V&V Analysis of Composite Web Service using WS Simulator for Trust Management in WS Lifespan

G. Raj[1], M. Mahajan[2], D. Singh[3]

[1]PhD. Scholar , Computer Science Department, IKG Punjab Technical University, kapurthala, India
[2]Computer Science Department, CGC College of Engineering, Landran, Mohali, India
[3]Computer Science Department, Chandigarh College of Engineering and Technology, Chandigarh, India

Corresponding Author: er.gaurav.raj@gmail.com, Tel.: +91-8587010020

Abstract— Validation and Verification in Composite web service development process is basic need to provide trust in between developers who are handling this development process using cloud service through different geographical locations. In this research work, V&V process simulated through Web Service Simulator using Asp. Net Web Services controlled by Web application. In continuity, complete demonstration of customers and web service interaction is simulated. This research work answers the questions as How data has been verified and validated so that it does not create any threats for the developers system, How intruder have not access to data without complete authentication. The research is also demonstrates the role based limitation in web service development. Web Services Simulator (WSS) used the concept of SOAP and it monitored and controlled security threats through a web application that are imposed via attackers at several points.

Keywords— Web Services, Composition of Web Services, SOAP , Validation and Verification, WSDL, UDDI, Web security Attacks, Threats Classification

I.   INTRODUCTION

The concept of interaction between two machines to share their data and resources iswell described in previous research works [1] [2]. Around the year 2000, the concept of WS came that helped the programmers sitting on different computers to share and use each other code to solve complex problems. Starting from that, much advancement have been made but with advancement there comes the risk of security issues and proper validation and verification of user and the WS is continuously increasing in demand to reduce the threats. A broad study about the threats has been done in this research which involved in both side i.e. from user side which asks for WS and from the server side as WS provider side.

Web Services used in this research is SOAP (Simple Object Access Protocol) based WS that is the first type of WS used to perform Complex tasks. WSDL file is required in XML format todescribe a set of endpoints nodes to operate on messages including document-oriented / procedure-oriented information. Paper will discuss several points regarding the development and monitoring of WS. The major issues discussedhereare, firstly, *the validation and* verification from WS developer side and user side and, secondly,the security threats involved during the interaction between WS and its users.

Nowadays we cannot rely on web services from any source and we have to take certain precautionary steps to reduce the chances of attack on our system. The simulator developed will help in giving information about the areas where the chances of threats are, what can be these threats and what steps we can take to remove these risk factors.

The WS provided through the unknown source cannot be relied on so there can be several steps with which web can check whether it is secure to use or not. They are:

i. WS can be checked based on its usage that is whatever the functions we are running on the system from the WS.WS can be checked separately and used in the system so that if there is any security threat, we can get information about it before it damages other applications.

ii. Multi-Layer checking of the Web Services can also be done such as by WS developer, Broker, regulators, Customer. These layers will reduce the chances of having any bug or harmful threat in WS that it may cause on our application.

iii. A set of test cases can be build and they can be used to Verify and Validate the WS. These test cases can be produced by the development group or any group associated directly or indirectly with the WS.

II. WS APPLICATION DEVELOPMENT

A Web Service is a small program that contains the functions that are needed in runtime for WEB 2.0 enabled browsing by the user. Composite web service is collection of these web services for solving complex functionalities in runtime browsing. For the user, there are several GUIs/APIs are available on the browser which have been used to solve the complex task. Server/browser calls the function required from the web services. WShas been used standardized XML messages to encode all communications to a web service.

The Designed simulator has different components that firstly, implementcomposite web service. Secondly,generate database and its connection and last but not the least, development of front-end to simulate verification and validationactivities.

