Dual Security Testing Model for Web Applications

Singh Garima
Research Scholar
Department of Computer Science and Engineering
JECRC University
Jaipur, Rajasthan, India

Kaushik Manju
Associate professor
Department of computer science and Engineering
JECRC University
Jaipur, Rajasthan, India

***Abstract*—In recent years, web applications have evolved from small websites into large multi-tiered applications. The quality of web applications depends on the richness of contents, well structured navigation and most importantly its security. Web application testing is a new field of research so as to ensure the consistency and quality of web applications. In the last ten years there have been different approaches. Models have been developed for testing web applications but only a few focused on content testing, a few on navigation testing and a very few on security testing of web applications. There is a need to test content, navigation and security of an application in one go. The objective of this paper is to propose Dual Security Testing Model to test the security of web applications using UML modeling technique which includes web socket interface. In this research paper we have described how our security testing model is implemented using activity diagram, activity graph and based on this how test cases are generated.**

***Keywords*—Web application testing; Security testing; UML modeling; Web socket programming**

I. INTRODUCTION

In recent times web based applications are frequently used by all. There is no need to install these applications on each system, but they are installed on the web server. A web server is an internet information service on which web application is implemented. With a growing concern about the quality of web applications web application testing is again an area of research to explore. An effective modeling technique is required to know particular challenges of web applications for testing [1]. In the normal daily routine types of web applications the security feature is implemented to verify the e-mail ID, cell phone number, landline number and other government approved identification with social identifications like e-mail and Face book account etc. After the formality of registration along with the collection of the general information about a customer or user, registration ID and password are provided to access the whole activity of website excluding the web server admin authority. At this stage it is not possible to identify whether the site is being accessed by the 100% authentic user whose records have been recorded. This is one of the critical types of task which identifies the authentication of use of ID and password. And in this situation, loosing rights in favor of user are sometimes critically harmful to the company. In order to provide a solution and to overcome this kind of situation there is a need of a self managing web application which handles the control itself ,as per need of the user , essential for security purpose. The proposed model gives a way to generate test cases and helps in web application testing. In this study, Unified Modeling Language (UML) approach has been used. UML based approach for modeling web applications was used earlier by different researchers for testing contents, to navigate the model. This research extends to model based testing to test security of web applications along with content and navigation. Specific Testing Process Model (STPM) gives composite view of content, navigation and security model to test web applications. In this paper researcher has elaborated Specific Testing Process Model and has implemented Dual security testing model of the STPM, which is one of the aspect of STPM.

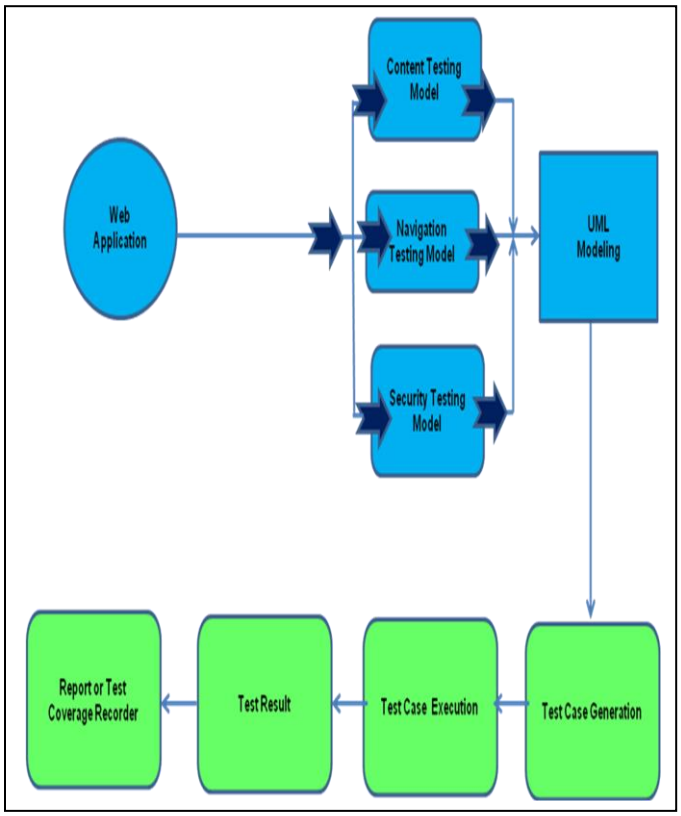

Fig. 1. Specific Testing Process Model

II. OBJECTIVES

A. To design a model (Dual Security Tesing Model) to test the security of web application by using UML modeling techniques including web socket interface.

