ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 2; Issue 7; Page No. 07-14

# A Survey on Intrusion Detection in Multitier Web Applications Using DoubleGuard

**Neha A. Mohadikar [1], Prof. M. V. Nimbalkar[2], Prof. S. A. Mane[3]**

[1]Research Scholar, Department of IT, Sinhgad College of Engineering, Pune, Maharashtra, India

[2]Associate Professor, Department of IT, Sinhgad College of Engineering, Pune, Maharashtra, India

[3]Assistant Professor, Department of IT, Sinhgad College of Engineering, Pune, Maharashtra, India

*nehamohadikar103@email.com*

**ABSTRACT**

The use of internet services & its applications in daily life are increase in large amount. This enables the communication and management of personal information. This results the increase in applications & data complexity. So web services run toward the multi-tiered design in which web server act as front end and data server or file server act as back end. There are risks of personal data gets hacked hence it need to provide more security to both web server and database server. This paper provides survey of several methods for intrusion detection. From all these methods, doubleguard intrusion detection system is more efficient for detecting and preventing attacks. Doubleguard,an IDS system which models network performance of user sessions across both front-end web server and back end database server. The system quantifies the detection accuracy when system attempt to model static and dynamic web requests. Proposed system built a well-correlated model for static websites and detects and prevents different types of attacks.

**Key Words:** Multitier Web Application, Intrusion Detection System, Anomaly Detection, Static website, Attacks.

## INTRODUCTION:

From past few years web delivered services and their applications have increased in both popularity and data complexity. We used web services and applications in the various fields like banking, shopping, travelling. Large amounts of data are stored in the databases of the web portals [1]. Since most of the web application is largely open, it is very easy to find security loopholes and turned as insecure web applications into potential victims for exploitation using various attacks.

Nowadays due to increase in web application and complexity, web services have moved to a multi-tiered design where the web server runs the web application at front-end and data is outsourced to a database server. To protect multitier web services, Intrusion detection systems (IDS) have been broadly used to detect different types of attacks by matching pervert traffic patterns or signatures. An IDS consists of a set of tools that can be used to detect and prevent attempts of intrusion [3].

Web IDS and database IDS can be able to detect unusual network traffic individually sent to either of them. But these IDS cannot detect the cases in which normal traffic is used to attack the webserver and the database server. Unfortunately, within the present multithreaded webserver architecture, it is not feasible to detect or contour such causal mapping between webserver traffic and DB server traffic because traffic cannot be clearly recognized to user sessions.

In this paper, Doubleguard is presented. It is a system that is used to detect attacks in multitier web services [1]. This approach models the network behavior of user sessions across both the front-end web server and the back-end database. It supervises both web requests, and finds out attacks that independent IDS would not be able to identify. For that, it uses a lightweight virtualization technique. In this technique, a dedicated container is assigned to each user's session. This can be present at virtual computing environment and can be isolated. The Container ID is used to accurately associate the web request with various database queries. Hence, Doubleguard system builds a causal mapping relationship by considering both web server and database traffic.

## 1. LITERATURE SURVEY:

### A. Introduction of IDS System

An essential part of our day-to-day life is Information Technology. Various web services and applications work on front end and back end server. Front end consist of application user interface logic back end server consist of

database for particular user data. All the vital information is stored on database server so attacker shifted their focus from front end to back end.

To detect the known attacks in the misuse traffic patterns or signatures, IDS system is a software application that supervises the system activities and finds malicious activities and produces alerts. It detects unknown attacks by identifying the unusual behavior of the network traffic action from previous behavior of IDS training phase. The attackers abnormal network traffic can be detected by database and web IDS. It stops the attacker to enter within the server. But when attacker used the normal traffic to attack on the web server and data server then this type of attack is unable to detect by IDS [4]. Figure 1 shows basic IDS system.

