Cybersecurity Network Prevention from DDOS Attack in Healthcare System

Ravi Tomar, Yogesh Awasthi

Abstract*: *In today's world of network security, wireless communication attacks such as Distributed Denial of Services (DDoS) attacks are one of the most severe cybercriminal attacks. For the information technology and computer systems, a cyber security rule is required to compel different group as well as businesses to secure their systems and information from cyber-attacks. The occurrence of attacks in the healthcare system is responsible for affecting financial as well as prestige losses the patient. To cyber defense networks from this type of attack, it is essential to design an autonomous detection system by considering some essential countermeasures. Our aim is to detect Distributed Denial of Service (DDoS) attack, which is one of the most commonly present cyber-attacks. This research presented an automatic cybersecurity system against DDoS attacks in healthcare applications. This paper focused on deep learning technology along with the concept of a nature-inspired optimization algorithm to detect the affected node. The designed network is simulated in MATLAB tool and provides better results in terms of Packet Delivery Rate, delay and detection rate with Cuckoo Search (CS) and Artificial Neural Network (ANN) as prevention algorithm. In this paper, author has discussed the importance of the information of the patient data in the healthcare. The detail architecture of the health care information system has also been demonstrated and various security requirement are also been discussed. To analyse the performance of this proposed work, the computed metrices are Throughput %, PDR, Detection Rate and Delay.

Keywords* : *Cyber network, healthcare system, Distributed Denial of Services, Cuckoo Search, and Artificial Neural Network.

I. INTRODUCTION

Health paradigm shifts to amalgamate physical medical devices and information technology into a distributed network that enables real-time and immediate transfer of information from the physical world to cyberspace for computing, storing, managing, and analyzing data [1]. On the other side, one can also say that the health care network can be considered as a cyber-physical system (CPS), which consist of interconnected physical systems through wireless means and transfer information (medical assessment/ to recognize medical events) to distance places based on some set of rules [2]. The cyber-world aims to access or monitored data from remote places with minimum human involvement. However, despite numerous advantages, the complexity of the healthcare system increases, which affects the cyber vulnerability of interconnected medical devices. According to a security survey conducted in 2016, on more than 700 health organizations, it has been revealed that about 75 % of security breaches were identified by the malicious threats [3-4]. New additions are being made to secure network as the size of the network is growing day by day, and it must adapt the volatile and huge data coming from several medical sensing nodes. But, still, now the research continues to design a secure communication cyber network for healthcare. In this research, we also present a secure healthcare system against DDoS attacks by using the concept of machine learning [5-6]. A Distributed Denial-of-Service Attack (DDoS) attack is a type of denial-of-service attack (DoS), which is a sub-type of a cyber-attack through which a large amount of data is originated from several sources. The DDoS attack affects the performance of the cyber network by simply blocking an individual source [7]. On the other side, Dos attack, the performer tries to find a network resource that is unavailable to its intentional user by disturbing the operation of a host either intentionally or temporary. DoS is generally accomplished by overloading the target system resource with excessive requirements and hence overload the systems and block the genuine information coming from legitimate users. A simple DoS attack usually stems from a single or a very small number of sources - a source that usually has a server or PC, which makes a connection to the Internet [8]. In the rest of this research paper, an overview of the existing methods performed by the number of researchers is provided in section II. In section III, the security mechanism process followed against DDoS attack is provided in the flow diagram as well as with their algorithmic details. The computed results are discussed in section IV with the conclusion in section V followed by references.

II. RELATED WORK

There are very few researchers who contributed to the security of the cyber network, particularly in the healthcare system. The researcher's contribution is described in the following section. Medical services and related medical research are becoming more and more complex, resulting in an enhanced volume of information. The advent of new technologies further promotes all this. To deal with this large volume of information is a complex process and hence limits the development of medical services. Tsai et al. (2007) [9] have analyzed weblog posts for multiple types of cybersecurity threats that are similar to the attacks which have to be detected. Existing intelligence research has focused on examine news/ forums related to cybersecurity, but very few people have looked at websites.

