INTRUSION DETECTION ARCHITECTURE FOR DIFFERENT NETWORK ATTACKS

Prerna U. Randive[1], D. P. Gaikwad[2]

[1]*Department of Computer Engineering, AISSMS CoE, Pune,Maharashtra, India*
[2]*Department of Computer Engineering, AISSMS CoE, Pune,Maharashtra, India*

Abstract

Now these days most of the work is carried out by internet. So web application becomes important part of today's life, such as online banking, social networking, online shopping, enabling communication and management of personal information. So web services now have shifted to multi-tier design to accommodate this increase in web application and data complexity. Due to this high use of web application networks attacks increased with malicious purpose. DoubleGuard is an Intrusion Detection System helps to detect and prevent the networks attacks. DoubleGuard is able to find out attacks after checking web and database requests. Along with this, in this paper adding one more level that is admin, it is responsible for the training to the system, log generation, blacklist and employee entry. This IDS system provides security to prevent both the web server and database server.

Key Words: *DoubleGuard; Web Application; Multitier; IDS; Attacks.*

--***--

1. INTRODUCTION

Because of rapid development of internet, use of internet is grown day by day. So popularity and complexity of web services have been rapidly increased around the world. Internet is helped in various daily needs such as online reading newspaper, online banking, social networking, online shopping, and can manage personal information and enabling communication. Such web services are accessed on web to run the application user interface logic at front end and at the backend database server helps to store database or files[13]. Because of the pervasive use of web services, generally they used for storage of personal and corporate data. So it has been targeted for the malicious goal. Due to moving of attention from attacking to front-end to take advantage of vulnerabilities of the web application to violet the back-end database system by the help of SQL injection. So the security of web application can only be gained through the best design of web application. To build system secure, it makes use of many preventing system such as Intrusion Detection System and Firewall.

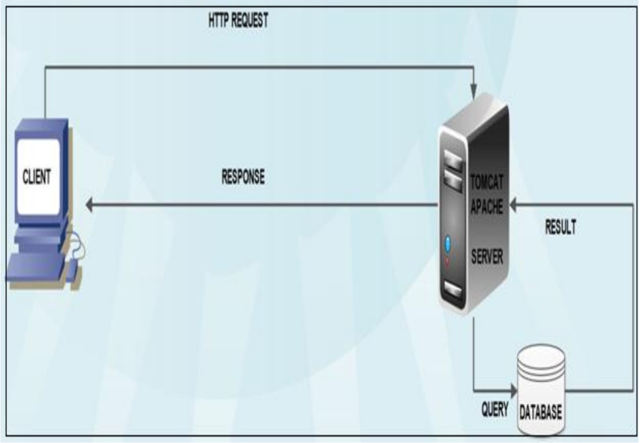


Fig. 1. Client Server Architecture

In above figure, Client sends request to server for getting response. After getting request, server produces responses by the help of database and generate responses depends on requests. So, attacker target front end and the back end for malicious purpose.

1.1 Intrusion Detection System

Intrusion Detection System (IDS) is a system developed to detect attacks against computer systems, networks and information system. It also alerts the to the web application for any kind of malicious activity.