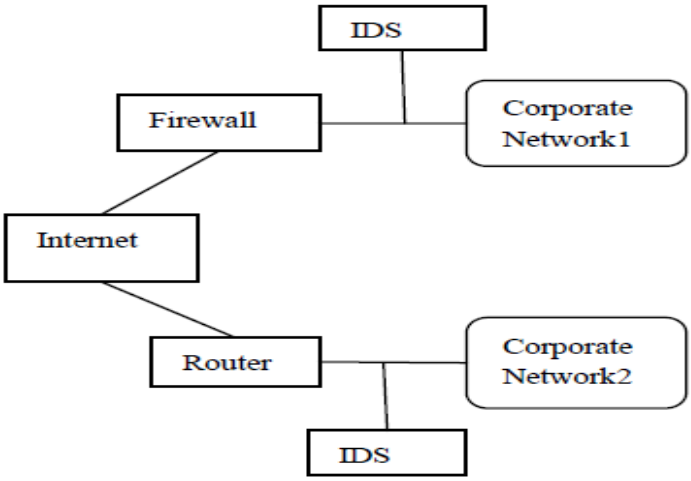


**Figure 1: IDS System**

Consider an example, an attacker can log into web server with non admin privilege using normal user access credentials he or she can find the path true issue privilege database query in the web server by exploiting vulnerabilities in that server. Only web IDS but also database IDS would not detect this type of attack detect. In such type of attack web IDS see the typical user login and the database IDS see the normal traffic of a privileged user. So, within the current multitier web application it is not possible to detect such causal mapping between web server and database server traffic [4].

There are two approaches for intrusion detection. Signature based IDS works as similar as anti-virus software. It put to use a signature database of well-known attacks and a successful match with current input hold up an alert. Signature-based IDSs fails to detect unknown attacks, as similar to antivirus software which cannot identify unknown viruses. Researchers have been developing anomaly-based IDSs to overcome this limitation. An Anomaly-Based Intrusion Detection System is a system which detects computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. It works by building a model of normal data or usage patterns, and then it compares the current input with the model. A compelling difference is marked as an anomaly [4].

The efficiency of IDS can be measure using following:

**A.** Completeness-If IDS is not able to detect attack then there is no completeness in the system the attack detection is not easy task because it is not possible to have a global knowledge about all the attacks [5].

**B.** Performance-The quality of system depends on it performances. The real time attack detection is not possible, if the performance of IDS is poor [5].

**C.** Accuracy-An IDS system signals that an abnormal action is taken in the given environment then in accuracy may be occurring [5].

**B. Multitier Web Architecture**

IDS systems have been widely used in order to protect multi-tier web services. Multi-tier web architecture often referred to as n-tier architecture. In figure 2, at the database side, we cannot able to tell which transaction corresponds to which client request. Also, the communication between the web server and the database server is not separated and we cannot understand the relationships among them [1].

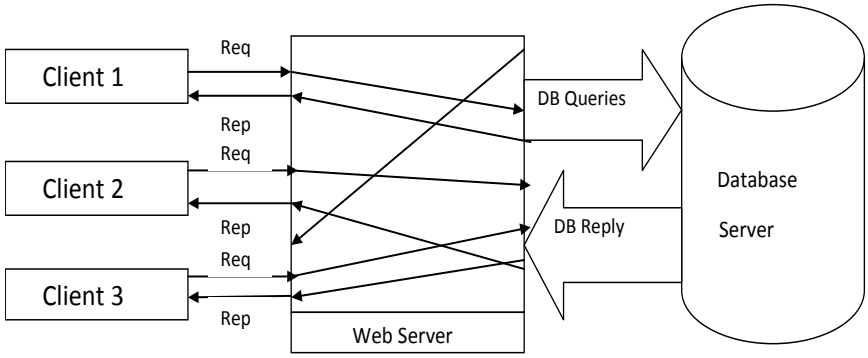


**Figure 2: Classic three-tier Architecture**

In multitier web architecture, firewall is used to protect the back-end database at behind and web application made it possible for user to access set of services from web servers which are remotely accessible over the Internet .The current IDS system installed at web server and at database server are unable to detect intrusions where a normal traffic is used for attacking back end database. It is also found that these IDS cannot detect cases wherein normal traffic is used to attack the web server and the database server. IDS are protected from direct remote attacks; but then also the back-end systems are vulnerable to attacks that use web requests as a means to exploit the back-end [3].