Revised Manuscript Received on September 05, 2020.

***** Correspondence Author

Ravi Tomar, School of Engineering & Technology (Department of CS), Shobhit Institute of Engineering & Technology, Meerut, India. Email: ravistc1@gmail.com

Yogesh Awasthi, School of Engineering & Technology (Department of CS), Shobhit Institute of Engineering & Technology, Meerut, India. Email: yogesh@shobhituniversity.ac.in

A probable latent semantic analysis tool has been used to identify keywords from cybersecurity websites for specific topics. After that, researchers presented the blogosphere keywords that can be measured in terms of topics and thus follow popular conversations along with its topics in the blog environment. The information retrieval from the weblogs can be increased by using a probabilistic approach. Javaid et al. (2012) [10] have discussed a variety of security attacks in an Un-named vehicle system. The designed system has been protected from various security attacks, and a secure path has been provided to the communicating UAVs. The designed model has assisted the users of UAV systems to understand the system's threat profile so that the user can address a variety of system weaknesses, recognize high-priority threats, and use methods to reduce those threats. Goztepe, K. (2012) [11] has designed a fuzzy rule-based technical approach to provide security to the cyber system; the designed expert system is known as the Fuzzy Rule-Based Cyber Expert System (FRBCES). To compute complex processes, a rule-based fuzzy system has been used. Semerci et al. (2018) [12] have presented an automatic defense system against DDoS threats in wireless communication systems. The designed system composed of mainly two elements, namely, a monitoring agent and discriminator agent, which is used to isolate the attacker node from the genuine node. The monitoring performed using the Mahalanobis distances that used the similarity index features, and the performance has been measured based on the throughput parameter. Tomar et al. (2019) [13] emphasizes the various aspects of ad-hoc networks. The different types of attacks that affect the system and are prevented by various algorithms mentioned. Since ad-hoc wireless networks have no basis and are consistently unreliable, therefore a large number of strikes are subject. The black hole attack is seen as one of the riskiest conditions of them. In this attack, the malicious node usually absorbs each data packets that are similar to separate holes in all things. Likewise, all packets have been dropped in the network. For this reason, various prevention measures should be employed in the form of routing finding first then the optimization followed by the classification. Tomar et al. (2019) [14] discuss research on cybersecurity has gained more attention and interest outside the availability of computer security experts. Cybersecurity is not a single issue, but a series of highly different issues involving multiple threats. The data accommodation in health care system is growing continuously, which demanded a highly efficient and intelligent system to deal with the health records. The increase in the data increases the probability of affecting data by the cyber attacker. Therefore, it becomes essential to deal with cyber-attacks. This research focused on the utilization of cybersecurity for healthcare organization using machine learning approach. Our aim is to detect Distributed Denial of Service (DDoS) attack, which is one of the most commonly present cyber-attacks. This type of attack is designed to prevent genuine user from the required network resources. By using the concept of Artificial Neural Network (ANN), the system is trained based on the database related to the clinical record, financial record, individual record etc. During the data communication process, cross-validation is performed using ANN approach, which matched the data with the database and at last check the performance parameters. The experiment results indicate that there is an increase in the True Positive Rate (TPR) and False Positive Rate (FPR) of 0.27 % and 8.79 % respectively has been observed [16].

III. PROPOSED WORK

A secure cyber network has been designed for the healthcare system using the concept of machine learning. The designed network has protected against the most affected malware attack found in the cyber network that is from a DDoS attack. The designed strategy has performed into three phases (i) Designed a network, (ii) optimization using CS, and (iii) classification of attacker node using ANN. The flow diagram of the entire work is depicted in Fig. 1.

