

# CYBER ATTACKS ON INTRUSION DETECTION SYSTEM

Priyanka Sharma<sup>1</sup> and Rakesh Singh Kunwar<sup>2</sup>

<sup>1,2</sup>Department of IT / Cyber Security, Raksha Shakti University, Ahmedabad, Gujarat

## **ABSTRACT**

*Soft Computing techniques are fast growing technology used for problem solving, Information security is of essence factor in the age of computer world. Protecting information, systems and resources from unauthorized use, duplication, modification, adjustment or any kind of cause which damage the resources such that it cannot be repaired or no longer exist to the real user is one of the part of soft computing. Researcher proposed several mechanism to fight against cyber attacks. Several existing techniques available intrusion detection systems are responsible to face upcoming cyber attacks. Soft computing is one of the best presently using techniques which is applied in Intrusion Detection System to manage network traffic and use to detect cyber attacks with increased efficiency and accuracy.*

## **KEYWORDS**

*Cyber attacks, Cyber Security, Intrusion Detection System, Countermeasure .*

## **1. INTRODUCTION**

Due to advancement in information technology and availability of internet. Malicious objects and contents in the form of open source software's, Integrated Development Environment (IDE), books, codes and online forums are easily available in just few clicks. So, misusing the existing technology the information stored at an interconnected computer in Internet and the information in transit is not secured[1]. Cyber attacks can occur, access the resources and destroy the valuable information which causes a big loss to the society. In 21<sup>st</sup> century various organizations such as healthcare, finance, power corporations, water, telecommunications, transportations, defence, education, research and development, all are hyper connected to the Internet. So, they are highly vulnerable to cyber attacks and such attacks could damage the whole economy so as to permanently and negatively alter the way of life[2][3]. It is very important to protect valuable information from these malicious cyber attacks by providing some means of cyber defence. The major problem face in cyber defence is the prediction about the time of next attack because the time of attack is totally stochastic. To predict the next attack in future, some time analysis of past data gathered from the surroundings of the system is also incomplete and insufficient. Hence, to make the analysed information complete and sufficient for the right prediction of the next cyber attacks Soft computing constructing intelligent systems such as Intrusion Detection Systems, Artificial Neural Network (ANN) and Artificial Intelligence fill the gap.

## **2. SOFT COMPUTING**

In real world, there are several problems with different faces which we have no way to solve logically or can solve theoretically but actually impossible because of huge resource requirement and huge time of computation. To solve these type of problems nature work very efficiently and effectively. The solutions obtained by these methods do not always equal to the mathematically strict solutions, a near optimal solution is sometimes enough in most practical purposes.

International Journal of Information Sciences and Techniques (IJIST) Vol.6, No.1/2, March 2016  
 Soft computing is based on the natural as well artificial ideas. It is referred as a computational intelligence which is differ from the conventional computing known as hard computing. Soft computing is tolerance of imprecision, uncertainty, partial truth of achieve traceability, robustness, approximation, low solution cost and better simulation with reality.

