# An Efficient Review and Comparative study of public testing techniques with 3-tier security model as concerns various parameters

Asst.Prof. Ami S. Desai[1], Dr. Raviraj Vaghela[2], Dr. Sanjay Buch[3]
PhD Scholar of RK University,Rajkot[1]
Assistant Professor of Computer Engineering, RK University, Rajkot[2]
Prof. IT & CE Dept., Chhotubhai Gopalbhai Patel Institute of Technology, UTU, Bardoli[3]

*Abstract :* Public methodologies, model, and tools for fusion testing focuses largely on a developer coding level and technical description of the testing process. Unfortunately, there is not appropriate testing mechanism, methodology and model focused on multi stake holder web source to make 100% tested, secure transaction and communications. It often results in a single website situation when the tests are badly planned, managed by multiple-stakeholders, differ from languages/environment and the vulnerabilities found are messily remediated. The goal of this article is to present a new security testing model called 3-Tier security model which is focused mainly on fundamentally and overall testing of multi stakeholder websites. Development of this methodology was based on the comparative analysis of current methodologies, model, and tools on the base of different parameters.

*IndexTerms* – **Vulnerabilities, Multi stakeholders, cybercrime, Security Testing, Testing Methodology, Software Engineering**

## I. INTRODUCTION

The use of web technology is considered to be a bonus in today's era, any age group is surely busy using the technology as we all are reliant on it. They are used to complete and done various tasks in our lives using web. Web technology is implemented in almost all the sectors and sections our lives, let it be business, communication, virtual relationships, purchasing, agriculture, banking[2], to keep check, control, and harness over natural forces, transportation; no matter which industry we deal in technology is used in a certain manner.

Online transaction and communication technology itself is independent and helpful but it is harmful too; people make the selection between many alternatives to use from the service providers that deliver the facilities to exchange ideas, information, videos, pictures, and graphics using multi stakeholder websites [3]. It also allows easy sharing and distribution of existing content to others so that personal information and professional work can be shared through networks.

There are certain issues regarding online swindle, better known as fraud occurs with people like hacking, phishing, theft, stalking, malware attack, child soliciting and abusing etc[5][8]. It is happened because of improper testing or lack of testing methodology or testing tools of websites which are used by users, developer or other. It is the cause of hacking and cybercrime increasing day by day. To resolve the hacking and cybercrime problem proper testing of each and every end of the website is needed. These ends may be handled and manage by single stake holder or multi stakeholder. Testing and hacking problems are more in Multi stakeholder rather than single stakeholder websites. What is lacking in current system? When it occurs? Why this hacking problem increased? This gap analysis identified by survey and practically checking using public tools as well as 3 tier security model used of multi and single stakeholder websites[4]. For searching, the gap of testing problem analysis, survey and literature reviews of related research papers are done it will explain in further section.

## II. RELATED WORK

Here relevant work is explained on the base of paper reviews and survey. Further comparative analysis of current tools with 3-tier security model discuss in next section

### *ACCORDING TO REVIEW OF PAPERS*

On the base of more than 50 research papers different methods and mechanism are findings. According to IT companies of India or out of India, They recognized bugs in browser prevention, online payment and transaction system, online threats, issues & risks, privacy & security issues, testing mechanism, vulnerabilities type & lifecycle, SQL injection, XSS, phishing, Sniffing, performance / load testing, DDOS attacks, mobile crime and so on. As per review all technology checked vulnerability at different ends. Thus, It is summaries in next Figure.