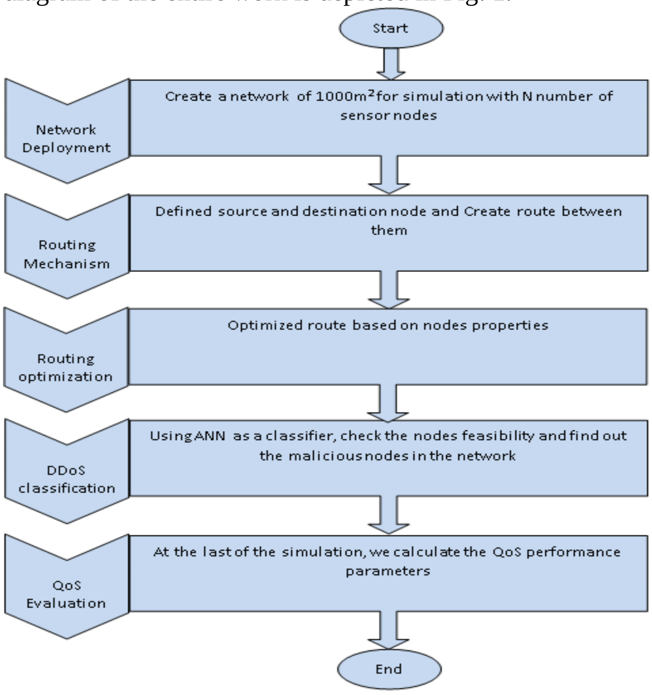

Fig. 1.Flow of proposed work

A. Network Creation

Initially, a network by deploying N number of sensor nodes is designed using a particular area that is (length and width of 1000×1000 meters, as shown in Fig. 2.

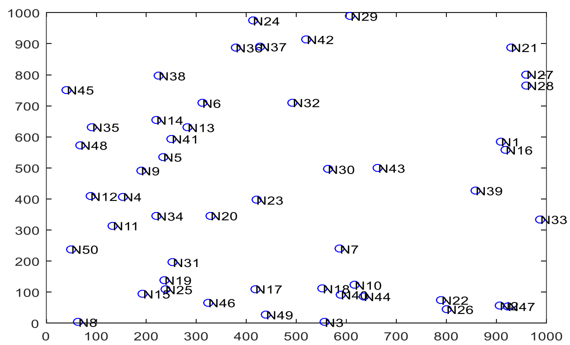

Fig. 2.Nodes Deployment

Retrieval Number: 100.1/ijitee.K78110991120
DOI: 10.35940/ijitee.K7811.0991120

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication

The coverage area of each node is defined by using the following equation

$$DefineCoverage\_set = \frac{20 * widthofnetwork}{100}$$

Based on this hypothesis, the transmitting node sends data to the neighboring node that comes under its coverage area.

B. Route Creation and Optimization

The route between the source and the destination node is created using the AODV as a routing mechanism. The working process of AODV is performed into two phases that are the route discovery process and route maintenance process. The node that wants to communicate broadcast Hello packet to their nearby nodes, as shown in Fig. 3.

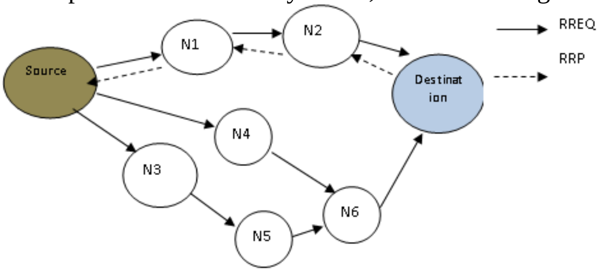

Fig. 3.AODV Process

The solid line represents the RREQ message generated by the source node as in the above figure node N1, N4 and N3 are the neighboring nodes of the source node. After receiving the RREQ message, the nodes send RREP messages towards the source node as an acknowledgment, and the data transmission begins between the source node and the destination node.

The main issue found using the AODV mechanism while transmitting data is that it does not know whether the node is affected or a real node. Therefore, the features of the nodes, such as delay, energy consumed by the nodes, etc. are used to solve this problem, and the nodes are then classified according to the healthy function of the Cuckoo Search (CS) algorithm.

C. Classification of Attacker Node using ANN

Based on the nodes propertied, a well-known ANN classifier is trained that helps to differentiate between the attacker (DDoS) node and the normal node in the cyber network. The architecture of ANN obtained after the simulation of code in MATLAB software is depicted in Fig. 4.

