IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor: 6.252

A Study on DDOS Attacks, Danger, and its Prevention

Mr. Ashwin Bhanudas Wankhede[1] and Dr. Priya Chandran[2]
Student, Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, India[1]
Assistant Professor, Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai, India[2]

Abstract: *The current era is entirely dependent on the Internet that serves as a global source of information for all users. Therefore, internet access is very important. Prohibition of service distribution is one of the most highlighted and most important types of cyber-attacks in today's world. This paper focuses on DDoS attacks that prevent network access by flooding the victim with high volume of illegal traffic grabbing its bandwidth, burdening it to prevent traffic from passing. We also described the several types of DoS attack strategies implemented in ISPs. The purpose of this study is to find a variety of strategies to prevent these attacks and their methods of mitigating and finding any possible solution. The dataset consists of Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP) normal and attack traffics. The dataset, including further than 100 thousand recordings, has statistical features similar as byte count, duration, sec, packet rate, and packet per inflow, except for features that define source and target machines.*

Keywords: DDos attacks; Security Challenges; Preventing DDos; DoS; Intrusion Detection; SDN

I. INTRODUCTION

The Internet is defined as the interconnected system of computer networks. The scope of the internet in everyday life is enormous. Provides comprehensive information, resources, resources that allow all sectors to be well connected as the demand for the Internet grows rapidly over time, various issues related to its security. The reason for the insecurity of the internet is basically related to its design because what was most troubling was its functionality rather than its security. So, a few types of attacks and threats are a cause for concern about cyber security.

Issues related to online security are security, integrity, accessibility, confidentiality, and non-compliance. Among all the DDoS (Distributed Denial of service) attacks is what prevents clients, users from accessing all the benefits of the services available to them on the server side. The number of DoS and DDoS attacks on Internet Service Providers has increased dramatically in the last few years. Service providers are under a lot of pressure preventing, monitoring and mitigating DDoS attacks targeted at their customers and their infrastructure.

In this study, we concentrate on the SDN to insure a featherlight mongrel model equipped with NCA and machine literacy approaches to contribute to icing a new- generation manageable network armature. In detecting DDoS attacks with machine literacy, some inflow characteristics(packet size, appearance time, response time, packet rate, packet per inflowed.) are used to identify whether the network business is normal. DDoS attacks frequently use the same average packet size.

II. RESEARCH METHODOLOGY

In this study, the public "DDOS attack SDN Dataset", which was created in the SDN environment and made publicly accessible to researchers for use in machine learning and deep learning research, was used [10]. This information set contains around 104345 DDoS Attack data that embrace differing kinds of attacks. The info is in CSV format (comma separated values). The model was trained employing a machine learning technique utilizing this dataset. This model is trained victimization Jupiter Notebook with range of various libraries like numpy, matplotlib, pandas etc. This dataset may have missed or null values, stop words, or duplicates that require to be eliminated before it is used. Python is employed to implement the machine learning techniques.

This dataset has been collected first. The dataset was then pre-processed, which included deleting duplicates, missing or null values, stop words, and so on. After then, the data is divided into two groups: train and test. These train and test sets

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor: 6.252

are used to apply machine learning algorithms. After that, the trained model is created, the data is processed in it, and the expected output is calculated.

2.1. Machine Learning Approach

Machine learning ways area unit want to analyze system performance and notice uncommon events that aren't in step with traditional network behavior. particularly in network systems wherever high-density information is current, abnormal movements area unit detected by mathematical models created victimization machine learning algorithms, and preventive policies are quickly applied to network systems. during this section, the options of the machine learning approaches employed in this study area unit concisely explained.

2.1.1 k-Nearest Neighbor (k-NN) Classifier

k-NN is one amongst the favored machine learning algorithms. it's a non-parametric, distance-based, and supervised approach that was introduced in 1951 [21]. This algorithmic rule measures the similarities within the dataset considering a distance operate. The look at information area unit classified supported the bulk votes of its k-nearest neighbors. A coaching set is outlined as X and Y pairs. Let X = wherever xi ∈ R^n n corresponds to the coaching information within the n-dimension feature set and let Y = match the target labels. A prediction for a take a look at information xˆ applied as input to the kNN model is realized as follows [22]: • A distance operate like a geometer one is employed to live similarity within the coaching information. for 2 points named a and b have philosopher coordinates (a1, a2) and (b1, b2), the space between a and b is calculated as given in Equation (1):

$$d(a, b) = \sqrt{(a1 - b1)^2 + (a2 - b2)^2} \quad (1)$$

The label of take a look at information xˆ is decided considering the bulk votes of its k-nearest neighbors.