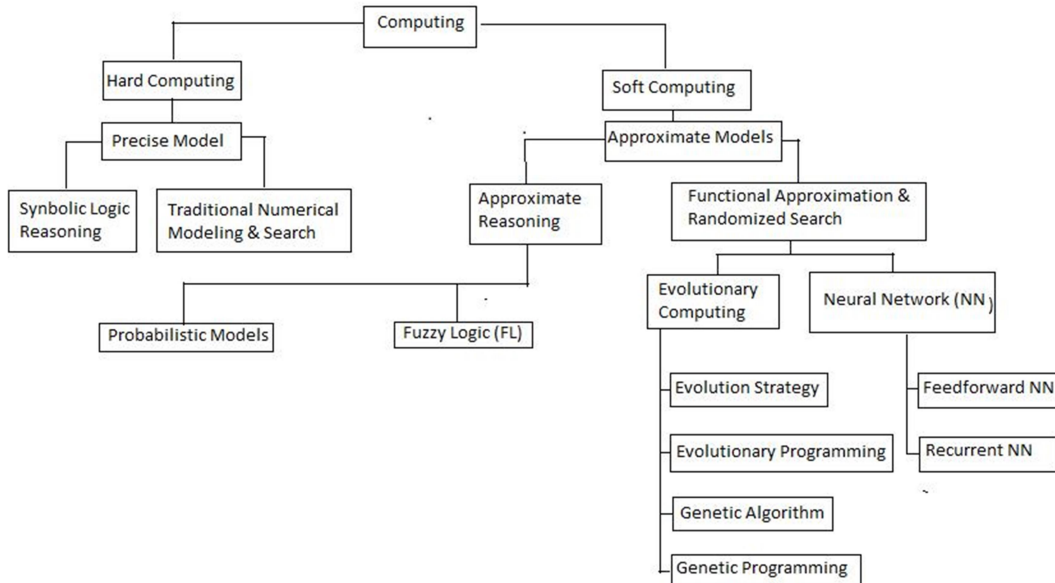


Fig. 1 Different techniques used in soft computing.

### 3. APPLICATIONS OF SOFT COMPUTING

Soft computing is used in various field of research and field as below:

- |  |                           |
|--|---------------------------|
| Handwriting recognition.               | Actuarial science         |
| Automotive systems and manufacturing.  | Agricultural Engineering  |
| Image processing and data compression. | Biomedical application    |
| Architecture                           | Civil engineering         |
| Decision support                       | Computer engineering      |
| Systems power systems                  | Crime forecasting         |
| Neuro fuzzy systems                    | Data mining               |
| Fuzzy logic control                    | Environmental engineering |
| Industrial Machineering                | Fault tolerance           |
| Mechanical engineering                 | Feature selection         |
| Medical diagnosis                      | Image processing          |
| Polymer extrusion process              | Nano technology           |
|  | Pattern recognition       |
|  | Process control           |

#### 4. SOME DISTRIBUTED DENIAL OF SERVICE ATTACKS

**UDP Flood** - UDP is a sessionless networking protocol which leverages the UDP.

Several UDP packets are sent by the attacker to the victim machine ports randomly which cause repeatedly check for the application listening at that port and after getting no application it reply with an ICMP Destination Unreachable packet. Due to which the whole process was busy host resources and can ultimately lead to inaccessibility [4].

**ICMP (Ping) Flood** – This type of attack can consume both outgoing and incoming bandwidth. An ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies. since the victim's servers will often attempt to respond with ICMP Echo Reply packets, resulting a significant overall system slowdown [5].

**SYN Flood** – An exploitation of a known weakness in the TCP connection sequence (the “three-way handshake” is known as SYN flood [6]. Distributed Denial of Service attack, in a TCP connection a SYN request is initiated from requester must be answered by a SYN-ACK response from that host, and then confirmed by an ACK response from the requester. In a SYN flood, multiple SYN request are send from the spoofed IP address and the attacker not respond the host's SYN-ACK response, which make host system to bind the resources until they get the acknowledgement of each of the requests. These type of binding resources ultimately causing denial of service.

**Ping of Death** – In ping of death attack, multiple malformed or malicious pings are send by the attacker to a victim computer. The maximum packet length of an IP packet including header is 65,535 bytes [7]. However, In Data Link Layer the limits to the maximum frame size is 1500 bytes over an Ethernet network. In this case, a large IP packet is split across multiple IP packets which are known as fragments and the recipient host reassembles the IP fragments into the complete packet. But when it reassembles it overflow memory buffers allocated for the packet, causing denial of service for legitimate packets.

**Zero-day DDoS** – “Zero-day” are simply unknown or new attacks, exploiting vulnerabilities for which no patch has yet been released. The term is well-known hacker community, and trading Zero-day vulnerabilities that can be used in attacks has become a popular activity [8].

**Smurf attack** – A smurf attack is an exploitation of the Internet Protocol (IP) broadcast addressing to create a denial of service [9]. To make network inoperable, attacks uses a program called "smurf" which take advantages of certain known characteristics of the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP) by exploiting it. The ICMP is used by network nodes and their administrators to exchange information about the state of the network [10]. ICMP can be used to ping other nodes to see if they are operational. An echo message was send back in response to a ping message in operational node.