B. To Implement Dual Security Tesing Model of STPM.

III. LITERATURE REVIEW

The motivation of present research is to work on three different perspectives of a web application by using a composite model called Specific Testing Process Model (STPM). This study proposes a secondary stage of testing navigation and security of web application by busing UML modeling techniques. Various models have already been proposed for testing web applications. According to the unique characteristics and challenges of web applications, these models have a different origin and test goals. Different methods using partial rewriting based specification language for both syntactic and semantic checking were developed [2] [3] for the static applications. Researchers focus on the content of web sites by correcting and reforming the syntax and semantic [4] [5]. In this study, UML diagrams have been used for content testing of web application. Based on these diagrams test cases are generated. Test cases can be generated efficiently for content testing by using UML modeling. For testing navigation of the applications, there are UML based models [6] [7] [8], graph based models [9] [10], state charts based models [11] [12]. Also, researcher proposed a novel approach to generate test cases from UML activity diagrams [13]. In this approach, navigation testing covers contextual and non-contextual hyperlinks of web application, Security aspects of the web application should be analyzed and modeled during entire development cycle to identify security requirement in the early stage of the development progress. There can be various security constraints like access control, availability, authentication, integrity, secrecy, etc. which should be taken care of. Numerous researchers have explored the use of the UML language for modeling, security aspects of web applications. Different security models [1] [14] [15] [16] used UML approach to understand security requirements. Web socket protocol can be used to develop web application [17]. Using HTML5 based web browser, web socket based applications can be executed. The creation of a real time application and live content facility can be done using web socket protocol. It gives more interaction between browser and application [18]. This study cover access control, security aspect of web application. It also provides the user with an interface by using web socket programming in order to have suggestions regarding the product purchase while using online shopping web application.

IV. TESTING MODEL

Different modeling methods are available to test the web applications at different levels, i.e., content, navigation and security, but no model has yet been developed which can test all three levels of modeling in integration as discussed in the literature above. Here Fig.1 shows a Specific Testing Process Model to test web applications. Researcher has used three sub-models which are as follows:

A. Content Testing Model

Information displayed on the web application and its presentation plays a vital role as we say first impression is the last impression. If a user finds inaccurate information and an unstructured layout of an application its quality and users will be affected. Researcher extends the content model [7], this model tests the completeness and the correctness of web application information displayed in the form of web pages i.e., its outlay. The content testing model is important because it describes where the objects (text, button, Audio, Image, Form, Video, Frameset, Frame) are placed.

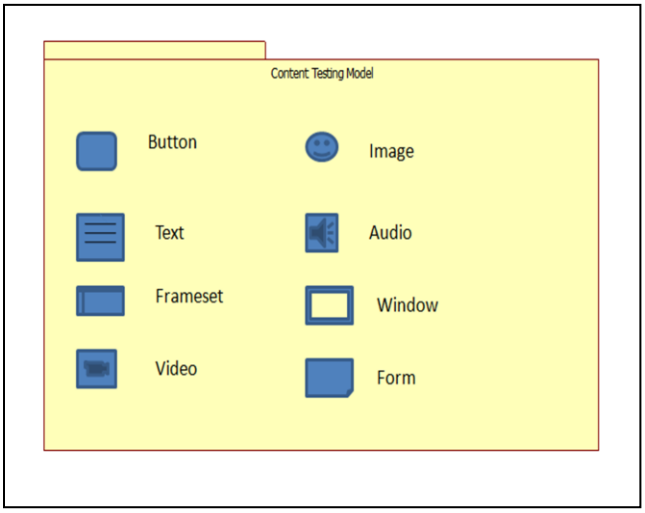

Fig. 2. Content Testing Model

B. Navigation testing model

Navigation of web application gives freedom to a user to move from one page to another within the same or different pages of an application, click on links, images etc. In other words navigation in context of a web application is the sequence of web pages that a user can browse to achieve a desired page or function. Here in this research, navigation testing model is a sub-model of Specific Testing Process Model, which allows a tester to test whether a user is able to reach information and navigate according to content testing model. The basic elements to test in the navigational testing model are contextual and non-contextual hyperlinks described in [19]. As shown in Fig. 3.

