International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Threshold-Based Method for Detection of Distributed Denial of Service Attack in IoT

Johnson Joseph, Maitreyee Dutta

Abstract: ***The internet of things is the decentralized type of network in which sensor devices can join or leave the network when they want. Due to such nature of the network malicious nodes enter the network which affects network performance in terms of certain parameters. This research work is based on the detection and isolation of distributed denial of service attack in internet of things. The distributed denial of service attack is the denial of service type attack which affects network performance to large extent. In the existing techniques there are two main drawbacks. The first drawback is that the technique does not pin point malicious nodes from the network. The second drawback is that the malicious node detection time is very high. In this research, the new technique will be proposed for the isolation of malicious nodes from the network. In this technique, similarity of the traffic is analyzed using the cosine similarity. The sensor node which is generated dissimilar type of traffic is detected as malicious nodes. The proposed technique has been implemented in MATLAB and results have been analyzed in terms of certain parameters. It is expected that proposed technique detect malicious nodes in least amount of time.***

Keywords: ***DDoS, IoT, Threshold.***

I. INTRODUCTION

The expectation of revolution in the transfer of data from human-to-human, human-to-things and things-to-things is prefer as IOT Information Communication Technology (ICT). On behalf of people smart devices can connect, transfer information and make decisions [1]. “Connectivity for anything” is the name given to this technology. Anywhere, anytime and with anything it can be connected. To any range of traditionally dumb or non-internet-enabled physical devices and everyday objects are included by extending internet connectivity beyond standard devices like desktops, laptops, smart phones and tablets [2].

Manuscript published on November 30, 2019.
* Correspondence Author
Johnson Joseph*, M.E. Computer Science & Engineering Student National Institute Of Technical Teachers Training And Research (Nitttr), Chandigarh Johnswayanad@Gmail.Com
Dr. Maitreyee Dutta, Professor And Head Of Department, Educational Television Centre
National Institute Of Technical Teachers Training And Research (Nitttr), Chandigarh D_Maitreyee@Yahoo.Co.In

Over the internet these devices can communicate and interact also they can be remotely monitored and controlled embedded with the technology. People are acquiring education and having knowledge regarding the technologies in the present day. Huge amount of data collection is led through the usage of social websites and using more internets where continuous updates exist.

For the establishment of an effective and rewarding big data solution of any organization that wants to embark on the big information adventure is completely a clear step by step procedure [3]. For building increased best result it leads to drive better decision making solution through usage of analytical methodology that involves descriptive, predictive, inquisitive and prescriptive analytics methodology. The most important for agriculture is the water which is a main thing. The yield of crops and loss can be affected through some amount of water that may lose in leaky channels. There is a difference in the water consumption of many kinds of crops [4]. For the prevention of water supply loss and loss in the growth of the crops water need to supply to the crops in required quantity and at the correct time. Regarding the soil moisture at different levels and features of the crop it is necessary for getting the information. On the basis of meteorology forcing the soil water content available to the crop utilization of simple model is done. At any time and at any place In IoT, all the devices and people are connected with each other to provide services [5]. With efficient security mechanisms and are vulnerable to various privacy and security issues e.g., confidentiality, integrity, and authenticity, etc Most of the devices connected to the internet are not equipped. To prevent the network from malicious attacks for the IoT, some security requirements must be fulfilled. Brief description is given on some of the most required capabilities of a secure network. In a summarized form the data aggregation component is responsible for the process in the collected data [6]. The aggregated information is more significant than an isolated reading of a device in general. At a specific moment in time the average number of readings for a device/sensor for a time period can be more significant than an isolated reading. About specific groups, with specific variables a common guideline for data aggregation is to obtain more information, the time period or the function performed by each device/sensor. An attempt of an attacker in which the system is made unavailable to genuine users is known as Denial of Service (DoS) attack [7]. All the available network or resources are consumed in the presence of a successful DoS attack. All the available network or resources are consumed in the presence of a successful DoS attack. The server can either crash or slowdown due to the presence of this attack. The server that provides service to its clients is the major target of DoS attackers [8].

The active server is flood in such a manner that the service becomes unavailable in the presence of large numbers of pending requests by the DoS attacker which behaves as a legitimate client. The service queue overflows as a result of this. With the attempt of making an online service unavailable to users, a Distributed Denial of Service attack is caused in the network.

The services of hosting server are either temporarily interrupted or suspended in the presence of this attack. From hundreds to thousands of sources the packets are flood in this scenario to the victim.

