International Journal of Computer Applications in Engineering Sciences
[VOL II, ISSUE III, SEPTEMBER 2012] [ISSN: 2231-4946]

Mobile Agent Based Distributed Intrusion Detection System: A Survey

Rajendra Tiwari[1], Rahul Kumar Gour[2]

[1,2]*Computer Scie. & Engg. Department, B.I.S.T.(Bhopal),India*

[1]ms.rejendratiwari@gmail.com
[2]rahul.gour2009@gmail.com

Abstract - Network security is a large and growing area of concern for every network. Intruders always search for vulnerabilities or flaws in target system and attack using different techniques. An intrusion detection system (IDS) is needed to detect and respond effectively whenever the confidentiality, integrity, and availability of computer resources are under attack. There is various type of IDS system have been proposed. Since last one decade intrusion detection through mobile agent is hot issue. This paper present a detailed review of all IDS system based on mobile agent. In this review process, only log file base distributed IDS system are considered. Mobile agent is efficient way to find out the intruder in distributed system. The main features of mobile agents are intelligence and mobility which is the core motivation to us to designed cost. In this paper we have reviewed on the different types of IDS system. The aim of this review work is to help user to select appropriate IDS systems as per their requirement and application.

***Keywords*—Intrusion-Detection, Mobile Agents, Network Security, Distributed System, Log File, RMI.**

I. INTRODUCTION

There is currently a need for an up-to-date, thorough taxonomy and survey of the intrusion detection. This paper presents such taxonomy, together with a survey of the important research intrusion detection systems and a classification of these systems according to the taxonomy. Significant the main focus of this survey is intrusion detection systems through mobile agent and its limitation. Now a day's intrusion detection with web log file is hot and burning issue. It has been seen in previous work that IDS with web log files are very flexible, efficient and scalable. Log file is a simple plain text file which record information about each user access. Log file contain information about user ID, IP address, date, time, bytes transferred, access request. A Web log is a file to which the Web server writes information each time a user requests a resource from that particular site. When user submit request to a web server that activity are recorded in web log file. Log file range 1KB to 100MB. Web log file is located in three different location Web server logs, Web proxy server, and Client browser [23].Display of log files data in three different format W3C Extended log file format, NCSA common log file format and IIS log file format. On the other hand traditional protection mechanisms like firewalls were not designed to protect web applications and thus do not provide adequate defense. Current attacks cannot be thwarted by just blocking ports 80 (HTTP) and 443 (HTTPS). This is the motivation of this work.

Mobile agents are designed for remote access or computation of data It reduces network traffic through perform data computation at remote/client side [29]. This characteristic make mobile agent best suitable in IDS system. Working of mobile agent is much like Remote procedure call (RPC), Remote method invocation [RMI] and .NET Remoting [30]. Its often create confusion concept of cloud computing with mobile agent because they are similar in a way that they work on loosely coupled distributed environment. Cloud is designed for resource sharing and mobile agent for remote computation [31].

II. INTRUSION DETECTION SYSTEM (IDS)

Intrusion means to interrupt someone without permission. Intrusion is an attempted act of using computer system resources without privileges, causing incidental damage. Intrusion Detection means any mechanism which detects the intrusive behavior. Intrusion Detection System (IDS) from the name itself, people could interpret that an IDS is a system used to monitors network traffic and detect its suspicious behavior against security. If it detects any threat then alerts the system or network administrator. The objective of IDS is to detect and inform about intrusions. IDS is a set of techniques and methods that are used to detect suspicious activities both at the network and host level [1].Intrusion detection systems (IDSs) are software or hardware systems that automate the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems [2].Intrusion detection can be performed manually or automatically [8]. Manual intrusion detection might take place by examining log files or other evidence for signs of intrusions, including network traffic. A system that performs automated intrusion detection is called an Intrusion Detection System (IDS) [13].

III. MA-IDS ARCHITECTURE

IDS implemented using mobile agent is one of new paradigms for intrusion detection. MAs are particular software agents having the capability to move from one host to another. Mobile agents offer unique features that can be used to improve the ways in which IDS are designed, developed and deployed in the network. The software agent can be treated as Mobile Agent, as they are able to migrate from one computer to another computer. Even if the host machine, which launched the agent, is eliminated from the network, the agent can still work. Thus, the mobile agents are very powerful programs, which can act even in the absence of the machine that initiated them. After completion of their assigned tasks, the mobile agents return to the host machine to report the result or simply terminate.