Contextual Hyperlinks: Link between objects is called contextual, as it carries information from its source to destination object. The contextual link can be the links provided within the web application having its source or a destination with in the application.

Non-Contextual Hyperlinks: The non-contextual link is the link which does not carry information within the application. The content of the required page does not depend on the content of its source page.

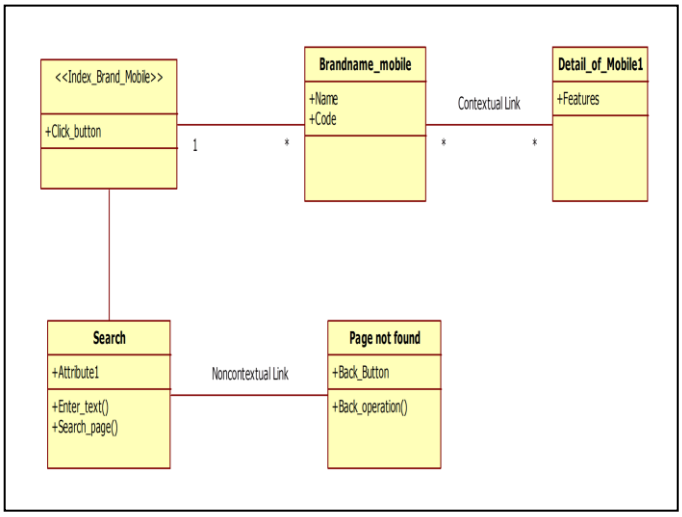

Fig. 3. Navigation model of contextual and non-contextual links

C. Security Testing Model

Model-driven security is an approach proposed by [16] and is used to simplify system design and generate artifacts. Security testing aims at verifying the effectiveness of the overall web applications defenses against undesired access by unauthorized users, its capability to prevent system resources from improper use and granting authorized users access to authorized services and resources. There has been only little work on the UML based security model. The focus of the security testing model is on Role Based Access Control (RBAC) [20]. It is an approach to restrict system access only to authorized user as shown in Fig4., One Time Password (OTP) [21] and Completely Automated Public Turing test to tell Computer and Human Apart (CAPTCHA) [22].

Researcher has elaborated dual security testing model which is one of the aspects of STPM. It provides a feedback on the users of online web application as shown in Fig. 5. Using the feedback facility current user can collect the views of previous users about the product they want to purchase. The feedback providers are already registered users of that application so the user can authenticate the validity of the product and also organizations can develop business intelligence. This process is accountable under the dual verification. Here, a registered user goes for dual verification so that organization is sure about the validity of the user and it can provide feedback details to the registered user. As soon as he/she logs in a One Time Password (OTP) SMS is sent to the registered mobile number or user registered mail account. Then the user fills an interface provided to him/her with the information about registration id ,OTP and CAPTCHA which are then verified in the database. Otherwise the user is asked to get registered first. After verification, if the user is found registered he/she can take the feedback information regarding the product and can also avail help of Customer Care Service (CCS). In CCS the browser control is given to the admin so that while using an interface he can help the user in buying the product by providing suggestions like product comparison.

In dual security testing model, the user's browser is controlled by admin of the web application when the user wants Customer Care Service (CCS) by using web socket programming. Using this dual security testing model, at the time of purchasing any product if user needs suggestions regarding the product price range, comparison with other similar product, then as he click on Customer Care Service (CCS), at this time the browser gets controlled by admin remotely using web socket programming interface, admin also sees the user browser activity.

As the user selects the product a suggestion message about the price range of the product with other similar product on the same online shopping application is displayed. By this model the customer is able to compare the price of the product on the visited online shopping site itself, he or she need not move on to another web site for a comparison of different range of the product. The dual security testing model helps in knowing the pattern of purchase for product line which includes ranges of products customer selects most, which is useful in data collection for companies.

