iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** III **Month of publication:** March 2022

DOI: https://doi.org/10.22214/ijraset.2022.40742

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

Review on Detection of DDOS Attack using Machine Learning

Tejaswini Ulemale
Student, Computer Engineering, DYPCOE, Akurdi, Pune

Abstract: ***Now days due to digitalization the drastic increment towards Computer technology and Computer network is increased rapidly. Various types of works are turned into Online Mode so due to increment in network connection various attack are been perform. One of the dangerous and powerful attack is Distributed Denial of Service [DDOS] is one of the major issues in the computer network. The Attacker target the server with the help of DDOS and tries to interrupt normal traffic. The Denial-of-service consist of subclass which includes Distributed denial of service. Therefore, to prevent the DDOS attack many researches have been carried out. To Prevent DDOS common technique which includes Machine learning and deep learning. The main focus is to detect DDOS attack.***

Keywords: Computer Network, DDOS, Machine Learning, Deep Learning.

I. INTRODUCTION

The network has become topmost and important business organization. The increase demand of network-based services increases the attack which halt response for users. The attack slows down all the network services which leads to application failure. The latest and important technology use by many users that is computer network therefore more security is required to prevent computer network. The DDOS attack is carried out by controlling computer system which are freely available and consist of internet. An attack which is done on servers basically to make the source unavailable to the authorized user. Here it totally blocks a single source of the user. Multiple digital device which are connected is more vulnerable. Hacker can also target to information, personal data which break them from unlawful additions [1]. The Attack Detection should be likely to be smart and should battel successful for hackers. The Availability, Confidentiality and integrity plays main role in security purpose.

A. Confidentiality

Confidentiality is also known as secrecy. The main work of confidentiality is to protect the information and personal data from unauthorized access. The Sharing information be valid for legitimate users with proper assurance. The Cryptography is more powerful which can protect confidentiality with more security.

B. Integrity

The term Integrity ensures that the data and system is not destroy by the unauthorized modification. The integrity protect also protects applications, operating system and hardware for unauthorized User.

C. Availability

Availability is the accessing information consistently to authorized users. It also consists of technical infrastructure and maintaining hardware which can display the information. To perform this attack firstly internet is required, through different hacking tools like botnet this attack is performed mainly focuses on targeted source IP address. It asks for request first and makes the user overwhelmed and then cuts the valid user from service. This attack is performed smoothly. The tools used to attack are made by the hackers. A trojan virus is made by the attacker first, where a trojan is nothing but a message sends to the authorized user in form of ad or any other way it is send by the attacker.

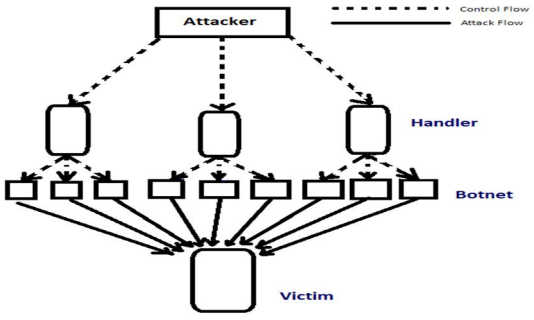


Figure 1. DDoS attack with botnet. [4]

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue III Mar 2022- Available at www.ijraset.com

II. VARIOUS TYPES OF DDOS ATTACK

A. ICMP (Ping) Flood

Her attacker send request for service to the valid user for that it uses ICMP echo request packets. The attack which can consume incoming and outgoing bandwidth and the servers will attempt the respond to packet which result in overall system slowdown.

B. SYN Flood

It can target to any device connected to system through internet. In the SYN flood sender sends multiple SYN request but it does not response to host SYN-ACK and send SYN requests with spoofed IP address. The host waits until the acknowledgement is provided which result in denial of service.

C. Ping of Death

It sends the targeted source a packet which is bigger than the allowable size into the system. Maximum length of packet of an IP packet is 65535 bytes. This attack can overflow memory buffer which is allocated of packet.

D. Slowloris

It sends request to the connectivity which is between single machine and a server. It creates connection to target server but sends partial request and it always send HTTP header but in incomplete format. The target server has all failure connection open so the maximum concurrent connection leads to denial of connections.

E. NTP Amplification

Here the attacker focuses on attacking the publicly accessible source with UDP traffic. The attacker obtains list of open NTP servers which can easily generate a high-volume and high-bandwidth.

