ISSN: 2321-7782 (Online)
Volume 2, Issue 1, January 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Paper
Available online at: www.ijarcsms.com

Survey on Intrusion Detection Systems

Neha Sava[1]
Computer Department
MIT College of Engineering
Pune-India

Priya Budhwani[2]
Computer Department
MIT College of Engineering
Pune-India

Sanika Talekar[3]
Computer Department
MIT College of Engineering
Pune-India

Shalaka Borle[4]
Computer Department
MIT College of Engineering
Pune-India

Nagesh Jadhav[5]
Computer Department
MIT College of Engineering
Pune-India

Abstract: ***In today's world due to increasing unauthorized access, illegitimate attacks on vulnerable data, there is a growing need to protect our data using certain tools which aim to prevent malicious activities like denial-of-service, stealing of valuable data etc. Such attempts to break into or misuse a system are termed as intrusion. Firewalls generally do a good job in such cases, but they can be circumvented. Thus, an effective and complimentary system called intrusion detection system (IDS) was introduced. Basically IDS are classified into two classes viz. anomaly based IDS and signature based IDS. To overcome the pitfalls of former IDS (Signature and anomaly based), knowledge based IDS was introduced. This is a survey paper on various improvements in IDS over time.***

Keywords: ***Intrusion detection system, Ontology, host based, network based, signature based, hybrid, knowledge based and situation aware.***

I. INTRODUCTION

Internet is a vast network which is spread worldwide and is growing day by day. Although internet has proved to be useful in various aspects, these benefits come with certain risks. The information on internet is publicly available; however, it can be used in a constructive as well as destructive way. Intrusions are caused by attackers accessing the systems from the Internet, authorized users of the systems who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given to them. [15] Anderson introduced the concept of intrusion detection in 1980, he defined intrusion as an unauthorized attempt to access information, manipulate information, or render a system unreliable or unusable. As a part of defensive measures, intrusion detection system is needed to monitor these types of attacks and to avoid compromise with confidentiality and integrity of systems. Intrusion Detection systems are an important component of security mechanisms for protecting computer systems and networks from abuse. One of the security mechanisms used widely is firewall. Firewalls work actively by the configured security policy but they cannot prevent all kinds of attacks and variants of the attacks. They do not examine the contents of the legitimate traffic and do not offer any protection if the network is breached. Firewalls have no clever way of telling whether the traffic is legit and normal, this is where IDS systems come into play. IDS are much more dynamic as compared to firewalls. But firewalls cannot be completely replaced by IDS; they are complementary to each other. IDS provide the information about intrusions that have taken place, which helps in the diagnosis improvement, recovery, and correction of factors causing it. They monitor the network and alert the security person with the specified patterns. IDS work by either looking for signatures of known attacks or deviation from normal behaviour. IDS works at host as well as network level depending on the type of data source.

Intrusions in a network may happen in various ways:

- Attempted break-in: An attempt to have an unauthorized access to the network.
- Masquerade: An attacker uses a fake identity to gain unauthorized access to the network.
- Penetration: The acquisition of unauthorized access to the network.
- Leakage: An undesirable information flow from the network.
- DoS: Blockage of the network resources (i.e., communication bandwidth) to the other users.
- Malicious use: Deliberately harming the network resources

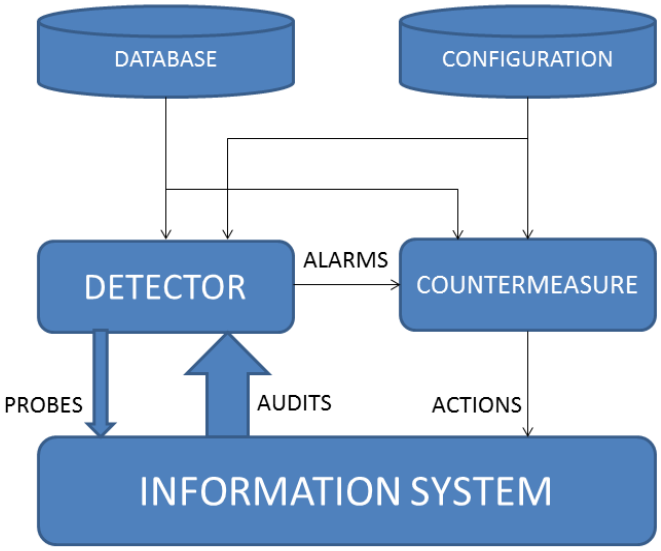

Fig.1 Intrusion-detection system[1]

