RESEARCH ARTICLE OPEN ACCESS

Prevention of Distributed Denial of Service Attacks In A LAN Using Centralized Intrusion Detection System

Sanjit Mazumder [1], Soumi Mondal Bera [2], Atikul Islam [3]
[1] Department of Computer Science & Engineering, Seacom Engineering College, Howrah, India
[2] Department of Computer Science & Engineering, Seacom Engineering College, Howrah, India
[3] Department of Computer Science & Engineering, Seacom Engineering College, Howrah, India

ABSTRACT
A Mobile Ad hoc Network (MANET) is a self-configuring network of mobile devices connected through wireless links, without the need for a fixed infrastructure. An infrastructure less wireless Mobile ad-hoc network (MANET) is presently become tremendous popular due to its flexibility, scalability, cost effective, robustness and privacy. MANETs are highly flexible, as they can be set up and configured quickly without the need for a centralized infrastructure. They can be used in a wide range of scenarios, from military operations to disaster relief efforts. MANET can scale to large number of nodes, allowing them to be used in both small and large-scale deployment without fixed infrastructure, which makes it more cost effective. It provides a high degree of privacy and security, as they do not rely on a centralized infrastructure that could be vulnerable to attacks. Every device in MANETs can move independently in anywhere and can change its connection to any device frequently. So among the different challenges MANET faces the security challenge is the prime challenge. Due to the unattended environment the chances of different attacks is increase. Among different attacks DoS and DDoS is main. Our aim is to confirm the attack and block it by analyzing the effect of DDoS attack, packet drop rate and delay of end to end packet delivery.
Keywords — Wireless mobile ad-hoc network, security attacks, defensive mechanisms, DDoS attack, MANET.

I. INTRODUCTION

computers and networking have become inseparable by now. huge numbers of private data transfer can be occurred in every hour and now a days computer are used in transmitting of data compare to processing the data. so network security is needed to prevent data hacking and to provide authenticated data transfer. thus security implementations on networking infrastructures are highly necessary, specifically, when organization and corporal networks are involved in financial transactions and valuable data administration.

Network security has become even more susceptible with the presence of the internet where users gained access not only to enormous volumes of information but also engaged in mean use of network interconnectivity. The network layer is a basic foundation layer of OSI 7 layer model. With respect to this model in filtrate or nab data are produced due to different type of attacks activity and hamper not only the network layer, but other layers also. Considering these potential attacks and organization's services and requirements, the network security is being defined by a policy-based implementation in the network. Describing a security policy is not a suitable procedure at all, so the network security development procedure is most difficult and important part of any security policy. A network security policy means if a costly high secured steel made door can fit with a tent's entrance or a door casing, then the mechanism will not be correct for the policy. So a good security policy needs to design and develop that matches with whole network security infrastructure.

Firewall is commonly used as security mechanisms in most of the systems of present time.

This paper examines the various threats and policies of the network security, and analyze that firewall can act as a concealing technology which considers t net filter and IP security as an implementation mechanism. Consequently, the virtualization of a test-bed network is another aspect of network security policy. So network security policy basically made with some internet protocol security techniques which can passes through some penetration test.

II. . PROBLEM STATEMENT

Prevention of distributed denial of service attack in a LAN using centralized intrusion detection system.0

III. OBJECTIVE

The main objectives of this research work are as follows:

1. To identify dirty nodes using patterns of traffic.
2. To filter packets using Deep Packet Inspection (DPI) method with multiple parameters.
3. To identify the malicious packet so that it can be dropped by the network administrator.

IV. ASSUMPTIONS

The proposed method has following assumptions

1. To drop traffics that are analyzed as malicious.
2. To store information about the traffic that look suspicious and need to be reported to the network administrator.

V. LITERATURE SURVEY

In this section a review is carried out on different techniques used by researchers in IP security field related to different DDoS attack. Enormous technologies of Packet Filtering are involved in design of this dissertation. Some prior works are discussed in this section based on the years.

i. 2016 – 2018

Sonia et al. (2016) proposed a three layer security protocol to secure the wireless network from external attack. First layer represent customize cryptography algorithm of AES to enhance security. Second layer will drop packets from authentic IP addresses. Third layer will authenticate user by providing login password security at application layer. Network layer firewalls define packet filtering rule sets, which provide highly efficient security mechanisms. Here the three layer security protocol had been applied. Here packet filter method is used which is a part of firewall. It is used to monitor & control the incoming & outgoing packets of any network and also give permissions to pass, halt or to go back. Basically it analyses the ip addresses, protocols, ports.