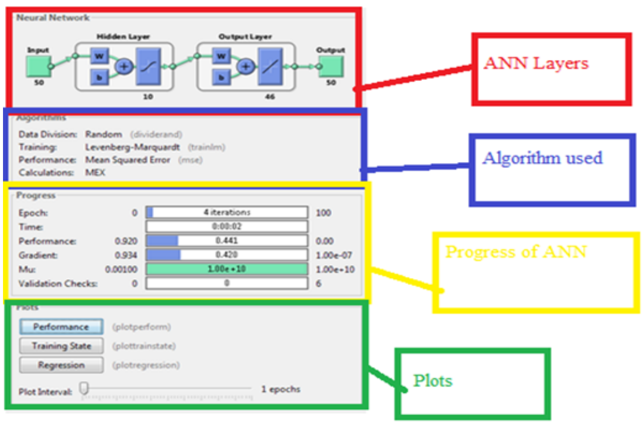

Fig. 4.Trained ANN Structure

The network is trained for 50 numbers of nodes, as shown in the input layer of ANN. The three-layer structure of ANN is used to train as well as to classify the DDoS attacker node. The accuracy of the trained ANN structure is measured on the basis of MSE value, as depicted in Fig. 5.

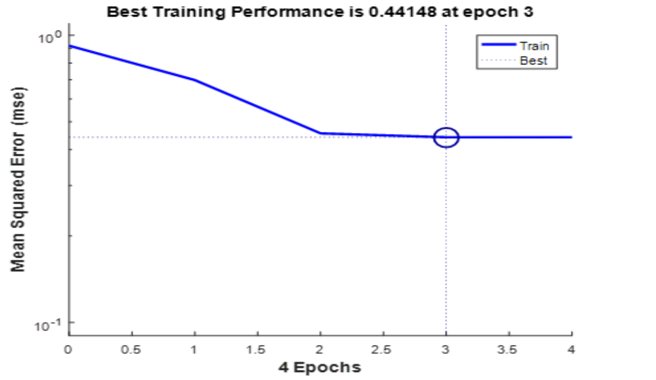

Fig. 5.MSE of ANN

The network is trained at the 3rd epoch with the best MSE of 0.44148. The proposed algorithm is listed below.

Table- I: DDoS Detection in the cyber network for healthcare system using Hybridization of ANN with CSA

Required Input:	T-Data←Properties list of sensor nodes as a Training Data
	Cat←Target/Category in terms of Normal or Abnormal Sensor Nodes
	N←Number of Carrier in terms of Neurons
Obtained Output:	DDoS Attacks←Attacker Nodes in the Network

1. Start
2. To optimize the T-Data, Cuckoo Search Algorithm (SCA) is used
3. Set up basic parameters of CSA:
   Egg Size (E) – Based on the number of sensor nodes properties
   OT – Other Eggs
   OT-Data – Optimized Training Data
   Fitness Function:
   $$F(f) = \begin{cases} 1\ (True); & if\ E_c < E_t = Other\ Threshold_{Properties} \\ 0\ (False); & Otherwise \end{cases}$$

Where Ec: It is properties of the current node (Current Egg) which are in T-Data and

E_t: It is the threshold properties of all nodes based on delay and position of sensor node with respect to the OT because the DDoS consider the time phenomenon

4. Calculate Length of T-Data in terms of R
5. Set, Optimized Training Data, OT-Data = []
6. For i =1→Length(OT-Data)
7. Ec = T (i) = ***Selected Node**$_{Properties}$* // Current Data from sensor nodes
8. Et = ***Threshold**$_{Properties}$* // Average OT
9. ***Fit(f)= Fit Fun (E_c,E_t)***
10. Best$_{Prop}$ = OT-Data = CSA (Fit(f), T-Data, Set up of CSA)
11. End – For