Network security and intrusion detection systems are one of the key research areas in the networking era as the most difficult problem today is how to deal with and rely on the huge volume of information that flows across the network while many network attacks are being reported every day. Hence there is always a need to increase the level of security to safeguard against network intrusion either wired or wireless. Solutions to security attacks against networks (wireless and/or wired) involve three main components [13]:

- Prevention i.e. defence against attack
- Detection i.e. being aware of the attack that is present
- Mitigation i.e. reacting to the attack.

Intrusion is an unauthorized (unwanted) activity in a network that is either achieved passively (e.g., information gathering, eavesdropping) or actively (e.g., harmful packet forwarding, packet dropping, hole attacks).Even in any security plan, Intrusion Detection Systems (IDSs) provide some or all of the following information to the other supportive systems i.e. identification of the intruder, location of the intruder (e.g., single node or regional), time (e.g., date) of the intrusion, intrusion activity (e.g., active or passive), intrusion type (e.g., attacks such as worm hole, black hole, sink hole, selective forwarding, etc.), layer where the intrusion occurs (e.g., physical, data link, network). This information would be very helpful in mitigating and remedying the result of attacks, since very specific information regarding the intruder is obtained. Therefore, intrusion detection systems are very important for network security.

Intrusion detection is defined to be the problem of identifying individuals who are using a computer system without authorization (i.e. crackers) and those who have legitimate access to the system but are exceeding their privileges (i.e. the insider threat)

According to [18], an IDS concludes either of four decisions (with non-zero probabilities) mentioned below as a result of the decision making process over an event:

- Intrusive but not anomalous (false-negative): There is an intrusion to the system, but the IDS fails to detect it and concludes the event as non-anomalous one.
- Not intrusive but anomalous (false-positive): There is no intrusion to the system, but the IDS mistakenly concludes a normal event as an anomalous one.
- Not intrusive and not anomalous (true-negative): There is no intrusion to the system, and the IDS concludes the event as non-anomalous one.
- Intrusive and anomalous (true-positive): There is an intrusion to the system, and the IDS concludes the event as an anomalous one.

Here the metrics for evaluating IDS are false alarms (false positives) and missed alarms (false negatives).

II. HOST BASE IDS

Host-based technology examines events like what files are being accessed and what applications are being executed. Host-based intrusion detection systems analyse the data that originates on computers, such as application and operating system event logs and file attributes. Host data sources are many and of various forms, such as operating system event logs and application logs. These host event logs contain information about file accesses and program executions associated with inside authenticated users.

Host-based intrusion detection guards against many attack scenarios. One of these scenarios is the misuse of privilege attack. In this type, the user has administrative or some other privilege and he uses it in an unauthorized manner to harm the system. Another scenario involves contractors with elevated privileges. This usually takes place when an administrator gives a contractor elevated privileges to install an application. A third attack scenario involves ex-employees utilizing their old accounts. They may use it to extract some sensitive information about the firm. Another scenario involves modifying web site data. There have been many cases, against government agencies in particular, that result in uncomplimentary remarks posted on websites [14]. Host-based system detects and responds to long term attacks, such as data thieving. However, they have poor real-time response and cannot effectively protect against one-time catastrophic events. Host-based systems are most useful when it comes to determining the extent of a compromise after loss.