#### 5. INTRUSION DETECTION SYSTEMS (IDS)

An intrusion is an activity or regularly set of activities which compromise the information assurance. Intrusion detection system (IDS) is a hardware or software application basically use to monitor the network activities and report the malicious activities to the network administrator.

Intrusions detection systems have a variety of techniques present aims to detect suspicious traffic in different ways. Intrusion detection prevention systems (IDPS) attempts to detect and respond to intrusions against information and information systems. Most of the IDSs are built with a set of components that together define an IDS model. A generic model of IDS is shown in Figure 1.

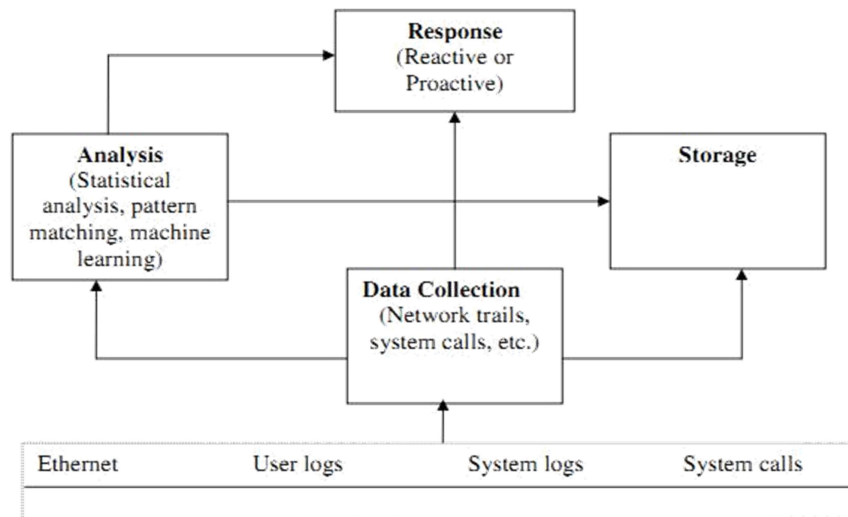


Figure1 Generic Intrusion Detection System Model [11]

From figure, data collections have responsibility to provides information to the system to take decision whether a specific activity is intrusive or not. It collects User logs, System logs, system calls etc. for the other IDS components for the further decision making. This module is very important because without it other modules are un-functional. It audit data reduction i.e. instead of passing the whole raw data to Analysis module to decide whether a activity is malicious or not, it eliminate audit information believed to be unimportant for intrusion analysis. It help in reducing the total complexity of the analysis module.

Analysis module analysis takes input from the data collection module. It focus on concentrated novel classifiers for better and faster classification, high accuracies and low false alarms etc. It uses several techniques for analysis like statistical analysis, pattern matching, machine learning, file integrity checkers and artificial immune system methods etc. It helps in reducing human intervention using automatic analysis and speed up the process of identifying intrusion in real time.

Storage module is used to provide a store to save data collected by data collection and analysis module in a secure way. It is used to store new signatures of malware and threats, updating verified users and system profiles, forensics analysis and identifying key audit information.

Response module can be active or proactive in nature. Generally IDS are designed to be proactive. They beep an alarm when an intrusion takes place. There are different technology like leap forward technology which makes IDS as a reactive devices rather than an aftermath device. Intrusion Detection Prevention Systems not only find out intrusion but also intercept and stop intrusions.

## 5. SOFT COMPUTING TECHNIQUES USED IN IDS

There are some techniques which are used to detect cyber attacks.

- Support Vector Machine (SVM)
- Neural Network (NN)

- Fuzzy logic (FL)

- Evolutionary computation (EC)

## **6. ATTACKS ON INTRUSION DETECTION SYSTEMS (IDS)**

Intrusion Detection Systems have very important role in security chain, from data collection to data analysis and then response, by alerting network or site administrator about the attempts to breach information security policy of the organization. If attackers breach the security then the flawed systems not only provide false information about the current security information but also generate large volumes of false alarms. Moreover, the value of information from faulty systems is not only negated, but potentially misleading [12]

## **7. VULNERABILITIES IN INTRUSION DETECTION SYSTEMS (IDS)**

Components of an IDS are vulnerable to multiple attacks such as:

Data collection module collects user logs, network trails and system calls etc. as a audit trails and tells other component as the suspicious indication for any particular activity is malicious or normal. But if an adversary attacks this module, the whole IDS become un-functional.