12. ANN Initialization using the following parameters
    -Number of Epochs (E) // Iterations used by ANN
    -Number of Neurons (N) // Used as a carrier in ANN
    -Performance: MSE, Gradient, Mutation, and Validation
    -Techniques: Levenberg Marquardt
    -Data Division: Random
13. For i = 1 → OT-Data
14. If OT-Data is a subset of Normal Sensor Nodes
15. G (1) = OT-Data(i)
16. Else if OT-Data is subset of Abnormal Sensor Nodes
17. G (2) = OT-Data(i)
18. Else
19. G (3) = OT-Data(i)
20. End – If
21. End – For
22. Initialized the ANN using Training data and Group
23. Model-Net = Newff (OT-Data, G, N) // Call the initialization function of neural network
24. Set the training parameters according to the requirements and train the system
25. Model-Net = Train (Model-Net, OT-Data, G)
26. Verification of Model:
27. Current Sensor Node = Properties of current sensor node
28. Verification Result = simulate (Model-Net, Current Sensor Node)
29. If Verification Result = True
30. Consider for data transmission
31. Else
32. DDoS Attacks = DDoS Attacker Node
33. End – If
34. Return: DDoS Attacks a list of Attacker Nodes
35. End – Function

IV. RESULT AND DISCUSSIONS

After designing the cybersecurity network for the healthcare system, performance parameters such as delay, packet delivery ratio, and detection rate are analyzed. To show the effectiveness of the work, the results with prevention mechanism and without prevention mechanisms are demonstrated.

Table- II: Computed Results

Number of iterations	Without Prevention Mechanism			With Prevention Mechanism		
	Delay	*PDR*	*Detection rate*	*Delay*	*PDR*	*Detection rate*
1	6.9	0.45	68	5.2	0.75	81
2	7.9	0.67	78	6.41	0.82	83
3	9.1	0.74	69	7.84	0.80	82
4	11.52	0.81	72	8.67	0.86	80
5	15.87	0.82	78	9.64	0.91	85
6	16.97	0.86	81	10.25	0.95	89

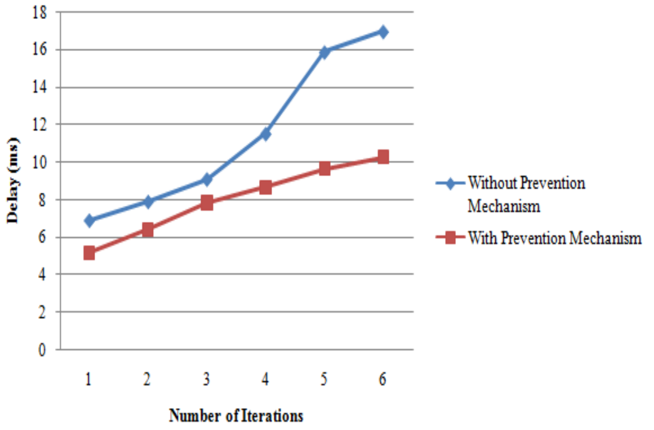

Fig. 6.Delay with without Prevention for Cyber Network

Fig. 6 illustrates the graphical representation of the delay parameter measured without and with the prevention mechanism by the blue and the red line, respectively. From the graph, it is clear the when the prevention mechanism that is CS with ANN approach has been used, the delay experienced by the communicating data to reach from the source to the destination node is less compared to the delay experienced while data is transmitted only due to the routing algorithm. The average delay analyzed for the proposed work without prevention and with prevention mechanism is 11.37 ms and 8.00 ms, respectively. Hence, there is an improvement of 29.64 %.