Computer systems generally have many dynamic (frequently changing) objects which intruders intend to modify. Host-Based intrusion detection system (HIDS) should monitor such malicious activities but their dynamic nature makes them unsuitable for the checksum technique which is generally employed by HIDS for intrusion detection. To overcome this problem, HIDS uses various other detection techniques such as monitoring changing file-attributes, fluctuations in size of log-files since last checked, and numerous other means to detect abnormal activities.

A system administrator has to construct a suitable object database with the help of HIDS installation tools and initialize the checksum-database. The HIDS then has all it requires to scan the monitored objects regularly and to report on anything that may appear malicious. Reports can be in terms of logs, emails or similar.

In the paper [21], they have designed and implemented a host-based intrusion detection system, which combines two detection technologies, one is log file analysis technology and the other is Back propagation (BP) neural network technology. Firstly, the HIDS uses log files as its primary sources of information, and through three steps of pre-decoding log file, decoding log file, and analysis log file, it can effectively identify various intrusions [21]. Secondly, based on BP neural network analysis technology and through establishment of system behaviour characteristics profile in advance, the HIDS can identify intrusions by comparison with threshold. Back propagation (BP) algorithm [20] is an approximate steepest descent algorithm, used to train multilayer neural networks and it is used widely in practice.

By combining two approaches in the HIDS, these two detection technology can complement each other, which can effectively improve the efficiency and accuracy of intrusion detection.

III. NETWORK BASED IDS

Network-based IDS is used to analyse the packets flowing in the network. Network intrusion detection differs from host-based intrusion detection, in terms of the nature of data processed. Host IDS analyses data related to data that originates on computers themselves, such as event and kernel logs. Although network packets can be extracted from the output of switches and routers present in the network, they are usually intercepted while travelling through the network. TCP/IP protocol is used most commonly in the computer networks, and thus it is attacked frequently. Network sources are unique because of their proximity to unauthenticated, or outside, users. They are arranged in a particular way to help detect denial of service attempts and access attempts which may arise outside the user's network.

Network intrusions are carried out in various forms like worms, viruses, spam, Trojan horse etc. They pose mainly two major threats and damage on the victims. First, the intruders examine, collect, and deduce sensitive information about target hosts' system to gain unauthorized access to them and their networks. Second, the intruders inject harmful and undesirable packets into the target networks, intending to disturb the normal communications and services provided by the target networks. It is, hence, very important to implement and install effective network intrusion detection systems (NIDSs) to monitor the network and detect the intrusions in a timely manner (Huang et al., 2009).

Packets of information that exchange between computers (network traffic) are inspected by network-based systems. It is effective at real-time detection and response as it relates to the network. Network intrusion detection can also be effective at detecting long-term attacks such as sniffer programs which regularly report information from outside the firewall.

Network intrusion detection can be used to trace the paths or connections in a network. However, there is a disadvantage to such network-based intrusion detection systems. If the incoming traffic is encrypted, then the detection engine is of no help as it cannot search for patterns of misuse in the payload of network packets.

Network intrusion uses many algorithms which help in detection of threats in the network. Visual analytics is a method used for intrusion detection for which Treemap algorithm is introduced. Treemap-NIDS implementation is based on a Two-layered architecture. An application of visual analytics system is developed for network intrusion detection system collaboratively operating a large-scale hierarchical data visualization technique. The effectiveness of a simplifying visualization in increasing situation awareness for users needing to synthesize large amounts of intrusive data and make critical decisions under time pressure is employed in this.

Thus, Network Intrusion detection systems provide comprehensive defence against identity theft, information mining, and network hacking. User information, access to the network, and firewall measures are all actively updated and looked after by network intrusion detection systems.

IV. ANOMALY BASED IDS

An anomaly based IDS states the normal behaviour of users and if any activity other than the defined behaviour is detected then it considers it as an attack/intrusion.

Any deviation from the normal behaviour is considered as an attack by this system, so it can generate large number of false positive as not every deviation is an intrusion. In many cases, an intruder is smart enough that he changes his behaviour accordingly to get involve it into definition. This may result into false negative. Despite of these shortcomings, it is best hope for autonomous, early detection of new malware.