II. LITERATURE REVIEW

Shah, T, et.al (2018) proposed between the server and the IOT device is a scheme which provides a secure authentication mechanism [9]. An important part of secure IOT systems is the mutual authentication between the IOT devices and IOT servers. On the basis of mutual authentication mechanism a multi-key (or multi-password) was presented in this paper. After every successful communication session final contents of the secure vault are shared between the server and the IOT device and the contents of the secure vault change. On IOT devices with memory and computational power constraints this mechanism on Arduino devices was implemented for proving the feasible algorithm. Security of the IOT systems is a field of tremendous research activities in last few years. Internet of Things is a topic of much interest in this proposed approach by the researchers.

Musale, P, et.al (2018) proposed the classification of the users using an accelerometer and linear acceleration data collected from the smart phones through Li-Gat, a lightweight Gait based Authentication Technique [10]. Exploiting information from the IOT devices such as the subconscious level of user activities uses through the authentication technique for IOT systems known as Li-GAT (Lightweight Gait Authentication Technique) for effective authenticate users with high accuracy during the decrease in the resource consumption. Using various machine learning classifiers the user authentication is done on a selected number of features. While using only the half number of features Li-GAT successfully authenticates users with high accuracy such as (96.69%) as compared to the existing technique is shown through the results.

El-hajj, et.al (2017) proposed in the literature an analysis of the different authentication schemes provided in this paper [11]. To a variety of attacks IoT authentication mechanisms took a lot of attention from researchers given that authentication-related weaknesses and vulnerabilities wide-open the door in the recent years. With respect to different criteria to help researchers in comparing and classifying other authentication schemes taxonomy of IoT authentication protocols is presented in this paper. An analysis for the most known authentication mechanisms is summarized via a table of comparison in addition. Of users' private information this wide spectrum of applications results in shared data containing large amount

Verma, K, et.al (2018) proposed the idea that elaborates that how IOT itself can provide security and facilitate the convenience with which internet can be used and the researcher has introduced comforts and insecurity too [12]. Through internet and ease out our lives it broadens our perspective of how simple things in our daily life can be interconnected. A big concern which needs to be discussed loquaciously is the Cyber Security. An effortless way of living life is making internet an artificially intelligent system. With its various relations and behaviors to achieve 100% cyber security the whole idea is based on thinking human as an object and trying to synchronize. Any user can completely rely on this. When it comes to achieve the decision taking system observing the environment introduction to big data becomes necessary. Internet can be made Artificially Intelligent Internet through this idea.

Alizai, Z. A, et.al (2018) proposed using multi-factor authentication for an IOT device through an idea of efficient device authentication scheme presented in this paper [13]. The combination of different authentication mechanisms and the addition of certain features in the scheme can actually mitigate various vulnerabilities which can be exploited through the adversary as described in this paper. Biggest problem is storing the keys now days in every scheme as the proposed scheme is secure enough to authenticate a device efficiently and securely. To authenticate a device the proposed scheme idea uses digital signatures and device capability. Due to nonce and timestamp the proposed scheme also mitigates the common attacks like replay and man in the middle.

Oh, S.-R, et.al (2017) proposed a collaborative environment of connected, intelligent and context-aware devices known as the IOT devices (Internet of Things) [14]. Security must be discussed as a main consideration in this context. IOT devices can be affected by the vulnerability of IOT platform that will affect IOT device directly and while their interworking process it will also cause a critical influence in all connected IOT platforms. Based oneM2M security component O Auth 2.0 is developed for providing authentication and authorization that are important security goals in IOT security and secure interworking between IOT platforms in this paper. Not only authentication and authorization, but also various security goals (e.g., non-repudiation) should be achieved according to the specific requirements of a specific domain.

III. RESEARCH METHODOLOGY

The cosine similarity is introduced through the proposed algorithm for the calculation of the similarity amongst vectors based on the packet-in-rate of the input port present on the boundary SD-IoT switches. Major steps followed through the proposed algorithm for the detection and mitigation of DDoS attacks in IoT is as follows:

a. For input port rate λ_m, achieving X and Y vectors:

Initially, for the input port α defined for the boundary SD-IoT switch, the packet-in rate λ_m is achieved at time interval Δt . Further, the set is generated where, $X = \{X_1, X_2, \dots X_n\} = \{\lambda_2, \lambda_4, \lambda_6, \dots \lambda_{2k}\}$, and $Y = \{Y_1, Y_2, \dots Y_n\} = \{\lambda_1, \lambda_3, \lambda_5, \dots \lambda_{2k-1}\}$. Here, the length of X and Y vectors is denoted by k.

b. Computation of Cosine Similarity for vectors X and Y denoted by $\rho X, Y$:

Through Cosine similarity calculation is done of the two similar vectors. The efficiency of cosine similarity is very high since the non-zero dimensions are included.