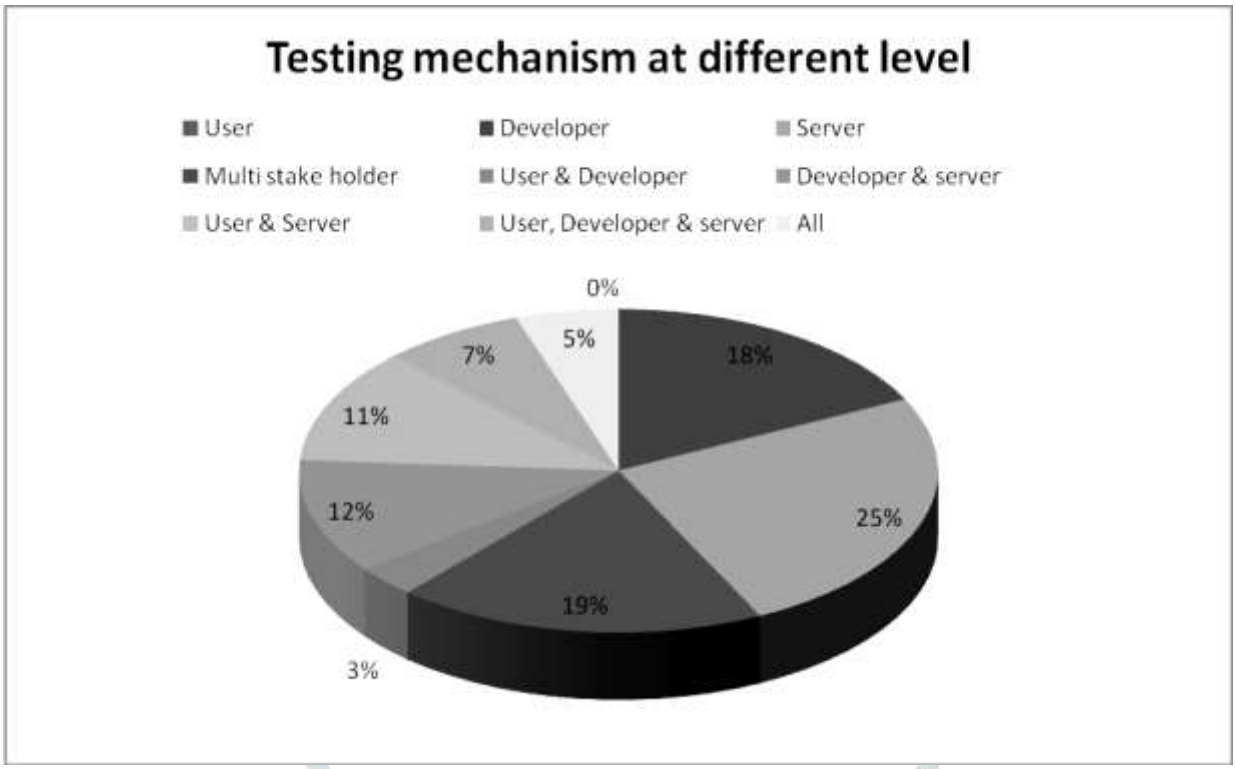


**Fig. 1.** Response for Testing at different level

According to Figure 1, testing is done using many testing methodology, the process model, algorithm or tools. Maximum testing done 25%, 19% and 18% on developer level, server level and user level respectively. Whereas only 3% for multi stakeholders hence 0% for all level. That implies some solution is required to make secure multi stakeholder website. And permanent and fruitful solution need to enhancement at the user end, developer end and server end which nearly equal to fulfilled in the 3 –tier security model.

***ACCORDING TO SURVEY***

As stated in collecting 100 responses, 26 companies have been visited and the individual survey has been taken. These Companies are engaged in the development of websites or web services. Individual surveys are taken from those who are working as a software developer, programmer, tester or team leader etc in IT companies.

In keeping with 100 samples result, 69.5% testing work is done manually using the testing methodology like white box, black box or gray box testing[1] and 28.5% testing is done using various tools, whereas 2% of them perform testing manually as well as using tools[6]. It is more elaborate percentage wise individually with companies and personal responses

Although the survey result states that maximum testing is done manually, but still tools and technologies are requiring or rather lacking. It may be lacking proper testing is not done using currently available testing tools[9].