In order to maintain the balance between rate of false negative and false positive and to keep it low, new approach was introduced. In this approach, multiple detectors are networked intelligently. In such a system, the probability of false positive is reduced as the different detectors are designed in such a way that they have different databases/ repository. It can be useful in

situations where many computers are involved or infected, such as large botnets. Thus it accomplishes the task what a single system cannot do. [6]

Another variation to DIS (Distributed Intelligent System) is Sharing Normal Behaviour Databases among different machines. In this system, normal behaviour data obtained on each machine is accumulated in a server and the integrated data is distributed to each machine. This system improves the detection correctness by integrating the data used for anomaly detection on each machine. Also known as Anomaly Detection using COllective INtelligence (*ADCOIN*) [5]

GBID which is an anomaly based IDS is proposed in [16]. In this Genetic algorithm is used for learning regularities in user's behaviour and anomaly in the usage of commands by individual users is used to detect intrusion. This approach has fewer false alarms as the user behaviour is learnt continuously and deviation from normal user behaviour is captured. Each user command forms a gene. Fitness function is used to measure the fitness of the behaviour gene. Using genetic operators on the fit behaviour genes of current generation next generation genes are produced.

V. SIGNATURE BASED IDS

Signature based Intrusion Detection System (IDS) works as a network packet sniffer, which compares the packet contents with the known virus signatures that are encapsulated in databases as rules and thus detects threats. A misuse based IDS states the signatures of attacks and parses audit files to detect any matches. For example when any person sends data inside the network so first of all it goes to server and server check and if found malicious (matched signature found) then server discards the packet otherwise send to destination system.

Sobh [20] pointed out that these systems are very much like the anti-virus systems, which can detect most or all known attack patterns, but one drawback is that it is of little use for the attack methods that are unknown yet. Snort is mostly used signature based IDS as it is an open source software. Its attack signature database can also be updated time by time. In signature based IDS system if pattern matches then attack can be easily found but when a new attack comes then system fails but snort overcome this limitation by analysing the real-time traffic, which is an advantage of snort little above the signature based. Whenever any packet comes into network then snort checks the behaviour of network if its performance degrades then snort stops the processing of packet, discards the packet and stores its detail in the signature database.

Sobh [20] identified the main distinction between the anomaly based detection and misuse based detection as: "anomaly detection systems try to detect the effect of bad behaviour but misuse detection systems try to recognize known bad behaviour.

Signatures are very much in use now days considering its advantages such as- There are low false positives as long as attacks are clearly defined in advance and Signature-Based Detection is easy to use. However this system has number of weaknesses such as

- It can be seen that misuse detection requires specific knowledge of intrusive behaviour. Collected data before the intrusion could be out of date and yet many times it is hard to detect newer or unknown attacks.
- Misuse detection has a well-known problem of raising alerts regardless of the outcome. For example a window worm trying to attack a Linux system, the misuse IDS will send so many alerts for unsuccessful attacks which may be hard to manage.
- This model may not always be so practical for inside attacks involving abuse of privileges.
- The knowledge about attacks is very dependent on the operating system, version and application hence tied to specific environments.

One of the foremost challenges for signature based IDS systems is how to keep up with large volume of incoming traffic when each packet needs to be compared with every signature in the database. In most cases, when an IDS cannot keep up with

the traffic flood, all it can do is to drop packets, therefore, may miss potential attacks. Even sometimes useful data get lost, which will eventually ruin organizational business. Thus, in order to promote the performance of network intrusion detection system and reduce the processing time of the traffic, parallel technique was proposed [3]. In this, with the use of two signatures based network Intrusion detection systems i.e. running Snort in parallel with a portion of packets and a subset of rules, it distributes the traffic between them, thus processing time of the traffic is reduced. Variant to this, another technique was introduced i.e. Dynamic Multi-Layer Signature based IDS[8] using Mobile Agents, which can detect imminent threats with very high success rate by dynamically and automatically creating and using small and efficient multiple databases, and at the same time, provide mechanism to update these small signature databases at regular intervals using Mobile Agents.