2.1.2 Decision Tree

The decision tree machine learning algorithmic program is employed for regression also because the classification of real-world issues. This model is impressed by a tree structure. However, the root of the tree is found at the highest. The branches area unit created considering objective rules relied on the options of the dataset, and also the call tree is additionally increasingly developed [23]. To create a call tree, the procedures delineated below is followed [24]:

1. The total dataset is split into 2 components as coaching and check sets.
2. The coaching set is applied because the input to the foundation of the tree.
3. The foundation is decided victimization scientific theory as delineated in Equation (2).
4. The prone procedure is dispensed.
5. The procedures between one and four area unit followed once more and once more till all nodes become leaf nodes.

$$\text{Entropy(P)} = -\sum_{i=1}^{N} pi \log(pi) \quad (2)$$

where the probability distribution of the dataset is denoted with p. To achieve an efficient decision tree, there are also other hyper-parameters, such as the minimum leaf size, minimum parent size, and the maximum number of splits to be set.

2.1.3 Random Forest Classifier

The Random Forest rule consists of various call trees, every with a similar node, however victimization totally different information that results in different leaves. It merges the calls selections of multiple decision trees so as to seek out a solution, which represents the common of these call trees.

When victimization the Random Forest algorithmic rule to unravel regression issues, your victimization the mean square error (MSE) to however your information branches from every node.

$$\text{MSE} = \frac{1}{N}\sum_{i=1}^{N}(fi - yi)^2$$

This formula calculates the space of every node from the anticipated actual price, serving to come to a decision to make your mind up to determine that branch is that the higher decision for your forest. Here, Yi is that the price of the info purpose you're testing at a particular node and fi is that the price came by the choice tree[23]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor: 6.252

2.1.4 Logistic Regression

One amongst the supervised learning techniques is supply regression. it's used within the answer of classification difficulties. supply regression can even be accustomed predict dependent variables given a collection of freelance variables. Binomial, multinomial, and ordinal supply regression area unit the 3 types of supply regression. Binomial supply regression was used during this study. There is area unit simply 2 attainable outcomes in Binomial supply regression. Equation for supply regression:

$$log\left[\frac{y}{1-y}\right] = b_0 + b_1x_1 + b_2x_2 + b_3x_3 + \cdots + b_nx_n$$

Pre-processing knowledge may be a step that much all models take. the knowledge is then separated into eighty % coaching and twenty % testing data in supply regression. we tend to need a model that may confirm whether or not AN email is spam. to coach the model, we tend to should 1st outline the model and so work train knowledge thereto. when the coaching, we can utilize take a look at knowledge to predict the result

2.1.5 SVM Algorithm

The SVM algorithmic rule is one in every of the foremost economical machine learning algorithms for classification and regression issues [25]. SVM determines a hyperplane which will separate the house into 2 or a lot of categories. The margin is unbroken giant as potential, and therefore the knowledge points during this border area unit known as support vectors [26]. The kernel is employed to divide the info non-linearly in SVM. to the current aim, the SVM searches support vectors, weights, and bias. For input data, z ∈ R^n, the SVM is decided as follows:

$$f(z)=\text{sign}(\sum_{i=1}^{N} vi\ \Psi(zi) + c)$$

Herein, Ψ(.) corresponds to the mapping perform, and v and c area unit weights and bias, respectively. The mapping perform may be linear SVM, polynomial SVM, radial basis function (RBF)-SVM. during this study, we tend to most popular RBF-SVM as a mapping perform for the classification task

Metric	Formulation	Definition
Accuracy	$\frac{TP + TN}{TP + TN + FP + FN}$	The overall accuracy of the model.
Sensitivity	$\frac{TP}{TP + FN}$	The performance of the model on detecting abnormal network traffic.
Specificity	$\frac{TN}{TN + FP}$	The performance of the model on detecting normal network traffic.
Precision	$\frac{TP}{TP + FP}$	The ratio of correctly predicted abnormal network traffic to the total abnormal network traffic.
F-Score	$\frac{2 * TP}{2 * TP + FP + FN}$	The accuracy of the model on the whole dataset.