F. HTTP Flood

With Http request this attack is performed. To perform this attack request is send to the end user by the attacker and through http the request is been send and attack has been performed.

III. RELATED WORK

For the prevention of DDOS attack the various researchers has been implemented [12][17][18]. Some major techniques are given studied below.

A. Parvinder Singh Saini et. al [2]

He said that nowadays DDOS is very common attack which cause damage to various network resources for the legitimate users [3]. He also found that 45% of entropy-based, 10% divergence-based and 38% of correlation-based techniques are used. Further he generated instruction for real-time by detection mechanism which is machine learning techniques.

To detect DDos attack various algorithm in machine learning are used which includes Support Vector Machine, Naive Bayes and Multilayer Perceptron.

He used dataset which consist of 5 different classes and 27 features. With the help of MLP, Naive Bayes, J48, Random Forest algorithms which classify the attack and finally he concludes that J48 has 98.64% more accuracy as compare to MLP, Naive Bayes and Random Forest.

B. Chin-Shiuh Shieh et. al [4]

He said that challenging issue of detection of DDos attack should be taken before mitigation measures. The Machine learning and Deep learning is applied for detection of DDoS attack. However, the success of full-scale is reach beyond the inherent so it called open Set Recognition problem.

In these problem situation machine learning fails with new instances which are not drawn from distributed model of training data. He said that this problem is particularly profound in detection of DDos attack so it keeps evolving and changes the characteristics traffic.

So, they propose a new DDos detection framework which do the featuring of Bi-Directional Long Short-Term Memory and the Gaussian Mixture Model. Finally, he concludes that the BI-LSTM is capable fully for performing the detection of DDoS attack.

C. Jiangtao Pei et. al [5]

In these they have use the DDoS attack tool which conduct local attacks. The packet capture tool which compares the capture attack with normal packets and finds the rules of data attack and then convert it into characteristics of data attack. Basically, in machine learning random forest algorithm was used to detect the DDoS attack. Firstly, it extracts the feature and format conversion which is used to perform the characteristics in large scale. These extracted features are used as input to random forest algorithm and obtained to detect the DDoS attack.

D. Abdullah Soliman Alshra et. al [6]

He stated that the concept of network virtualization which can offer malicious attacker to vulnerable aspect and the network architecture. Therefore, it suggests Deep learning algorithm which can achieve success in different application. It also stated that the art uses GRU for RNN and LSTM.In research paper they have evaluated the performance which consist of 48 features similar to SDN environment with rate of high detection. The work of LSTM takes more time compared with GRU and RNN.In further study the researchers said that the performance of machine learning will be better with features and aggregating the existing features and finally the model will be applied to real-time classification network.

E. Swathi Sambangi et. al [7]

The researchers talk about detection of DDoS attack which is more common like Cloud and is very important to detect the attack which causes cloud unavailability. So, to identify the DDoS attack various machine learning models are used for training and testing of DDoS detection datasets. The objective was to ensemble the feature selection and gain information and analysis of regression. The accuracy of the ensemble model is 97.86% based on 16 attributes which are obtained from the information of regression analysis and feature selections. It also proves importance of that model and consideration of model for prediction.

F. Nisha Ahuja et. Al [8]

The Software Defined Networking [SDN] is defined by the software were the traffic is controlled and centralized which direct between hosts. The dataset of SDN are used to trained the model and which can create mininet emulator. In these research paper the author has use Random Forest and Support Vector machine [SVM] for classifying traffic with the help of SVC result and filter over the Random Forest. The accuracy of the model is 98.8% and the precision is 98.27% so it indicates that the class are correct in many cases. The accuracy let us known that detection is done in absence of traffic control. The research also talks about the future to analyze and perform DDoS attack with deep learning model along topology attack identification.

G. Ancy Sherin Jose et. Al [9]

The authors say that the OpenFlow which enable SDN to collect flow feature which can obtain derived features. They also said that classification of DDoS was perform with dataset which collect emulated network. For evaluation of experimental the features are used to study and detecting DDoS more accurately. They had taken 7 features of group 3 feature and overall accuracy was 99.99%. They found out best 2 features which help us to detect the DDoS attack. The used features can build a model which is light weight for multistage classification. The protocol entropy can decrease when multiple attack are perform at same time.