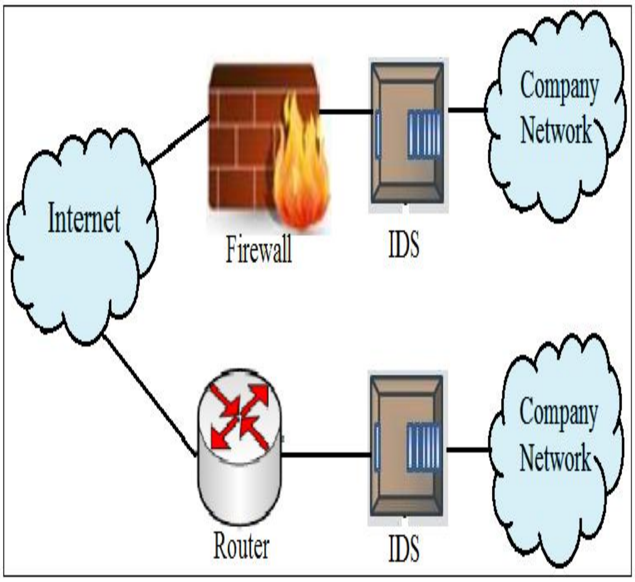


Fig. 2. Simple Intrusion Detection System

Intrusion detection system is used as a software or hardware device to prevent from malicious activity. [12] It is mostly helps to detect known attacks by looking two things that is matching misused traffic patterns or signatures. By using machine learning, IDS can also detect unknown attacks. During the training phase abnormal network traffic can be identified. When attacker makes use of abnormal traffic for the attacking purpose then the web IDS and the database IDS both can individually detect abnormal network traffic. In the normal traffic case, when attacker makes use of normal traffic for the attacking purpose, it targets the web server and the database server. Those kinds of attack cannot detect by the IDS. The work of the web IDS is to see typical user login traffic and the database IDS only see normal traffic of a privileged user. If database IDS can detect that a privileged request from the web server is not associated with user privileged access, then this kind of attack can be easily identified by IDS. Following are some of the benefits to effectiveness in intrusion detection system.

1.1.1 Benefits of Intrusion Detection System:

Accuracy of attack detection: Accuracy of intrusion detection system is depending on identification of attack and it is based on mismatch types and signature. In multi-tier web application, it uses IDS and database IDS to find out such attacks.

It is easy to deploy: Intrusion Detection System is easier to deploy due to it does not affect existing system or infrastructure.

Timeliness of attack detection: IDS performs its analysis of server as early as possible, so that security officer can take action before more damage has been happened. It can be also prevent attacker from defeating the audit source and IDS itself.
Performance of IDS: The performance of IDS is depends upon the rate at which audit events are processed. If performance is well then it can also be used to find out real-time attacks.

1.2 Attack Scenarios

There are different kinds of attacks on web server and database server; this approach can capture the following attacks.

1.2.1 SQL Injection Attacks: These types of attack do not happened on web server, attacker use weak points in web server logic to inject the back-end database. This SQL injection attacks can gives unauthorized access to database. Attacker gives input which consists of malicious code that included in to the query. Further that query is treated like input, by this attack attacker can modify or extract information from database. There are various kinds of SQL injection attack is as follows:

[1]. Tautology Attack: In such tautology attacks, Attacker use one or more conditional statements by injecting SQL queries so that it evaluated to true and then it shows 1. In this type of attack, attacker exploits the WHERE clause fields, such field that can be inject-able.

[2]. “SELECT * FROM empInfo WHERE empid = ’prerna’ OR 1=1”

[3]. In the example, code is injected at WHERE clause and it retrieves the results because of the WHERE clause is always true. If attacker succeeds in it, all records of database table will return. This is one of the simplest attack among all attacks.

[4]. Union Queries: By making use of tautology attack, attacker can bypass the authentication pages, but it does not allow to attacker to extract information from database. In such kind of attack, attacker uses unprotected parameter for formation of injected query and then joins the injected query to original query with the word “UNION”.

[5]. “SELECT username FROM empInfo WHERE empid= ‘ ‘ UNION SELECT password FROM empInfo ”

[6]. Final data retrieved will be union of both results.

[7]. Piggybacked Querie: It is one of the harmful attack. Attacker does not change the original query like the UNION query; attacker attaches more additional injected queries with the original query i.e piggybacked on the original query. The original proper query executes normally but the other afterwords queries are injected queries.

[8]. “ SELECT name FROM empInfo WHERE userid=’prerna’AND passsword=’ ’; drop table emp – AND pin=’123’ ”

[9]. The queries are separated by the delimiter (‘;’) and both the queries are executed. The query before delimiter is original query and the query after delimiter is injected query. In database the loan table is dropped by injected query. So the data from that table is deleted.