There are three major components that are involved in WS working:

A). *Simple Object Access Protocol – SOAP* is lightweight protocol to exchange structured information in distributed environment.[15][16]

B). *Universal Description, Discovery and Integration – UDDI*offer a unified way to find service providers through a centralized registry. [15]

C). *Web Service Description Language– WSDL*detached the description of the abstract functionality from concrete details of WS description.[8][15]

During the design and making of the strategy of how to build WS application there can be several old methods to develop the application such as specification design, implementation and testing. The old and often used technologies are now not sufficient in current time. The new dynamic approaches has been studied or tried to build up in order to secure the web application.So in this sequence, steps used are asfinding, discovering, matching, run time composition and verification sequentially. More specifically, Create the Implementation of WS, Assemble the WS in Composite WS, Assemble the Client to access WS, Deploy and Configure the WS, Test for each deployed WS separately, Perform Post Deployment Tasks as changing security and logging policies[14]. This approach provides the user with ability to use the web application without any hesitation of having threat of user files and database security. This development process will build the base for trust in WS. Thus a new type of functionality can be created at run time with full, half or its partial usage.

There are several challenges that are faced in testing a WS as includes:

1). When the WS are used without knowledge of source code of it. (This condition arises from the situation when consumer uses the WS from an unknown developer.)
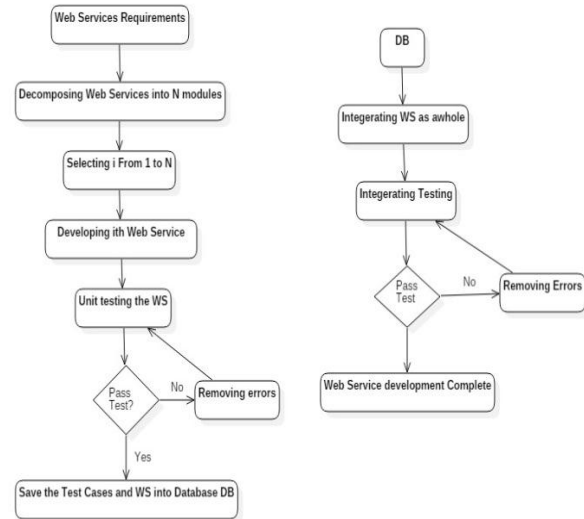

Fig. 1 Web Service Application Development
[i and ii]

2). While WShas been tested on several conditions on run time. (*This is common issue in WS orchestration, where many organizations are involved.*) It is very difficult to know how many users are accessing the WS, who are invoking them, at these points.It is attacks prone situation where system or testing process can easily be slowed down.

3). While WS has been used for single task. (The large number of WS available online for a single task, so testing all those Web Services is a tedious task.)

III. VERIFICATION & VALIDATION OF WS

Verification and Validation of the WS is the main part of this paper. Although the V&V part is been shown for both of the Customer and the WS but in this paper, V&V for WS has been shown in detail. Verification is intended to check that a product, service, or system (or portion thereof, or set thereof to meets a set of design specifications. Whereas Validation is there to ensure a product, service, or system results in a product, service, or system that meets the operational needs of the user. V&V of the product as well as for the customer both are the important thing as both are potentially dangerous for each other.

V&V for the user is been done on the authentication and authorization level. All the users are verified by giving each and every one of them using a specific ID and password. In the background, a database created to store all their file and

information that only an Administer can have the access to retrieve or delete or update the record.

Users of the WS or their developer are also been authorized to use only those parts of WS to which they are working with. They are not allowed to access the files or any documents related to other user or employee related to work different from his/her.

IV.   WEB SERVICES TESTING

Testing is an important aspect in any product development and its marketing. Each and every product that is in production, they all are tested with some test cases. WS composition generally requires Unit Testing as well Integration Testing. For the testing to work, test cases are required and for each and every type of testing a set of test cases is stored in the simulator. As already shown in Figure 1 that after generation of every module of WS, Unit testing is performed and so it will be explained in Figureure2 how it is done.

Testing can be done in many ways as it has been discussed in this paper earlier. They areas follows:

A.   Specification Based Testing
In this testing, WS developed can be tested only at certain points where the testing is needed and not on complete System. This helps in not only saving money and time but also makes the whole testing efficient. But this type of testing has a certain limitations such as it can be only applied to WS whose weak points are already known or it has been tested already. Weak points are nothing but the area where the chances of having an error is maximum. It can also be only applied to projects which are simpler and smaller and for large and complicated projects this testing cannot be done. Generation of test cases in this is also done only for points where we have the information about the weak points. These Test cases are furthermore can be analysed as well if we want to enhance the later stages of testing.
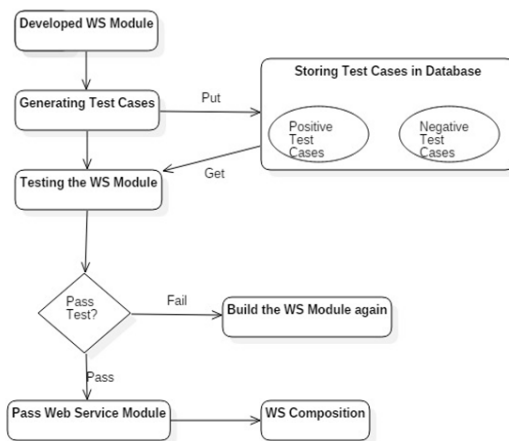

Fig. 2 WS Unit Testing

B.   Collaborative Testing
It involves the combined efforts of all the persons that are associated with the WS starting from developer, broker, consumer, regulator, etc. Earlier software is tested using testing techniques that have independent V&V property in them. In this testing is done by aseparate group different from the development group. This is considered to be the good practice as it removes the chances of any common errors and also helps in cross checking each other mistakes. However it is not enough for WS testing. A WS provider can build another WS from existing WS from different providers without having its detailed information. Therefore, a WS needs to be tested via group of users, brokers, providers, and other organizations such as research institutions, standard organizations, and regulators.

C.   Team Testing
This testing is done for the projects that are very complicated in nature and difficult to develop it. It is done by the combine efforts of large number of people involved in the development and testing process. As the projects are very complicated and composition of WS is not an easy task to do. During the composition of the web services, there are many other alternative WS from which the best suited one has to be chosen in our composition[2]. And so in that case employee involved they not only have to test that particular WS which is been choose but also the all those alternatives which can be the candidate for the single WS to be used in the project composition.

V.   THREAT IN THE SYSTEM

Threats are caused when an unwanted harmful substance comes in the system and it has the ability to disrupt the functioning/working of the system. In this paper, there will be a threat classification that will give the idea of what can be the threats that are involved in the system and particularly in this Designed Simulator [3] [4]. In this simulator threats are broadly classified as:

A list of security attacks is generated after reviewing number of literatures. We have to design a framework which will help in protection of WSL from these attacks and weaknesses.

But due to this large list framework will face number of issues listed as follows:

i.   It Need huge computing resources for monitoring and managing the intermediate states of lifespan.

ii. Network Congestion and bandwidth is also creating big issue at the time of Composite web service monitoring.

iii. Cost and Budget estimation of any Composite web service will be very complex and time consuming.

iv. Quality Assessment & Assurance will be tough.

As a step wise solution generation of these issues, firstly I had classified the above list as per the possibilities of its implementation areas. This task I had done by further categorisations.

These are the threats on which the analysis will be shown in this paper and also the comparison will be made and shown between the expected threat and how much these threats are affecting the Simulator.

This paper not only talks about the security of the system and the process that takes place in the simulator but also tells about the security of the database and how the threats can be classified and protected.

Figure 3 shown below are some of the techniques that can be used to secure the database. Behind every important application running in this real world there is some backend database that is been used either to store the analysis report or the records of the users or employees. From a simple inventory shop to a complex and dangerous database of the army and security related information, all the system working are having the database and it is very important to secure them.

Table No.1 Threats Classification

Attacks	Weak Points
Abuse of Functionality	Application Misconfiguration
Buffer Overflow	Improper File System Permission
Content Spoofing	Improper Input Handling
Cross-Site Scripting	Information Leakage
Denial of Service	Insufficient Anti-automation
FingerPrinting	Insufficient Authentication
SQL Injection	
Xml Injection	
Xquery Injection	

These threats after studying and research, this paper gathers information about its chances of having into the system. Its percentage wise analysis is given below in figure 3.
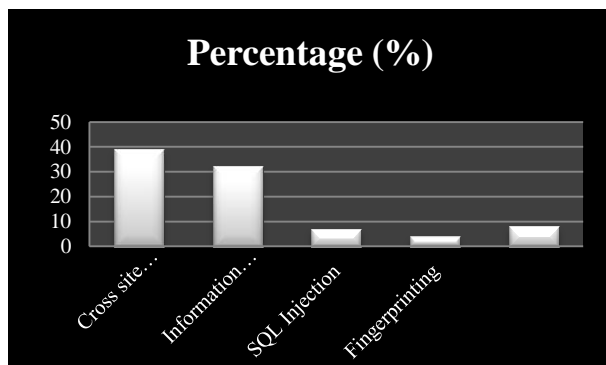

Fig. 3.Percentage of Vulnerabilities.

