Recent Developments in Electronics and Communication Systems
KVS Ramachandra Murthy et al. (Eds.)

doi:10.3233/ATDE221274

Artificial Intelligence Based System for Securing Computer Networks: A Survey

Bidawat Tarajit Singh[a], Bollarapu Sundara Kumar[b], T. Rama Reddy[c], B.S.Kiruthika Devi[d,1]

[a,b] *Department of CSE, Aditya Engineering College (A), Surampalem, India*
[c] *Professor, Department of CSE, Aditya Engineering College (A), Surampalem, India*
[d] *Research Mentor, CL Educate Ltd., New Delhi, India*

Abstract. The security of computer networks is crucial in today's computer systems. A number of software technologies are now being developed in order to impose high levels of protection against harmful attacks. Because of their potential to detect and prevent assaults by malicious network users, intrusion detection systems have recently become a hot research issue. This article discusses various recent techniques such as anomaly, signature, open source IDS such as SNORT, machine learning, and edge assisted technologies in detail, along with the advantages and disadvantages of the deployed system. The tools used, datasets, performance metrics, and the accuracy of the methodologies are compared, and it gives a clear view of further advancements in computer networks. Based on the studies, it can be said that machine learning algorithms work better than other traditional methods and make security better.

Keywords. Anomaly based detection, signature based detection, SNORT detection, BP neutral network, focal loss neural network, edge-assisted internet of things.

1. Introduction

Artificial intelligence has a vast range of applications, ranging from general domains like vision and logical thinking to specific tasks like chess, from proving mathematical theorems to producing poetry and diagnosing diseases [1-3]. Expert systems, intelligent controls, neural networks, and natural language processing are just a few examples of how AI staff can apply their methods to every field of human intellectual activity. For difficulties that humans face in a variety of domains, AI technology gives excellent answers in a minimal number of steps [4-7]. It primarily consists of state graph search tools, predicate logic reasoning techniques, and organized problem-solving approaches based on state graphs, reasoning techniques based on predicate logic, and solving techniques based on organized knowledge representation, such as semantic and ES-networks, are a few examples [8-12].

When artificial intelligence is combined with computer network technology, a greater number of user-friendly services can be supplied and applied. Intrusions are attempts or

[1] Corresponding Author, B.S.Kiruthika Devi, Research Mentor, CL Educate Ltd., New Delhi, India; E-mail: kiruthika.devi@accendere.co.in

activities that are made to compromise the confidentiality, integrity, or availability of a computer or network [13-17]. The Intrusion Detection System (IDS), which entails a software or hardware system that tracks, analyses, and recognizes ongoing events from both inside and outside the network as illegal activity, is one of the best methods for detecting attacks. IDS's performance was harmed by the large amount of data, and it was also harmed by the redundant and irrelevant information detected in its traffic [18-20]. The Internet has become a crucial part of everyday communication via social media interaction, e-mail, e-learning, etc. No doubt, some risks are incurred owing to the use of ineffective and inefficient security tools, which invite intrusions from Internet hackers. IDS enables a range of functions in computer networks, including automatic data collection, fast fault diagnosis, and online performance analysis, among others. If a fault arises, it will not only respond quickly but will also take a number of specific actions. Intrusion detection is the most important part of computer network security management because it is what makes sure that network security services are delivered well [21-23].

2. Related Work

Mushtaq et al. developed a new intrusion detection system using fuzzy logic and genetic algorithms. A genetic algorithm combined with fuzzy logic allowed him to improve his results by taking advantage of the rule reduction that is inherent in fuzzy logic. Detection of infiltration is done using neural networks and fuzzy clusters [1]. IDS systems are classified into two types: host-based intrusion detection systems (HIDS) [17] and network-based intrusion detection systems (NIDS) [2]. Hodo et al. developed a multi-layered neural-network trained that uses feedforward and backward learning methods. In some instances, attacks on systems were detected with great accuracy by the proposed approach, with an average accuracy of 94 percent [3]. Rinku Sen et al. designed a modular back propagation neural network (BPNN) architecture to identify the invasion using an anomaly detection technique. According to their findings, the BPNN architecture with four hidden layers and a neuron combination of 3-4-5-3, when applied to a 70–30% split of the KDD-dataset, produces the best results [4]. With the rapid expansion of artificial intelligence, machine learning-based intrusion detection has lately gained prominence. A machine can develop a distributed IDS using fog computing. The attacker was interpreted by this IDS once it identified an incursion in the path of the fog nodes, as opposed to traditional, centralized IDS [5]. A working principle of an artificial neural network (ANN) is based on supervised learning from the system's previous experiences using labelled data as a training set. The system's performance is influenced by a number of factors such as training function, magnitude of the data, capability of the computer, and so on [6]. Xiang et al. proposed a hierarchy-based hybrid method. The number of false positives produced by this method is larger. Using various elements of the dataset, Chen et al. used evolutionary techniques to create base classifiers for the ensemble [7]. A novel network-based detection framework for IoT intrusion detection that coordinates sensor nodes and edge routers while taking resource constraints into account was proposed by Arshad et al. [8]. By removing the highly non-linear correlations that exist between the various fields, neural networks aid in real-time intrusion detection. They have a high degree of generality, which means they can calculate the desired result [9], [10].