Pandikumar et al. (2017) proposed a security policy through distributed firewall to give more data security in LAN than conventional firewall. The security policy will include two techniques, i.e.

a) Pull Technique: When the host started to boot it pings the central management server to request if the central management server is active or not. After the activation it registers itself with central management server. Finally it request the server which security policy should implemented and in return the server gave the answer and host installed the security policy as per this answer.
b) Push Technique: This technology check the updated policyis installed in host or not at any time. This policy ensures the monitoring & controlling of inbound & outbound network traffic with their domain. It can also take decision which packet should be rejected or passed thgrough the system at the application layer.

This security policy of distributed firewall gives very good impact on DoS (Denial of service) attack and has give network data security from threat which brings down the server.

Lawal et al. (2018) proposed SFlow and IP Sec protocol for improving Software Defined Network (SDN). The proposed method ensures real-time detection and mitigation of attacks such as Distributed Denial of Service (DDoS) attacks, Man in the Middle attacks (MITM), Replay attacks, etc. on the SDN network. The protocol has been divided into two segments, i.e.

a) SFlow Technology: SFlow is an open source statistical time-based real-time traffic sampling technology for monitoring traffic in data networks at high speed. Fractions of all packets transiting the network are collected by the SFlow agent(s) and are forwarded to the collector for analysis. The analyzer generates and communicates handling rules to the controller if it detects any anomalies on the network.
b) Flow based IP Sec : Here the flow based IP security protocol is used which is a SDN control security protocol and have the same function like traditional IP security to give support to SDN services. The flow-based IPsec supports and creates a secured path for both host to gateway and gateway to gateway transmission. The flow-based IPsec can be programmatically built on the application layer and it communicates with the controller. The controller then translates the security requirements and implements them on the forwarding agents. The flow-based IPsec is a controller-based data protection service which allows the protection of data traffic based on predefined security policies.

For ICMP Dos attack this model gives us a good result. The threshold was set to 700,000 packets per second, the sampling rate was S of 20 and polling interval I of 30 seconds. It has found that at the start of the attack, the packet flow soared to a peak of approximately 1,700,000 packets per second but since measures were taken to curb it, the packet drops below the threshold of 700,000 packets per second after about approximately 15 seconds of implementation. The SFlow technology gave response detection time is about 5 secs and control time is approximately 15 secs which makes it a probable solution to mitigate the DDoS attack posed on the SDN network resources.

Patgiri et al. (2018) proposed a model to prevent DDoS using Bloom Filter. Here Bloom filter algorithm is used, that returns either true or false value. The Bloom filter algorithm has 3 phases. First phase is detection engine phase 1 that will check traffic information at receiver end. The second phase is detection engine phase 2 that stored the IP address which is extracted from previous phase information into database. This phase is also checks whether an IP address is malicious or not, if it is then the packet is sent to decision engine to take further action. The third phase Bloom filter phase that gives aalarmto every connected system on that network if it gets any responses regarding malicious IP address from decision engine. Bloom filter used the following formula to count the number of probability of set bits, where m is the size of Bloom filter, n is the size of input and k is the no of hash function.

$$\left(1-\left(1-\frac{1}{m}\right)^{nk}\right)$$

ii. 2019 – 2022 Mihaloset al. (2019) proposed a Security Policies with Design and Implementation of Firewall using Linux IP tables. This paper examines the network security threats, policies and mechanisms and analyses the firewall as a network concealing technology by elaborating the Net filter / IP tables as an implementation mechanism. The

security policy is being built by taking into consideration two main principles, i.e-(i)Defense-in-Depth and the (ii) Compartmentalization of Information.

(i) Defense-in-Depth: The main firewall implementation is situated at the choke point of the network's communication with the untrusted network using this technique.

(ii) Compartmentalization of Information: The concept of the compartmentalization principle is to make information and services available to different network users, trusted and untrusted thus, retaining security and confidentiality amongst all users.

The above method results into constraining the whole outgoing email size into a small volume, to avoid attachments. Web-based email accounts such as Gmail, Yahoo and Hotmail are forbidden. It is able to prevent, different types of DDoS attacks.Yin et al. (2020) proposed a model that is honeyfarm architecture for data controlling. This paper explains the design of data control process with IDS & data redirection concepts maintaining the honeyfarm system. The horizontal port scanning problem and DDoS attack problem are addressed in the proposed honeyfarm. Honeypot represent itself as a malicious node. In the meantime, using monitoring software, security professionals can record intruders' behaviors on the compromised system for forensic analysis, so that it can better understood from their motivations, toolkits and tactics.