These vulnerabilities are divided into three broad types of risk: Low, Medium and High. The risk factors are analysed in the Simulator and there percentage are obtained. Figure 4 shows this classification.
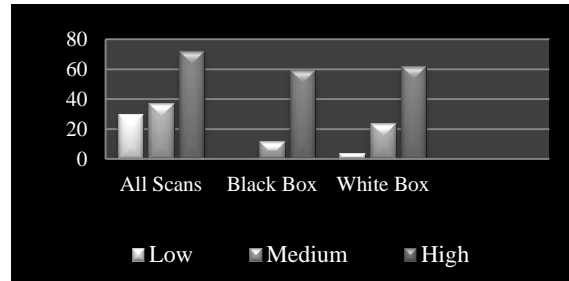

Fig. 4. Distributed threats based on Low, Medium and High

At the end of analysis of the Simulator, a comparative study is been made between the expected percentage of vulnerabilities and the actual report of it.
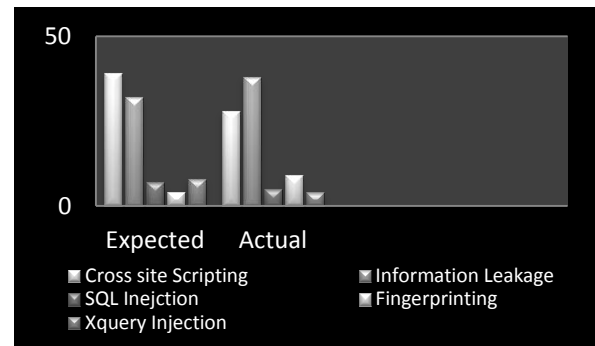

Fig. 5. Comparison between Expected vulnerabilities and Actual chances of Vulnerabilities

From all of the above mentioned attacks, database security can also be harmed from some of those threats such as:
A). SQL Injection
B). XQuery Injection
C). Damage to the software
D). Damage to the Hardware.
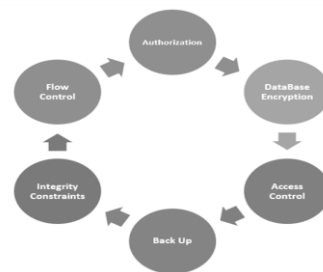Techniques involved in Securing the Database:

Fig. 6.Database Security Techniques.

Threats always affects the system at the points where the system is most vulnerable [5]. In this paper, those vulnerabilities have to be checked but firstly those vulnerabilities have to be found and after analysing the simulator the vulnerabilities have been found out. These are:

Table 2: Vulnerabilities of Threats

Vulnerabilities	Design	Implementation
Abuse Of Functionality	*	
Buffer Overflow		*
Content Spoofing		*
Cross-Site Scripting		*
Denial Of Service	*	*
Fingerprinting	*	
SQL Injection		*
XML Injection		*
Xquery Injection		*

All these threats are caused either in Design part or in the Implementation part. These vulnerabilities are caused due to some programming error or it can be caused due to wrong method implementation [5]. These are not the only threats that a system faces since advancements are made continuously, the system will be updated and changed and with changes some errors are always tend to occur.

After research and analysis of several threats that are involved in most of the projects and systems, this paper includes how much all of these threats can affect or have the potential to affect. The threats are represented with their percentage of how much chances there are for these threats to be in the system in general and after that this paper will help in making a comparison between the Expected threat potential and Actual potential of these threat.