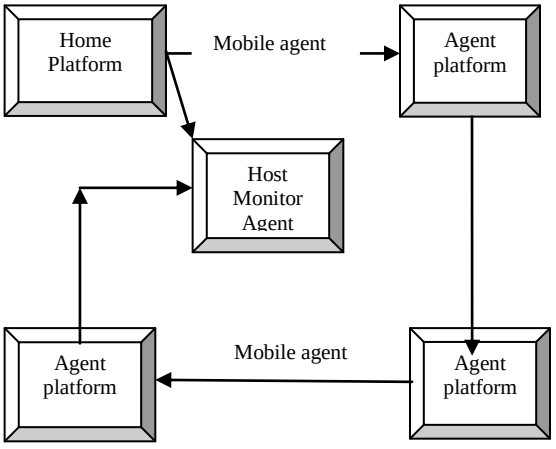

Fig.1 Movement of Mobile Agent

Fig.1 depicts the movement of an agent among several agent platforms. The platform where a mobile agent originates is referred to as the home platform (controlling device), and normally is the most trusted environment for an agent. One or more hosts may have an agent platform, and an agent platform may support multiple locations or meeting places where agents can interact. Mobile agent technology has benefited from the work done on intelligent agents, which emphasizes static autonomous agents capable of applying application domain knowledge, and the development of software systems capable of supporting mobile code on heterogeneous hardware (e.g., Java technology).figure show that mobile agent gathered data and send back to the controlling device. Controlling device is a rule based device which applies some rule on that gathered data for finding intrusion detection or future analysis. Each monitored host (controlling host) in the network is installed with a Host Monitor Agent. The Host Monitor Agent has type of rule to complete local intrusion detection function. If the intrusion can be determined at monitored host, the Host Monitor Agent reports the intrusion directly and takes appropriate action against intrusion. Otherwise the Host Monitor Agent keeps record of all activity. This record is used for future analysis. Fig.2 shows the working of host mobile agent.

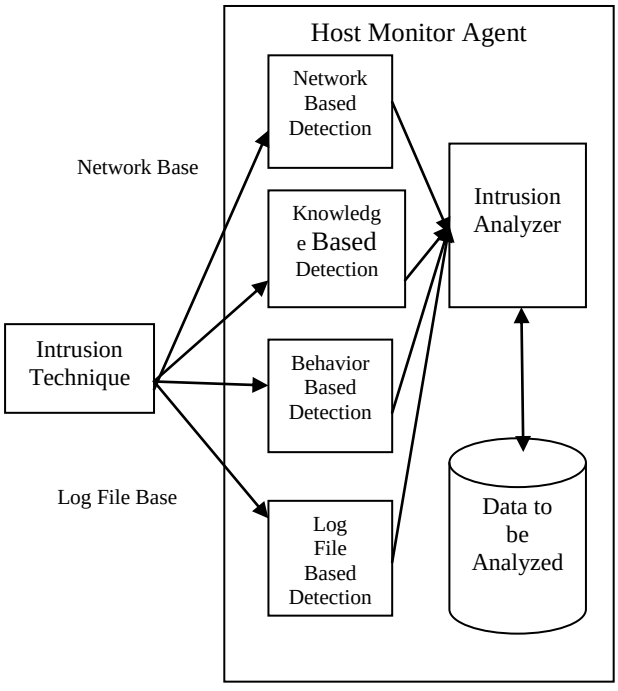

Fig.2 Host Monitor Agent Structure

IV. TYPES OF INTRUSION DETECTION SYSTEM

There are two ways to protect our network against malicious attempts. First is to build complete secure network system by applying all complicated cryptographic, authentication and authorization methods. However, this solution is not realistic. In practice, it is impossible to have completely secure system, because the user uses operating system and other applications to accomplish his/her job. Almost all applications have one or the other vulnerabilities. Second way is to detect an attack as soon as possible preferably in real-time and take appropriate action. This is essentially what an Intrusion Detection and Prevention System (IDS and IPS) does. An IDS does not usually take preventive measures when an attack is detected; it is a reactive rather than pro-active [3].