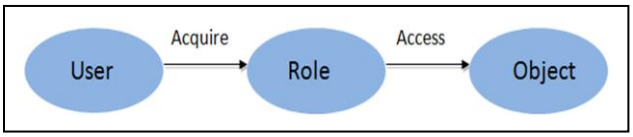

Fig. 4. Role Based Access Control

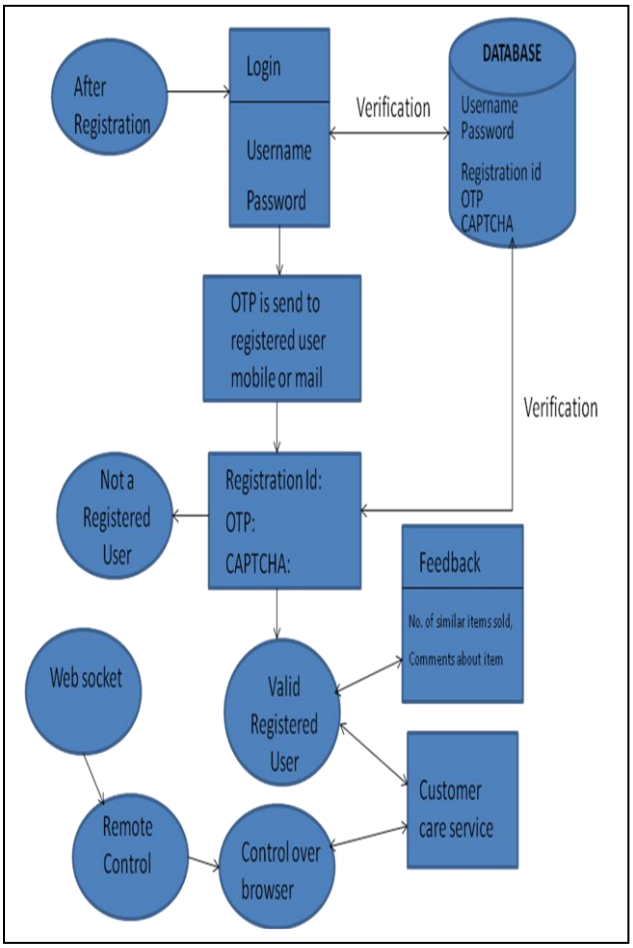

Fig. 5. Dual Security Testing Model

V. PROPOSED IMPLEMENTATION METHODOLOGY

In this section, researcher discusses proposes an approach towards implemention of the model and generation of a test case from an activity diagram. The proposed approach passes through three basic steps. These three basic steps are as follows:

A. Activity Diagram

Designing activity diagram with the required information. The activity diagram describes the guideline about the modeling and necessary information required. Here in the proposed methodology the activity diagram is designed to implement the modeling, which is shown in the above mentioned Fig. 5, about "Dual Security Testing Model". The activity diagram changes the state of an object from previous object and the output at various stages. Activity diagram creates object during the execution according to decision and conditions. Finally, activity diagram Fig. 6 provides the highest level of the abstractions.