The doubleguard system uses a new container-based web server architecture that enables us to separate different information flows by each session. It track the information flows to database server. The main purpose of double guard system is to model the mapping patterns between database queries and http requests to detect malicious user sessions.

## 2. INTRUSION DETECTION APPROACHES:

We summarize different approaches used by intrusion detection systems to detect an intrusion.

### A. Rule Based Systems

Martin [7] proposed a open source IDP (intrusion detection and prevention) system. This is based on rules. It identifies different attacks on the basis of rules. Also it identifies the characteristics such as behavior, content that different from normal data. Signature is nothing but the combination of these characteristics and it becomes important database part of attack signatures. If the IDS found data matching the signature it gives an alarm. This approach is that which combine the advantages of signature and protocol and anomaly based detection. Disadvantages of this approach are that it requires training to learn rules that the normal behavior of a system is captured. If it is not matching with any such rule it is considered as an attack.

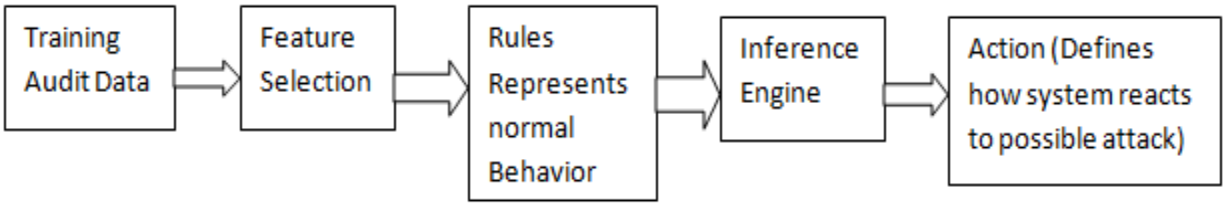


**Figure 3: Rule Based Intrusion Detection Approach**

### B. SWADDLER

M Cova, D Balzarotti and Giovanni [8] proposed an approach which is consist of characterization of the different internal state of a web application, by means of a number of anomaly model detection. In web application the state is defined as information of single client and server interaction or simply the information associated with single user session. The session ID should be passed between the browser and the server to notify the rest of the state data. The advantage of this is that it keeps track of all states to detect intrusion. System operates in two modes Training and Detection. In the training phase the profiles are formed with the help of events and using sensors events are generated. In detection phase these profiles are used to detect the anomalous application states with the help of profile. Major advantage here is that there are attacks that can't be detected only by observing the external behavior of web application. In this approach detection of attacks which gives an inconsistent exceptional state.