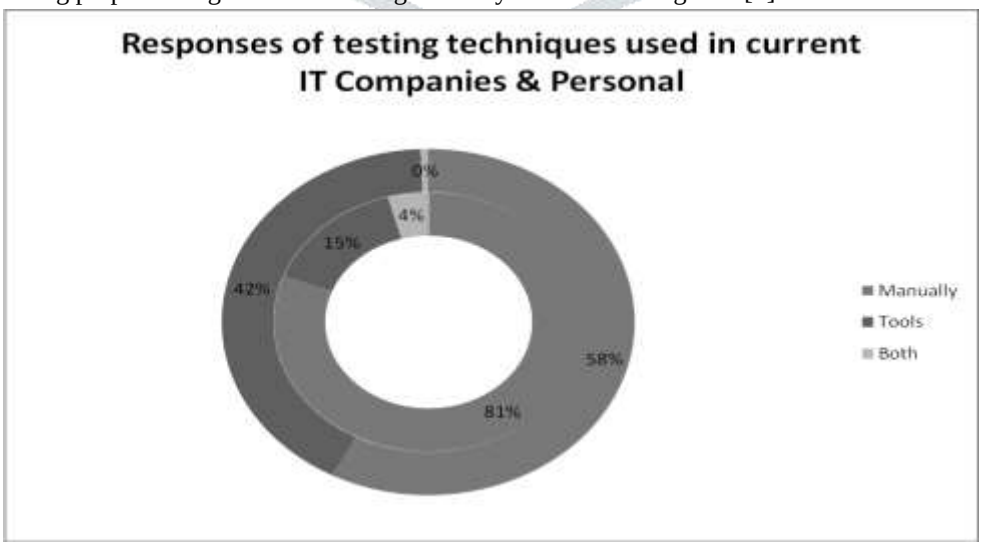


**Fig. 2.** Responses of testing techniques used in current IT companies & Personal

According to the Figure 2, as per companies' responses 81% testing manually testing and 15% using different tools whereas 4% responded that they can do testing manually as well as using tools.

Approximately more than 70 employees responded, from that 58% of employees done testing process manually and 42% using tools. Finally according to, IT companies and personal opinion, currently they used tools for the various testing process like functional testing, requirement testing, validation testing, performance testing, resolution testing, SQL injection testing and so on are categorized as bellowed.

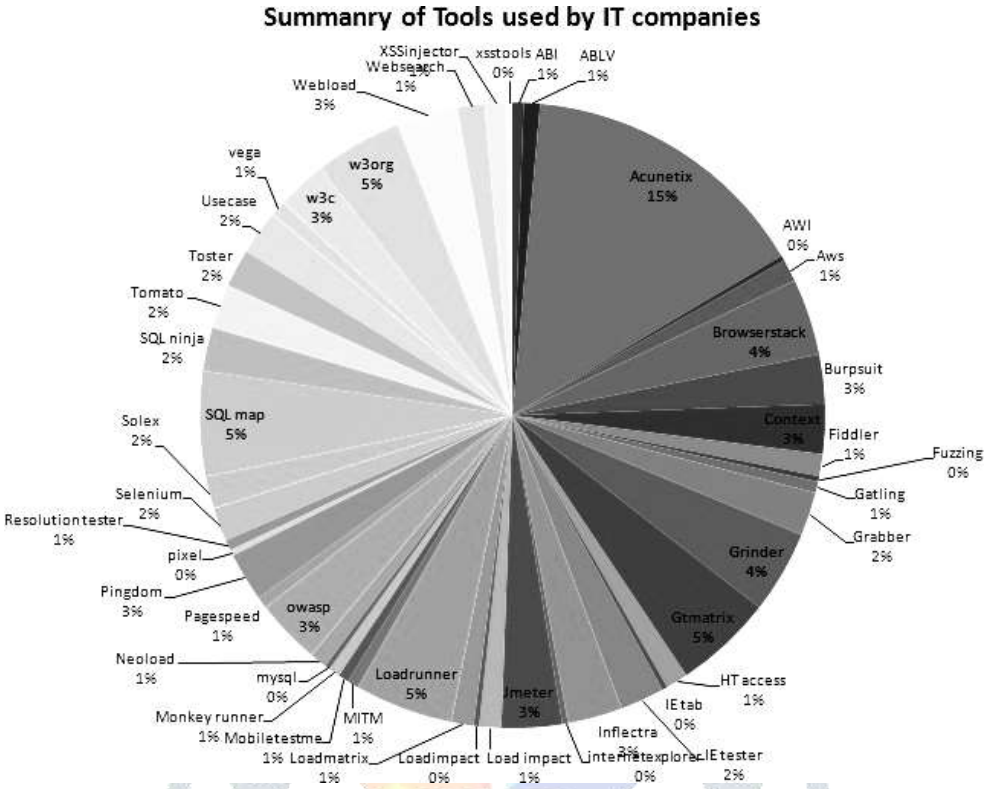


**Fig. 3.** Responses for tools used in current IT companies

According to the response of Figure 3, maximum responded that 15% companies used acunetix. GTmatrix, Sql map, webload, grinder tools are used by companies 5%, 5%, 3%, and 4% respectively.

As stated in the survey, there are many tools available for functional testing, load testing, performance testing, resolution testing, SQL injection, security testing, XSS testing, web service testing, scanning/block open port, sniffing and traceroute. But still, there are several limitations of every tool that implies that it requires the enhancement of security checking mechanism.