H. Chenguang Wang et. al [10]

They have analyzed the features of DDoS attack and the detection of novel model and detection of RDF-SVM attack. They have extracted the DDoS flow and SVM rescreen features which can optimize the subset.The algorithm can compute experimental result and features such that the algorithm can be better classified by their performance and optimal feature. It can also detect unknown attack as well as known attack and can compare the IP address randomly and more effectively with different methods.

I. Pheeha Machaka et. al[11]

In this paper, they have used various machine learning algorithms like Logistic Regression (LGR), K-Means, and Artificial Neural Networks (ANN). They have obtained promising accuracy of 94.00%. The algorithm they have implemented was build only after performing data preprocessing and data manipulation process.

J. Sara Abdalelah Abbas [13]

In this work, they have implemented dimensionality reduction techniques named as principal component analysis (PCA). They have reduced the number of features used for the training purpose. Also, they have trained the model various machine learning model. They have obtained accuracy of 99.97 using the best trained machine learning algorithm.

K. Pande S., et.al [14]

They have used various feature selection technique like univariate feature selection, principal component analysis, recursive feature elimination and univariate feature selection. Initially their dataset consists of 42 features. After performing feature selection, they have reduced the number of features to 11 and finally they have trained the machine learning algorithms. They have used five different machine learning algorithms like SVM, perceptron, K-nearest neighbor, stochastic gradient descent, and XGboost for training the model. They have obtained the best accuracy as 98.87%

L. Rami J. Alzahrani [19]

In this paper they have performed Security Analysis using Machine Learning Algorithms in Networks Traffic. They have used K_Nearest_Neighbors (K-NN), super vector machine (SVM), naïve bayes (NB), decision tree (DT), random forest (RF) and logistic regression (LR).They have obtained best results as 99.00%.

Sr.	Topic	Author Name	Algorithms	Accuracy
1	Detection of DDos attack using machine learning algorithms	Parvinder Singh Saini,Sajal Bhatia, Sunny Behal	Support Vector Machine, Naive Bayes and Multilayer Perceptron	98.64%
2	Detection of Unknown DDoS Attacks with Deep Learning and Gaussian Mixture Model	Chin-Shiuh Shieh, Wan-Wei Lin, Thanh-Tuan Nguyen, Chi-Hong Chen, Mong-Fong Horng and Denis Miu	Bi-Directional Long Short-Term Memory and the Gaussian Mixture Model	95.3% and 99.8%
3	A DDoS Attack Detection Method Based on Machine Learning	Jiangtao Pei, Yunli Chen, Wei Ji	Random Forest Algorithm	99.49%
4	Deep Learning Algorithms for Detecting Denial of Service Attacks in Software-Defined Networks	Abdullah Soliman Alshra'a, Ahmad Farhat, Jochen Seitz	Gated recurrent units and Recurrent Neutral Network	91.3% and 91.11%
5	A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression	Swathi Sambangi and Lakshmeeswari Gondi	Ensemble Model and Multiple Linear Regression	97.86%
6	Automated DDOS attack detection in software defined networking.	Nisha Ahuja, Gaurav Singal, Debajyoti Mukhopadhyay, Neeraj Kumar	Random Forest and Support Vector machine	98.8%
7	Detecting Flooding DDOS Attacks Over Software Defined Networks Using Machine Learning Techniques	Ancy Sherin Jose, Latha R Nair, Varghese Paul	Support Vector Machine	99.99%.
8	DDoS Attacks Detection Based on RDF-SVM	Chenguang Wang, Jing Zheng, Xiaoyong Li	RDF-SVM Algorithm	98.72%
9	DDoS Attacks in IoT Networks using Machine Learning	Pheeha Machaka, Olasupo Ajayi, Hloniphani Maluleke , Ferdinand Kahenga, Antoine Bagula, Kyandoghere Kyamakya,	Logistic Regression (LGR), K-Means, and Artificial Neural Networks (ANN)	94.00%
10	Feature selection and comparison of classification algorithms for wireless sensor networks	Pande S., Kamparia A., Gupta D	SVM, perceptron, K-nearest neighbor, stochastic gradient descent, and XGBoost.	98.87%
11	Distributed Denial Of Service Attacks Detection System By Machine Learning Based On Dimensionality Reduction	Sara Abdalelah Abbas , Mahdi S. Almhanna	PCA	99.97%
12	Machine Learning Approach Equipped with Neighbourhood Component Analysis for DDoS Attack Detection in Software-Defined Networking	Özgür Tonkal , Hüseyin Polat , Erdal Ba¸saran, Zafer Cömert and Ramazan Kocao˘glu	k-Nearest Neighbor (KNN), Decision Tree (DT), Artificial Neural Network (ANN), and Support Vector Machine (SVM) algorithms.	100%