VI. Specification Based Ids

Another type of intrusion detection system is Specification based IDS which combines the advantages of both misuse and anomaly based detection techniques. Similar to Anomaly based IDS, it detects attacks as deviation from normal behaviour, and has low false alarm rate similar to Misuse based IDS. In these IDS, system's legitimate behaviour is described by a set of manually developed specifications and constraints. The correct execution of a program or protocol is checked with the already defined specifications and constraints. [13]

This method was introduced in [13]. Along with low false alarm rate, this IDS detects novel and previously unknown attacks. But to achieve this low false alarm rate, it is very important to develop specifications and constraints in a proper manner and it is very time consuming as it is done manually.

VII. Knowledge Based Ids

Existing IDS are signature based and if the signature of an attack is not available in their database, they cannot detect it. Various monitoring tools like Wireshark, Cacti, etc. use a rule-based alerting mechanism, where the activities in the infrastructure are monitored and checked against a pre-defined set of rules. Corresponding actions are taken when certain events match predefined rules. Thus, current intrusion detection system lacks clear description of relations between intrusion behaviour and detection ability is limited. These mechanisms can be complemented with ontology to improve their performance level. To incorporate more intelligent behaviour in intrusion detection architecture, ontology is necessary.

Using ontology, the relationships between collected data can be expressed and these relationships can be used to deduce that the particular data represents an attack of a particular type.

Ontology determines exact meaning of the collected data through strict definition and also the relation between the collected data, accordingly comes out with mutually accepted shared knowledge.

In hierarchical model, central IDS aggregates information of malicious activities from all member IDS present at lower level which cooperate with central IDS to form global IDS. It detects attacks in an effective and structured way but it increases the cost. [4] presents an ontology-based intrusion detection model with advantages of hierarchical and collaborative models overcoming their disadvantages, and then the deduction of expert system was used to detect the complex attacks. This model is divided into detection regions, each including sensors, translator, intrusion ontology and knowledge database and is administered by a deduction engine. Deduction engine works in the equal collaborative model and the entire network does not exist in single central processing node. The collaborative nature of the network reduces the amount of transmission data between components within the overall network. System transfers the established intrusion ontology into facts in knowledge database of expert system and also stores the ontology instances into knowledge database as rules.

Undercoffer et. al [18], underscored the importance of ontological linking of the vulnerabilities for a more effective IDS mechanism. Ontological specification of attacks and intrusions provides superior definitions of the concepts and semantic

relations between them, as compared to the conventional taxonomic representation. This provides better reasoning and analysis of the available information.

As stated in the paper by F. Abdoli and M. Kahani [15] the idea of semantic web is applied to Intrusion Detection Systems and ontology is used to extract semantic relations between computer attacks and intrusions. Proposed Distributed Intrusion Detection System is a network which contains a special MasterAgent which contains proposed attacks ontology and some IDS agents which report MasterAgent when an attack or new mistrusted condition is detected. It then updates its ontology, extract the semantic relationship among computer attacks and suspected situations in the network with proposed ontology and alerts the respective system.

Using ontological representation of the intrusions and attacks, Undercoffer [18] presented a host based intrusion detection system, whose performance level was better than the conventional signature-based IDS.