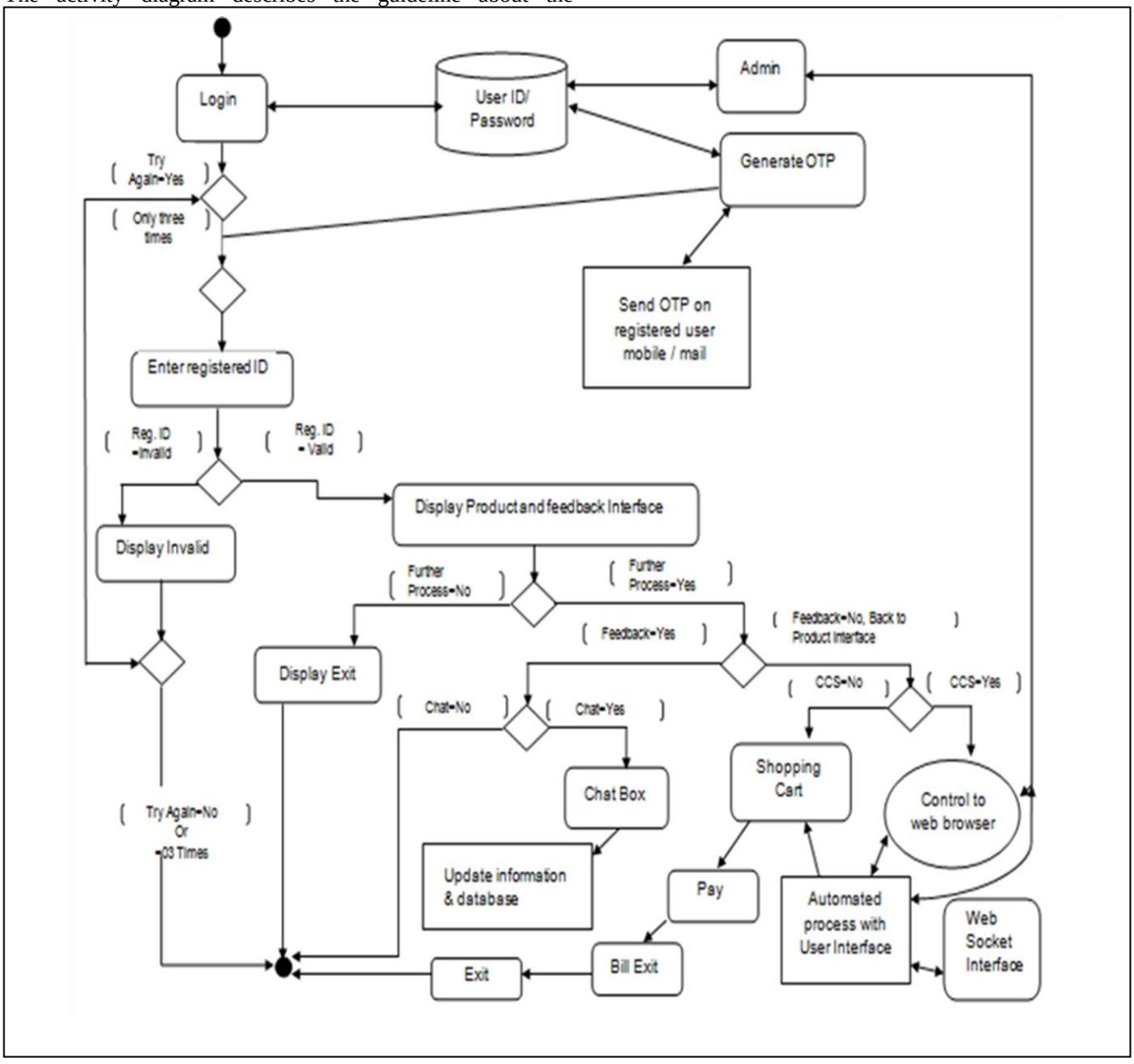

Fig. 6. Activity diagram of online shopping cart

B. Activity Graph

Converting the activity diagram into an activity graph.

The activity graph is a converted form of the activity diagram used for recognizing the activity and flow procedure of modeling. An activity graph is a directed graph where each node in the graph represents a construct for eg. initial node, flow final node, decision node, guard condition, join node, merge node etc., and each edge of activity graph represents the flow in the activity diagram. The activity graph encapsulates

constructs of an activity diagram in a systematic and suitable manner. In the present study a set of rules for mapping constructs for an activity diagram is proposed. Nodes of an activity graph are as follows:

S: Start Node

E: End Node

A: Activity

D: Decision

C: Condition

T: Transaction

Fig. 7 represents the activity graph for the activity diagram in Fig. 6. To form edges, consider one-to-one mapping from an edge of the activity diagram into an edge between two nodes in the activity graph. The graph is labeled for better understanding the flow and activity. Each labeled node is acting as the storage of information as the data structure, which is known as the Node Description Table (NDT). To understand activity graph Fig. 7, refer Table I. Node Description Table.

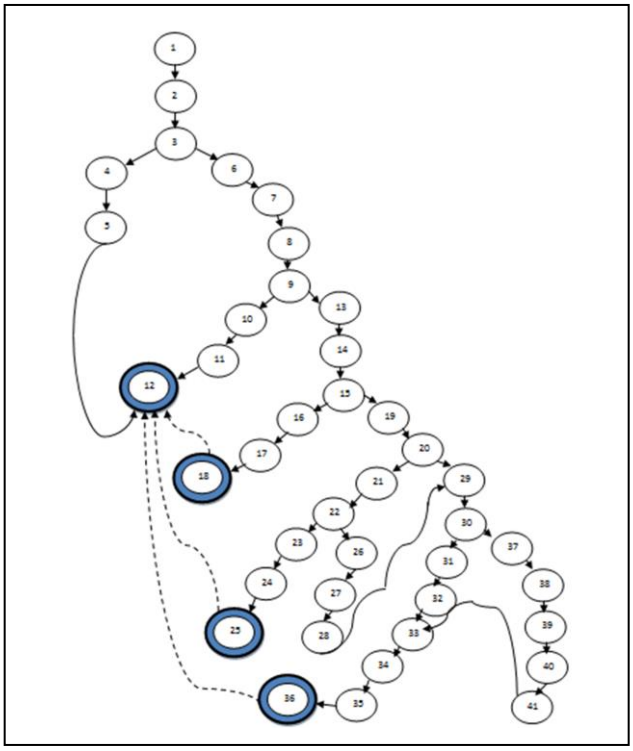

Fig. 7. Activity Graph

C. Generating Test Cases

Generating test cases from the activity graph.