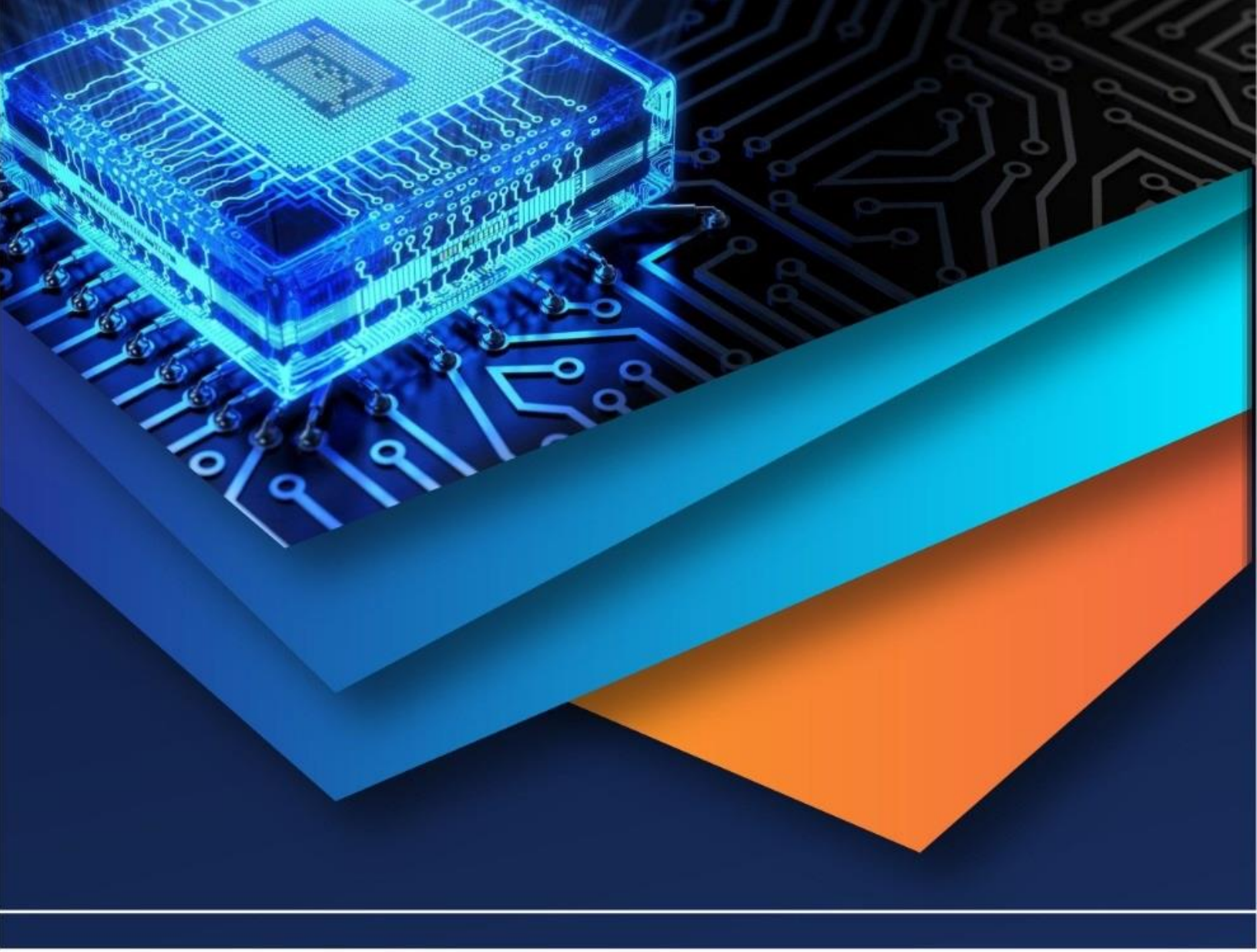
13	An intrusion detection system for healthcare systems using machine and deep learning	Pande S., Kamparia A., Gupta D	Artificial Neural Network(ANN)	99.00%
14	Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Networks Traffic	Rami J. Alzahrani and Ahmed Alzahrani	K_Nearest_Neighbors (K-NN), super vector machine (SVM), naïve bayes (NB), decision tree (DT), random forest (RF) and logistic regression (LR).	99.00%

IV. CONCLUSION

DDOs attack will remain a biggest threat to many big and small organizations, because it causes many different damages to the online users. The areas which may depend on human operator, long computing time and lack of data which is available free. Still, lots of areas need to be focus to detect DDoS attack. Various algorithm such as Linear Regression, Random Forest, Support Vector Machine, Gaussian and Naïve Bayes classifier are used for detection of DDoS attack. The deep learning also plays major role for detection of DDoS attack which uses Convolution neural network. So, we have review on various technique to detect DDoS attack.

