Journal of Science, Computing and Engineering Research (JSCER)
Volume-9, Issue-3, March 2026.
DOI: *https://doi.org/10.46379/jscer.2024.0709*
ISSN: 2708-1079

Key Challenges for IDS in Detecting and Mitigating Web Cyber Attacks

S.Dhannabasava,M. Shennashetty, M.Majashekhar and K.Vijaykumar

Assistant Professor,SNR Sons College, India

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.

Corresponding Author:

Saroja Gajendran

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

Citation: Saroja Gajendran, Naamasivam, "Challenges of WEB Cyber Attacks on Intrusion Detection System", Journal of Science, Computing and Engineering Research, 9(3), March 2026.

I. INTRODUCTION

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.

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 21st 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.

II. 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.

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.

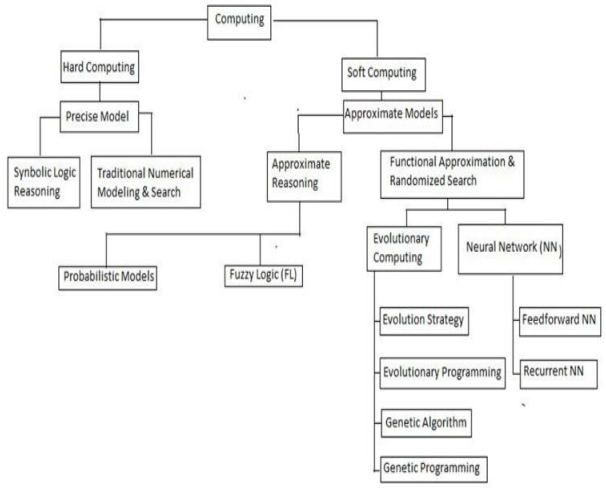

Fig. 1 Different techniques used in soft computing.

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

IV. 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 an 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 toping other nodes to see if they are operational. An echo message was send back in response to a ping message in operational node.

V. 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.

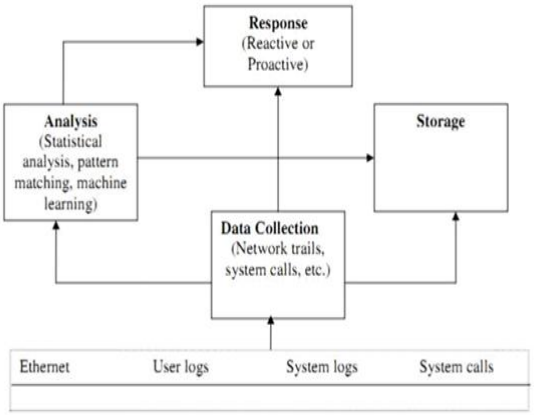

Figure1 Generic Intrusion Detection System Model [11]

Figure1 Generic Intrusion Detection System Model

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 an

Comparator is a circuit that output is binary information depending upon the comparison of two input voltages here the comparison in between analog voltage and reference voltage. Analog voltage is greater than reference voltage, and then comparator output is logic '1'. The comparator output is logic '0', when analog voltage is less than reference voltage. Comparators are effectively used in analog to digital (ADC) converters. In analog to digital conversion process [1], the analog voltage is converted in to samples for getting accuracy. Those samples are given to set of comparators in order to achieve equivalent binary information.

VI. 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) 194 Evolutionary computation (EC)

VII. 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]

VIII. 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.

IX. CONCLUSION

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.

REFERENCES

[1]. P. Nirmala, T. Manimegalai, J. R. Arunkumar, S. Vimala, G. Vinoth Rajkumar, Raja Raju, "A Mechanism for Detecting the Intruder in the Network through a Stacking Dilated CNN Model", Wireless Communications and Mobile Computing, vol. 2022, Article ID 1955009, 13 pages, 2022. https://doi.org/10.1155/2022/1955009.

[2]. D. Sathyanarayanan, T. S. Reddy, A. Sathish, P. Geetha, J. R. Arunkumar and S. P. K. Deepak, "American Sign Language Recognition System for Numerical and Alphabets," 2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), Chennai, India, 2023, pp. 1-6, doi: 10.1109/RMKMATE59243.2023.10369455.

[3]. J. R. Arunkumar, Tagele berihun Mengist, 2020" Developing Ethiopian Yirgacheffe Coffee Grading Model using a Deep Learning Classifier" International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-4, February 2020. DOI: 10.35940/ijitee.D1823.029420.

[4]. Ashwini, S., Arunkumar, J.R., Prabu, R.T. et al. Diagnosis and multi-classification of lung diseases in CXR images using optimized deep convolutional neural network. Soft Comput (2023). https://doi.org/10.1007/s00500-023-09480-3

[5]. J.R.Arunkumar, Dr.E.Muthukumar," A Novel Method to Improve AODV Protocol for WSN" in Journal of Engineering Sciences" ISSN NO: 0377-9254Volume 3, Issue 1, Jul 2012.

[6]. R. K, A. Shameem, P. Biswas, B. T. Geetha, J. R. Arunkumar and P. K. Lakineni, "Supply Chain Management Using Blockchain: Opportunities, Challenges, and Future Directions," 2023 Second International Conference on Informatics (ICI), Noida, India, 2023, pp. 1-6, doi: 10.1109/ICI60088.2023.10421633.