An analysis module takes input from the data collection module to decide about any particular activity is normal or malicious. But, if an adversary knows the analysis techniques then he can mislead and malfunctions the IDS.

Storage module provides a mechanism to store data by data collection and analysis module. This data is useful to create and save new signatures, updating users and system profiles etc. If attacker that can compromise the storage module can change the logging setting and easily remove the attack information. It can easily insert or delete the audit info, can change in profiles and can change the intrusion detection signatures of the IDS.

Response modules have mechanism for aftermath operations. A compromise on it will allow the attacker to continuously attack the system without generating an alarm. An Attacker can make the system in such a manner that it deny legitimate activity and accept malicious activity even it is reactive device.

## **8. CONCLUSIONS**

In this chapter we outline the different areas of soft computing with the working of several distributed denial of service attacks. In it we also present the current cyber security challenges from an intrusion detection system and vulnerabilities present in the IDS. With the advancement of technology, it also encourages the soft computing techniques to be secure and available into both every day and advanced applications.

## **ACKNOWLEDGEMENTS**

I would like to thank Research & Development department, Raksha Shakti University, which provide me a platform to research in internal security field. I would like to express my sincerest thanks to Dr. Priyanka Sharma for their continue support and feedback for the work.

## REFERENCES

- [1] Dinesh Kumar Saini “Sense the Future” Campus Volume 1- Issue 11, Page No14-17, February 2011.
- [2] Antonatos S., Akritidis P., Markatos E. P., Anagnostakis K. G. “ Defending against hit-list worms using network address space randomization.Proceedings of the 2005 ACM workshop on Rapid \ malware. ACPress NewYork NY, USA. pp. 30-40; 2005. [tps://www.symantec.com/about/news/release/article.jsp?prind=20110721\\_01](https://www.symantec.com/about/news/release/article.jsp?prind=20110721_01)
- [3] Dinesh Kumar Saini “A Mathematical Model for the Effect of Malicious Object on Computer Network Immune System” Applied Mathematical Modeling, 35(2011) Page No. 3777-3787 USA,doi:10.1016/.2011.02.025.<https://www.isaca.org/About-ISACA/Press-room/News-Releases/2010/Pages/Top-Five-Social-Media-Risks-for-Business-New-ISACA-White-Paper.aspx>
- [4] Abhijeet Prakash “Hack the world- Ethical Hacking”. Module 8, Denial of Service.
- [5] <http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack>.
- [6] <https://www.incapsula.com/ddos/ddos-attacks>. Accessed on 13 Jan 2016.
- [7] <http://blog.ddos-guard.ir/distributed-denial-service-ddos-attack>. Accessed on 14 Jan 2016.
- [8] <http://ongoingoperations.com/blog/2013/05/how-many-kinds-of-ddos-attacks-are-there-part-4>. Accessed on 14 Jan 2016.
- [9] <http://heelpbook.altervista.org/2014/what-is-a-smurf-attack>. Accessed on 14 Jan 2016.
- [10] <http://searchsecurity.techtarget.com/definition/smurfing>. Accessed on 14 Jan 2016.
- [11] Mukkamala S., sung A. ,Abraham A. “Cyber Security Challenges: Designing Efficient Intrusion Detection Systems and Antivirus Tools”.
- [12] Ptacek H. T., and Newsham N. T. (1998) Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection. Secure Networks Inc.

### Authors:

#### 1) Priyanka Sharma

She is a professor of the Department of Information Technology and Cyber Security in the Raksha Shakti University. Prior to beginning academic career, she have 16 + year experience. Her main research area is knowledge based management system. She has published more than 80 article and research papers in several national & international journal.



#### 2) Rakesh Singh Kunwar

He is a Research Scholar in Cyber Security from Raksha Shakti University. His topic of research is Social media security analysis. He have 4 years academic experience after his Master in computer Application from HNBGU Utrakhand and M.Tech in computer networking from Graphic Era University.

