69.
17. Lars Hermerschmidt, Stephan Kugelmann, Bernhard Rumpe. "Towards More Security in Data Exchange:Defining Unparsers with Context-Sensitive Encoders for Context-Free Grammars." *IEEE CS Security and Privacy Workshops* (IEEE), 2015: 134-140.
18. Mary-Luz Sánchez-Gordóna, Lourdes Morenoa. "Toward an integration of Web accessibility into testing processes." Edited by Procedia Computer Science 27. *5th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-exclusion, DSAI 2013.* ELSESIVER, 2014. 281 – 291.
19. Mike Ter Louw, V.N. Venkatakrishnan. "BLUEPRINT: Robust Prevention of Cross-site Scripting Attacks for Existing Browsers." *Security and Privacy, 2009 30th IEEE Symposium on* (IEEE), may 2009: 331 - 346.
20. Mohammada, Atif Farid, and Hamid Mcheickb. "Cloud Services Testing: An Understanding." Edited by Procedia Computer Science. *The 2nd International Conference on Ambient Systems, Networks and Technologies(ANT).* ELSEVIER, 2011. 513–520.
21. Naik, Umesha, and D Shivalingaiah. "Comparative Study of web 1.0,web 2.0 and web 3.0." *International CALIBER.* March 2008. 499-502.
22. Netmarcom, Symantec. - *WHITE PAPER: DEFEND YOUR INSTITUTION AGAINST TROJAN-AIDED FRAUD .* SYMANTEC, 2009.
23. Nontarak, S., and Leelawat T. "Securely Web-Based Application for Construction Material Testing." *International Journal of Computer Applications* 42, no. 11 (March 2012): 44-48.
24. Pressman, Roger S. *Software Engineering.* Vol. 1. New york: McGraw-Hill, 2001.
25. Reisa, Zerrin Ayvaz, Sevinç Gülseçenb, and Betül Bay. "To Develop an Education System for Secure Internet Banking: GIBES." *Procedia Computer Science 3* (ELESIVER), 2011: 1333-1340.
26. Satoh, Fumiko, and Takehiro Tokuda. "Security Policy Composition." *IEEE TRANSACTIONS ON SERVICES COMPUTING,* (IEEE) 4 (OCT-DEC 2011): 314-327.
27. Sharma, Abhishek, Theodore D. Hellmann, and Frank Maure. "Testing of Web Services – A Systematic Mapping." *IEEE*, June 2012: 172 - 178.
28. Sultana, Sahida, Mohd Sadiq, and Waseem Ahmad. "A Tool To Automate The Test Cases Of Software Using Gray Box Testing Approach." *International Journal of Advanced Research in Computer and Communication Engineering* 3, no. 8 (August 2014): 7689-7695.

29. Tan Phan, Jun Han, Garth Heward,Steve Versteeg. "Protecting Data in Multi-Stakeholder Web Service." no. 978-1-60558-799. ACM, april 2010.
30. Torry, Harris. "SOA Test Methodology." (Torry Harris Business Solutions) 2007: 10.
31. Yunus, Mamoon. "Fundamentals of SOA Security Testing." *Service Technology Magazine*, Feb 2012: 1-6.
32. Zayaraz, G., and Poonkavithai Kalamegam. "A Test Framework based on CPN Model for Functional Testing of Web Service Composition." *International Journal of Advanced Science and Technology*, April 2013: 135-150.
33. Zulkernine, Hossain Shahriar and Mohammad. "Injecting Comments to Detect JavaScript Code Injection Attacks." *Computer Software and Applications Conference Workshops (COMPSACW), 2011 IEEE 35th Annual* (IEEE), july 2011: 104-109.
34. Zulkernine, Hossain Shahriar and Mohammad. "S2XS2: A Server Side Approach to Automatically Detect XSS Attacks." *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference* (IEEE), Dec 2011: 7-14.