Detection of Man-In-The-Middle Attacks on IoT: A Review

Arpita Thakur[1], Naveen Kumar[2], Ritesh Rana[3], Sandeep Kumar[4], Ashok Kumar Kashyap[5]
[1, 3]Dept of Computer Science
[2]Assistant Professor, Dept of Computer Science
[4,5]Assistant Professor (CS), Dept of Computer Science
[1, 2, 3] Himachal Pradesh University, Shimla
[4, 5]ICDEOL, Himachal Pradesh University, Shimla

Abstract- *In the past few years, Internet has become a significant part of our day-to-day life, and the number of devices connected to the Internet has increased. Network connectivity, including Internet access, is no longer restricted to basic systems such as PCs, laptops, or servers, but has expanded to include appliances, automobiles, cameras, pacemakers, and many more devices. These electronic devices are categorized under the Internet of Things (IoT), which is a complex network of various interconnected devices that communicate with each other over wireless and wired networks. IoT usage is increasing across a wide range of applications due to its significant impact at low implementation cost. It contributes to the creation of a smarter world by connecting intelligence to things or entities that use the Internet and integrating them into multiple systems that offer helpful services. With the increase in the use of IoT, frequency of IoT attacks is also increasing day by day. IoT attacks are cyber-attacks that employ any IoT device to obtain consumer's sensitive data. One of the most common and dangerous attacks on IoT is the Man-In-The-Middle (MITM) attack which intercepts and alters the communication between the device and the network it is connected to. This paper provides a study of various machine learning and deep learning techniques used for the detection of Man-In-The-Middle attacks in the IoT network. The comparative study of various existing machine learning and deep learning techniques help us to decide the best method used for the detection of attacks.*

Keywords- Man-In-The-Middle (MITM), Internet of Things (IoT), Machine Learning (ML), Deep Learning (DL)

I. INTRODUCTION

Internet of Things (IoT) Overview:

A new computing environment termed as the Internet of Things (IoT) or smart object networks connects a lot of constraint devices to the Internet. IoT is the collective network of various physical objects or things integrated with some electronics, software, sensors, and network connectivity that enables online data collection and sharing. It refers to using the Internet to access and manage commonly used equipments and devices [1].The fundamental goal of IoT is to enable all items to connect with one another or with people at any time, from any location, and via any network, path, or service. It contributes to the creation of a smarter world by connecting intelligence to things or entities that use the Internet and integrating them into various structures that offer helpful services. IoT is affecting every aspect of our day to day lives, from wearable technology to smart homes and it is quickly changing how we interact with technology [2].

Man-In-The-Middle Attack:

Today, the Internet is used in every aspect of life which includes online banking, online entertainment, online shopping, social networks and many more. These online services store or transfer user’s sensitive information which can be easily accessed by the hacker. Hackers don’t only target individuals but also the enterprises and organizations which can lead to huge loss. One of the most frequent attack on the IoT network is Man-In-The-Middle attack. MITM attack is the type of passive attack that makes this attack difficult to detect.The word "Man-In-The-Middle" is taken from a basketball scenario where two players are attempting to pass the ball to each other while a third player tries to intercept the pass. This attack is also sometimes referred to as a "bucket brigade attack," "fire brigade attack," or "monkey-in-the-middle attack" [3].A MITM attack refers to a cyber-attack where an attacker intercepts communication between two parties, such as a website and its user, and eavesdrops on their conversation. The attacker can then manipulate the communication by inserting or altering messages, which may be used to steal sensitive information or credentials, redirect the user to a malicious website, or gain unauthorized access to the user's system [4].

Various types of Man-In-The-Middle Attack:

Different types of the MITM attacks in the IoT which are discussed below:

(a) **Wi-Fi Eavesdropping:** Unencrypted Wi-Fi networks can easily be observed just like in a public discussion; anyone can take part.Though access is restricted by setting your computer to "public," which disables Network Discovery. This setting stops other network users from abusing the configuration [4].

(b) **DNS Spoofing:** In DNS (Domain Name System) poisoning or spoofing, the attacker modifies the DNS records to direct users to a fake website or a domain that is under their control. Every time the victim uses the internet, a hacker will intervene between the server and the user and alter the user's DNS. Updating DNS involves changing the website’s destination IP addresses [4].

(c) **IP Spoofing:**Each device has a distinct IP (Internet Protocol) address in a number of internal web networks of businesses. IP spoofing attackers impersonate a reliable console. A network perceives the system as authorized [4].