VI.   WS SIMULATION AND ANALYSIS

In this paper the WS Simulator is been made which not only describes the interaction between the user Web Application and the WS but its main function is to verify and validate the web services that are involved as well to analyse the performance of those. Authentication and Authorization of the user, employee and the Administer is been used to bring limitation to functionalities of the people involved [11]. This helps greatly in securing the system as well as its database. The Simulator has three major components. They are:
1. Database Creation and its connection.
2. Web Services Composition
3. Development of the Web application that will monitor and control the WS.

The Database named "**VVReal**" created in the backend of the Simulator contains 5 different tables namely:
Admin_Data_Table: This table stores the details of all the administrators of the project and they can control and the information of the employees/ users that are associated with the development of the Simulator.

Employee_Detail_Table: This is the table that stores all the details related to the employees and users. Their ID and password related knowledge, address, email, etc. all are stored in this table.
Employee_WS1_Table: This is table that stores all the information related to first Web Service that is created in the Simulator. All the files related information to WS1 are stored in this table, their address and name of the files.

Employee_WS2_Table: This is table that stores all the information related to first Web Service that is created in the Simulator. All the files related information to WS1 are stored in this table, their address and name of the files.

WSAnalysis_Table: This is the table that gives the analysis of the Web Services that are used in the Simulator with respect to time. The details stored in this table are name of the WS and the time taken in seconds by each WS when used in the Simulator.

A. Implementation of the Simulator
The implementation of the Simulator is been done in several parts. The projects main part is the Web Application that not only monitors the tasks that are being performed in it but also controls its flow and with this allowing the control to be given to whichever WS it wants. This Web Application calls the WS to perform its tasks that are needed to be done. The user/employee can do the task and also can choose the director or path where they want to save the file after working. The tasks are:
1. To create a file and also it can read the content from it.
2. To write a file with contents provided by the employee and it can also store the file at the desired location.
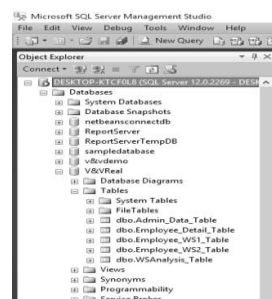

Fig. 7: Database of the Simulator   Fig. 8. Administer Page.

Both of these tasks involve a lot of conditions and situations where a system can be in the real world. The Web Application contains different pages. They are:

Administrator Page:

This is the page for the administrator where he/she can check the performance of the WS as well as monitor the work done by the employees. Administrator can also check the database of the employees and can update it.

Fig. 9. Administrator Login Page

Fig. 10. Employee Login Page.

Administrator Login Page:

This is the page where administrator has to enter his/hers details in order to log into the application. The detail includes Id, Name and Password. These details are already stored in the database and when the administrator tries to login, the id, name and password are been first cross checked with the database and then only the permissions to monitor or bring any changes are provided.

Employee Login Page:

This is the page where Employee has to enter his/hers details in order to log into the application. The detail includes Id, Name and Password. These details are already stored in the database and when the administrator tries to login, the id, name and password are been first cross checked with the database and then only the permissions to monitor or bring any changes are provided. There are two more links that are provided in this page through which a new user can register himself/herself or can login as an Administrator if it is an Admin.

Employee Registration Page:

This is the page where Employee has to enter his/hers details in order to register into the application. The detail includes, Name, password, Email Id, Address and Working Area. These details entered will be added to the database with new Id for the employee.The Id generated for the employee will be unique and will serve for its identity i.e. the employee will be represented through that Id in any case. After registering successfully, the new employee will be provided with that Id.There is one more button that links us to the employee login page after we get the Id and then employee can login himself/herself into the application.

Fig. 11.Employee Registration Page.

After employee has registered itself and chose a specific working area, he/she will be only limited to that work only and files related to that working field. No employee can interfere with the files or work not related to his/her working field. Therefore there are different pages for the different WS are developed so they don't interfere.

Simulator WS1 Page:

First is Employee WS1 page where all the employees related to the working of WS1 are there and can only access files related to it. First WS is related to creation of files and collecting the data that it receives. Figure 9 shows the WS1.
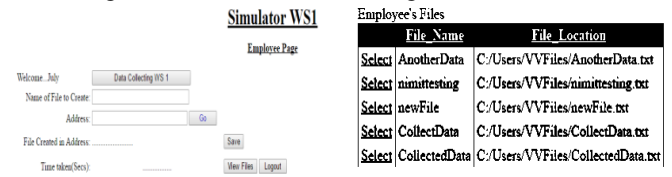
Fig. 12. Simulator WS1 Page.