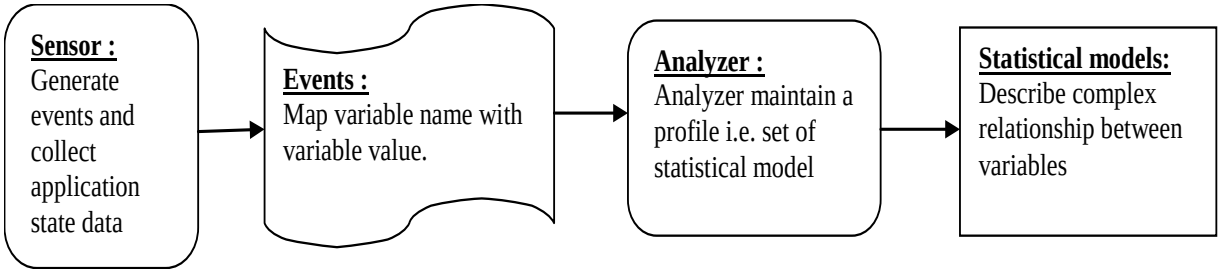


**Figure 4: Profile Creation Phase in SWADDLER**

**C. Combined Approach for Analysis of Web Request and Database Request**

Giovanni Vigna, Fredrik Valeur, Davide Balzarotti, William Robertson [9] proposed a system for anomaly detection which is composed of web-based anomaly detector, a reverse HTTP proxy, and a SQL query anomaly detector. IDS is implemented at both at web server and database server. It allows the system to detect malicious requests which are mistakenly considered as normal behavior. Also when this type of query is detected with the normal web request a description of anomaly is sent to the webserver of anomaly detection system in order to update the system accordingly. The web request which is mistakenly treated as anomalous is simply send to the webserver. If the web request does not require to access the sensitive data that request will be correctly served. Hence the system provides less service in false positive level.

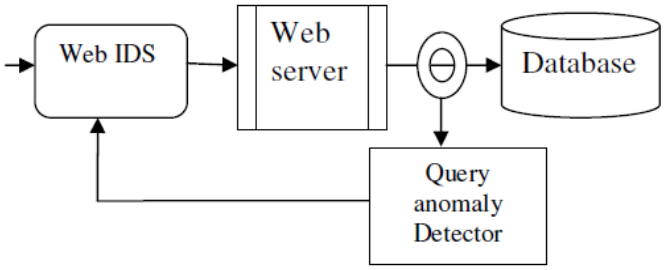


**Figure 5: Combined analysis web request and database request.**

Figure 5 shows combined analysis of web request and database request. The disadvantage of this approach is that it cannot detect attack where normal web requests are used as means to exploit back end database.

**D. Histogram-Based Traffic Anomaly Detection**

Andreas Kind, Marc Ph. Stoecklin, and Xenofontas Dimitropoulos [10] described a new approach in which we simulate different traffic feature with the help of histogram. This system model out histogram patterns, and identifies deviations from the created models. Figure 6 shows histogram based traffic anomaly detection.

The real world network traffic data is collected and depending upon number of detected anomalies'. It identifies and quantifying those how two histograms is similar. Number of approaches can be used to quantify how similar histograms. To identifying and patterns of normal behavior we require clustering. It then distinguishes the clusters that correspond to behavior like normal and anomalous. Different set of clusters that model the normal behavior of a network. Every feature the anomaly detection system computes a vector. This vector encodes the network behavior. Here if the vector falls within the scope of clusters, then the network behavior is considered normal, otherwise it is considered as abnormal.

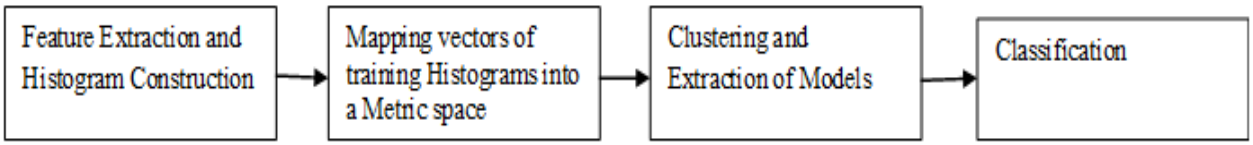


**Figure 6: Histogram-based traffic anomaly detection**

**E. DOUBLEGUARD**

The limitations of all above discussed approach are considerably removed by this approach where normal traffic is used as means to exploit back end database systems.

Meixing Le, Angelos Stavrou, Brent ByungHoon Kang [1] proposed a new approach called Doubleguard system in figure 7 to detect intrusions in multitier web applications. This approach assumes that there is causal mapping of web requests and resulting SQL queries in a given session. Modeled attack can be readily detected if the database IDS can determine that a privileged request from the web server is not associated with user-privileged access. And the entire approach of Doubleguard is based upon the mapping model which maps the web request along with set of resultant query invoked by that request within an individual session. The mapping model it can be used to detect abnormal behaviors. Both the web request and the database Queries within each session should be in accordance with the model. If there exists any request or query that violates the normality model within a session, then the session will be treated as a possible attack.