## III. METHODOLOGY

As per section II, maximum testing works done manually. There are some testing tools methodology and model available but still some enhancement is needed. The 3-tier security testing model resolves security testing problems. This model checks vulnerability at different ends, which provides user end security checking to prevent user's data at the time of online transactions like encryption, data validation check. 3-tier security model checks security at developer end and makes sure the developer's environment is safe with a secure database and code before uploading any website. 3-tier security model also provides security suggestions and security checking after uploading website. Verification of 3-tier security model tested by many single stakeholders and multi-stakeholders IT companies for security testing of their websites. Based on testing results from comparative analysis reports generates between 3-tier security model with the current testing model, methodology, and tools. Some of them will describe in the next section. It is clear evidence of 3-tier security model give a concept to a resolved security problem.

## IV. COMPARATIVE ANALYSIS AND RESULTS

Several tools name describe with their use in II section. The form that lists out tools trial versions of several tools like quttera, webinspector, sucuri, penetest-tools etc are available so it is selected to generating comparison reports with 3-tier security model. Testing is done and comparison generated on the base of commercial websites which are already uploaded. Some of the Comparison reports of various tools with a 3-tier security model put on view as bellow.

*A. Testing level parameter*

TABLE 1. TESTING LEVEL AT DIFFERENT ENDS VS TOOLS

| Tools name | User end | Developer End | Server End | Multistake Holder |
|---|---|---|---|---|
| Quttera 3.3.2 | 1 | 1 | 0 | 0 |
| Webinspector 0.6.0 | 0 | 1 | 1 | 0 |
| Sucuri 1.8.19 | 1 | 1 | 1 | 0 |
| pentest- Tools | 0 | 1 | 1 | 0 |
| SiteguardinG | 1 | 1 | 0 | 0 |
| Virustotal 2.0 | 0 | 1 | 0 | 0 |
| Foregenix 5.1 | 0 | 1 | 1 | 0 |
| Scanmyserver | 0 | 1 | 1 | 0 |
| QUALYS: Ssllabs 1.3 | 1 | 1 | 1 | 0 |
| Grabber | 1 | 1 | 0 | 0 |
| Acunetix 11 | 1 | 1 | 1 | 0 |
| 3-tier security Model | 1 | 1 | 1 | 1 |

Table-1 shows the comparison of 10 tools Vs 3-tier security model. It shows that the maximum 44% checking by public tools done on developer level than 22% and 30% at the user end and server end. and minimum checking is done on the multistakeholder website. Only 3-tier security checking provide security checking at the multistakeholder end[6] whereas server end checking done minimum by public tools.

Due to this security testing is needed to enhance clients and server end. Server level security scanning is very essential. In case of website publishing, website published on the shared server is may be the next target of the hackers. If the user end security testing is not properly performed, then his/her personal or account information can be misused by cyberpunk[7]

## *A. Reporting & Suggestion parameter*

The table below shows the comparison of public tools with 3-tier security model with other models with respect to suggestion Mechanism. The 3-tier security model not only gives the highest number of suggestions at each stage of software development but it also generates preventative functionality for secure website generation. It also generates the report of suggestions. For other models maximum at three stages the suggestions are generated but in 3-tier security model at all stages of software development, suggestions are provided along with the report.

**TABLE 2.** REPORTING & SUGGESTION MECHANISM AT DIFFERENT ENDS VS TOOLS

[GENERATE – G, NOT GENERATE – NG ]

| Tools Name | Report | Suggestion |
|---|---|---|
| Quttera 3.3.2 | G | G |
| Webinspector 0.6.0 | G | NG |
| Sucuri 1.8.19 | G | NG |
| pentest- Tools | G | NG |
| Siteguarding | G | NG |
| Virustotal 2.0 | NG | NG |
| Foregenix 5.1 | NG | NG |
| Scanmyserver | NG | NG |
| QUALYS: ssllabs 1.3 | G | NG |
| Grabber | G | G |
| Acunetix 11 | NG | G |
| 3-tier security model | G | G |

Table-2 shows the comparison of 10 tools Vs 3-tier security model. It shows that 67% provide report facility, in these reports highlights of the check, is displayed. They do not describe the suggestion mechanism to enhance security. As per that report 89% tools not provide suggestion mechanism by public tools. The 3-tier security model generates report and detail suggestion for enhancing security mechanism.