Fig. 13. Employees Files with WS1 Working Field.

This page clearly shows that what it does. And in this employee can create the file content in the desired location as there is the option of giving the path where the file has to be stored. As previously, there is been discussed that this application shows the performance of the WS with respect to time. Here in this page, it can be clearly seen that there is the area given where it shows the amount of time the WS has taken to perform its tasks (in secs). After completion of work, employee can store the working and everything that will be stored by just clicking on one button "Save" which is shown on the page. Here in this page there is also one option for "View Files" with employee can see the files that are related to his/her work along with the address and location of it so that he/she can get to know where he has option of saving or updating the files. Either he/she can create a new file or employee can use the previous created files and update it. When employee clicks on to the button "View Files", a new page is opened which is "Employee_WS1_Table". This table will store the information related to the files that are created during the working of WS1. In Fig. 10 it is shown.

Simulator WS2 Page

Fig. 14 is showing the working of the Simulator for WS2 is the second web service that is been used in the Simulator. In this Figure it can be seen that this WS has the work for Data analysing and Data filtering. The employee uses the previous files to work on them and then makes an update if he/she wants to or just creates a new file and writes onto that. In this WS, the first WS is been used to read the file from the location employee wants. It has the access of the previous made files as over here employee job is to read the data from the file and update it on the new file or onto the same file.
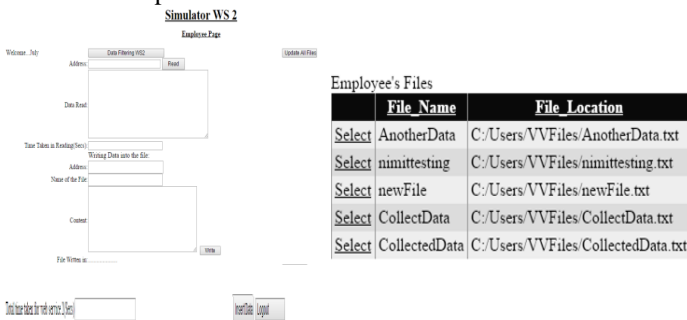
Fig. 15. Employee Files with WS2 Working Field

Fig. 14. Simulator WS2 Page

Here also this WS shows its performance with respect to time. Since this WS is the combination of two WS i.e. Data Filtering and Data Writing so therefore the performance calculated is by adding both the time taken by both the Web Services. This time is represented in the "Total Time" section (in secs). There is also button for inserting the data that is been gathered after working of the WS2 is completed. This data is been stored in the database for showing the future analysis by the Administrator.

There is also the option of updating all files that does the task of deleting the files that are created with the same name and location and helps in removing the redundancy in the database. A button to show the files under this WS is also there which on clicking links to the new page that shows the files that are associated with the WS2. Figure 12 will show that page. This page is same as that for the WS1 showing table with same attributes like File Name and File Location.

Data Management Page

This is the page that is directly linked to the Administrator which can monitor database employee and bring changes as he/she desires.

Fig. 16(i). Employee Database

Fig. 16(ii). Employee Database

Web Service Analysis Page

This is the page that shows the performance of the WS after the Simulator finishes its job. The data gathered after the working of the Simulator is been stored in the database and then based on that data, analysis is been made on the performance via showing a table and a graph of the Web Services that are involved in it. This functionality can be used only by the Administrator so that he/she can use that analysis to make the working of the system more efficient and enhanced. Figure 14& 15.Shows this page for the performance of the WS.

	Web_Service Name	Time taken
Select	WS2	0.1272674
Select	WS2	6.4932298
Select	WS2	1.0989660
Select	WS1	0.0138309
Select	WS1	01.4398687
Select	WS2	1.3412701

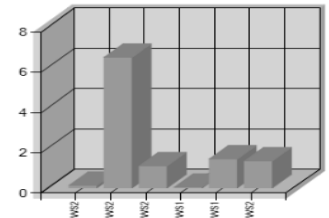Fig. 17 Time Based Table Performance of Web Services

Fig. 18. Bar Graph Showing the Performance of Web Services.