III. LITERATURE REVIEW

Internet of effects(IoT) technology is prospering and entering every part of our lives, be it education, home, vehicles, or healthcare. With the increase in the number of connected biases, several challenges are also coming up with IoT technology diversity, scalability, and quality of service, security conditions, and numerous further. Security operation takes an aft seat in IoT because of cost, size, and power. It poses a significant threat as lack of security makes druggies skeptical towards using IoT bias. This, in turn, makes IoT vulnerable to security attacks, eventually causing enormous fiscal and reputational losses. It makes up for a critical need to assess present security pitfalls and bandy the forthcoming challenges to be ready to face the same. The accepted study is a multi-fold check of different security issues present in IoT layers perception subcaste, network subcaste, support subcaste, operation subcaste, with farther focus on Distributed Denial of Service(DDoS) attacks. DDoS attacks are significant pitfalls for the cyber world because of their eventuality to bring down the victims. Different types of DDoS attacks, DDoS attacks in IoT bias, impacts of DDoS attacks, and results for mitigation are bandied in detail. The presented review work compares Intrusion Detection and Prevention

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor: 6.252

models for mollifying DDoS attacks and focuses on Intrusion Discovery models. likewise, the bracket of Intrusion Discovery Systems, different anomaly discovery ways, different Intrusion Discovery System models grounded on datasets, colorful machine literacy and deep literacy ways for data pre-processing and malware discovery has been bandied. In the end, a broader perspective has been envisaged while agitating exploration challenges, its proposed results, and unborn fancies.

3.1 Related Works

In recent times, numerous studies have been done to secure SDN using machine literacy ways. In this section, we bandy several studies of DDoS security mechanisms grounded on machine literacy and deep literacy ways. Kyaw, Aye Thandar, May Zin Oo, and Chit Su Khin[11] used two machine literacy algorithms to descry UDP flooding attacks in the SDN terrain. They used the Scapy tool for business packet generation. Their system collects the inflow statics via the OpenFlow switch. After the point birth phase, they compared the bracket performance of Linear and Polynomial SVM models. Experimental results show that the Polynomial SVM algorithm has a 34 lower false alarm rate with 3 better delicacies. Janarthanam,S.,N. Prakash, and. Shanthakumar[12] proposed the security frame that detects DDoS attacks on the SDN terrain. The frame is grounded on an adaptive literacy model that uses the literal dataset for business bracket. They used across-validation approach for effective bracket results. Although the results attained are promising, the adaptive security model should be tested on different datasets attained from the real terrain to be more realistic. Tan, Liang etal. [13] proposed a new security model for DDoS attacks in the SDN terrain. The model involves two modules grounded on ML algorithms. The data- processing module uses the K- Means algorithm for stylish point selection and the discovery module uses the k- nearest neighbor(kNN) algorithm to descry attack overflows. Compared to the distributed- tone-Organizing Map(SOM) and entropy- grounded system, their system has a98.85 delicacy with a98.47 recall rate.

IV. PROBLEM DEFINITION

4.1 Internet Service Provider (ISP)

An Internet Service Provider (ISP) provides Internet access and services. ISP providers may be configured in a variety of ways, such as commercial, public, non-profit, or other private. The services provided by the ISP are as follows:

- **Internet Access: -** ISP-provided Internet access is a process that enables individuals and organizations to connect to the Internet through computer terminals, computers, mobile devices, sometimes via computer networks so that users can access online resources, such as email and World Wide Web.
- **Internet Transit:** - It is a service that allows network traffic to disconnect or "transfer" a computer network, often used to connect a small ISP to a large Internet.
- **Domain Name Registration:** A domain name is a series of identifiers that define the domain of governance, authority, or control within the Internet.
- **Web Hosting:** It is a type of web hosting service that allows individuals and organizations to customize their website via the World Wide Web.
- **USENET Service:** It is a computer-wide chat system available online. It is like the notification board system (BBS) and is a preview of the most widely used online forums today.
- **Single location:** A shared location is a type of data center where equipment, location, and bandwidth are available for rent to retail customers.