A. Knowledge-Based IDS

Knowledge-based design detects intruders by pattern-matching user activity against known attack signatures. Signatures are kept in a database containing a repertoire of information describing normal, suspicious, or attack behavior. Strength of misuse detection paradigm is that when it signals that an attack has occurred, it is very likely that an attack has actually occurred [21]. On the

other hand we can say that it applies the knowledge accumulated about specific attacks and system vulnerabilities. The intrusion detection system contains information about these vulnerabilities and looks for attempts to exploit these vulnerabilities. When such an attempt is detected, an alarm is triggered. It means any action that is not explicitly recognized as an attack is considered acceptable. Therefore, the accuracy of knowledge-based intrusion detection systems is considered good. However, their completeness (i.e. the fact that they detect all possible attacks) depends on the regular update of knowledge about attacks.

PROS:

1) Very low false alarm rate.
2) It will provide good prevention method.
3) It is easy to understand the problem and take prevention or correction action.

CONS:

1) Difficult to gathering the required information on the known attack.
2) It is required to keep information up to date with new vulnerabilities and environment.
3) It is time-consuming because it is required carefully analysis of each vulnerability.
4) It's depending on the operating system version, platform and application because knowledge about attack are focused on operating system.

B. Host Based IDS

Host-based intrusion detection systems analyze data that originates on computers, such as application and operating system event logs and file attributes. Host data sources are numerous and varied, including operating system event logs, such as kernel logs, and application logs such as syslog [1] [22]. These host event logs contain information about file accesses and program executions associated with inside users. If protected correctly, event logs may be entered into court to support the prosecution of computer criminals [19]. HIDS monitor traffic on its host machine by utilizing the resources of its host to detect attacks[4] [9].

PROS:

1) Host-based IDS can analyze activities on the host so it can determine which processes and/or users are involved in malicious activities.
2) Host-based IDS is easy to use in switch based network (HIGH SPEED NETWORK).
3) Host-based IDSs can use host-based encryption services to examine encrypted traffic, data, storage, and activity.
4) Host-based intrusion detection detects insider misuse .

CONS:

1) Host based IDS serves the purpose to detect attack patterns that can only or easier to be found on a host level basis.
2) Data collection occurs on a per-host basis so if host is damaged , it will harm overall performance on the detection.
3) Writing to logs or reporting activity requires network traffic and can decrease network performance.

C. Network Based IDS

Network-based intrusion detection systems (NIDS) are IDSs that operate as stand-alone devices on a network. NIDS monitors traffic on the network to detect attacks such as denial of service attacks; port scans or even attempts to crack into computers by monitoring network traffic[1] [8] [9]. Network based intrusion detection systems come in the form of software or fully integrated appliance. [14] [18][22] .Intrusion detection is network-based when the system is used to analyze network packets. Network based Intrusion Detection and Prevention System (NIDPS) capture the network traffic from the wire as it travels to a host. This can be analyzed for a particular signature or for unusual or abnormal behaviors. Several sensors are used to sniff the packets on network which are basically computer systems designed to monitor the network traffic. If any suspicious or anomaly behavior occurs then they trigger an alarm and pass the message to the central computer system or administrator (which monitors the IDPS) then an automatic response is generated [19] [20] [26]

PROS:

1) Network-based IDSs can monitor an entire, network and impose little overhead on a network.
2) Network-based IDSs are mostly passive devices that monitor ongoing network activity without adding significant overhead or interfering with network operation.
3) Easy to secure against attack and may even be undetectable to attackers.
4) Network intrusion detection detects outsider misuse.

CONS:

1) Introduction Detecting Attacks on Web Applications High traffic load makes it difficult to analyze network traffic (in real time).

2) The HTTP traffic may be SSL encrypted (HTTPS) There may be no NIDS (hard to deploy; another zone of attack).
3) NIDS are designed to work on the TCP/IP level, and thus they may not be as effective on the HTTP layer; IDS evasion techniques (HTTP, encoding).
4) NIDS cannot be analysis encrypted data
5) NIDS may not be able to monitor switch-based (high-speed).

D. Behavior-Based IDS

When the intrusion-detection system uses information about the normal behavior of the System Behavior on detection describes the response of the intrusion detection system to attacks [16]. The behavior-based design uses statistical methods or artificial intelligence in order to detect attacks. Profiles of normal activity are created and stored in a database. Activity gathered by the event generator that deviates from the normal profile in a statistically significant way can be deemed as suspicious activity or an attack. The strength of anomaly detection systems is that they can detect new attacks and there is no requirement to enter attack signatures into a database [21].

PROS:

1) Able to detect new and unforeseen vulnerabilities.
2) Less dependency on operating -system-specific mechanism.
3) It is also useful to detect "abuse of privilege" types of attack.
4) Its speed is fast comparing to the knowledge based IDS because it is not depend on the rules.