3. Methodology Used

In this methodology section, the various types of detection methods based on anomaly, signature, machine learning, open source, and edge computing are being discussed in detail.

3.1. Anomaly detection with feature selection

Undoubtedly, one of the most significant issues is the high computational time complexity associated with many feature selection techniques. Due to these advantages over other search algorithms, the cuckoo search algorithm (CSA) was used to choose the attributes in this study. Mutation Cuckoo Fuzzy (MCF) is a new feature selection method that combines the mutation-operator with cuckoo-search and Fuzzy C-Means (FCM) clustering to produce a feature selection method that is both fast and accurate [11], [13]. An evaluation criterion can be divided into two main categories based on the learning algorithms that will be used to apply the selected feature subset. Independent criteria and dependent criteria are the two types of criteria that are used. The feature selection process comes to an end while the task is completed.

3.2. Signature detection and anomaly based detection

DDoS attacks' signatures are used to compare traffic within the network for known attacks in a database of signatures. A neural network-based anomaly detection technique has been created [4]. This detector runs on Apache Spark and makes use of the BigDL deep learning library. Spark is a distributed and rapid processing engine. An auto-encoder is a type of neural network that has been constructed. Backpropagation is commonly used to make the output equal to the input values. The signature-based attack detection makes use of specified characteristic sets to identify alarms. In order to build our signatures against DDoS attacks, Suricata, an open-source IDS, is used. Rules are continually being added and modified to meet changing circumstances. The detection system can be made better by changing how precise the rule set is while it is being run [17], [18].

3.3. Deep auto encoder with fruit fly optimization

An auto-encoder is a type of multilayer-perceptron in which the input and output layers have the same number of neurons [112]. As with Deep Belief Networks (DBNs), a deep auto-encoder will be built by stacking numerous auto-encoders. It is utilized to extract more complicated representations from the raw data. The auto-encoder's design consists of two important components, such as an encoder and a decoder. Each layer in a deep auto-encoder receives its input from the preceding layer. The auto-encoder is taught to turn the raw input into a hidden or abstract representation, and then to use this compressed representation to reconstruct the output.

3.4. Improved Back Propagation (BP) neural network

The susceptibility of classical back propagation (BP) to sliding into training inertia and slow convergence are two of its major flaws. When the intrusion detection system's data acquisition module is activated, the system collects data from var

ious sources inside the networks and extracts a subset of that data to be used in the system's initial training set. A neural network's connection weight and learning rate may be optimized using data sources, and the optimum weight and rate can be changed by altering the neural network as shown in Figure 1 [14]. The major aspects that need to be considered are: i) Detecting intrusion behavior using the enhanced neural network detection system ii) After fine-tuning the parameters, reviewing and updating the knowledge base and training base iii) Halting the settings when the system is in a better state, or else initiating the optimization process.