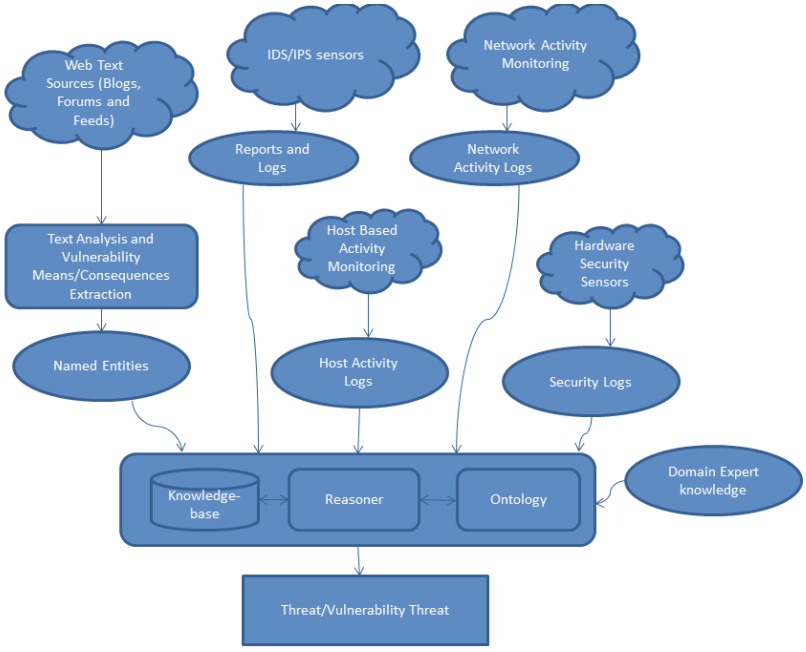

Fig.2 Situation Aware Intrusion Detection System Architecture[2]

Conventional systems are also point-based solutions which are currently incapable of integrating information coming from heterogeneous sources. Hence, threats whose signatures are not present in the knowledge base cannot be detected. Therefore, a semantically rich approach to intrusion detection is needed; where integration of data gathered from different sources and reasoning over such information-rich knowledge base will improve the detection of an attack or threat. Sumit More et. al proposed a situation aware Intrusion Detection model which collects data from heterogeneous sources for threat detection. This model is mainly composed of two sections: data streams and ontology knowledge-base and reasoner. The data streams constitutes of different channels that provide useful information related to an attack. The second section consists of knowledge base which contains information from different data channels in encoded format and the reasoning logic module takes inputs from these streams, the knowledge asserted into the knowledge-base, and the ontology to infer the possibility of a threat/attack.

VIII. HYBRID IDS

Another variation of IDS is hybrid system which is obtained by combining packet header anomaly detection (PHAD) and network traffic anomaly detection (NETAD) which is anomaly-based IDSs with the misuse-based IDS Snort. NETAD finds suspicious packets based on unusual byte values in network packets, while Packet header anomaly detector (PHAD), which is the first anomaly-based approach, added to Snort, acts as a pre-processor .This hybrid approach extracts signatures from the output of anomaly detection system (ADS) and adds them into the SNORT signature database for fast and accurate intrusion

detection. Thus, it combines the advantages of low false-positive rate of signature-based intrusion detection system (IDS) and the ability of ADS to detect novel unknown attacks. This IDS is more powerful and detects many new attacks.

IX. CONCLUSION

In this paper, we briefed various types of intrusion techniques, need for intrusion detection and the classification of intrusion detection systems is explained. Also the advancements to existing IDS viz. Dynamic Multi-Layer Signature based IDS using Mobile Agents; IDS using parallel technique are discussed. Furthermore effective IDS by ontological linking and knowledge based approach are also discussed.

ACKNOWLEDGMENT

We express our sincere thanks to our guide **Prof. Nagesh Jadhav** (Assistant Professor, MIT College of Engineering, Pune) for his support, guidance & motivation. The faith & confidence shown by him in us boosted our moral and motivated us to perform better.

References

1. Herve Debar, "An Introduction to Intrusion Detection Systems", IBM Research, Zurich Research Laboratory, Saumerstrasse 4, Switzerland

2. Sumit More, Mary Matthews, Anupam Joshi, Tim Finin, "A Knowledge-Based Approach To Intrusion Detection Modeling", IEEE Symposium on Security and Privacy Work, © 2012

3. Farzaneh Izak Shiri, Bharanidharan Shanmugam, Norbik Bashah Idris,"A Parallel Technique for Improving the Performance of Signature-Based Network Intrusion Detection System", ©2011 IEEE

4. Mingjun Wei, Guangli Xu and Xuebin Chen, Chaochun Xu, "Study on Ontology-based Intrusion Detection", 2010 International Conference on Computer Application and System Modeling (ICCASM 2010)