[10]. Alternate Encoding: Special characters are used as input by different attackers to attack on the web application. To avoid such attacks few prevention techniques are used to block these inputs. The alternate encoding technique provides provision to attacker to change the injected string so that the filter based and signature based checks are avoided. The attacker can caught in simple scan of query to avoid this he can use encoding techniques such as Unicode, ASCII and Hexadecimal. These encoding techniques can be used in simultaneity with other techniques.

1.2.2 Denial of Service Attacks: The denial of service attacks, which is predetermined one. It attempts to halt legitimate users from accessing a specific network resource.

2. LITERATURE SURVEY

There are some techniques helps to detect and prevent from vulnerabilities and malicious activity. From such techniques web application program can improve them to reduce vulnerability and malicious activity. Some techniques are described below.

DoubleGuard [1], is one kind of intrusion detection system. DoubleGuard composes container-based IDS with the multiple input streams for alert creation and generation. It is happened by monitoring web and consequent database requests, it can find out attacks. Using DoubleGuard, it can be expose and detect wide range of multiple attacks with 100 percent accuracy. A.S. Gadgikar has mentioned negative tainting approach [2]. It is helped to prevention from SQL injection attacks without change in existing code. It can used to reduce time and space complexity. This technique includes detection of weak spot from web application, further it inserts the newly identified SQL injection attacks to improve the accuracy of the system. Other technique like Swaddler: An Approach [3] is used to detection of attacks against web applications, which are depend upon the analysis of the internal application state. In web application, Swaddler firstly models values of session variables in association with the critical execution points. Authors also mentioned novel detection model which relies on multi variable invariants to detect web-based attacks. Attack identification is made by leveraging the internal that is hidden state of a web application

.

Nidhi Srivastav et.al mentioned Novel Intrusion Detection System [5]. In this paper, they have presented layered framework integrated with neural network. This system has evaluated with Knowledge Discovery & Data Mining 1999 dataset. The built system has much high attack detection accuracy and less false alarm rate. Evaluation of Web Security Mechanisms [6] suggested by José Fonseca.al e. Authors suggested a technique and the prototype tool to evaluate web application for security mechanisms. Authors also present implementation of Vulnerability & Attack Injector Tool (VAIT) that permits the automation of whole process. This tool is performed to run the group of experiments that demonstrate the feasibility and effectiveness of the suggested technique. The injection of the vulnerabilities and attacks is the good way to compute the security mechanisms and to point out both their weakness and improvement. Another technique like TDFA [7], is having of three main components that are Detection, Traceback, and Traffic Control. In this method, the purpose is to keep packet filtering as near to the attack source. By doing this, the traffic control component at the victim side aims to put up limit on packet forwarding rate to victim. This kind of technique used to reduce the rate of forwarding the attack packets and thus improves the throughput of legitimate traffic.

3. PROPOSED ARCHITECTURE

The main aim is efficiently detection of intrusion to protect multi-tier web application. The objective is to prevent and detect attacks by using Artificial Neural Network and adds one more level that maintains log. In this way, some modification will be do in existing DoubleGuard to increase its reliability, performance in case of static and dynamic web sites both.

As shown in fig. 3, firstly client sends request to the server and waits for the response from server. At the server side server firstly accept the request and process that request. For this request, server arranges particular session for each client and it process that session. If it consists of malicious content in the request then server deny that request. Such kind of attack is Distributed Denial of Service attack (DDoS) attack. This generally happened on the web server. (DDoS) occurs when large numbers of compromised systems attack a single machine. Due to the effect of DDoS attack, network resources are being unavailable to its intended users.

Further, at the back-end, user makes request in the form of SQL query, if it is safe then it processes query. If the query consisting of malicious contents then it deny that query. Because this is SQL injection attacks. Such kind of attack happened on the database server. From this attack, attacker can modify database, can extract information from database. If the query is safe then it connects to the database and generates the result with the help of the database server and gives feedback to the client as the response.