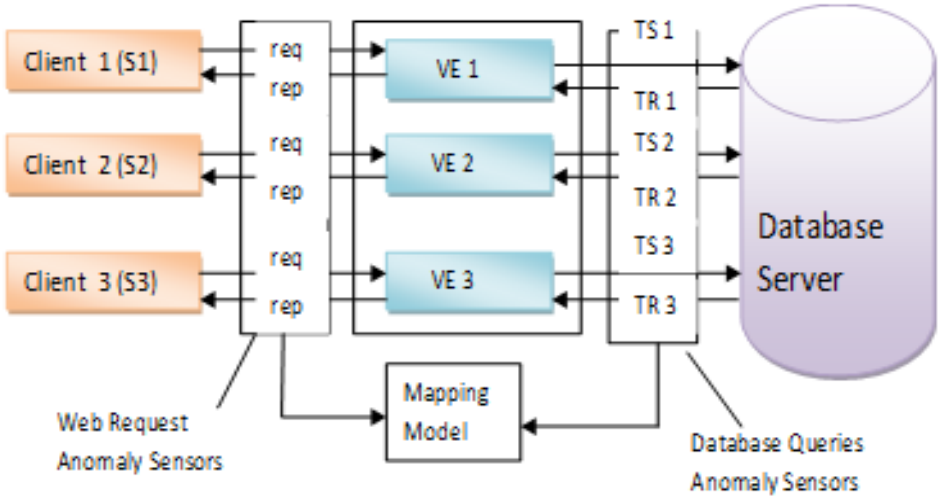


**Figure 7: Doubleguard System**

**3. ATTACK OVER THE WEB:**

The Doubleguard system is effectual at capturing the following types of attacks:

**A.** Injection Attack

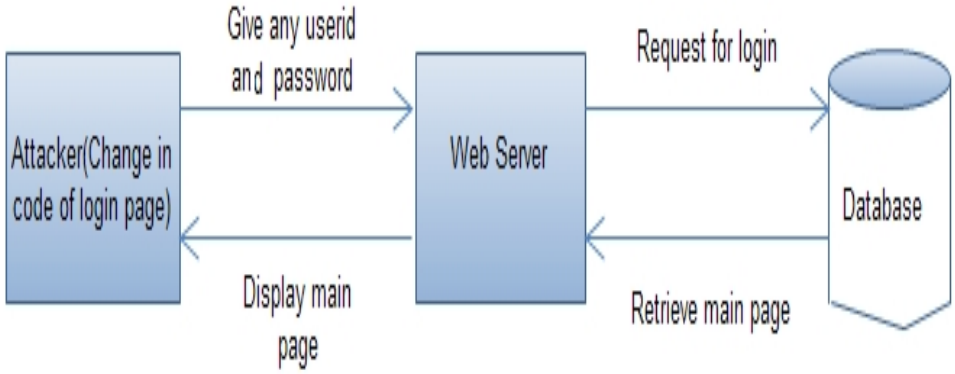


**Figure 8: SQL Injection Attack**

In figure 8, attackers can use accessible vulnerabilities in the web server logic to infuse the data or string that contains the abuse and then use the web server to relay these exploits to attack the back-end database. Attacker enter particular line (' OR 1 = 1; --) into user name and enter any password he/she login into account and access system as authorized user. Since the SQL injection attack modifies the SQL queries structure, it would generate SQL queries in a structure that could be noticed as a deviation from the SQL query structure [11].