The test case generation is basically an approach to cover all the coverage or the criterion of coverage of all the activities. The present approach of generating test cases from an activity graph is following the given test coverage criterion.

TABLE I. NODE DESCRIPTION TABLE

Node Index	Type of Node	Description of activity
1	S	Start
2	A	Enter Login ID / Password
3	D	Decision
4	C	LoginID=Not Valid (Try Again)
5	A	Display Not Valid
6	C	LoginID=Valid
7	T	Generate OTP
8	A	Enter Registration ID
9	D	Decision
10	C	Registration ID= Not Valid
11	A	Display Not Valid
12	E	End Node
13	C	Reg ID = Valid
14	A	Display Product & Feedback Interface
15	D	Decision
16	C	Further Process = NO
17	A	Display Exit
18	E	End Node
19	C	Further Process = YES
20	D	Decision
21	C	USER Feedback = YES
22	D	Decision
23	C	ChatBox = NO
24	A	Display Exit
25	E	End Node
26	C	ChatBox = YES
27	A	ChatBox Entry
28	T	Update Information
29	C	USER Feedback = NO
30	D	Decision
31	C	CCS = NO
32	A	Display Shopping Cart Interface
33	T	Payment
34	T	Billing
35	A	Display EXIT
36	E	End Node
37	C	CCS = YES
38	A	Display Control Transfer to Web Browser
39	T	Automated Controlled User Interacted Shopping Process
40	T	Control Activity with Socket Programming (Security+Admin)
41/32	A	Display Extended Shopping Cart
42/33	T	Payment
43/34	T	Billing

a) Basic Path Coverage Criterion: At this, firstly define the basic path in activity graph. A basic path is sequence of activities where an activity in that path occurs exaclty once.

b) Simple Path Coverage Criterion: A Simple path is considered for activity diagrams that contain concurrent activities. It is representative path from a set of basic path whwre each basic path has the same set of activities, and activities of each basic path satisfy an identical set of partial order relations among them.

c) Activity Path Covergae: The aim of this covergare os to cover both loop testing and concurrency among the activities of activity diagrams.

TABLE II. MACRO TEST CASES FROM ACTIVITY GRAPH

Test Case No	Sequence of Branch Condition	Activity Sequence	Object State	Expected Result	Actual Result
1	Login ID = Invalid TryAgain = Yes	Enter Login / Password, Display Invalid	False	True	True
2	Login ID = Valid TryAgain = No	Enter Login / Password, Generate OTP	True	True	True
3	RegID = Invalid	Enter RegID, Display Invalid	Invalid	True	True
4	RegID = Valid	Enter RegID, Display Interface	Valid	True	True
5	RegID = Valid Further Processing = No	Further Processing, Display Exit	Valid	True	True
6	RegID = Valid Further Processing = Yes	Further Processing, Display User Feedback	Valid	True	True
7	RegID = Valid Further Processing = Yes	Further Processing, Display User Feedback	Invalid	False	True
8	RegID = Valid Further Processing = Yes ChatBox = No	Further Processing, Display User Feedback Display Exit	Invalid	False	True
9	RegID = Valid Further Processing = Yes ChatBox = Yes	Further Processing, Display User Feedback	Valid	True	True
10	Further Processing = Yes ChatBox = Yes	Further Processing, Display User Feedback, ChatBox Entry	Valid	True	True
11	ChatBox = Yes	ChatBox Entry, Update Information	Valid	True	True
12	ChatBox = Yes	ChatBox Entry, Update Information,	Valid	True	True
13	Further Processing = Yes	User Feedback = No, CSS = No	Invalid	True	True
14	Further Processing = Yes CSS = NO	CSS = No, Display Shopping Cart Interface	Invalid	True	True
15	Further Processing = Yes CSS = NO	CSS = No, Display Shopping Cart Interface Payment	Valid	True	True
16	Further Processing = Yes CSS = NO	CSS = No, Display Shopping Cart Interface Payment +Billing + Display Exit	Valid	True	True
17	Further Processing = Yes CSS = Yes	CSS = Yes ,	Valid	True	True
18	Further Processing = Yes CSS = Yes	CSS = Yes , Display Control Transfer to WB	Valid	True	True
19	Further Processing = Yes CSS = Yes	CSS = Yes , Display Control Transfer to WB, Automated Control User Interaction Shopping	Valid	True	True
20	Further Processing = Yes CSS = Yes	CSS = Yes , Socket Security + Admin Controlled	Valid	True	True
21	Further Processing = Yes CSS = Yes	CSS = Yes , Socket Security + Admin Controlled, Display Extended Shopping Cart	Valid	True	True
21	Further Processing = Yes CSS = Yes	CSS = Yes , Socket Security + Admin Controlled, Display Extended Shopping Cart	Invalid	True	False
22	Further Processing = Yes CSS = Yes	CSS = Yes , Socket Security + Admin Controlled, Display Extended Shopping Cart,	Valid	True	True