VII.   CONCLUSION AND FUTURE SCOPE

Web Services in the past are often and always relied on its traditional testing methods to make sure a WS is safe to use or not. But at present situation is very difficult as there are so many WS providers are there over the internet that it has become so confusing and difficult to choose that WS which is both secure and safe to use. Many providers are unknown and proper techniques are to be applied to check its validity and functionality. Dynamic Testing has become so much important because most of the times the users cannot trust the validity of WS. People over here often use many WS without knowing its source code or the provider whether it is valid or not. This may work in small projects or applications but in the company where there is so many things to handle and so many important data is there which if revealed to any outsider can cause a great harm to it. So building a technique to trust the provider and its WS has become a very important agenda nowadays.

In this paper, a discussion over the Simulator has been done which is been used as a tool to get an idea of how dynamic testing and its validation and verification can be done. A list of threats and its classification is also been discussed with its vulnerabilities and weak points. This paper shows the importance of recognizing the weak points where a threat has maximum capacity to attack and

harm the system. This Simulator also succeeds in showing and comparing the performances of the Web Services that are been used in this Simulator. This Simulator also has the future scope as using this in a broader and larger way, this simulator can tell which WS or application has maximum ability to do the work efficiently and in a secure way. This might help the companies to make them prevent from unknown harms and also may prevent some threats in advance before affecting the System.

REFERENCES

[1] M. D. Priya, A. Lavanya, "Intrusion Detection System Using Raspberry Pi Honeypot in Network Security", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 3, pp. 41-45, January-February 2018.

[2] E. Manigandan, C. Kalaiarasi, E. Manigandan, Prof. C. Kalaiarasi, "Cryptography in Cloud Computing : A Basic Approach to confirm Security in Cloud", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 3, pp. 58-63, January-February 2018.

[3] W. T. Tsai, Y. Chen, R. Paul N. Liao, and H. Huang, "Cooperative and Group Testing in Verification of Dynamic Composite Web Services", in Workshop on Quality Assurance and Testing of Web-Based Applications, in conjunction with COMPSAC, September 2004, pp.170-173.

[4] Vicente Aguilera Diaz, Robert Auger, Amit Klein, Dennis Groves, Cesar, "MX Injection : Capturing and Exploiting Hidden Mail Servers", OWASP Spain chapter meeting of June 16th, 2006.

[5] TasosLaskos, "Arachni Framework v1.4 &WebUI v0.5.10", Web Application Security Scanner, Feb 09 2016,01:04AM,http://www.securityfocus.com/archive/107/537488/30/0/threaded

[6] "Common Vulnerabilities and Exposures, The Standard for Information Security Vulnerability Names", sponsored by US-CERT at the U.S. Department of Homeland Security. Copyright © 1999–2016, The MITRE Corporation. CVEhttp://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0800

[7] Kumar, Vipin, Srivastava, Jaideep, Lazarevic, Aleksandar, "Managing Cyber threats: Issues, Approaches and Challenges", Springer Publishers,2005, ISBN 978-0-387-24226-2.

[8] S. K. Singh, "Database systems: Concepts, Design and applications", Pearson Education India, 2011, ISBN 978-81-317-6092-5.

[9] Web Application Security Consortium.http://www.webappsec.org

[10] Roberto Chinnici, Hugo Haas, Amelia A. Lewis, Jean-Jacques Moreau, David Orchard,SanjivaWeerawarana, "Web Services Description Language (WSDL) Version 2.0 Part 2": AdjunctsW3C Recommendation 26 June 2007.Copyright © 2007 W3C® (MIT, ERCIM, Keio)

[11] Kung-Kiu Lau and Cuong Tran, "Composite Web Services", Chapter: Emerging Web Services Technology, Volume II, Part of the series:Whitestein Series in Software Agent Technologies and Autonomic Computing, pp 77-95

[12] DimkaKarastoyanova and Alejandro Buchmann, "Development Life Cycle of Web Service-based Business Processes. Enabling Dynamic Invocation of Web Services at Run Time", ICSOC'05: The 3rd International Conference On Service Oriented Computing, 2004.