The cosine similarity $\rho X, Y$ of vectors that exist for packet-in rate of port α is the calculation of the equation provided below:

$$\rho X, Y = \cos(\theta) \quad \ldots(1)$$

$$= \frac{\sum_{i=2m,j=2m-1}^{2k}(\lambda_i \times \lambda_j)}{\sqrt{\sum_{i=2m}^{2k}\lambda_i^2} \times \sqrt{\sum_{j=2m-1}^{2k-1}\lambda_j^2}} \quad \ldots(2)$$

Here, $m = 1,2, \ldots k$. For two vectors X and Y, the values of all elements are greater than or equal to 0. Therefore, $0 \leq \rho X, Y \leq 1$. The closeness of angle of two vectors explains the closeness of two vectors X and Y in case when the same cosine $\rho X, Y$ is close to 1. The highest similarity exists amongst vectors X and Y in case when $\rho X, Y$ is equal to 1.

c. Determination of Occurrence of DDoS attack

The threshold value of cosine similarity is estimated to be η_U for the differentiation of DDoS attack flow from genuine flow. In the input port of SD-IoT switch is $\eta_U \leq \rho X, Y \leq 1$ a DDoS attack might exist in the input. In case if $0 \leq \rho X, Y \leq \eta_U$ the data packet of port is assumed to be a normal request. It is necessary to select appropriate threshold η_U for the cosine similarity for the assurance of the proposed algorithm performance.

d. Discarding the DDoS attack packet

it is necessary to sample the multiple ρ values for the enhancements of the reliability and accuracy of the results for differentiating the DDoS attack flow from normal flow. Achievement of $P = \{\rho_1, \rho_2, \ldots, \rho_l\}$ of the set is done here. The numbers of samples ρ that meet that condition $\eta_U \leq \rho \leq 1$ is denoted utilizes the *sum* of the number of sample ρ is donated here. The port that is attacked through the DDoS attacker is determined based on the value of sum achieved. Discard of any specific type of data packet that exists at the port is done here.

The flowchart of the proposed research work is given in figure 1.

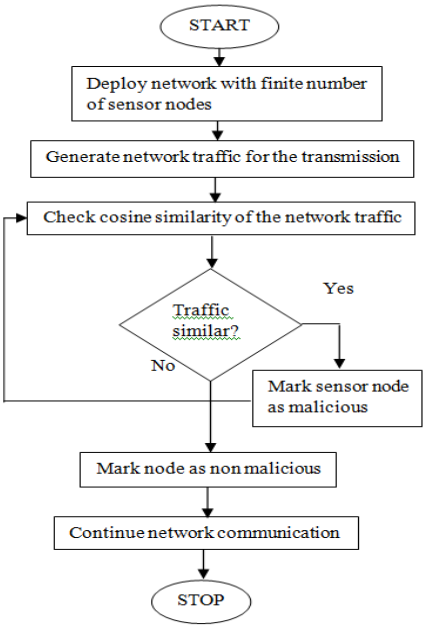

Fig.1: Proposed Flowchart

In this research work, the following algorithm is used for detecting malicious nodes from the given set of input nodes.

Proposed Algorithm

Input : Sensor Nodes

Output: Malicious Nodes

1. Deploy the network with fixed number of mobile nodes and in fixed area
2. Divide whole network into fixed size clusters and select cluster head in each cluster
3. Cluster head selection ()
4. Node = 0 /// Node identification
5. For (I = 0; I < n ; i++)
6. If(distance and energy (a(i)) <a(i+1);
7. Node = a(i);
8. Else
9. Node = 0;
10. End
11. The shortest path will be established from cluster head to sink
12. Check similarity = D(n)
13. Verify secure path ()
14. Get coordinate of node whose id is 0
15. For (I = 0; I < n; i++)
16. A(i) = a(i-1) + D(n);
17. End
18. Calculate distance between all nodes ()
19. Distance = (a(i+1) - a(i))^2 + (a(y+1) - a(y))^2
20. If (any nodes adjacent node != saved information)
21. That node will be detected as malicious node in the network