These 22 test cases in Table II. Are the cases represent a broad canvas of activity based test case generation. Further, all the test cases can extend at micro level to generate the test case for content and navigation level.

VI. RESULT

a) Dual Security Testing Model has been implemented using an online shopping application. As shown in Fig 6. activity diagram is developed to describe user registration process through modeling.

b) An activity graph is constructed from activity diagram to understand the flow procedure of the application.

iii. Each node of the activity graph has been described in Table I.

c) The model has been implemented through different test cases generated from activity graph (Table II.)

d) The testing approach provide an easy way to find errors in web applications.

VII. CONCLUSION

Researcher has developed a model (Dual Security Tesing Model) to test the security of web application by using UML modeling techniques including web socket interface. The model has been implemented through test cases. The test cases are generated and system conformance can be checked with the system model. It is suitable with automated admin controlled customer care service system which is beneficial for the cutomers using web applications. The model helps in data collection for the organization which sales their product online. This helps in knowing the buyers pattern, so that the product range can be enhanced. The Future task would be validation of the model through automation and web engineering applications.

ACKNOWLEDGMENT

This research is supported by the JECRC University, Jaipur, Rajasthan, India.

REFERENCES

[1] Alafi MH., Cordy JR., Dean TR. (2012), 'Recovering role-based access control security models from dynamic web applications', in Brambilla M., Tokuda T., Tolksdorf R. (eds.) , *Web Enginerring,12th International conference, ICWE 2012*, Berlin, Germany, July 23-27, 2012. Springer, pp. 121-136.

[2] Alpuente M., Ballis D., Falaschi M. (2005), 'A Rewriting-based Framework for Web Sites Verification', S. Abdennadher S., Ringeissen C. (eds.), *Proceedings of the 5th International Workshop on Rule-Based Programming (RULE 2004), Rule-Based Programming 2004*, June 1, 2004. Aachen, Germany, Elsevier, pp.41–61.

[3] Alpuente M., Ballis D., Falaschi M., Romero D. (2006), 'A Semi-Automatic Methodology for Repairing Faulty Web Sites', in Hung DV. And Pandya P. (eds.) *Software Engineering and Formal Methods, Fourth IEEE International Conference, SEM 2006*, Pune, India, September 11-15, 2006. IEEE, pp. 31–40.

[4] Coelho J, Florido M. (2006), 'VeriFLog: A Constraint Logic Programming Approach to Verification of Website Content', in Shen HT., Li J., Li M., Ni J. and Wang W. (eds.) *Advanced Web and Network Technologies, and Applications, International Workshops:XPA, IWSN, MEGA,and ICSE, APweb 2006*, Harbin , China, Jan 16-18, 2006. Springer Berlin Heidelberg, pp. 148–156.

[5] Coelho J. and Florido M. (2007), 'Type-Based Static and Dynamic Website Verification',in Werner B. (ed.) *Internet and Web Applications and Services, Second International Conference ICIW 2007*, Morne, Mauritius, May 13-19, 2007, IEEE, pp.32.

[6] Bellettini C., Marchetto A., Trentini A. (2004), 'WebUML: reverse engineering of web applications', in Liebrock LM. (ed.), *Applied Computing, the ACM Symposium SAC 2004*, Nicosia, Cyprus, March 1-17 2004. ACM, pp.1662–1669.