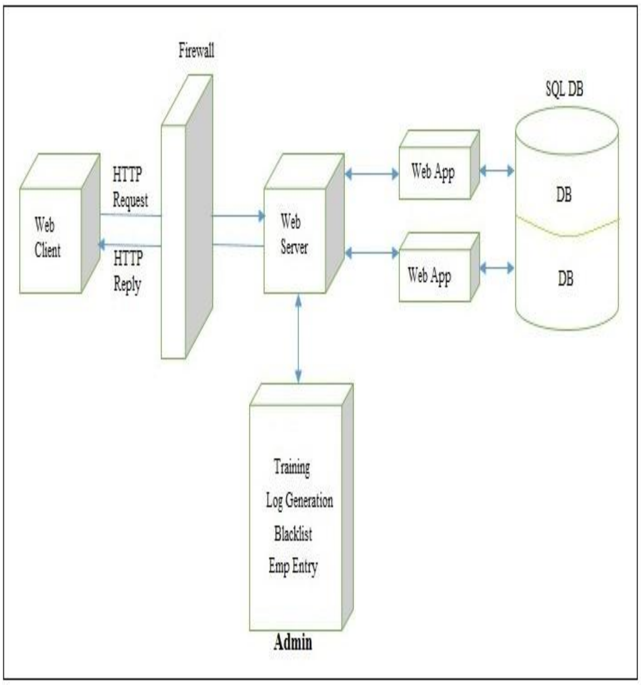


Fig. 3. Proposed Architecture

Along with the detection and prevention from attack, proposed system architecture consists of admin log at server side. Admin is responsible for the training to the system, log generation, blacklist and employee entry. Admin can add any number of employee details in the employee list, the log consist of different parameters that keep information regarding attacks, IP address of attacker system, time of the request and difference of request. By keeping this information it can blacklist that particular request and machine also. So this log is very helpful to maintain history. Further, attacker cannot send any type of request with same system to the web server or database server. Admin has rights to train the system with the Artificial Neural Network. He can train system at any number of time. ANN for training to the system and K-means is for clustering of request difference. Depend on the difference between two subsequent request times it shows which is DDoS attack and normal one. It is done by the clustering of all request time. Finally it will able to expose or detect a wide range of multiple attacks with high accuracy.

Artificial Neural Network

1. First apply the inputs to the network and works out the output remember this initial output could be anything, random numbers were initial weights.

2. Next work out the error for neuron B. The error is what you want what you get, in other format,

$\text{Error}_B = \text{Output}_B\ (1 - \text{Output}_B)\ (\text{Target}_B\text{Output}_B)$

3.Let W^{+}_{AB} be changed new (trained) weight and W_{AB} be initial weight.

$W^{+}_{AB} = W_{AB} + (\text{Error}_B \text{ x Output}_A)$

4. Evaluate the Errors for hidden layer neurons. Unlike output layer, cannot evaluate these directly, so we Back Propagate them from output layer. This is done by taking the Errors from the output Neurons and to get the hidden layer errors running them back via the weights.

$\text{Error}_A = \text{Output}_A(1 - \text{Output}_A)(\text{Error}_B W_{AB} + \text{Error}_C W_{AC})$

5. Having obtained the Error for the hidden layer neurons now

proceed as in stage 3 to change the hidden layer weights. By repeating such method, can train a network of any number of

layers.

K-means algorithm:

Let X = {x1, x2 x3…….xn} be set of data points and V = {v1, v2, v3 …vc} be set of centers.

1. Randomly select centers of clusters as 'c'.
2. Evaluate the distance between each data point and cluster centers.
3. Give data point to cluster center who are nearer to all the cluster.
4. Recalculate the cluster center using,

$$v_i = \left(\frac{1}{C_i}\right) + \sum_{j=1}^{C_i}(x_i)$$

Where, Ci denotes number of data points in ith cluster.