[13] Karthikeyan Bhargavan, Ricardo Corin,CedricFournet,Andrew D. Gordon, "Secure Sessions for Web Services",ACM Workshop on Secure Web Services, October 29, 2004, Fairfax VA,USA.Copyright 2004 ACM 1-58113-973-X/04/0010

[14] Muhammad Ahtisham Aslam, Jun Shen,Michael Herrmann, "An Integration Life Cycle for Semantic Web Services Composition",11th International Conference on Computer Supported Cooperative Work in Design, 2007, E-ISBN :1-4244-0963-2, Print ISBN:1-4244-09624 DOI:10.1109/CSCWD.2007.4281485, Page(s):490 – 495.

[15] Zhaohao Sun, Dong Dong, Jun Han, "A Demand Driven Web Service Lifecycle", New Trends in Information and Service Science, 2009. NISS '09, DOI: 10.1109/NISS.2009.135

[16] Oracle® Application Server Web Services Developer'sGuide, 10g (10.1.3.5.0), Part Number E13982-01

[17] F. Curbera, M. Duftler, R. Khalaf, W. Nagy, N. Mukhi,and S.Weerawarana, "Unraveling the Web Services Web: An Introduction to SOAP, WSDL, and UDDI," IEEE Internet Computing, vol. 6,no. 2, pp. 86-93, Mar./Apr. 2002

[18] Martin Gudgin, Marc Hadley,Noah Mendelsohn, Jean-Jacques Moreau, Henrik Frystyk Nielsen, Anish Karmarkar, Yves Lafon, "SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)", W3C Recommendation 27 April 2007.
.

Authors Profile

Mr. G. Raj pursed Bachelor of Technology from UPTU, Lucknow, India in 2006 and Master of Technology from MNNIT, Allahabad, India in year 2010. He is currently pursuing Ph.D. from Punjab Technical University, Kapurthala , Punjab, India and currently working as Assistant Professor in Department of Computer Sciences, Amity University Uttar Pradesh, India since 2013. He has worked in Lovely Professional University as Assistant Professor from 2010 to 2013. He is a professional member of IEEE since Jan.,2018. He has published more than 40 research papers in reputed international conferences and journals including IEEE, ACM , Springer and it's also available online. His main research work focuses on Web Service, Software Engineering, Cloud Security and Privacy, Service Prediction, IoT and Computational Intelligence based education. He has 10 years of teaching experience and 5 years of Research Experience.

Dr M. Mahajan pursed Bachelor of Technology and Master of technoology from MMEC, Mullana in Information Technology and Ph.D. in Computer Science from Punjab Technical University, Kapurthala in 2016 . He is currently working as Assoc. Professor and HOD in Department of CSE in CGC, Landran from 2015. He is a professional member of IEEE,. He has published more than 20 research papers in reputed international journals including Thomson Reuters (SCI & Web of Science) and conferences including IEEE and it's also available online. His main research work focuses on Cloud Security and Privacy, Big Data Analytics and Data Mining,. He has 5 years of teaching experience and 4 years of Research Experience.

Dr D. Singh Presently working as Associate Professor in Computer Science & Engineering Department at Chandigarh College of Engineering & Technology (CCET), Chandigarh He has published and presented 82 research papers in National & International Journals (Including IEEE, Springer, ELSEVIER & having good impact factor) /Conferences. He is having 12 years of experience of teaching at reputed Engineering Colleges.Had done B.E.(Computer Science & Engineering.), M.Tech(Computer Science & Engineering.), PhD(Computer Science & Engineering.)He has guided 8 PhD Thesis, 10 M Tech Thesis, 19 B Tech Projects. He is Member of reviewer Panel of International Journal of Information Technology & Knowledge Management and Member of reviewer Panel of International Journal of Research in Engineering & Technology, Life member of IETE. His main research work focuses on Web Enginering, Software Engineering, Cloud Security and Privacy, Big Data Analytics and Data Mining.