The security policy of the DOID gateway has four components in order to achieve a good data control purpose:

(1) Containment: implementing policies, e.g. dropping and forwarding, on incoming and outgoing traffic.

(2) ARP responder: At honeypot ends the network gateway is configured and it does not situated in resource pool. So the data redirection gateway have to response with ARP request.

(3) Monitoring: listening for configuration requests and making changes to DOID gate way configurations.

(4) Virtual machine (VM) manager: This component is responsible to control the VM honeypots.

For data controlling two external components are required. One is intrusion detection system (IDS) that differentiates attack and non-attack traffic. The other is a reverse firewall, which functions as a firewall, but it implements policies on outbound traffic instead of inbound traffic so that it prevents the outside world from being attacked by honeypots in the honeyfarm.The result for performance evaluation for introducing delay time of Totally IDS and the reversefirewall cause around 6 ms delay to the system. The difference of transmission time for a 400 and 1400 byte packet is not significant.

VI. CONCEPT AND PROBLEM ANALYSIS

1) The network involves setting of an environment with appropriate connectivity to simulate the environment. The proposed method's environment consisted of two networks with the couple of machine and the machines would be connected via a device that will analyze the traffic. This device could be a physical Linux system with two networks interfaces, one for each of the network system. The proposed approach has certain salient feature that it supports, they are mentioned below:

i. This particular solution has the advantage of using not licensed 3rd party software which is very often a constraint in implementation.

ii. The routing features are allowed to be handled by Linux IP tables and the proposed approach can only focus to identify the bad traffics.

iii. The metrics are parameterize so that any change in parameter would mean configuration changes only. This would allow for no port changes in such situation.

The approach taken for the different use cases is derived from standard solution frameworks used universally.

6.1. Data Collection

The data that flows through the network is has to pass through the IDS device. The device captures the packet, analyzes them and store the data for future reference. In addition this solution needs master data based on which the IDS works. The master data is entered by the user for the functionality of the IDS proposed algorithm.

6.2. Methodology Description

This approach consists of systems that are considered to be external network (IP addresses: 192.168.1.x and connected to interface eth0 on the Linux device that acts as a router) and traffic from this subnet would be filtered and then routed to a subnet (IP: 192.168.0.x and connected to wlan0) of this routing device.

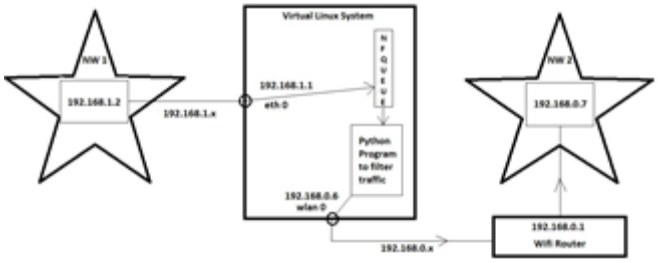


Fig-1

6.3 Hardware Specifications

Three systems are required (that can be virtual or physical) Linux is run in one machine and windows is run on other two machines.

The linux system consists of two network interfaces –one is eth0 and another one is wlan0.A router is required with both wireless and Ethernet interfaces for this dissertation.

6.4 Software Specifications

I. PCAP

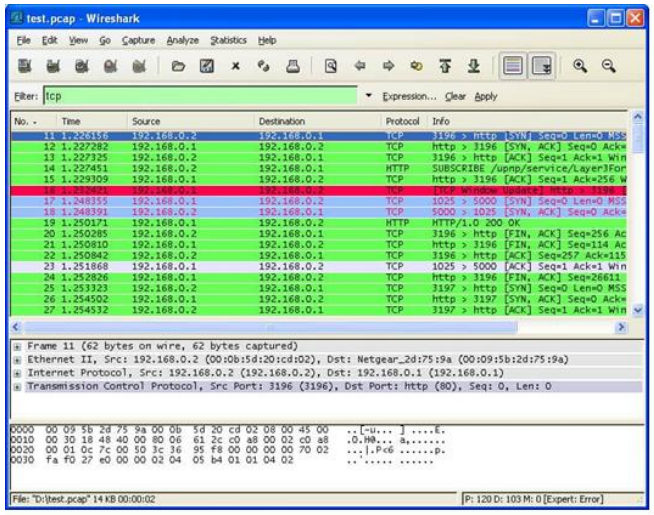
PCAP is known as packet capture or libpcap. It is an application programming interface that captures analyze and monitor the network traffic and extracts source ip, destination ip, port no, type of packet parameters from OSI layer 2 to 7 and acts as a network intrusion system. PCAP uses the platform wireshark and recorded all the details of packets. PCAP file are represented with '.pcap' extensios.