(d) **HTTPS Spoofing:** HTTPS spoofing is a technique in which the attacker uses a domain that closely resembles one of the target websites. Your browser may be tricked into thinking as if it is accessing a reputable website and not by an attacker and lead your browser to a suspicious website in order to gather data [4].

(e) **ARP Spoofing:** An attacker creates a false response in response to an ARP (Address Resolution Protocol) request sent by a client. As they are acting as a computer modem in this situation, the attacker has access to the traffic flow. Local area networks (LANs) that use the ARP protocol are typically the only ones that are impacted [4].

(f) **E-mail Hacking:** In this type of cyber security breach, an attacker uses the user's email system as a tool. While acquiring information and possibly listening to the conversation, the invader also keeps a low profile. The Attackers might use a unique pattern of scanning that seeks for words like "financial" or "secret Democratic policies" [4].

(g) **Session Hacking:** Exploiting an active computer session is known as session hijacking or cookie side-jacking. This Man-in-the-Middle technique allows the hacker complete access to the internet account. The session cookie knowledge of the attacker is necessary for the session hijacking attack. If the attacker obtains your session cookie, they can perform a lot of things with your account [4].

(h) **SSL Stripping:** Another type of man-in-the-middle attack, also referred to as SSL stripping, occurs when a hacker is successful in staging an SSL stripping scheme against the victim. The attacker intercepts any information going between the server and the user's computer during an SSL hijacking by using a different computer and secure server [4].

(i) **MITB Attack:** In a Man-In-The-Browser (MITB) attack, an attacker gains access to a Web browser being used by one of the parties and enters the communications channel between the two trusting parties with the intention of listening in, stealing data, and/or changing sessions [4].

Machine Learning:

Machine learning is the branch of artificial intelligence whose main goal is to build machines which can behave and understand like humans do. According to Arthur Samuel, Machine learning is defined as the field of study that gives computers the ability to learn without being explicitly programmed [7]. Machine learning is a method of data analysis that automates the analytical model building. It allows computers to automatically learn and improve from experience without being explicitly programmed [6]. Various examples of machine learning methods are Linear Regression, Multilinear Regression, Gaussian Naïve Bayes, Logistic Regression, Decision Tree, Support Vector Machine, K-Nearest Neighbors, K Means Clustering etc.

Deep Learning:

Deep Learning is the sub-field of machine learning that uses multi-layered Artificial Neural Networks (ANNs) which deliver state-of-the-art accuracy in various tasks such as object detection, speech recognition and language translation [5]. Deep learning is a subset of machine learning that utilizes neural networks to solve complex problems. Deep learning models are inspired by the structure and function of the human brain, and they are capable of learning from unstructured and unlabeled data. Deep learning differs from traditional machine learning techniques in that they can automatically learn representations from data such as images, videos, or text, without introducing hand-coded rules or human domain knowledge. Their highly flexible architectures can learn directly from raw data and can increase their predictive accuracy when provided with more data [6]. Various examples of deep learning methods are Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Multilayer Perceptron (MLP), Long Short-Term Memory (LSTM), Generative Adversarial Networks (GAN), Deep Reinforcement Learning (DRL), Self-Organizing Maps (SOM) etc.

II. LITERATURE REVIEW

(a)Detection of MITM attacks on IoTusing Machine Learning Techniques

In 2016, Mauro Conti et al. extensively analyzed and categorized the scope of MITM attacks. Categorization is done by taking a reference model, such as the Open Systems Interconnection (OSI) model and widely used network technologies, i.e., GSM and UMTS. MITM attacks have been classified by them based on several parameters, like nature of a communication channel, location of an attacker in the network, and impersonation techniques. Existing countermeasures have been surveyed by them and the comparison among them has been discussed [8].

In 2020, Jerry John Kponyo et al. proposed a technique for detecting End-Point (EP) MITM attacks based on the ARP analysis using machine learning method. Machine learning techniques used were Gaussian Naïve Bayes, SVC (Support Vector Classifier), Linear SVC, Logistic Regression, Random Forest (RF), KNN (K-Nearest Neighbors), Decision Tree (DT) and Gradient Boosting. The proposed method combinessignal processing and machine learning to achieve high accuracy. The experimental results show that Linear SVC and Gaussian Naive Bayes has the highest accuracy 99.72% [9].