CONS:

1) It is difficult to implement.
2) It may be more resource-hungry than knowledge-based IDS.
3) It may require frequent fine-tuning by administrator.

E. Anomaly Detection Systems

Anomaly detection technique store the systems normal behavior such as kernel information, system logs event, network packet information, software running information, operating system information etc into the database. If any abnormal behavior or intrusive activity occurs in the computer system which deviates from system normal behavior then an alarm is generated. Anomalous activities that are not intrusive are flagged as intrusive. This will result in false-positive, i.e. false alarm. Intrusive activities that are not anomalous result in false negative [1] [10]. The anomaly based detection is based on defining the network behavior. The network behavior is in accordance with the predefined behavior, then it is accepted or else it triggers the event in the anomaly detection. The accepted network behavior is prepared or learned by the specifications of the network administrators [5] [11].The normal profiles (or normal behaviors) of users are kept in the system. The system compares the captured data with these profiles, and then treats any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response [16][25].

PROS:

1) New attacks and vulnerability will be detected as soon as they take place.
2) ABS can be applied also to ad-hoc networked systems such as web-based services.

CONS:

1) ABS needs an extensive model building phase: a significant amount of data (and thus a significant period of time) is needed to build accurate models of legal behavior.

F. Misuse Detection Systems

The system keeps patterns (or signatures) of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. Like a virus detection system, it cannot detect new kinds of attacks [6] [17]. Misuse detection, attempts to encode knowledge about attacks as well defined patterns and monitors for the occurrence of these pattern and monitors for the occurrence of these pattern for example, exploitation of the fingered and send mail bugs used in the Internet Worm attack .on the other hand it say that This technique involves the comparison of a user's activities with the known behaviors of attackers attempting to penetrate a system. Misuse detection also utilizes a knowledge base of information. The misuse knowledge bases include specific metrics on the various techniques employed by attackers when the knowledge base was created [24] [27].

PROS:

1) Misuse detection also utilizes a knowledge base of information.
2) It is the best technology to detect intruder on the previous knowledge.
3) Misuse detection system looking for the exploitation of known weak points in the system, or sequence of events or data.

CONS:

1) Misuse detection systems suffer from the potential performance degradation it is depended on audit trails for input.
2) It is required previous knowledge to detect intrusion.
3) For the known weak point in the system it required a specific pattern.

V. IDS CHALLENGES

Some shortcomings are inherent when IDSs are constructed [28]. The most common shortcomings include the following items

A. Lack of Efficiency

IDSs are often required to evaluate events in real time. This requirement is difficult to meet when faced with a very large number of events as is typical in today's networks. Consequently, host-based IDSs often slow down a system and network-based IDSs drop network packets that they do not have time to process.

B. High Number of False Positives

Most IDSs detect attacks throughout an enterprise by analyzing information from a single host, a single application, or a single network interface, at many locations throughout the network. False alarms are high and attack recognition is not perfect. Lowering thresholds to reduce false alarms raises the number of attacks that get through undetected as false negatives

C. Burdensome Maintenance

The configuration and maintenance of intrusion detection systems often requires special knowledge and substantial effort. For example, misuse detection has usually been implemented using expert system shells that encode and match signatures using rule sets. Upgrading rule sets involves details peculiar to the expert system and its language for expressing rules sets, and may permit only an indirect specification of the sequential interrelationships between events. Similar considerations may apply to the addition of a statistical metric, typically used for detecting unusual deviations in behavior.

D. Limited Flexibility

Intrusion detection systems have typically been written for a specific environment and have proved difficult to use in other environments that may have similar policies and concerns. The detection mechanism can also be difficult to adapt to different patterns of usage. Tailoring detection mechanisms specifically to the system in question and replacing them over time with improved detection techniques is also problematic with many IDS implementations. Often the IDS needs to be completely restarted in order to make changes and additions take effect Vulnerability to Direct Attack

E. End-to-end Encryption

With security improvements in communications protocols, the ability to encrypt traffic on an end-to-end basis is on the rise. Besides thwarting an eavesdropper, encrypted content keeps network-based IDS from peeking into packets and analyzing their contents for intrusions.

F. High Speed Communications

Higher communication traffic rates directly affect the processing speed needed to analyze packet content, potentially resulting in lost packets. The trend toward switched communications over broadcast also increases the difficulty for network-based IDS to monitor multiple communications streams.