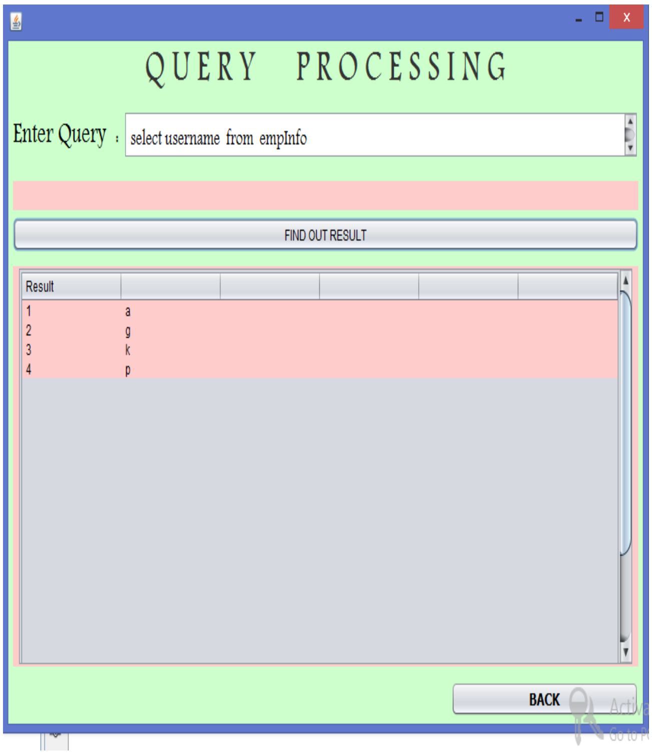
5. Re-evaluate the distance between each data point and new generated cluster centers.
6. If there is no data point was reassigned then end the process, otherwise continue from step 3.

4. RESULTS

We will apply different possible attacks on IDS, which are mentioned in introduction section. This is expected that our IDS will be able to detect front-end attack that is DDos attack and back-end attack that is SQL injection attacks. Along with this, admin, it is responsible for the training to the system, log generation; blacklist and employee entry. Admin's blacklist will block the malicious request of the attacker system. Further no any request of attacker will accepted by server.

In the client Module, Client can establish connection with particular server by entering IP address of server in the field. This module also consists of help and information about project. After establishing connection client can generate request in the form of SQL query. If it is safe query server generate response and client get results in the form of database. And if query consist of malicious code then server generate response as the no result found. this kind of attack is called as SQL injection attack. This kind of attack is happened

only at the back-end side. DDOS attack is done at front-end side by making resource unavailable to the user. Such kind of attack is called DDOS attack.

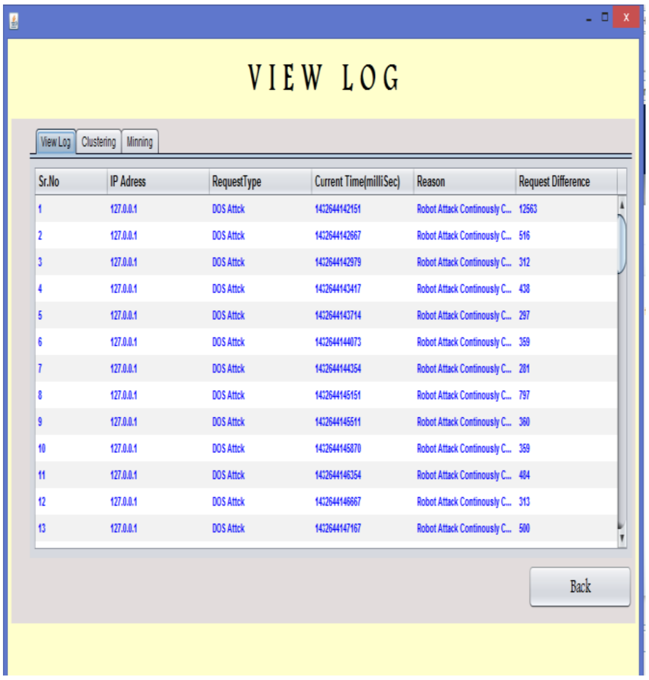


Enter Query : select username from empInfo

Result	
1	a
2	g
3	k
4	p

Fig. 4. Client Module

In this admin module it consists of blacklist, log, bar graph and employee management as shown in following figure.