In 2020, Sai Kiran et al. proposed the development of an Intrusion Detection System (IDS) for IoT environments using various machine learning techniques. The challenges of securing IoT devices and the need for an IDS to detect and prevent attacks was discussed. Also, the architecture of the proposed IDS, which includes data collection, feature extraction and classification using machine learning algorithms were described. Machine learning techniques used in the paper were Naïve Bayes, SVM, decision tree, Adaboost. Evaluation of performance of the IDS using a dataset of IoT network traffic was done. The decision tree classifier had the best accuracy among all the models used [10].

In 2020, Hitesh Mohapatra et al. proposed a model for detecting and isolating man-in-the-middle attacks in wireless sensor networks using an intrusion detection system technique. The proposed model called MITM-Intrusion Detection System (MITM-IDS) was validated by considering two factors, throughput, and packet loss. The experimental results showed that the proposed method has a higher throughput rate compared to the scenario without any security mechanism. The packet loss scenario also showed that the proposed method has a lower packet loss rate compared to the scenario without any security mechanism. The proposed model can detect and isolate MITM attacks in wireless sensor networks with a productivity rate of 89.147% [11].

In 2020, Henry Wong et al. introduced a new scheme that uses the Message Queuing Telemetry Transport (MQTT) protocol using machine learning algorithms for communications for MITM attack detection on IoT devices. It consists of an MQTT Parser that dissects and alters messages at the bit level and a novel BERT- based adversarial model that generates malicious messages using an approach inspired by GAN. It demonstrated how the created attack strategy avoids anomaly detection models based on logistic regression, random forest, k-nearest neighbor, and support vector machine (SVM). To conduct experiments, an environment for testing employing IoT hardware and software, such as Raspberry Pi, WiFi Pineapple, Mosquitto, etc. were used. Results were found that the MITM attack is effective against a wide range of typical anomaly detection mechanisms [12].

In 2020, Otily Toutsop et al. examined real-life IoT device attack dataset to optimize the monitoring and detection time of Man-In-The-Middle attacks in the network from the Hacking and Countermeasure Research Lab (HCRL) using three machine learning techniques which were LR, RF and DT and found that the overall detection accuracy is 98-100%, more promising than traditional Intrusion Detection Systems (IDS). Logistic regression approach showing an accuracy of 98.6%, a random forest showing 100% and a decision tree with a high F1 score [13].

In 2021, Farouq Aliyu et al. proposed an Intrusion Detection and Prevention System (IDPS) to detect Man-In-The- Middle (MITM) attacks in the fog layer of a network. Exponentially Weighted Moving Average (EWMA) is added to the system to smooth out noise and improve accuracy by 15% and detect the intrusion 0.25-0.5 s faster than without EWMA. The system used special nodes called Intrusion Detection System (IDS) nodes to monitor the behavior of fog nodes in the network and detect intrusion. The approach was anomaly-based and aimed to discover MITM reliant intrusive activities in the fog layer. The use of EWMA affects the latency of services provided by fog nodes by at least 0.75–1.3 s. OMNET++ simulator was used for the implementation of proposed system [14].

In 2022, Bilal Ahmad Mantoo and Parveen Kaur discussed the security concerns related to IoT devices and developed a machine learning model for detecting Man-In-The-Middle (MITM) attacks efficiently using KNN algorithm over unsecured devices, which can compromise the security of Wi-Fi networks. The dataset was being prepared using TP-link gateway connecting multiple devices. Analysis of the features of IoT attacks and use of data obtained through Wireshark to develop the model were described. The model used different sets of data obtained using Wireshark and showed an accuracy of 0.98 [15].

In 2023, Alvaro Michelena et al. presented a new approach for detecting Man-In-The-Middle attacks in Internet of Things (IoT) environments using Message Queuing Telemetry Transport (MQTT). The approach was based on intelligent algorithms and machine learning techniques. The author highlighted the importance of security in IoT environments and the need for effective intrusion detection systems. The proposed approach was compared with other existing approaches and shows promising results. Four machine learning algorithms such as KNN, DT, RF, ANN were compared using Python language. Dataset from joseaveleira website was used. The experimental results stated that ANN works better with 99.2% accuracy [16].

In 2023, Juboori et al. focused on preventing network attacks, specifically Man-In-The-Middle (MITM) and denial of service (DoS) attacks, on physical connected devices in any network. Datasets related to these attacks from the Kaggle website and several machine learning algorithms (random forest, eXtreme gradient boosting, gradient boosting, and decision tree) to detect and prevent these attacks were used. Preprocessing techniques to the datasets were also applied. Results were found that all the four algorithms were able to detect MTM attacks with over 99% accuracy in all metrics and DoS attacks with over 97% accuracy in all metrics [17].

(b) Use of Deep Learning Techniques for the Detection of Attacks on IoT

In 2019, Robert A. Sowah et al. aimed for detection and prevention of Man-In-The-Middle (MITM) spoofing attacks using predictive techniques in Artificial Neural Networks (ANN) in Mobile Ad-Hoc Networks (MANETs) by using NS2 as the simulation platform. The performance metrics that had been used are recall, precision, accuracy, and f-measure. They are using 7 to 18 nodes as the experiment scenarios. The result stated that it could generate accuracy rates in the range of around 79%-93% from 7-18 nodes. A final detection rate of 88.235% is measured [18].

In 2021, Fahiba Farhin et al. proposed the attack detection model for IoT using Software-defined network (SDN) and a fuzzy neural network (FNN).Proposed attack detection system was considered to detect attacks such as man-in-the-middle, distributed denial of service, side-channel, and malicious code. The FNN was trained and tested using NSL-KDD datasets. The evaluated performance showed that the FNN based attack detection system can detect the above four attacks with an accuracy of 83% [19].

In 2022, Usman Inayat et al. provided a comprehensive survey of learning-based methods for detecting cyber-attacks in IoT systems, focusing on different types of attacks such as DoS, DDoS, probing, U2R, R2L, botnet, spoofing, and MITM attacks. The literature review was conducted using various data sources, including ACM, SCOPUS, IEEE Xplore, Science Direct, MDPI, and Web of Science. The search covered the years 2016 to 2022 and included papers from English-language journals [20].

III. COMPARATIVE ANALYSIS

Various machine learning and deep learning techniques help us to detect MITM attacks in the IoT environment. The study shows the comparison between different machine learning and deep learning techniques based on their performance metrics. A comparison of various machine learning and deep learning techniques is shown in Table 1. Table 1 presents the comparison of various methods and datasets used for the detection of MITM attacks on the IoT environment. This comparison is done by reviewing various literature which helps in providing necessary information on the theoretical work for conducting research on various machine learning and deep learning techniques. Various performance metrics which are used for the comparative analysis of machine learning algorithms are described below:

(a)Accuracy: Accuracy is a ratio of correctly predicted observation to the total observations.

(b)Sensitivity (Recall or True positive rate): Sensitivity is calculated as the number of correct positive predictions divided by the total number of positives. It is also called recall (REC) or true positive rate (TPR). The best sensitivity is 1.0, whereas the worst is 0.0.

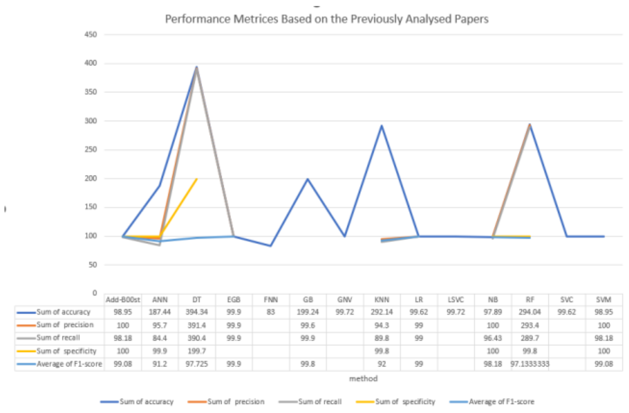
(c)F1- Score: It is the weighted average of precision and recall.

(d)Precision: Precision is the fraction of relevant instances among the retrieved instances.

(e)Specificity: Specificity (SP) is calculated as the number of correct negative predictions divided by the total number of negatives. It is also called true negative rate (TNR). The best specificity is 1.0, whereas the worst is 0.0. [21]

Table 1: Comparative Analysis of various methods used for the detection of MITM attacks on IoT environment

Ref.	Problem on which author	Data Set	Methods	Accuracy (%)	Precision	Recall	Specificity	F1-Score	Best Algorithm found
	worked	Used	Used		(%)	(%)	(%)	(%)	(Accuracy)
[9]	End- Point MiTM Attack detection on ARP analysis	Dataset with 5,300	LinearSVC	99.72	-	-	-	-	LinearSVC &
		rows of the feature vectors	GNB	99.72	-	-	-	-	GNB
			SVC	99.62	-	-	-	-	99.72%
			LR	99.62	-	-	-	-	
			RF	99.44	-	-	-	-	
			KNN	99.34	-	-	-	-	
			DT	99.34	-	-	-	-	
			GB	99.34	-	-	-	-	
[10]	Intrusion Detection System for IoT environme nt	Sensor 480	NaiveBayes	97.89	100	96.43	100	98.18	DT
		Dataset	SVM	98.95	100	98.18	100	99.08	100%
			DT	100	100	100	100	100	
			Adaboost	98.95	100	98.18	100	99.08	
[13]	Optimizing monitoring & detecting time of MiTM	Collected	LR	-	99	99	-	99	-
	attack	by real- life Internet	RF	-	100	100 100	-	100	
		devices	DT	-	100		-	100	
[15]	Detection of MiTM	Dataset made							KNN
	attack over	using	KNN	98	-	-	-	-	98%
	unsecured network								
[16]	New approach for detecting MITM attack on IoT environme nt	Dataset available on Internet	KNN	94.8	94.3	89.8	99.8	92	ANN
			DT	95.1	91.5	90.5	99.7	91	99.20%
			RF	94.8	93.8	89.8	99.8	91.7	
			ANN	99.2	95.7	84.4	99.9	91.2	
[17]	Preventing network attacks; MiTM and DoS attacks		RF	99.8	99.6	99.9	-	99.7	eXtreme
		Kaggle	eXtremeGB	99.9	99.9	99.9	-	99.9	GB
			GB	99.9	99.6	99.9	-	99.8	DT
			DT	99.9	99.9	99.9	-	99.9	99.90%
[18]	Use of predictive techniques in ANN for MITM spoofing attacks in	Net- work varied traffic	ANN	88.24%	-	-	-	-	ANN
	MANETs								88.23%
[19]	IoT attack detection model for using SDN and a FNN	NSL-KDD	FNN	83%	-	-	-	-	FNN
									83%



	Add-B00st	ANN	DT	EGB	FNN	GB	GNV	KNN	LR	LSVC	NB	RF	SVC	SVM
Sum of accuracy	98.95	187.44	394.34	99.9	83	199.24	99.72	292.14	99.62	99.72	97.89	294.04	99.62	98.95
Sum of precision	100	95.7	391.4	99.9		99.6		94.3	99		100	293.4		100
Sum of recall	98.18	84.4	390.4	99.9		99.9		89.8	99		96.43	289.7		98.18
Sum of specificity	100	99.9	199.7					99.8			100	99.8		100
Average of F1-score	99.08	91.2	97.725	99.9		99.8		92	99		98.18	97.1333333		99.08

Figure 1 Comparative Performance Metrices Graph

A detailed review, comparative analysis table and graph for the comparative performance metrics is made for the comparison of various algorithms used for the detection of MITM attacks using machine learning and deep learning. Figure 1 shows the sum of all the performance metrices for different algorithms used in previous papers,

IV. CONCLUSION

The rapid expansion of IoT devices has created opportunities for hackers and malicious users to exploit vulnerabilities within the system, enabling them to compromise device security and launch attacks on the entire IoT network. Various ML and DL algorithms can be used for the detection of MITM attacks on the IoT environment. After reviewing and analyzing them it has been found that Decision Tree is the most accurate machine learning classifier and has a promising recall rate. Maximum value of precision, specificity and f1-score is found similar for two to three classifiers. Also, Random Forest (RF) and Decision Tree (DT) classifiers are the most commonly used methods and perform better than other classifiers.

REFERENCES

[1] Gokhale, P., Bhat, O. and Bhat, S., 2018. Introduction to IOT. *International Advanced Research Journal in Science, Engineering and Technology*, *5*(1), pp.41-44.

[2] Swan, M., 2012. Sensor mania! the internet of things, wearable computing, objective metricssom the quantified self 2.0. *Journal of Sensor and Actuator networks, 1(3)*, pp.217-253.

[3] Nayak, G.N. and Samaddar, S.G., 2010, July. Different flavours of man-in-the-middle attack, consequences and feasible solutions. In *2010 3rd International Conference on Computer Science and Information Technology* (Vol. 5, pp. 491-495). IEEE.

[4] www.javatpoint.com. (n.d.). Cyber Security | Man-in-the-middle (MITM) Attacks - javatpoint. [online] Available at: https://www.javatpoint.com/cyber-security-mitm-attacks (Accessed on 27-04-2023).

[5] *Deeplearning* (2023).Availableat: https://developer.nvidia .com/deep-learning. (Accessed on: 05/09/2023)

[6] Sharifani, K. and Amini, M., 2023. Machine Learning and Deep Learning: A Review of Methods and Applications. *World Information Technology and Engineering Journal*, *10*(07), pp.3897-3904.

[7] Mahesh, B., 2020. Machine learning algorithms-a review. *International Journal of Science and Research (IJSR).[Internet]*, *9*(1), pp.381-386.

[8] Conti, M., Dragoni, N. and Lesyk, V., 2016. A survey of man in the middle attacks. *IEEE communications surveys & tutorials*, *18*(3), pp.2027-2051.

[9] Kponyo, J.J., Agyemang, J.O. and Klogo, G.S., 2020. Detecting End-Point (EP) Man-In-The-Middle (MITM)

attack based on ARP analysis: a machine learning approach. *International Journal of Communication Networks and Information Security*, *12*(3), pp.384-388.

[10] Kiran, K.S., Devisetty, R.K., Kalyan, N.P., Mukundini, K. and Karthi, R., 2020. Building a intrusion detection system for IoT environment using machine learning techniques. *Procedia Computer Science*, *171*, pp.2372-2379.

[11] Mohapatra, H., Rath, S., Panda, S. and Kumar, R., 2020. Handling of man-in-the-middle attack in wsn through intrusion detection system. *International journal*, *8*(5), pp.1503-1510.

[12] Wong, H. and Luo, T., 2020, August. Man-in-the-middle attacks on mqtt-based iot using bert based adversarial message generation. In *KDD 2020 AIoT Workshop*.

[13] Toutsop, O., Harvey, P. and Kornegay, K., 2020, October. Monitoring and detection time optimization of man in the middle attacks using machine learning. In *2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)* (pp. 1-7). IEEE.

[14] Aliyu, F., Sheltami, T., Mahmoud, A., Al-Awami, L. and Yasar, A., 2021. Detecting Man-in-the-middle attack in fog computing for social media.

[15] Mantoo, B.A. and Kaur, P., 2022, October. A machine learning model for detection of man in the middle attack over unsecured devices. In *AIP Conference Proceedings* (Vol. 2555, No. 1, p. 020005). AIP Publishing LLC.

[16] Michelena, Á., Aveleira-Mata, J., Jove, E., Bayón-Gutiérrez, M., Novais, P., Romero, O.F., Calvo-Rolle, J.L. and Aláiz-Moretón, H., 2023. A novel intelligent approach for man-in-the-middle attacks detection over internet of things environments based on message queuing telemetry transport. *Expert Systems*, p.e13263.

[17] Al-Juboori, S.A.M., Hazzaa, F., Jabbar, Z.S., Salih, S. and Gheni, H.M., 2023. Man-in-the-middle and denial of service attacks detection using machine learning algorithms. *Bulletin of Electrical Engineering and Informatics*, *12*(1), pp.418-426.

[18] Sowah, R.A., Ofori-Amanfo, K.B., Mills, G.A. and Koumadi, K.M., 2019. Detection and prevention of man-in-the-middle spoofing attacks in MANETs using predictive techniques in Artificial Neural Networks (ANN). Journal of Computer Networks and Communications, 2019.

[19] Farhin, F., Sultana, I., Islam, N., Kaiser, M.S., Rahman, M.S. and Mahmud, M., 2020, August. Attack detection in internet of things using software defined network and fuzzy neural network. In *2020 Joint 9th International Conference on Informatics, Electronics & Vision (ICIEV) and 2020 4th International Conference on Imaging, Vision & Pattern Recognition (icIVPR)* (pp. 1-6). IEEE.

[20] Inayat, U., Zia, M.F., Mahmood, S., Khalid, H.M. and Benbouzid, M., 2022. Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects. Electronics, 11(9), p.1502.

[21] GeeksforGeeks.(2020). *ML|Evaluation Metrics*. [online]Available at: https://www.geeksforgeeks.org/metrics-for-machine-learning-model/. Accessed on: 09/09/2023