G. Breadth of Attacks

As new attacks are conceived, IDSs must be updated to discover them. While new attacks are added frequently, old ones can seldom be dropped. Typically, the greater the attack coverage, the more processing time that is needed by the detection algorithm.

VI. BEST SOLUTION WITH MOBILE AGENT

The software agent can be treated as Mobile Agent, as they are able to migrate from one computer to another computer. Even if the host machine, which launched the agent, is eliminated from the network, the agent can still work. Thus, the mobile agents are very powerful programs, which can act even in the absence of the machine that initiated them. After completion of their assigned tasks, the mobile agents return to the host machine to report the result or simply terminate [15]. So Mobile agent is a type of software agent, with the feature of autonomy, social ability, learning, and most import, mobility. Mobile agents have some advantages that are [7] [13].

A. Overcoming Network Latency

Since agents operate directly on the host, where an action has to be taken, their response is faster than hierarchical systems, where the actions are taken by central coordinator.

B. Reducing Network Load

Instead of sending audit data from sensors to central stations, sending the code of the agent may cause little network load, because audit data may become huge amounts.

C. Autonomous Execution

In order to prevent letting the whole network undefended, when a part of the IDS fails, agents can work autonomously even if their creators don't operate anymore.

D. Platform Independence

Where the agents run on the agent platform, they are independent from the platform of the host.

E. Dynamic Nature

The dynamic nature of mobile agents enables them to be moved around the network. This makes it possible to reconfigure the system during runtime also. Mobile agents can be cloned, dispatched or put to sleep when the network configuration has to be changed

F. Heterogeneous Environment

Mobile agents can be interoperable on multiple platforms. This is possible because of the virtual interpreter installed on the host machine. Mobile agents are generally computer and transport-layer independent and are dependent only on the execution environment. This feature enables the mobile agents to be used on several different platforms without compatibility problems.

G. Structure and Platform Independence

Mobile agents can be used in IDS with a flexible structure. For example, one agent can be designated for collecting the data in the network, the other agent can be used to detect and report anomalies while the rest of them can be used to take appropriate action.

H. Dynamic Adaption

The system can be reconfigured at run-time because of the agent's dynamic behavior.

I. Static Adaption

When a new attack signature has to be added to the IDS, the algorithm of the agents can be updated without restarting the whole system.

J. Scalability

Mobile agents reduce the computational load on the system by dividing it different hosts

VII. CONCLUSIONS

Different intrusion detection systems and its pros, cons are discussed in this paper to support the security of an organization against unwanted threats or attacks. On the other side attackers are discovering new techniques and ways to break these security policies. Firewalls, antivirus and antispyware are limited to provide security to the system against threats. The only way to beat them is to up to date knowledge about their techniques that they use for attack. We also discussed about mobile agents and how it can be worked up on the log data. Moreover, using mobile agents in IDS would increase the integrity of a database in which it would keep records of what type of intrusion the mobile agent .Common communication format for exchanging rules or log between agents to remote agent are also in consideration.

ACKNOWLEDGMENT

I would like to acknowledge and extend my heartfelt gratitude to Mr. Vivek Tiwari, Researcher (PhD) at Maulana Azad National Institute of Technology (MANIT-Bhopal), for their expertise, stimulating suggestions, experience and encouragement in all the times of research period.

REFERENCES

[1] U. A. Sandhu , S. Haider , S. Naseer , and O. U. Ateeb , "*A Survey of Intrusion Detection & Prevention Techniques*", IPCSIT vol.16, IACSIT Press, Singapore 2011.

[2] K. Maskat, Md. A. Shukran, Md. A. Khairuddin, and Md. R. Isa, "*Mobile Agents in Intrusion Detection System: Review and Analysis* ", Vol. 5, No. 6, December 2011.

[3] Dr. B. Trivedi , J. Rajput , C. Dwivedi ,and P.Jobanputra, "*Distributed Intrusion Detection System using Mobile Agents* ", Proc .of CSIT vol.1 IACSIT Press, Singapore 2011.

[4] N. Verma, Dr. Md. Husain,and M. K. Shukla, "*Research on Mobile agent based network intrusion*", Vol. 2, ISSue 2, June 2011.

[5] V. Jyothsna, V .V. Rama Prasad,and K . Munivara Prasad, "*A Review of Anomaly based Intrusion Detection Systems* ", Volume 28– No.7, August 2011.