In this work, a universal structure for SD-IoT has been explained. The proposed structure contains a controller pool, SD-IoT switches incorporated with the IoT gateway, and IoT devices. The controller pool is designed like a vertical control framework. This framework includes a main control layer and a fundamental control layer.In this work, a novel algorithm is proposed with the SD-IoT structure to detect and mitigate DDoS attacks. The proposed algorithm is based on the cosine similarity of the vectors of the packet-in rate at the port of the boundary SD-IoT switches. The proposed algorithm helps to obtain the threshold value of the cosine similarity and vectors' length. The simulation results demonstrate that the proposed algorithm is able to find the IoT device within less time duration that is used to launch DDoS attack. The DDoS attack within IoT can be managed and mitigated rapidly by the proposed algorithm. In order to control different types of hardware, SDx paradigm makes use of software. SDN is a wide-ranging application of SDx paradigm.

IV.EXPERIMENTAL RESULTS

The proposed research is implemented in MATLAB and the results are evaluated by comparing proposed and existing techniques in terms of various performance metrics like throughput, energy consumption and packet loss. These metrics are evaluated by comparing their performances when security and handoff mechanism is applied.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Various simulation parameters and their values involved for the proposed network is shown in the Table 1.

Table 1: Simulation Parameters with their values

Parameter	Value
Propagation Model	Two Ray Ground model
Area	250 * 250 meters
Number of nodes	100
Network type	Wireless Networks
Range	250 meters
Transmit Energy	50nJ/bit
Receive Energy	50nJ/bit
Initial energy	0.1 Joules
Amplification Energy	10pJ/bit/m^2
Data Aggregation Energy	5pJ/bit/signal

4.1 PERFORMANCE PARAMETERS

Following the various parameters which are used for the performance analysis:-

1. Throughput: - The throughput is the parameter which is used for the performance analysis. The throughput parameter measure number of packets which are successfully received at the destination in the per unit time

$$\text{Throughput}=\frac{\text{Number of Packets Received at Destination}}{\text{Total Number of Packets Transmitted}} *\text{time}$$

2. Packet loss: - The Packet loss is the which parameter which measure the number of packets which are lost during data transmission

Packet loss=Number of Packets Send- Number of Packets Receive

3. Dead Nodes:- The number of dead node is the parameter which count number of dead nodes in the network

Dead Nodes=Nodes which has zero energy

4.2 PERFORMANCE EVALUATION OF THE PROPOSED PROTOCOL

Here, the performance evaluation of the proposed protocol is done step by step.

4.2.1 Deployment of Network

The IoT network deployment is done in this step. As shown in Fig. 2, the IoT network is deployed with the finite number of sensor nodes. The base station is deployed at the center of the network.

4.2.2 Cluster Head Selection

On the basis of LEACH protocol the nodes are placed in number of clusters, each cluster contains cluster head and normal nodes. The cluster heads are involved for the hand off mechanism in the network.

The cluster heads are selected in the network. The technique of threshold is applied for the detection of malicious nodes from the network

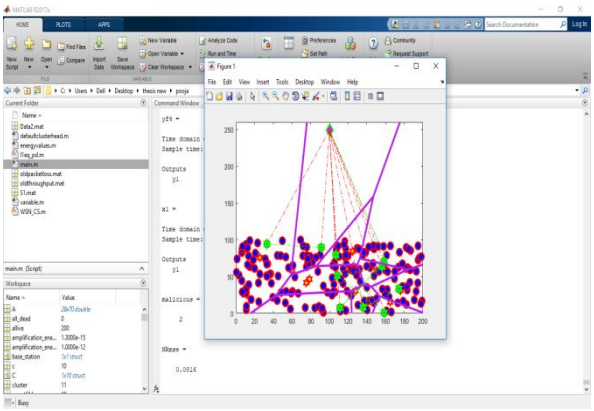

Fig 2: Deployment of network

The data transmission from sensor nodes to base station is done in this step. As shown in Fig. 2, the network is deployed with the finite number of sensor nodes. The whole IoT network is divided into fixed size clusters and cluster head get selected in each cluster. Then the cluster head send data to the base station and data is transmitted between them.

4.2.3 Throughput

Throughput is the total number of packets delivered over the total simulation time. In the Fig 3, Green line indicates the values obtained from the existing algorithm when no security is applied whereas; Red line indicates the values of throughput obtained from the proposed algorithm with the security algorithm. As it is clear from the Fig. 3, when no security is applied the value of throughput is less.