II. Scapy

Scapy is a library function used in python program to capture, analyze and take decision for network traffic. In this dissertation it takes the packets from NFQueue and process it according to the packet filter and reverse proxy algorithm. Scapy runs on Linux, Windows etc.

7. Linux IP Tables

IP table contents a set of rules inbuilt in Linux system. When new rules are imposed on IP tables, the old rules have to remove. IP tables take the decision after analyzing a packet that it is malicious or not. After that it forwarded the packet to packet filter algorithm in this proposed method. Firewall is an example of IP tables.



8. Algorithm Description

This algorithm is implemented in centralized IDS to prevent. This algorithm is implemented in centralized IDS to prevent different DDoS attacks.

In order to mitigate UDP attack traffic before it reaches its target, this algorithm drops all UDP traffic not related to DNS at the network edge.

TABLE-1
Table 1: Rules for Filtering Packets

This algorithm prevents ICMP flooding attack by providing a cap on the no of ICMP packets that is going to receive per second from all sources together.

The handshake process is provided by withholding the connection with the targeted server until the TCP handshake is complete. This strategy takes the resource cost of, maintains the connections with the bogus SYN packets off from the targeted server and placed it on the solution. This algorithm mitigates the Ping of Death attacks by dropping malformed packets before they reach the targeted host computer.

In order to prevent the Slowloris and HTTP flood attacks this algorithm implements a reverse proxy HTTP Server running on

Sl No.	Type	Threshold/min	Direction	Allow
1	ICMP Flood Attack	50	Incoming	No
2	TCP SYN Flood Attack	50	Incoming	No
3	HTTP flood Attack	100	Incoming	No
4	UDP Flood Attack	200	Incoming	No
5	Ping of Death Attack	65538	Incoming	No
6	Slowloris Attack	200	Incoming	No

port 6666. This reverse proxy sits on the Linux device (192.168.0.5). The client would know the URL http://192.168.0.5:6666. Once an http request comes in, this algorithm checks to see the number of http connections from the same client IP that are open at that point. If that exceeds a certain

threshold, the http request is dropped.

Otherwise, this algorithm forwards the request to the target web server with URL http://192.168.0.7:9999. This way, the

number of active http sessions are limited the risk of Slowloris and HTTP flood attacks.

8.1 Steps of Packet Filtering Algorithm

The key to the intrusion detection system is a set of parameters that will be monitored against certain parameters and their threshold values. These determine what patterns to look into in a traffic so as to classify it as Block, Report or Allow. Based on this classification the traffic will be allowed or disallowed into the network which the proposed work is meant to protect. The parameters and their sample values are mentioned in the table no. 1 above. The values can be tweaked depending on the network and the ability of the solution to correctly classify the traffic

8.1.1. Setup the infrastructure and networking

The network involves setting of an environment with appropriate connectivity to simulate the environment. This environment consisted of two networks with the couple of machine and the machines would be connected via a device that will analyze the traffic. This device could be a physical Linux system with two networks interfaces, one for each of the network system.

8.1.2. Packet Capture

The Linux system is used:

i. A firewall called IP tables that can be configured to send certain packets and it can receive specific destinations. The following steps are used to configure the IP tables-

a) Have to clear the existing rules from IP tables.

"sudoiptables -F

sudoiptables -t nat -F

sudoiptables -X"

b) In the next steps any packets on the inbound interface will be forwarded to queue no. 77. Algorithm is used the Ethernet interface eth0 as inbound. The following command will be used for the purpose-

"sudoiptables -t filter -A FORWARD --in-interface

eth0 -j NFQUEUE --queue-num 77".

After the algorithm is used to analys the packet it is conditionally forwarded to the destination network. It is assumedWifi interface as wlan0 of the Linux system for the out bound interface. It is done by using the following commands.

"sudoiptables --table nat --append POSTROUTING --

out-interface wlan0 -j MASQUERADE".

c) Finally IP forwarding needed to be enabled which can be done by the following commands.

"echo "1" > /proc/sys/net/ipv4/ip_forward"

i) A feature called Net Filter Queue is used which can receive the packets via IP tables on a specific queue. The queue no 77 is chosen arbitrarily.