[7]. Arunkumar, J. R. "Study Analysis of Cloud Security Chanllenges and Issues in Cloud Computing Technologies." Journal of Science, Computing and Engineering Research 6.8 (2023): 06-10.

[8]. J. R. Arunkumar, R. Raman, S. Sivakumar and R. Pavithra, "Wearable Devices for Patient Monitoring System using IoT," 2023 8th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2023, pp. 381-385, doi: 10.1109/ICCES57224.2023.10192741.

[9]. S. Sugumaran, C. Geetha, S. S, P. C. Bharath Kumar, T. D. Subha and J. R. Arunkumar, "Energy Efficient Routing Algorithm with Mobile Sink Assistance in Wireless Sensor Networks," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ACCAI58221.2023.10201142.

[10]. R. S. Vignesh, V. Chinnammal, Gururaj.D, A. K. Kumar, K. V. Karthikeyan and J. R. Arunkumar, "Secured Data Access and Control Abilities Management over Cloud Environment using Novel Cryptographic Principles," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ACCAI58221.2023.10199616.

[11]. Syamala, M., Anusuya, R., Sonkar, S.K. et al. Big data analytics for dynamic network slicing in 5G and beyond with dynamic user preferences. Opt Quant Electron 56, 61 (2024). https://doi.org/10.1007/s11082-023-05663-2

[12]. Krishna Veni, S. R., and R. Anusuya. "Design and Study Analysis Automated Recognition system of Fake Currency Notes." Journal of Science, Computing and Engineering Research 6.6 (2023): 16-20.

[13]. V. RamKumar, S. Shanthi, K. S. Kumar, S. Kanageswari, S. Mahalakshmi and R. Anusuya, "Internet of Things Assisted Remote Health and Safety Monitoring Scheme Using Intelligent Sensors," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ACCAI58221.2023.10199766.

[14]. R. S. Vignesh, R. Sankar, A. Balaji, K. S. Kumar, V. Sharmila Bhargavi and R. Anusuya, "IoT Assisted Drunk and Drive People Identification to Avoid Accidents and Ensure Road Safety Measures," 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ACCAI58221.2023.10200809.

[15]. I. Chandra, G. Sowmiya, G. Charulatha, S. D, S. Gomathi and R. Anusuya, "An efficient Intelligent Systems for Low-Power Consumption Zigbee-Based Wearable Device for Voice Data Transmission," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ICECONF57129.2023.10083856.

[16]. G. Karthikeyan, D. T. G, R. Anusuya, K. K. G, J. T and R. T. Prabu, "Real-Time Sidewalk Crack Identification and Classification based on Convolutional Neural Network using Thermal Images," 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2022, pp. 1266-1274, doi: 10.1109/ICACRS55517.2022.10029202.

[17]. R. Meena, T. Kavitha, A. K. S, D. M. Mathew, R. Anusuya and G. Karthik, "Extracting Behavioral Characteristics of College Students Using Data Mining on Big Data," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ICECONF57129.2023.10084276.

[18]. S. Bharathi, A. Balaji, D. Irene. J, C. Kalaivanan and R. Anusuya, "An Efficient Liver Disease Prediction based on Deep Convolutional Neural Network using Biopsy Images," 2022 3rd International Conference on Smart

Electronics and Communication (ICOSEC), Trichy, India, 2022, pp. 1141-1147, doi: 10.1109/ICOSEC54921.2022.9951870.

[19]. I. Chandra, G. Sowmiya, G. Charulatha, S. D, S. Gomathi and R. Anusuya, "An efficient Intelligent Systems for Low-Power Consumption Zigbee-Based Wearable Device for Voice Data Transmission," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ICECONF57129.2023.10083856.

[20]. Revathi, S., et al. "Developing an Infant Monitoring System using IoT (INMOS)." International Scientific Journal of Contemporary Research in Engineering Science and Management 6.1 (2021): 111-115.

[21]. J.R.Arunkumar, Dr.E.Muthukumar,‖ A Novel Method to Improve AODV Protocol for WSN‖ in Journal of Engineering Sciences‖ ISSN NO: 0377-9254Volume 3, Issue 1, Jul 2012.

[22]. R. S. Vignesh, A. Kumar S, T. M. Amirthalakshmi, P. Delphy, J. R. Arunkumar and S. Kamatchi, "An Efficient and Intelligent Systems for Internet of Things Based Health Observance System for Covid 19 Patients," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ICECONF57129.2023.10084066.

[23]. I. Chandra, K. V. Karthikeyan, R. V, S. K, M. Tamilselvi and J. R. Arunkumar, "A Robust and Efficient Computational Offloading and Task Scheduling Model in Mobile Cloud Computing," 2023 International Conference on Artificial Intelligence and Knowledge Discovery in Concurrent Engineering (ICECONF), Chennai, India, 2023, pp. 1-8, doi: 10.1109/ICECONF57129.2023.10084293.

[24]. R. K, A. Shameem, P. Biswas, B. T. Geetha, J. R. Arunkumar and P. K. Lakineni, "Supply Chain Management Using Blockchain: Opportunities, Challenges, and Future Directions," 2023 Second International Conference on Informatics (ICI), Noida, India, 2023, pp. 1-6, doi: 10.1109/ICI60088.2023.10421633.

[25]. J. R. Arunkumar, and R. Anusuya, “OCHRE: A Methodology for the Deployment of Sensor Networks.” American Journal of Computing Research Repository, vol. 3, no. 1 (2015): 5-8.