**B.** Privilege Escalation Attack

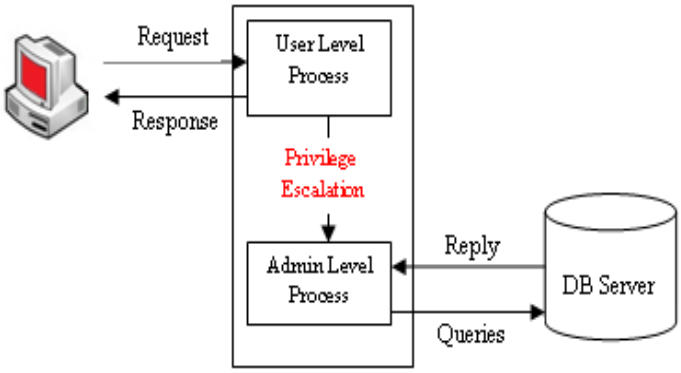


**Figure 9: Privilege Escalation Attack**

For a normal user, the web request $r_u$ will prompt the set of SQL queries $Q_u$; for an administrator, the request $r_a$ will activate the set of admin level queries $Q_a$. Assume that an attacker logs into the web server as a normal user, improves their privileges, and triggers admin queries as a result to obtain an administrator's data. This attack cannot be detected by either the web server IDS or the database IDS because both $r_u$ and $Q_a$ are authentic requests and queries. This approach, can detect this type of attack in view of the fact that the DB query $Q_a$ does not match the request $r_u$, according to the mapping pattern [3].

**C.** Direct DB Attack

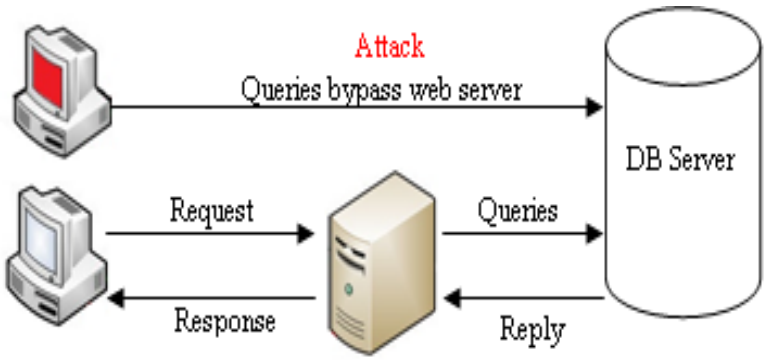


**Figure 10: Direct DB Attack**

It is possible for an attacker to bypass the web server and connect directly to the database as shown in figure 10. An attacker takes over the web server and submitting queries from the web server without sending web requests [3].

**D.** Hijack Future Session Attack

This attack is mainly aimed at the web server side shown in figure 11. An attacker will usually grab the web server and then hijacks all subsequent valid user sessions to initiate attacks. For example, by capturing other user sessions, the attacker can snoop, send spoofed replies, and/or drop user requests. A session-hijacking attack can be further categorized as a Spoofing/Man-in-the-Middle attack, a Denial-of-Service or a Replay attack or a Packet Drop attack [4].


**Figure 11: Hijack Future Session Attack**

**E.** DDOS Attack

Distributed Denial of Service, is a type of DOS attack shown in figure 12 where multiple compromised systems which are frequently infected with a Trojan. Trojans are used to target a single system causing a Denial of Service (DoS) attack. Fatalities of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in this distributed attack [12].