8.1.3. Packet analysis to drop or allow

This part consisted of two program units:

i) A program that would subscribe to NFQueue no. 77 and therefore would receive all packets that was configured in step 2.This is the source of packet of the proposed approach.

ii) A program that receives the packets from the above program and analyses the packets to determine whether to send the packet to the destination or to drop them.This decision is based on a configurable state of rules in the Rulesfor Packet Filter table (table no. 1).It needs to be noted that the traffic will be regulated on-the-wire but the decision rules are preconfigured. This module does not attempt to alter the rules based on traffic patterns- it just regulates it.

9. Implementation and Result

This section describes the results and performance calculation and analysis of the proposed method to prevent Distributed Denial of Service (DDoS) attack in a LAN using Centralized Intrusion Detection System (IDS). Python is used for developing the proposed model.

In order to test the accuracy of this algorithm for blocking ICMP Flood attacks, standard windows ping commands have run from the source 192.168.1.2 to 192.168.0.7 via a Linux system connecting the two subnets192.168.0.x(wlan0) and 192.168.1.x(eth0). This algorithm uses a configurable threshold that is set equal to 45 ICMP packets per minutes on the inbound eth0 interface for the experiment

The performance metric and confusion metric are calculated for the proposed algorithm from the performance evaluation.

9.1. Confusion Metric for ICMP

From the table no. 4minimum, maximum & average delay time of DDoSAttack (ICMP Flood Attack) can be calculated using the proposed algorithm & without using algorithm.

n = Total number of packets/min

TN = True Negative, FP = False Positive, FN = False Negative, TP = True Positive

TABLE-2
Confusion Metric

9.2. Performance Metric for ICMP

The accuracy, sensitivity specificity score of the proposed algorithm are depicted by the performance metrics and these value (table no 3) are calculated based on the table no 2 Confusion metrics value.

TABLE-3

REFERENCES

[2]

Serial No	Parameter	Predicted: No	Predicted: Yes	Value (in %)
1	Accuracy			93.61%
Actual: No	TN = 88		FP = 6	94
2	Sensitivity			0%
Actual: Yes	FN = 0		TP = 0	0
3	Specificity			93.61%
Total	88		6	94

9.3 Average ping response time calculation

From the table no. 4minimum, maximum & average delay time of DDoSAttack (ICMP Flood Attack) can be calculated using the proposed algorithm & without using algorithm.

TABLE-4
Average ping response time

Cases	Minimum Delay	Maximum Delay	Average Delay
Using proposed algorithm	9 ms	2092 ms	269 ms
Direct pinging without proposed algorithm	3 ms	29 ms	5 ms

10. CONCLUSION

This dissertation is a step towards a full blown implementation of the concepts that has been learnt and ideas that has implemented. While there were constraints with the infra, the working of the concepts were proven ready to be reused in a more real life setup. This is also realized that there are lots of enhancements. That can be done on top of this work some of which have mentioned in 'future scope'.

11. FUTURE SCOPE

In future, the proposed work can further be extended by applying artificial intelligence for dynamic routing decision and mitigation of a multi-vector DDoS attack

1. Sonia Jhajharia, SurenderPunia , "The Review Paper on Securing Wireless Network from External Threats", International Journal of Computer Science and Mobile Computing, Vol. 5, no. 5, pp. 808 – 813, May 2016.
2. Dr.T.Pandikumar, MekonnenGidey, "Data Security in LAN using Distributed Firewall", International Research Journal of Engineering and Technology (IRJET), Volume: 04 , no. 05, pp. 867 – 873, May 2017.
3. BabatundeHafisLawal ,Nuray At, "Improving Software Defined Network Security Via sFlow and IPsec Protocol", Eskiehir Technical University Journal of Science and Technology a- Applied Sciences and Engineering, Vol.19 , No. 3, pp.555-564, 2018.
4. Ripon Patgiri, SabuzimaNayak, Samir Kumar Borgohain, "Preventing DDoS using Bloom filter: A

1) survey", EAI Endorsed Transactions, pp. 1-7, October 2018.