[6] D. Damopoulos, S. A. Menesidou,G. Kambourakis, M.Papadaki2, N.Clarke and S. Gritzalis, *"Evaluation of Anomaly-Based IDS for Mobile Devices Using Machine Learning Classifiers* " , Security Comm. Networks ,1–9 ,2011.

[7] P. jain, S. Raghuwanshi and P. rk, "*new mobile agent-based intrusion detection systems for distributed networks* ", Volume 1, Issue 1, 2011.

[8] J. S. Rathore, "*Survey on Intrusion Detection and Prevention System and Proposed Cost Effective Solution Using Software Agent*" ,Volume 1, Issue 3, May 2012.

[9] K.K.R and A. Indra*," Intrusion Detection Tools and Techniques – A Survey*", December, Vol.2, No.6, 2010.

[10] O. Adaobi, M. Ghassemian, "*Analysis of an Anomaly-based Intrusion Detection System for Wireless Sensor Networks*",International Conference on Communication Enginering, December 2010.

[11] M. Tavallaee, N. Stakhanova, and Ali A. Ghorbani*," Toward Credible Evaluation of Anomaly-Based Intrusion-Detection Methods*", IEEE SEPTEMBER 2010

[12] Syurahbil, N. Ahmad, M. F. Zolkipli, Ahmed N. Abdalla," *Intrusion Preventing System using Intrusion Detection System Decision Tree Data Mining*", Science Publications, 2009.

[13] Y. Li, R. Wang, J. Xu, *"A Novel Distributed Intrusion Detection Model Based on Immune Mobile Agent* " May 22-24, 2009.

[14] R. Meyer, "*Detecting Attacks on Web Applications from Log Files*", 26 January 2008.

[15] M. Singh, S. S. Sodhi, "*Distributed Intrusion Detection using Aglet Mobile Agent Technology* ", March 23, 2007.

[16] D. Bolzoni, S.Etalle, P. Hartel,"*POSEIDON: a 2-tier Anomaly-based Network Intrusion Detection System*, 2006 IEEE.
[17] T.Anantvalee ,and J. Wu, "*A Survey on Intrusion Detection in Mobile Ad Hoc Networks* " , pp. 170 - 196 ,Springer 2006.
[18] A. Fuchsberger*," Intrusion Detection Systems and Intrusion Prevention Systems*", Information Security Technical Report ,2005.
[19] H. Kozushko, "*Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems*", September 11, 2003.
[20] H. Debar, M. Dacier , and A. Wespi, "*Towards a taxonomy of intrusion-detection systems*" ,Research Report, 1999.
[21] A.Yasinsac, S. Goregaoker, *" An Intrusion Detection System for Security Protocol Traffic* ", Florida State University, Florida 2002.
[22] C. Petersen," *an introduction to network and host based intrusion detection*", 2003.
[23] P. Patil, U. Patil, " *Preprocessing of web server log file for web mining*", NCETCT-2012.
[24] J. C. J. Harrell, "*A Comparative Analysis of Current Intrusion Detection Technologies*".
[25] R. Shanmugavadivu, "*network intrusion detection system using fuzzy logic*", ijcse,2011.
[26] H. Albag, "*Network & Agent Based Intrusion Detection Systems* ", Istanbul Tech. Uni ,TU Munich.
[27] J. S. Balasubramaniyan, J. O.Garcia-Fernandez,D. Isacoff, E.Spafford, D. Zamboni"*An Architecture for Intrusion Detection using Autonomous Agents*",1998.
[28] W. A. Jansen, "*intrusion detection with mobile agents*",2002.
[29] V. Tiwari, Dr. S.K. Lenka &S. Gupta.(June-2010)," *Performance Evolution of Java Remote Method Invocation and Mobile Agent Techniques in Context of Distributed Environment*" IEEE International Conference on Networking and Information Technology (ICNIT 2010) Manila, Philippines, IEEE Catalog Number:CFP1023K-PRT, ISBN:978-4244-7577-3.
[30] V. Tiwari & S. Gupta" *Computational Study of .NET Remoting and Mobile Agent in Distributed Environment*" International Journal of Computing, Volume 2, Issue 6, June-2010, ISSN: 2151-9617.
[31] V.Tiwari & U. Bindal*", Cloud Computing: A next generation revolution in IT with e –Governance*" CiiT International Journal of Networking and Communication Engineering, Volume 2, DOI: NCE052012006, ISSN 0974-9616, May 2012.