4.2 DOS: A major threat to IPS

The impact of successful DDoS attacks on ISPs is widespread. Site performance is highly compromised, leading to frustration for customers and other users. Service level agreements (SLAs) are violated, resulting in costly service credits. The growing reliance on the Internet makes the impact of effective DDoS attacks. DDoS in ISPs results in the following:

- Lost income
- Lost production
- Increased IT costs
- Reduction costs
- Loss of customers

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor: 6.252

Point A: This is the ISP entry point
Point B: This is the ISP exit point
Point C: This is the access point to your network

A. Understanding DDOS Attacks

The bushwhackers aim to produce heavy business with further than one machine, to consume the coffers on the target machine, and to help it from serving after a while by DDoS attacks. bushwhackers use " botnets " created from bias called zombies commandeered by internet hackers. DDoS attacks are carried out with many machines, so it's veritably delicate to descry and block. The frequency and inflexibility of DDoS attacks are constantly adding and can have fatal goods on numerous network services[14,15]. For this reason, quick discovery and forestallment of DDoS attacks are some of the most important problems for network service providers and directors. Different SDN layers can be impaired by filling communication channels between the regulator and the switch or between the regulator and the operation subcaste with gratuitous inflow information by DDoS attacks. There's no erected- in security medium on the regulator that can distinguish between attack business and normal business. thus, it's veritably delicate to descry an attacked attacks are grouped into three orders: operation- subcaste attacks, resource consuming attacks, and volumetric attacks[16]. operation-subcaste attacks correspond of complex attacks. They target specific services using lower bandwidth and sluggishly consume network coffers. thus, it's delicate to descry. Hypertext Transfer Protocol(HTTP) and sphere Name System(DNS) attacks can be estimated in this order[17]. In resource consuming attacks, waiters are rendered unapproachable by taking advantage of vulnerabilities in protocols enforced on the network subcaste. TCP- SYN Flood consumes the coffers of the target machine(memory, CPU, and storehouse)[18]. It aims to consume the bandwidth of the network with volumetric attacks. Common attacks similar as ICMP, UDP, and TCP- SYN flood tide is performed by using vulnerabilities in Subcaste 3 and Subcaste 4 protocols[19]

V. OBJECTIVE/SCOPE

The DDoS attack, as the name suggests, is launched to overwhelm the target, and disrupt services. The DDoS attack requires many devices for launching an attack,and for this, IoT devices are well suited. As in most cases,users will not understand that the device is compromised; for example, baby monitors and smart toys have a user interfacewith limited access. They may generally work even after being part of a Botnet army. With the increasing volume of IoT devices, there is an urgent need to detect attacks timely to remove compromised devices. IoT devices were used as Botnets by Mirai in a significant DDoS attack, and several such attacks have taken place [5]. The severity of DDoS attacks can be understood from, which comprises major DDoS attacks from 2013 to 2020. Leading service providers like Amazon Web Serviceshave been the victim of DDoS attacks. KrebsOnSecurity, Cloudflare, AWS, and more DDoS attack victims are them- selves' security providers against such attacks [6], [7].Therefore, attacks on these major establishments hamper companies financially and impede their reputation. In a Denial of Service (DoS) attack, the attacker tries to disrupt the services of the target by utilizing its resources with the help of fake requests. Distributed Denial of Services (DDoS) is an amplified DoS attack. In a DDoS attack, requests are initiated from many sources, and hence it is named as distributed DoS. Due to this, it becomes challenging to mitigate DDoS attacks. There are many types of DDoS attacks: TCP SYN Flood attack, Teardrop attack, Smurf attack, Ping of Death attack, Botnets.DDoS attacks can also be classified as Reflection and Amplification attacks. In a reflection attack, the size of the requestand response is the same [8], whereas, in an amplification attack, the size of the response is many times bigger than thatof the request [9].