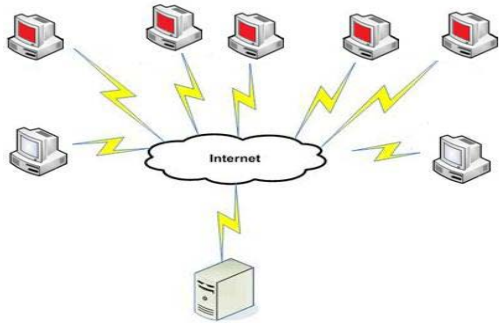


**Figure 12: DDOS Attack**

## 4. COMPARISON:

**Table 1:**

| Parameter | Rule based Approach [7] | SWADDLER [8] | Combined Approach for Analysis of Web Request and Database Request [9] | Histogram-Based Traffic Anomaly Detection [10] | DOUBLEGUARD [1] |
|---|---|---|---|---|---|
| Technique | Based on communication pattern and Combines the benefits of signature, protocol, and anomaly-based inspection. | Web application internal state is defined as information. The minimum state information is passed as a cookie to a browser. | The web request which is mistakenly treated as anomalous is simply send to the web server having limited access to the database and if request does not need to access the sensitive information that request will be served correctly. | Simulate different traffic feature with the help of histogram. Model out histogram patterns, and identifies deviations from the created models. | Based on the mapping model which detects abnormal behaviors. Both the web request and the database Queries within each session should be in accordance with the model. |
| Efficiency | Less efficient | Moderate | Moderate | - | More efficient. |
| Accuracy | High accuracy in detecting known attack. | High accuracy in detecting known attack. | - | - | High accuracy in detecting unknown attack |
| Use of intrusion alerts aggregations and alerts correlation | No | No | No | No | Yes |
| Cost | More expensive. | Expensive. | Moderate expensive. | Expensive. | Less expensive. |

## 5. CONCLUSION:

We surveyed few techniques that used for intrusion detection against multitier web applications. Some of the technique use single IDS to detect and prevent webserver from malicious request while some approach use combined approach to detect intrusions at both web and database level. Doubleguard approach has some additional detection capability to detect where normal traffic is used as means to launch database attack. Doubleguard also use multiple input streams to produce alerts because of container based and session separated approach. This correlation of different data stream provides better characterization of the system for Anomaly detection. This approach is more advantageous

because it monitors both web and subsequent database requests; hence it is able to detect various attacks that independent IDS would not be able to identify.

**6. REFERENCES:**


1. Meixing Le, Angelos Stavrou, Brent ByungHoon Kang,"DoubleGuard: Detecting Intrusions in Multitier Web Applications", IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 4, MARCH 2014.
2. V. Felmetsger, L. Cavedon, C. Kruegel, and G. Vigna, "Toward Automated Detection of Logic Vulnerabilities in Web Applications," Proc. USENIX Security ACM ., 2010.
3. M.Sujitha, P.Suganya, T.Shampavi, S.Anjanaa, "Dual Safeguard: Intrusion Detection and Prevention System in Web Applications", International Journal of Computer Application, Volume 67– No.9, April 2013.
4. SnehalKhedkar, Mangal Vetal, Surekha Kotkar, R. S. Tambe, " Security Model for Multi-Tier Web Application by Using Double Guard", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 2, February 2014.
5. G. A. Fink, B. L. Chappell, T. G. Turner, K. F. O'Donoghue, "A Metrics-Based Approach to Intrusion Detection System Evaluation for Distributed Real-Time Systems", Information Transfer Technology Group, Code B35, Naval Surface Warfare Center, Dahlgren Division, April 2002.
6. Sachin J.Pukale, M. K.Chavan, "A Review Of Anomaly Based Intrusions Detection In Multi-Tier Web Applications", International Journal Of Computer Engineering & Technology, Volume 3, Issue 3, October - December (2012), pp. 233-244.
7. http://www.snort.org.
8. M. Cova, D. Balzarotti, V. Felmetsger, and G. Vigna, "Swaddler: An Approach for the Anomaly-based Detection of State Violations in Web Applications" RAID 2007.
9. G. Vigna, F. Valeur, D. Balzarotti, W. K. Robertson, C. Kruegel, E. Kirda, "Reducing errors in the anomaly-based detection of web-based attacks through the combined analysis of web requests and SQL queries", Journal of Computer Security, 2009.
10. Andreas Kind, Marc Ph. Stoecklin, and Xenofontas Dimitropoulos, "Histogram-Based Traffic Anomaly Detection" IEEE transactions on network service management, vol. 6, no. 2, June 2009.
11. Shinde Jyoti R, Prof. Dabhade Sheetal V, "Advance Double Guard System: Detecting & Preventing Intrusions in Multi-Tier Web Applications", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 6, June 2014.
12. Vincent Shi-Ming Huang, Robert Huang, Ming Chiang, "A DDoS Mitigation System with Multi-Stage Detection and Text-Based Turing Testing in Cloud Computing", 27th International Conference on Advanced Information Networking and Applications Workshops, IEEE 2009.