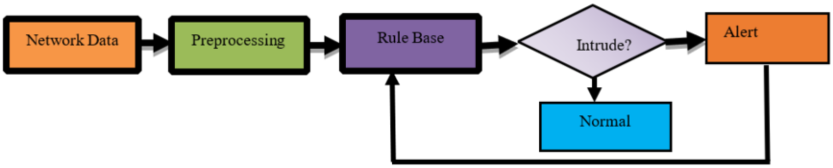

Figure 1. BP neural network

3.5. Snort based smart and swift intrusion detection system

Snort is separated into several components that operate together to identify certain assaults and generate outputs from the detection system [13]. Snort-based IDs are made up of packet decoders, preprocessors, detection engines, logging and alerting systems, and output modules. A packet decoder processes the packets in the network. Preprocessors involve normalization of protocol headers, detection of anomalies, reassembly of packets, and re-assembly of TCP. The detection engine defines the rules and the packets are inspected for their patterns. The logging and alerting system is responsible for the generation of log-messages and alerts. The output process processes the alerts and logging activity and generates the end result. Artificial neural networks [14] are excellent tools for categorizing into many groups, especially in applications where formal analysis is difficult or impossible, such as non-linear system identification and pattern recognition. A novel approach for intrusion detection has been provided in the proposed system, which makes use of Multi-Layer Perceptron (MLP) for intrusion detection [1].

3.6. Edge-assisted Internet of Things

The proposed edge-assisted IDS consists of three primary components such as feature selection, dataset learning, and intrusion detection. In order to properly implement intrusion detection, it is necessary to first pick the features and build the model. The edge-assisted IDS has two steps: data-based intrusion detection and time-interval intrusion detection. The BP neural-network [8] module is used in the data-based technique to identify anomalous data which does not resemble the characteristics of normal data streams. The RBF neural network is utilized in a time-interval-based system to detect each attack fraction in the periodicity of data creation.

3.7. Focal loss neural network

One of the most serious issues in an intrusion detection system is sample imbalance between classes. Therefore, the sample imbalance will result in bad training on the parameters. In this research, we use the focal loss [6] to improve the intrusion detection system's sample imbalance effects as shown in Figure 2. Due to the current complex worldwide scenario, cyber security has recently been one of the most popular applications in both the industrial and academic worlds. The internet has infiltrated every facet of existence. This impact will continue to expand with the advancement of technologies such as the Internet of Things and 5G [15].

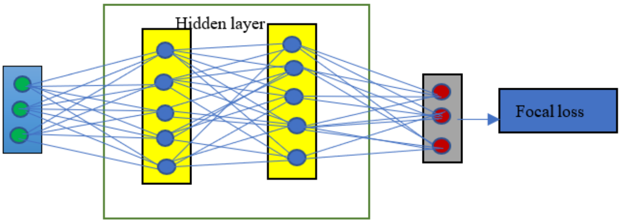

Figure 2. Focal loss neural network

4. Results and Discussions

Table 1 shows the comparison between various intrusion detection systems in the cloud along with the advantages, disadvantages, tools used, dataset, performance and accuracy.

Table 1. Comparison between various intrusion detection systems in cloud

S.No	Techniques Used	Advantages	Disadvantages	Tools Used	Dataset	Performa-nce	Accuracy
1	Anomaly [10]	It can detect any unknown attacks	Detection accuracy is low.	MLP,CSA, MVO	NSL KDD	False alarm	98.81%
2	Signature [13]	Detection accuracy is high	It can't detect any unknown attacks	SNORT IDS	KDD '19	Accuracy	98%
3	Fruitfly [11]	Simple and easy to deploy	Optimization is required.	Deep auto encoder	NSL KDD	Time	94%
4	BP Neutral [12]	Distributed memory.	Sensitive to noisy data.	MATLAB	KDD' 99	Detection rate	93.31%
5	Smart swift [13]	Highly customized	Needs further tuning	SNORT	KDD'99	Alert	99.87%

6	Focal loss [6]	Information storage	The time for threat exposure is unknown.	KDD99	UNSW NB15	Loss	99.22%
7	MLP [1]	Can learn non-linear models.	Parameters are fully connected.	Penetration detection	KDD99	Precision	94%
8	Edge-assisted IoT [8]	Improved security.	Security issues persists.	Edge-assisted IDS	KDD’99	False alarm	92.96%

5. Conclusion and Future Work

People's daily lives cannot be separated from the computer systems in the workplace. As a result, artificial intelligence technology must be implemented to analyses problems that cannot be solved purely through computer technology. In this study, various techniques such as anomaly, signature, open source IDS such as SNORT, machine learning, and edge-assisted based detection are studied in detail. The methods are compared with various performance metrics and their accuracy. To meet the needs of this new field, artificial intelligence needs more research and contributions to its growth. Based on the studies, it is clear that learning-based systems make computer networks safer.