VI. ANALYSIS & FINDINGS

After Applying the five Different types of algorithms KNN algorithm' Classifier, Logistic Regression , Decision Tree algorithm ,Random Forest Classifier and SVM Algorithm on same dataset .
as a result, the accuracy percentage level by the Random Forest Classifier is 99.99% which is the highest of all five, the accuracy achieved by Decision Tree algorithm is 98.22% which is also good and the KNN algorithm is 98.0% accurate last accuracy and Accuracy SVM algorithm is 97.0% followed by the Logistic Regression algorithm 76.64%.
So, looking at the Overall result we can see that the Random Forest Classifier algorithm has the highest accuracy.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor: 6.252

Random Forest Classifier algorithm can be considered as the most accurate classifier for Detection of DDoS Attack as it gives the more accuracy compared to the others. Other algorithms may also be accurate depending on their working which you can learn in other research papers.

Classifiers	Accuracy(%)	Precision	F1-score	Recall
Random Forest Classifier	99.99%	1.00	1.00	1.00
Decision Tree algorithm	98.22%	0.98	0.99	0.99
KNN algorithm	98.00%	0.99	0.99	0.99
SVM algorithm	97.0%	0.97	0.97	0.98
Logistic Regression	76.64%	0.84	0.81	0.79

Below are the values of precision, recall, f1-score and accuracy of all the three model which are Random Forest Classifier, KNN algorithm , SVM algorithm, Logistic Regression and Decision Tree which are obtained by training the data.

VII. CONCLUSION

In this study, traditional and attack traffic within the dataset obtained from the SDN atmosphere was classified victimization machine learning algorithms. The made-to-order SDN-based dataset consists of transmission control protocol, UDP, and ICMP traditional and attack traffics. The dataset has applied math options like byte_count, duration_sec, packet rate, and packet per flow except for options that outline supply and target machines. The NCA algorithmic program has been wonted to perform a good classification and to pick the foremost appropriate options. once analyzing22 network options NCA algorithms, fourteen effective options were selected and given as input to machine learning algorithms. quite one hundred thousand network records were classified by kNN, DT, Random Forest Classifier ,Linear Regression , and SVM algorithms once preprocessing and have choice. The experimental results show that Random Forest Classifier contains a higher accuracy rate than the opposite algorithms with 99.99%.

DDoS has become a major part of a long-term threat campaign and the rate of automatic attacks has increased. Several attempts by ISPs to combat them but they have not yet been able to completely overcome this problem, instead it could be a major threat in the future. Many weaknesses such as distributed and unparalleled internet infrastructure frameworks, business policies, privacy policies and investment returns have diminished ISP's interest in eliminating DDoS completely. Instead, DDoS protection itself is growing as a new market. Under such circumstances it seems impossible to eliminate DDoS in public. By following the recommendations given in the paper the local ISPs will be able to deal with DDoS attacks effectively. In future studies, it is planned to increase the diversity of attacks and compare the classification performances of machine learning models with feature selection algorithms.

REFERENCES

[1]. https://journals.sagepub.com/doi/full/10.1177/ 1550147717741463
[2]. International journal of Distributed Sensor Network
[3]. https://blog.eccouncil.org/types-of-ddos- attacks-and-their-prevention-and-mitigation- strategy/
[4]. http://users.eecs.northwestern.edu/~khh575/pu b/pub/Report-DDoS-1.pdf
[5]. G. Perrone, M. Vecchio, R. Pecori, and R. Giaffreda, ‘‘The day after Mirai: A survey on MQTT security solutions after the largest cyber-attack carried out through an army of IoT devices,’’ in Proc. Big Data Secur. (IoTBDS), Apr. 2017, pp. 246–253.
[6]. Cloudflare. (2020). Famous DDoS Attacks | Cloudflare. Accessed: Mar. 20, 2021. [Online]. Available: https://www.cloudflare. com/learning/ddos/famous-ddos-attacks/
[7]. P. Nicholson. (2020). Five most famous DDoS attacks and then some. A10 Blog. Accessed: Mar. 20, 2021. [Online]. Available: https://www.a10networks.com/blog/5-most-famous-ddos-attacks/
[8]. S. Hussain, R. Atallah, and A. Kamsin, ‘‘DDoS reflection attack based on IoT: A case study,’’ in Proc. Comput. Sci. Line Conf. Cham, Switzerland: Springer, 2019, pp. 44–52.
A. Colella and C. M. Colombini, ‘‘Amplification DDoS attacks: Emerg- ing threats and defense strategies,’’ in Proc. Int. Conf. Availability, Relia- bility, Secur., in Lecture Notes in Computer Science: Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinfor- matics, vol. 8708, 2014, pp. 298–310.