5. Sho Ohtahara, Takayuki Kamiyama, Yoshihiro Oyama, "Anomaly-based Intrusion Detection System Sharing Normal Behavior Databases among Different Machines", IEEE Ninth International Conference on Computer and Information Technology

6. Benoît Morel, "Anomaly-based Intrusion Detection using Distributed intelligent systems", Third International Conference on Risks and Security of Internet and Systems: CRiSIS'2008

7. BO SUN AND LAWRENCE OSBORNE, YANG XIAO, SGHAIER GUIZANI, "INTRUSION DETECTION TECHNIQUES IN MOBILE AD HOC AND WIRELESS SENSOR NETWORKS", IEEE Wireless Communications • October 2007

8. Mueen Uddin, Kamran Khowaja and Azizah Abdul Rehman, "Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010

9. Vinod Kumar, Dr. Om Prakash Sangwan, "Signature Based Intrusion Detection System Using SNORT", International Journal of Computer Applications & Information Technology Vol. I, Issue III, November 2012

10. Olusegun Folorunso, Adio Taofiki Akinwale, Aderonke Justina Ikuomola, "Using Visual Analytics to Develop Situation Awareness in Network Intrusion Detection System", Computer and Information Science Vol. 3, No. 4; November 2010

11. M. Ali Aydın, A. Halim Zaim, K. Gökhan Ceylan, "A hybrid intrusion detection system design for computer network security", Computers and Electrical Engineering 35 (2009) 517–526

12. F. Abdoli, M. Kahani, "Ontology-based Distributed Intrusion Detection System", Proceedings of the 14th International CSI Computer Conference (CSICC'09), ©2009 IEEE

13. Ismail Butun, Salvatore D. Morgera, and Ravi Sankar, "A Survey of Intrusion Detection Systems in Wireless Sensor Networks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION

14. Harley Kozushko, "Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems", Thursday, September 11, 2003, Independent Study

15. Peddisetty Naga Raju, "State-of-the-art Intrusion Detection: Technologies, Challenges, and Evaluation" Information theory Divison, Dept of Electrical Engineering, Linkoping University.

16. B. Balajinath, S.V. Raghavan, "Intrusion detection through learning behavior model", Computer Communication (2001), ©Elsevier science

17. A. Fuchsberger, "Intrusion detection systems and intrusion prevention systems", *Elsevier J. Information Security Technical Report*, vol. 10, num. 3, pp. 134-139, 2005

18. J. Undercofer, "Intrusion Detection: Modeling System State to Detect and Classify Aberrant Behavior," Ph.D. dissertation, University of Maryland, Baltimore County, February 2004.

19. T.S. Sobh, "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of the-art", *Elsevier J. Computer Standards and Interfaces*, volume 28, number 6, pages 670-694, 2006.

20. Russell, S. and P. Norvig, 2003, Artificial Intelligence: A Modern Approach [M], 2nd Edn, Prentice Hall, Inc.

21. LIN Ying, ZHANG Yan, OU Yang-Jia. "The Design and Implementation of Host-based Intrusion Detection System", Third International Symposium on Intelligent Information Technology and Security Informatics

Author Profile

Neha Sava, currently pursuing B.E. from Computer Department, M.I.T. College of Engineering, Pune, Maharashtra. 411038

Priya Budhwani, currently pursuing B.E. from Computer Department, M.I.T. College of Engineering, Pune, Maharashtra. 411038

Sanika Talekar, currently pursuing B.E. from Computer Department, M.I.T. College of Engineering, Pune, Maharashtra. 411038

Shalaka Borle, currently pursuing B.E. from Computer Department, M.I.T. College of Engineering, Pune, Maharashtra. 411038

Nagesh Jadhav, received the BE and ME degrees in Information technology from the Bharati Vidyapeeth Deemed University and University of Pune respectively. Currently, he is assistant professor at MIT college of Engineering, Pune, India. His research interests span the following areas: web computing, quality of service based web services discovery and artificial intelligence.