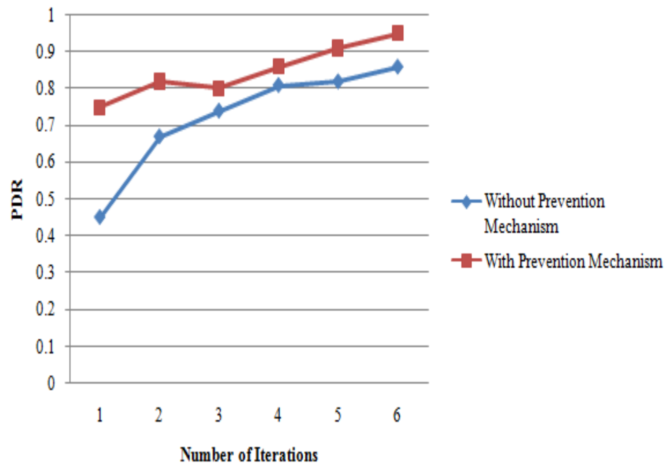

Fig. 7.PDR with and without Prevention for cyber Network

The packets delivered to the receiving node compared to the total data packets transmitted from the source node are represented in terms of PDR. From the graph, the PDR that is the packet delivered to the receiver node is higher than that of the PDR obtained without a prevention algorithm. This is due to the proper selection of a routing algorithm using the concept of CS and ANN approach. Since the proper and secure route is decided by knowing the properties of the node on an early basis and detecting the attacker node that is DDoS attacker node using ANN classifier. The improvement of about 16.28 % has been observed while using prevention mechanism.

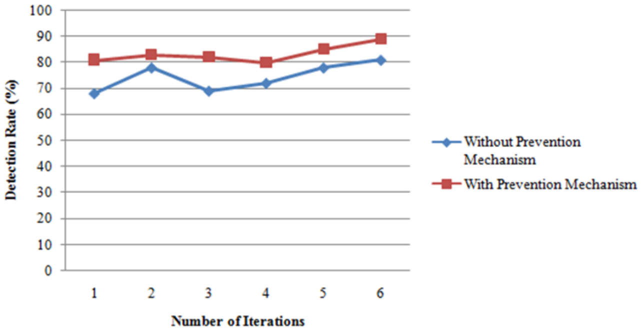

Fig. 8.Detection rate with and without Prevention for cyber network

The detection rate represents the rate of accuracy of the designed network against the detection of a DDoS attack. In Figure 8, we have seen clearly that the detection rate of the proposed work (CS with ANN) is higher compared to the network when no protection algorithms are used. This is possible only with the use of a machine learning algorithm. The detection rate of proposed work for six numbers of simulations of about 83.33 % has been attained. The improvement of about 12.11 % has been attained compared to the network without a prevention algorithm.

V. CONCLUSION

The present transition to health care organization is based on the flow of information in real-time, the integration of information and communication technologies with physical equipment to provide a coherent system that can better track the patient's health in real-time and improve overall health services. As data communication is performed through wireless means therefore, the tendency to affect or steal data by an unauthorized person increases. This problem has been resolved by designed a secure healthcare system based on ANN approach. The detection rate represents the rate of accuracy of the designed network against the detection of a DDoS attack. In Fig. 8, we have seen clearly that the detection rate of the proposed work (CS with ANN) is higher compared to the network when no protection algorithms are used. This is possible only with the use of a machine learning algorithm. The detection rate of proposed work for six numbers of simulations of about 83.33 % has been attained. The improvement of about 12.11 % has been attained compared to the network without a prevention algorithm.