[9]. Ahuja, N.; Singal, G.; Mukhopadhyay, D. "DDOS attack SDN Dataset", Mendeley Data, V1; Bennett University: Greater Noida, India, 2020.

[10]. Kyaw, A.T.; Oo, M.Z.; Khin, C.S. Machine-Learning Based DDOS Attack Classifier in Software Defined Network. In Proceedings of the 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications, and Information Technology (ECTI-CON), Phuket, Thailand, 24–27 June 2020; pp. 431–434.

[11]. Janarthanam, S.; Prakash, N.; Shanthakumar, M. Adaptive Learning Method for DDoS Attacks on Software Defined Network Function Virtualization. EAI Endorsed Trans. Cloud Syst. 2020, 6, 166286.

[12]. Tan, L.; Pan, Y.; Wu, J.; Zhou, J.; Jiang, H.; Deng, Y. A New Framework for DDoS Attack Detection and Defense in SDN Environment. IEEE Access 2020, 8, 161908–161919.

[13]. Nazih, W.; Elkilani, W.S.; Dhahri, H.; Abdelkader, T. Survey of countering DoS/DDoS attacks on SIP based VoIP networks. Electronics 2020, 9, 1827.

[14]. Horak, T.; Strelec, P.; Huraj, L.; Tanuska, P.; Vaclavova, A.; Kebisek, M. The vulnerability of the production line using industrial IoT systems under ddos attack. Electronics 2021, 10, 381.

[15]. Hu, C.; Han, L.; Yiu, S.M. Efficient and secure multi-functional searchable symmetric encryption schemes. Secur. Commun. Netw. 2016, 9, 34–42.

[16]. Praseed, A.; Thilagam, P.S. DDoS attacks at the application layer: Challenges and research perspectives for safeguarding web applications. IEEE Commun. Surv. Tutor. 2019, 21, 661–685.

[17]. Mahjabin, T.; Xiao, Y.; Sun, G.; Jiang, W. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. Int. J. Distrib. Sens. Netw. 2017, 13.

[18]. Yusof, M.A.M.; Ali, F.H.M.; Darus, M.Y. Detection and Defense Algorithms of Different Types of DDoS Attacks. Int. J. Eng. Technol. 2018, 9, 410–444.

[19]. Fix, E.; Hodges, J.L. Discriminatory Analysis. Nonparametric Discrimination: Consistency Properties. Int. Stat. Rev. Rev. Int. Stat. 1989, 57, 238–247.

[20]. Akbulut, Y.; Sengur, A.; Guo, Y.; Smarandache, F. NS-k-NN: Neutrosophic Set-Based k-Nearest Neighbors Classifier. Symmetry 2017, 9, 179.

[21]. Altunta¸s, Y.; Kocamaz, A.F.; Cömert, Z.; Cengiz, R.; Esmeray, M. Identification of Haploid Maize Seeds using Gray Level Co-occurrence Matrix and Machine Learning Techniques. In Proceedings of the 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), Malatya, Turkey, 28–30 September 2018; pp. 1–5.

[22]. Cömert, Z.; Kocamaz, A.F. Comparison of Machine Learning Techniques for Fetal Heart Rate Classification. Acta Phys. Pol. A 2017, 132, 451–454.

[23]. . Hagan, M.T.; Demuth, H.B.; Beale, M.H.; De Jesús, O.; De Jesús, O. Neural Network Design, 2nd ed.; Hagan, M.T., Ed.; 2014. Available online: https://www.amazon.com/Neural-Network-Design-Martin-Hagan/dp/0971732116 (accessed on 21 May 2021) ISBN 9780971732117

[24]. Hastie, T.; Tibshirani, R.; Friedman, J. The Elements of Statistical Learning; Springer: Berlin/Heidelberg, Germany, 2009; ISBN 9780387848570.

[25]. Diker, A.; Cömert, Z.; Avci, E.; Velappan, S. Intelligent system based on Genetic Algorithm and support vector machine for detection of myocardial infarction from ECG signals. In Proceedings of the 2018 26th Signal Processing and Communications Applications Conference (SIU), Izmir, Turkey, 2–5 May 2018; pp. 1–4.