[7] Knapp A., Zhang G.(2006), 'Model Transformations for Integrating and Validating Web Application Models', in Heinrich C. and Ruth B. (eds.) *Modellierung, International workshop, MOD 2006*, Innsbruck, Austria; Springer, pp.115–128.

[8] Nora K., Baumeister H., Hennicker R. and Mandel L. (2000), 'Extending UML to model navigation and presentation in web applications', in Winters G. and Winters J. (eds.) *Modelling Web Applications in the UML Workshop, UML 2000*., England, UK, October 2-3, 2000, York, pp. 1.

[9] Sabharwal S., Bansal P., Aggarwal M. (2013), 'Modelling the navigation behavior of dynamic web application', *International journal of computer applications-Scholarly peer reviewed research publishing journal*, **65(13)**, pp. 20-27.

[10] **S**ciascio, D. E., Francesco D. M., Mongiello M., Piscitelli G. (2003), 'Web application design and maintenance using symbolic model checking', in Canfora G., Brand M.V.D., Gymothy T. (eds.) *Software maintenance and reengineering*, Seventh European conference CSMR 2003, Benevento, Italy, IEEE, pp.63-72.

[11] Han M, Hofmeister C. (2006), 'Modeling and verification of adaptive navigation in web applications', in Wolber D., Calder N. Brooks C and Ginige A. (eds.) *Web Engineering, 6th International Conference ICWE 2006*, Palo Alto, California, July 11-14 2006, ACM press, pp.329–336.

[12] Winckler M, Palanque PA. (2003), 'StateWebCharts: A Formal Description Technique Dedicated to Navigation Modelling of Web Applications', in Jorge J., Nunes N. and Cunha J. (eds.) *Interactive Systems. Design, Specification, and Verification, 10th International Workshop 2003*, Maderia Island, Portugal, June 11-13 ,2003, Springer, pp.61–76.

[13] Debasis Kundu and Debasis Samantha (2009), ' A Novel Approach to Generate test Cases from UML Activity Diagrams', *Journal of Object Technology*, Vol-8, No-3, May –June 2009, pp-65-83.

[14] Chehida S. and Rahmouni M.K.(2012), 'Security requirements analysis of web applications using uml', in Malki M., Benbernou S., Benslimane S. and Lehireche A. (eds.) *Web and information technologies, 4th International conference ICWIT 2012.*, April 29-30, 2012, Sidi Bel-Abbes, Algeria, IEEE, pp. 232-230.

[15] David B., Manuel C. and Marina E. (2011), 'A Decade of model driven security', in Ruth B., Cramton J. and Lobo J. (eds.) *Access control models and technologies, 16th ACM symposium*, Innsbruck, Austria, June 15-17, 2011, ACM, pp.1-10.

[16] Zhendong M., Wanger C., Woitsch R., Skopik F. and Bleier T. (2013), 'Model-driven security: from Theory to application', *International journal of computer information systems and industrial management applications*, **5(1)**, pp.151-158.

[17] Furukawa Y. (2011), 'Web based control application using web socket', in Robichon M., Cassady C., Finlay C., Graham Y. (eds.) *Accelerator and large experimental physics control systems, International conference, ICALEPCS 2011*, Grenobal , France, Oct-10-14 2011, pp. 673-675.

[18] Zhangling Y and Mao D.(2012), 'A real time group communication architecture based on web socket' *International journal of computer and communication engineering*, **1(4)**, pp. 408-411.

[19] Nora K., Andreas K. (2003), 'Towards a common meta-model for development of web applications', in Lovelle J., Rodriquez B., Aguilar L., Gayo J. and Ruiz M. (eds.) *Web Engineering, 3rd International conference, ICWE 2003*, Oviedo, Spain, July 14-18, 2003, Springer, pp.497.

[20] Sandhu R., Coyne E. Feinstein H. Youman C. (1996), 'Role-based access control', *Journal of IEEE computer*, **29(2)**, pp. 38-47.

[21] Leung M. (2009), 'Depress phishing by CAPTCHA with OTP', in Luk K. (ed.) *Anti-counterfeiting, security and identification in communication, 3rd International conference ASID 2009*, Hong Kong, August 20-22, 2009, IEEE, pp. 187-192.

[22] Graeme B. (2012), 'Strengthening CAPTCHA based web security', *First Monday peer reviewed journal on internet*, **17(2)**, pp. 1-33.