REFERENCES

1. Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., and Madnick, S. "Health care and cybersecurity: a bibliometric analysis of the literature." in *Journal of medical Internet research*, 21(2), 2019.
2. Coventry, L., and Branley, D. (2018). "Cybersecurity in healthcare: A narrative review of trends, threats, and ways forward. Maturitas," 113, 2018, pp. 48-52.
3. Smith, C. "Cybersecurity Implications in an Interconnected Healthcare System." In *Frontiers of health services management*, 35(1), 2018, pp. 37-40.
4. Monisha, K., and Babu, M. R. "A Novel Framework for Healthcare Monitoring System Through Cyber-Physical System." In *the Internet of Things and Personalized Healthcare Systems Springer, Singapore.*, 2019, pp. 21-36.
5. Dogaru, D. I., and Dumitrache, I. "Cybersecurity in healthcare networks." In *2017 E-Health and Bioengineering Conference (EHB)*, June 2017, pp. 414-417.
6. Perakslis, E. D. "Cybersecurity in health care. N Engl J Med," 371(5), 2014, pp. 395-397.
7. Chen, Y., Hwang, K., and Ku, W. S. "Collaborative detection of DDoS attacks over multiple network domains." in *IEEE Transactions on Parallel and Distributed Systems*, 18(12), 2007, pp. 1649-1662.
8. Sterne, D., Djahandari, K., Balupari, R., La Colter, W., Babson, B., Wilson, B., ... and Linden, S. "Active network-based DDoS defense." *In Proceedings DARPA Active Networks Conference and Exposition*, May 2002, pp. 193-203.
9. Tsai, F. S., and Chan, K. L., "Detecting cybersecurity threats in weblogs using probabilistic models." In *Pacific-Asia Workshop on Intelligence and Security Informatics. Springer, Berlin, Heidelberg*, April 2007, pp. 46-57.
10. Javaid, A. Y., Sun, W., Devabhaktuni, V. K., & Alam, M. 2012, November). "Cybersecurity threat analysis and modeling of an unmanned aerial vehicle system." In *2012 IEEE Conference on Technologies for Homeland Security (HST)*, November 2012, pp. 585-590.
11. Goztepe, K., "Designing a fuzzy rule-based expert system for cybersecurity." in *International Journal of Information Security Science*, 1(1), 2012, pp. 13-19.
12. Semerci, M., Cemgil, A. T., & Sankur, B., "An intelligent cybersecurity system against DDoS attacks in SIP networks." in *Computer Networks, 136*, 2018, pp. 137-154.
13. Tomar, R., and Awasthi, Y. "Prevention Techniques Employed in Wireless Ad-Hoc Network." In *2nd International Conference on Advanced Science and Engineering*, April 2019.
14. Tomar, R., and Awasthi, Y. "Analysis Against DDOS Flooding in Healthcare System using Artificial Neural Network." In *International Journal of Advanced Trends in Computer Science and Engineering*, 8(1.5), November 2019, pp. 405-410.

AUTHORS PROFILE

Ravi Tomar is a research scholar at Shobhit Institute of Engineering & Technology, Meerut and also serving as one of the key promoter for various educational institutes under the banner Shivam Group of Institutions. He has received his Bachelor of Technology from Shobhit Deemed University in 2012, Master of Technology from Swami Vivekanand Subharti University in 2014 with specialization in Computer Science Engineering. Presented a paper on Prevention Techniques in Wireless Ad-Hoc Networks in ICOASE 2019, IEEE, Research Paper Published in IJATCSE Vol 8, No.1.5, 2019 on Analysis against DDOS flooding attacks in Healthcare Systems using Artificial Neural Network and author or co-author of few scientific papers on international reviews. Currently working on Optimization of Route Identification and Alleviate Effects of Attacks in MANET using Soft Computing.

Yogesh Awasthi has join the Africa University, Mutare, Zimbabwe in July 2020. He has also served in various academic institutions at International and National Level. Milestones of the service career includes, Lebanese French University, Erbil(2018-2020), Shobhit Institute of Engineering and Technology (Shobhit Deemed University)(2004-2018), Teerthanker Mahaveer University(2002-2004) and Delhi University. He has received his B.Sc. degree from Lucknow University in 1997, Master of Computer Applications (MCA) degree in 2002 from Rajiv Gandhi Technical University (RGTU), Bhopal, Second Master Degree i.e. Master of Technology (M.Tech.) in Computer Science Engineering in 2011 from Dr. A.P.J. Abdul Kalam Technical University (AKTU), Lucknow and Doctor of Philosophy (Ph.D.) in Computer Engineering & Information Technology from Shobhit Deemed University, India in 2015. He is member of various academic and administrative bodies. He has published 23 papers and articles in International and National Journals/Conferences. His area of research includes Artificial Intelligence, Watermarking Techniques, Cloud Computing and IoT. He has written a book on Java Programming titled as "Lets Play with JAVA". He was the Chairman and Head of various academic and administrative position in the university. He is a member of Computer Society of India, Member of International Association of Engineers, Hong Kong, and Member of Editorial Board of peer reviewed journals. He has guided more than 50 Master's and Graduate projects.