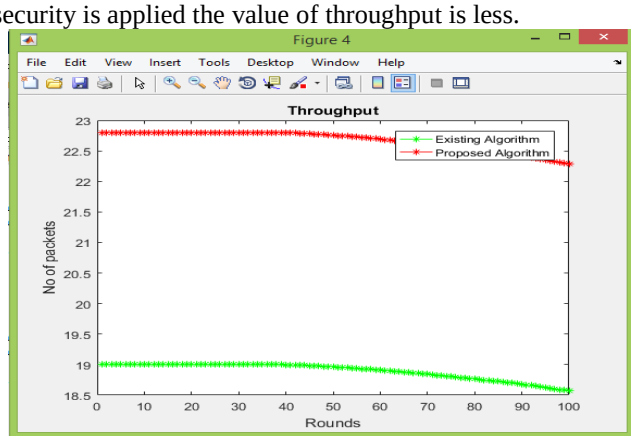

Fig 3: Throughput Comparison

As shown in Fig. 3, the throughput of the proposed technique in which cosine similarity is applied for the secure channel is analyzed. It is analyzed that throughput is increased at steady rate. The value obtained for each iteration is shown in the table 2.

Table 2: Throughput Comparison of Existing and Proposed technique

Number of Rounds	Existing Technique	Proposed Technique
10	19 packets	23 packets
40	20 packets	24 packets
80	19 packets	25 packets

4.2.4 Packet loss

Packet Loss is the total number of packets which are lost during data transmission. In the Fig. 4, Green line indicates the packet loss values obtained from the existing network whereas; Red line indicates the packet loss values obtained from the proposed network with threshold technique.

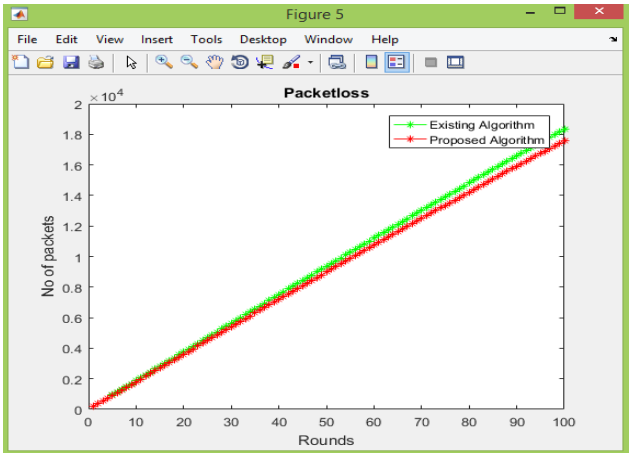

Fig 4: Packet loss Comparison

As shown in Fig 4, when the threshold technique is applied, the malicious node is detected from the network which reduces packet loss. In the figure, the x axis shows number of rounds and y axis shows number of packets. The value obtained for each iteration is shown in the table 3.

Table 3: Packet Loss Comparison of Existing and Proposed technique

Parameter	Existing Technique	Proposed Technique
10	2000	1000
40	6000	5000
80	14000	13000

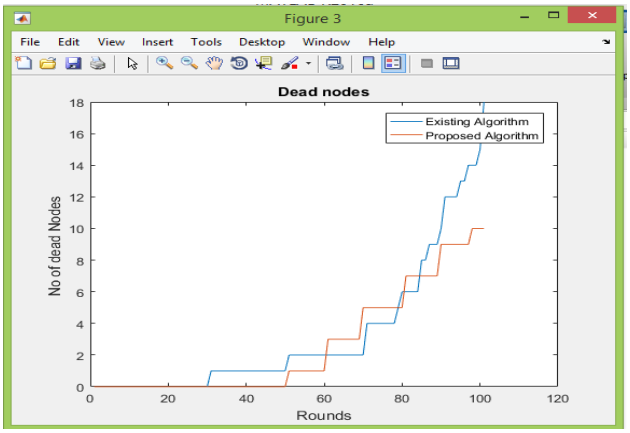

Fig 5 : Comparison of Dead Node

As shown in Fig 5, the graph is shown in which number of dead nodes are shown versis number of rounds. On the x-axis the number of rounds are shown and on the y-axis the number of dead nodes are illustrared. The proposed technique has less number of dead nodes as compared to existing technique