5. M. G. Mihalos, S. I. Nalmpantis, and K. Ovaliadis, "Design and Implementation of Firewall Security Policies using Linux Iptables", Journal of Engineering Science and Technology Review, pp 80-86, March.
6. Wei Yin, Hongjian Zhou, Mingyang Wang and Zhiwen Jin, "A Honeyfarm Data Control Mechanism: Design, Implementation, Evaluation and Forensic Study ", International Journal of Computer Science and Network Security, Vol.18, No.6, June 2018.
7. MengWang ,Yiqin Lu andJiancheng Qin, "A dynamic MLP-based DDoS attack detection method using feature selection and feedback", Elsevier Ltd. , pp. 1-14, October, 2019.
8. Bashar Ahmad Khalaf,SalamaA.Mostafa , Aida Mustapha,Mazin Abed Mohammed , Moamin A. Mahmoud, Bander Ali Saleh Al-Rimy, ShukorAbdRazak , Mohamed Elhoseny, and Adam Marks, "An Adaptive Protection of Flooding Attacks Model for Complex Network Environments", Hindawi Security and Communication Networks, April 2021.
9. SushmitaChakraborty, Praveen Kumar, Dr. BhawnaSinha, "A StudyOn DDOS Attacks, Danger And Its Prevention", International Journal of Research and Analytical Reviews, Vol.6, May 2019.
10. TasnuvaMahjabin , Yang Xiao , Guang Sun and Wangdong Jiang, "A survey of distributed denial-of-service attack, prevention, and mitigation techniques", international Journal of Distributed Sensor Networks, Vol. 13, 2017.
11. V.Priyadharshini, Dr.K.Kuppusamy, "Prevention of DDOS Attacks using New Cracking Algorithm", International Journal of Engineering Research and Applications, Vol. 2, pp.2263-2267, June 2012,.
12. S. Renuka Devi, P. Yogesh,"DETECTION OF APPLICATION LAYER DDOS ATTACKS USING INFORMATION THEORY BASED METRICS", Department of Information Science and Technology, College of Engg.Guindy, Anna University, 2012.
13. AnupBhange, Amber Syad and Satyendra Singh Thakur, "DDoS Attacks Impact on Network Traffic and its Detection Approach", International Journal of Computer Applications, Vol. 40, No.11, February 2012.
14. Jérôme François, IssamAib and RaoufBoutaba, "FireCol: A Collaborative Protection Network for the

Detection of Flooding DDoS Attacks", Institute of Electrical and Electronics Engineering, VOL. 20, NO. 6, DECEMBER 2012.

15. B. B. Gupta, ManojMisra and R. C. Joshi, "An ISP Level Solution to Combat DDoS Attacks using Combined Statistical Based Approach", Journal of Information Assurance and Security, June, 2008.
16. B. B. Gupta, R. C. Joshi and ManojMisra, "Dynamic and Auto Responsive Solution for Distributed Denial-of-Service Attacks Detection in ISP Network", International Journal of Computer Theory and Engineering, Vol. 1, No. 1, April 2009.
17. Kejie Lu , Dapeng Wu, Jieyan Fan, SinisaTodorovic, Antonio Nucci, "Robust and efficient detection of DDoS attacks for large-scale internet", Computer Networks, ELSEVIER Pvt. Ltd., September 2007.
18. Dan Tang, XiaohongKuang, "Distributed Denial of Service Attacks and Defense Mechanisms", IOP Publishing, 2019.
19. NipaPatani, Rajan Patel, "A Mechanism for Prevention of Flooding based DDoS Attack", International Journal of Computational Intelligence Research, 2017

SwathiSambangi, Lakshmeeswari Gondi, "A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression", Proceedings, December 2020.

BIOGRAPHIES

Mr. Sanjit Mazumder obtained his MTech in Computer Science & Engineering from West Bengal University of Technology and presently pursing his PHD. His field of interest is in Cryptography and Network Security, Machine Learning etc. He has more than eight publication in different international journals. Presently he is working as assistant professor and head of the department CSE at Seacom Engineering College , Howrah, West Bengal, India.

Mrs.Soumi Mondal Bera is a full-time Assistant Professor at the Department of Computer Science & Engineering, Seacom Engineering College Dhulagarh, Howrah., West Bengal, India. She has more than 3 years of teaching experience. Her research interests include Image Processing, cloud computing, and Machine Learning

Atikul Islam is currently an Assistant Professor in the Department of Computer Science and Engineering at Seacom Engineering College in Howrah, West Bengal, India. He is pursuing a PhD in Computer Science and Engineering at Kalyani University. He holds a Master of Technology and a Master of Computer Applications from Aliah University, Kolkata, and graduated with a Bachelor's degree in Computer Applications from MAKAUT (formerly WBUT). His research interests encompass pattern recognition, data mining, computational biology, machine learning, and bioinformatics.