Sr.No	IP Adress	RequestType	Current Time(milliSec)	Reason	Request Difference
1	127.0.0.1	DOS Attck	1432644142151	Robot Attack Continously C...	12563
2	127.0.0.1	DOS Attck	1432644142667	Robot Attack Continously C...	516
3	127.0.0.1	DOS Attck	1432644142979	Robot Attack Continously C...	312
4	127.0.0.1	DOS Attck	1432644143417	Robot Attack Continously C...	438
5	127.0.0.1	DOS Attck	1432644143714	Robot Attack Continously C...	297
6	127.0.0.1	DOS Attck	1432644144073	Robot Attack Continously C...	359
7	127.0.0.1	DOS Attck	1432644144354	Robot Attack Continously C...	281
8	127.0.0.1	DOS Attck	1432644145151	Robot Attack Continously C...	797
9	127.0.0.1	DOS Attck	1432644145511	Robot Attack Continously C...	360
10	127.0.0.1	DOS Attck	1432644145870	Robot Attack Continously C...	359
11	127.0.0.1	DOS Attck	1432644146354	Robot Attack Continously C...	484
12	127.0.0.1	DOS Attck	1432644146667	Robot Attack Continously C...	313
13	127.0.0.1	DOS Attck	1432644147167	Robot Attack Continously C...	500

Fig. 5. Admin Log

The log consist of difference of two request from this it concludes that it is normal user or robot attack. After of generation of request difference it clusters the request time. In this project it is making two clusters. The first one is for normal user and second is for the robot attack. By the time difference between two request it separate the request time in two clusters. from this clustering mining is done.

The results are shown by using the bar graph. The following figure shows attack analysis. In this it consist of number of request and attack types.

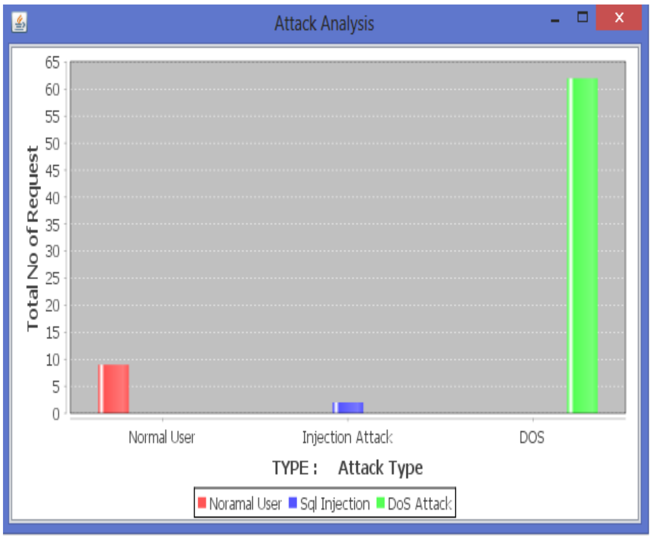


Fig.6. Bar Graph

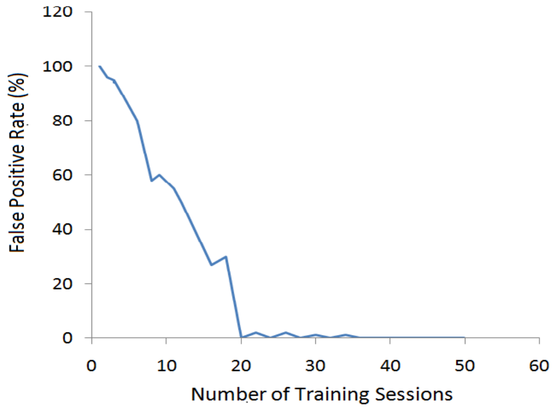


Fig.7. False Positives vs. Training Time in Static Website

As shown in above figure, it shows the training process. As the number of training session increased the rate of false positive is decreased. Which means that model became more accurate. After more training session the false positive rate decreased and finally it stayed at 0.