References

[1] Tavoli R. Providing a method to reduce the false alarm rate in network intrusion detection systems using the multilayer perceptron technique and backpropagation algorithm. In2019 5th Conference on Knowledge Based Engineering and Innovation (KBEI) 2019 (pp. 001-006). IEEE.

[2] Luo X. Model design artificial intelligence and research of adaptive network intrusion detection and defense system using fuzzy logic. Journal of Intelligent & Fuzzy Systems. 2021 Jan 1;40(4):8227-35.

[3] Almiani M, AbuGhazleh A, Al-Rahayfeh A, Atiewi S, Razaque A. Deep recurrent neural network for IoT intrusion detection system. Simulation Modelling Practice and Theory. 2020 May 1;101:102031.

[4] Chiba Z, Abghour N, Moussaid K, El Omri A, Rida M. A novel architecture combined with optimal parameters for back propagation neural networks applied to anomaly network intrusion detection. Computers & Security. 2018 Jun 1;75:36-58.

[5] Nie L, Ning Z, Wang X, Hu X, Cheng J, Li Y. Data-driven intrusion detection for intelligent Internet of vehicles: A deep convolutional neural network-based method. IEEE Transactions on Network Science and Engineering. 2020 Apr 27;7(4):2219-30.

[6] Cheng Z, Chai S. A cyber intrusion detection method based on focal loss neural network. In2020 39th Chinese Control Conference (CCC) 2020 Jul 27 (pp. 7379-7383). IEEE.

[7] Zhao H, Li M, Zhao H. Artificial intelligence based ensemble approach for intrusion detection systems. Journal of Visual Communication and Image Representation. 2020 Aug 1;71:102736.

[8] Wu D, Yan J, Wang H, Wang R. Multiattack intrusion detection algorithm for edge-assisted internet of things. In2019 IEEE International Conference on industrial internet (ICII) 2019 Nov 11 (pp. 210-218). IEEE.

[9] Karri KP, Anil Kumar R, Kumar S. Multi-point Data Transmission and Control-Data Separation in Ultra-Dense Cellular Networks. InICCCE 2020 2021 (pp. 853-859). Springer, Singapore.

[10] Solomon IA, Jatain A, Bajaj SB. Neural network based intrusion detection: State of the art. InProceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India 2019 Feb 26.

[11] Sarvari S, Sani NF, Hanapi ZM, Abdullah MT. An efficient anomaly intrusion detection method with feature selection and evolutionary neural network. IEEE Access. 2020 Apr 7;8:70651-63.

[12] Sekhar R, Sasirekha K, Raja PS, Thangavel K. A novel GPU based intrusion detection system using deep autoencoder with Fruitfly optimization. SN Applied Sciences. 2021 Jun;3(6):1-6.

[13] Yang A, Zhuansun Y, Liu C, Li J, Zhang C. Design of intrusion detection system for internet of things based on improved BP neural network. Ieee Access. 2019 Jul 19;7:106043-52.

[14] Priya BJ, Kunda P, Kumar S. Design and Implementation of Smart Real-Time Billing, GSM, and GPS-Based Theft Monitoring and Accident Notification Systems. InProceedings of International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications 2021 (pp. 647-661). Springer, Singapore.

[15] Olanrewaju RF, Khan BU, Najeeb AR, Zahir KN, Hussain S. Snort-based smart and swift intrusion detection system. Indian Journal of Science and Technology. 2018 Jan 14;11(4):1-9..

[16] Alzahrani AS. An optimized approach-based machine learning to mitigate DDoS attack in cloud computing. International Journal of Engineering Research and Technology. 2020;13(6):1441-7.

[17] Gundabathula G, Kunda P, Nandan D, Kumar S. Implementation of Cloud Based Traffic Control and Vehicle Accident Prevention System. InICCCE 2020 2021 (pp. 1125-1134). Springer, Singapore.

[18] Eskandari M, Janjua ZH, Vecchio M, Antonelli F. Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE Internet of Things Journal. 2020 Jan 30;7(8):6882-97.

[19] Otoum Y, Nayak A. As-ids: Anomaly and signature based ids for the internet of things. Journal of Network and Systems Management. 2021 Jul;29(3):1-26.

[20] Martins I, Resende JS, Sousa PR, Silva S, Antunes L, Gama J. Host-based IDS: A review and open issues of an anomaly detection system in IoT. Future Generation Computer Systems. 2022 Mar 15.