Table 4: Number of Dead Nodes Comparison of Existing and Proposed technique

Parameter	Existing Technique	Proposed Technique
40	1	0
80	7	1
100	12	2

V. CONCLUSION

The internet of thing is the decentralized type of network in which sensor devices can sense information and pass sensed information to base station. The sensor devices are configured and it can first transmit information to its hub which later passes it to base station. Due to dynamic nature of the network malicious nodes enter the network which triggers various type of active and passive attacks. The DDOS attack is the active type of attack in which is triggered by malicious nodes. In this work, the novel approach is proposed which is based on the cosine similarity. It is analyzed that extra hardware and software is required for the detection of malicious nodes. The proposed technique has less complexity due to which malicious nodes will be detected in least amount of time.

REFERENCES

1. M. A. Jan, P. Nanda, X. He, Z. Tan, and R. P. Liu, "A robust authentication scheme for observing resources in the internet of things environment," in Trust, Security and Privacy in Computing and Communications (Trust Com), 2014 IEEE 13th
2. H. Marzouqi, M. Al-Qutayri, and K. Salah, "Review of Elliptic Curve Cryptography processor designs," Microprocessors and Microsystems, vol. 39, pp. 97-112, 2015
3. S. Kalra and S. K. Sood, "Elliptic curve cryptography: survey and its security applications," in Proceedings of the International Conference on Advances in Computing and Artificial Intelligence, 2011
4. V. Mayer-Schönberger, "Delete: The Virtue of Forgetting in the Digital Age", Princeton University Press, 2009.
5. S.-D. Lee, M.-K Shin H.-J. Kim, "EPC vs. IPv6 mapping mechanism", in: Proceedings of Ninth International Conference on Advanced Communication Technology, Phoenix Park, South Korea, and February, 2007
6. Trappe, W.; Howard, R.; Moore, R.S., "Low-Energy Security: Limits and Opportunities in the Internet of Things", IEEE Secur. Priv. 2015, 13, 14–21.
7. Zhang, F., Nagaraja, K., Zhang, Y., Raychaudhuri, D. "Content Delivery in the Mobility First future Internet Architecture", In Proceedings of the 35th IEEE Sarnoff Symposium (SARNOFF), Newark, NJ, USA, 21–22 May 2012; pp. 1–5.
8. Su, K.; Bronzino, F.; Ramakrishnan, K.; Raychaudhuri, D. "MFTP: A Clean-Slate Transport Protocol for the Information Centric Mobility First Network", In Proceedings of the 2nd ACM International Conference on Information-Centric Networking, San Francisco, CA, USA, 30 September–2 October 2015; pp. 127–136.
9. Shah, T., & Venkatesan, S "Authentication of IoT Device and IoT Server Using Secure Vaults", International Conference On Trust, Security And Privacy In Computing And Communications 12th IEEE International Conference On Big Data Science And Engineering, 2018, 17th, IEEE
10. Musale, P., Baek, D., & Choi, B. J "Lightweight gait based authentication technique for IoT using subconscious level activities", World Forum on Internet of Things, 2018, IEEE, 4th

11. El-hajj, M., Chamoun, M., Fadlallah, A., & Serhrouchni, A "Analysis of authentication techniques in Internet of Things (IoT)", Cyber Security in Networking Conference (CS Net), 2017, 1st
12. Verma, K., & Jain, N. "IOT Object Authentication for Cyber Security : Securing Internet with Artificial intelligence", International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), 2018, IEEE
13. Alizai, Z. A., Tareen, N. F., & Jadoon, I. "Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures", International Conference on Applied and Engineering Mathematics (ICAEM), 2018
14. [14] Oh, S.-R., & Kim, Y.-G, "Development of IoT security component for interoperability", International Computer Engineering Conference (ICENCO), 2017, 13th

AUTHORS FROFILE

Johnson Joseph, Received His Bachelor's Degree In Computer Science And Engineering From Calicut University, And Currently Perusing Master's Degree In Computer Science And Engineering From NITTTR, Chandigarh. His Current Research Interest Include Data Communication And Computer Networks.

Dr. Maitreyee Dutta, Received Her Bachelor's Degree In Electronics And Communication Engineering From Guwahati University And Master's Degree In Electronics And Communication Engineering From Panjab University, Chandigarh. She Did Her Ph.D. Degree In Engineering And Technology From Panjab University, Chandigarh. Her Current Research Interests Include Digital Signal Processing, Advanced Computer Architecture, Data Warehousing And Mining, Image Processing.