*B. Cost of Website Vulnerability Scanning*

The table shows the comparison of the cost of Website Vulnerability Scanning of 3-tier security Model with other models. The cost of other tools ranges from $.249 to $9588. Some of the tool's cost change based on the size of website, environment, type of website and requirements. The 3- tier security model can be developed with no cost and 12 Audit features checking facility is provided. That features include user end, developer end, server end and multi-stakeholder end checking, reporting and suggestions also in no costing.

**TABLE 3.** PUBLIC TOOLS VS 3-TIER SECURITY MODEL COST BASE PARAMETER [6]

| Tools name | Scanning Charge per year (in $) |
|---|---|
| Quttera 3.3.2 | 249 |
| Webinspector 0.6.0 | 259.2 |
| Sucuri 1.8.19 | 299.9 |
| pentest- Tools | 950 |
| SiteguardinG | 299.5 |
| Virustotal 2.0 | Not fix |
| Foregenix 5.1 | Not fix |
| Scanmyserver | 359.4 |
| QUALYS: Ssllabs 1.3 | Not fix |
| Grabber | 2064 |
| Acunetix 11 | 120 to 9588 |
| 3-tier security Model | No cost |

By means of comparison analysis A, B, and C, the testing methodology, the process model or tools are lacking behind on various issues like testing of multi-stakeholder websites. Thus a 3-tier security model is a way to overcome security challenges at the user's end, developer's end server's end, and multi-stakeholder end.

## V. FUTURE WORK

Currently the 3-tier security model checked vulnerability of every end for PHP and ASP.net website preliminary. Future work includes extending this approach for any kind of web source with no cost and open source.

## VI. CONCLUSION

The 3-tier security model is designed and developed to make the secure multi-stakeholder website. This model was designed for the management of secure transaction and communications. In any online communications system, user's and developer's data, after published on server end security checking dispute are considered as an indicator of the security loop holes which generate limitation in the system protection and vulnerable to attacks. As per result of survey and research papers, it analyze that a perfect and proper solution is requires for security testing of multi-stakeholder websites. Based on the comparative analysis and reports 3- tier security testing model is useful and fruitful for the multi-stakeholder website for a secure and safe mode to user and developer. This model will reduce testing cost and increase security. It provides suggestion and preventive mechanism for fight with cyber criminal.

## VII. REFERENCES

1. Sultana, s., sadiq, m. And ahmad, w. (2014) 'a tool to automate the test cases of software using gray box testing approach', 3(8), pp. 7689–7695.
2. Darwish, s. M. And hassan, a. M. (2012) 'a model to authenticate requests for online banking transactions', alexandria engineering journal. Faculty of engineering, alexandria university, 51(3), pp. 185–191. Doi: 10.1016/j.aej.2012.02.005.
3. Al-ghamdi, a. S. A.-m. (2013) 'a survey on software security testing techniques', international journal of computer science and telecommunications, 4(4), pp. 14–18.
4. Goel, j. N. And mehtre, b. M. (2015) 'vulnerability assessment & penetration testing as a cyber defence technology', procedia computer science. Elsevier masson sas, 57, pp. 710–715. Doi: 10.1016/j.procs.2015.07.458.
5. Desai, Ami S., Et Al. Need To Enhancement Of Public Testing Approach For Vulnerability Scanning

& Security Testing For Multi-Stakeholder. International Journal Of Creative Research Thoughts, ISSN: 2320-2882, Volume 6, Issue 1, March 2018,265-271.
6. Desai, Ami S., Et Al. Three Tier Security Testing Model Required for a Protective and Suggestive Mechanism for the Multi-Stake Holder. International Journal Of Basic And Advanced Research, Issn 2454-4639(P), 2456-1372 (O) Volume 4, Issue 5, May 2018,124-131.
7. Baby, a. S. Et al. (2013) 'protecting data in multi-stakeholder web service system', ieee communication surveys & tutorials online, 3(3), p. 1163. Doi: 10.1109/comst.2014.2321628.
8. Gunatilaka, d. (2011) 'a survey of privacy and security issues in social networks', proceedings of the 27th ieee international conference on computer communications, pp. 1–12.
9. Mainka, c., somorovsky, j. And schwenk, j. (2012) 'penetration testing tool for web services security', 2012 ieee eighth world congress on services, pp. 163–170. Doi: 10.1109/services.2012.7.