5. RESULTS

The presented intrusion detection system has invents models of normal behavior for the multi-tier web applications from front-end web request and back-end query. So this approach produces a container based intrusion detection system by using multiple input streams for making alerts. For the reason wider range of attacks can be discovered by intrusion detection system. Along with this admin is responsible for the training to the system, log generation, blacklist and employee entry. The log used to blacklist the malicious request. Due to this log the upcoming request from attacker system get stopped. So, such Intrusion Detection System is able to detect the wide range of various many attacks with minimal false positive. The number of false positives relies on size and coverage of training sessions took place.

REFERENCES

[1] Meixing Le, Angelos Stavrou, and Brent ByungHoon Kang, “DoubleGuard: Detecting Intrusions in Multitier Web Applications,” IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 4, July/August 2012.

[2] A.S. Gadgikar, “Preventing SQL Injection Attacks Using Negative Tainting Approach,” 2013 IEEE International Conference on Computational Intelligence and Computing Research, 978-1-4799-1597-2/13/$31.00 ©2013 IEEE.

[3] Marco Cova, Davide Balzarotti, Viktoria Felmetsger, and Giovanni Vigna, “Swaddler: An Approach for the Anomaly-based Detection of State Violations in Web Applications”.

[4] Mihai Christodorescu Somesh Jha, “Static Analysis of Executables to Detect Malicious Patterns”.

[5] Nidhi Srivastav, Rama Krishna Challa, “Novel Intrusion Detection System integrating Layered Framework with Neural Network,” 2013 3rd IEEE International Advance Computing Conference (IACC), 978-1-4673-4529-3/12/$31.00_c 2012 IEEE.

[6] Jose Fonseca, Marco Vieira, Henrique Madeira, “Evaluation of Web Security Mechanisms using Vulnerability & Attack Injection,” IEEE Transactions on Dependable and Secure Computing.

[7] Vahid Aghaei Foroushani A. Nur Zincir-Heywood, “TDFA: Traceback-based Defense against DDoS Flooding Attacks,” 2014 IEEE 28th International Conference on Advanced Information Networking and Applications.

[8] H. Debar, M. Dacier, and A. Wespi, “Towards Taxonomy of Intrusion-Detection Systems,” Computer Networks, vol. 31, no. 9, pp. 805-822, 1999.

[9] Muthu Kumara Raja, Bala Sujitha.T.V, “Intrusion Detection System in Web Services,” International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 2, February 2013.

[10] Lwin Khin Shar, Hee Beng Kuan Tan, “Defeating SQL Injection,” Published by the IEEE Computer Society.

[11] Narmadha.S, Deepak Lakshmi Narashima, “Multilayer Intrusion Detection System in Web Application Based Services,” Narmadha.S et al. / International Journal of Engineering and Technology (IJET), Vol 5 No 2 Apr-May 2013.

[12] K.Karthika, K.Sripriyadevi, “To Detect Intrusions in Multitier Web Applications by using Double Guard Approach,” International Journal of Scientific & Engineering Research Volume 4, Issue 1, January-2013 ISSN 2229-5518.

[13] Bogadhi Swetha, A .Kalyan Kumar, “Detection of Intrusion in Multitier Web Application: A Perspective View,” International Journal of Computers Electrical and Advanced Communications Engineering Vol.1 (3), ISSN: 2250-3129.