REFERENCES

[1] Ganorkar, S. S., Vishwakarma, S. U., & Pande, S. D,An information security scheme for cloud-based environment using 3DES encryption algorithm. International Journal of Recent Development in Engineering and Technology, 2014.
[2] Parvinder Singh Saini, Sajal Bhatia, Sunny Behal. Detection of DDos attack using machine learning algorithms published in research gate in March 2020.
[3] S Behal, K Kumar and M Sachdeva, Characterizing DDos attack and flash events: Review, research gaps and future directions, ELSEVIER Computer Science Reviews 25(2017) 101-114.
[4] Chin-Shiuh Shieh, Wan-Wei Lin, Thanh-Tuan Nguyen, Chi-Hong Chen, Mong-Fong Horng and Denis Miu. Detection of Unknown DDoS Attacks with Deep Learning and Gaussian Mixture Model , IEEE ICICT 2021
[5] Jiangtao Pei, Yunli Chen, Wei Ji." A DDoS Attack Detection Method Based on Machine Learning" published in ICSP 2019.
[6] Abdullah Soliman Alshra'a, Ahmad Farhat, Jochen Seitz. "Deep Learning Algorithms for Detecting Denial of Service Attacks in Software-Defined Networks" published in ScienceDirect Year 2021.
[7] Swathi Sambangi and Lakshmeeswari Gondi."A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression" published in 25 December 2020.
[8] Nisha Ahuja, Gaurav Singal, Debajyoti Mukhopadhyay, Neeraj Kumar. Automated DDOS attack detection in software defined networking published in Science Direct 2021.
[9] Ancy Sherin Jose, Latha R Nair2, Varghese Paul. Towards Detecting Flooding DDOS Attacks Over Software Defined Networks Using Machine Learning Techniques published in Genetic 2021.
[10] Chenguang Wang, Jing Zheng, Xiaoyong Li. Research on DDoS Attacks Detection Based on RDF-SVM published in IEEE in 2017.
[11] Pheeha Machaka, Olasupo Ajayi, Hloniphani Maluleke , Ferdinand Kahenga, Antoine Bagula, Kyandoghere Kyamakya,Modelling DDoS Attacks in IoT Networks using Machine Learning,2021
[12] Dutta Sai Eswari1, P.V.Lakshmi, A Survey On Detection Of Ddos Attacks Using Machine Learning Approaches, Turkish Journal of Computer and Mathematics Education,2021
[13] Sara Abdalelah Abbas , Mahdi S. Almhanna ,Distributed Denial Of Service AttacksDetection System By Machine Learning Based On Dimensionality Reduction, Icmaict 2020
[14] Pande, S., Khamparia, A. & Gupta, D. Feature selection and comparison of classification algorithms for wireless sensor networks. J Ambient Intell Human Comput (2021).
[15] Pande S, Khamparia A, Gupta D (2021) An intrusion detection system for healthcare systems using machine and deep learning. World J Eng 2021.
[16] Tonkal, Ö.; Polat, H.; Başaran, E.; Cömert, Z.; Kocaoğlu, R. Machine Learning Approach Equipped with Neighbourhood Component Analysis for DDoS Attack Detection in Software-Defined Networking. Electronics 2021.
[17] Pande S., Kamparia A., Gupta D. Recommendations for DDOS Threats Using Tableau. In: Gupta D., Polkowski Z., Khanna A., Bhattacharyya S., Castillo O. (eds) Proceedings of Data Analytics and Management. Lecture Notes on Data Engineering and Communications Technologies, vol 91. Springer, Singapore 2021.
[18] Alzahrani, R.J.; Alzahrani, A. Security Analysis of DDoS Attacks Using Machine Learning Algorithms in Networks Traffic. Electronics 2021, 10, 2919. https://doi.org/10.3390/electronics10232919.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY