Journal of Theoretical and Applied Information Technology
15th May 2024. Vol.102. No 9
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMPLEMENTATION OF ATTACK DETECTION AND MITIGATION FOR SECURING CLOUD BASED IOT NETWORK

ARCHANA D.WANKHADE[1], KISHOR P.WAGH[2]

[1]Research Scholar, Computer Science and Engineering Department,
Government College of Engineering,
Amravati, India
[2]Assistant Professor, Computer Science and Engineering Department,
Government College of Engineering,
Amravati, India
E-mail: [1]archanadwankhade@gmail.com, [2]kishorpwagh2000@gmail.com

ABSTRACT

Now a day's Internet of Things (IoT) has become fastest computing technology which makes human life easier and comfortable. IoT is important for smart system like homes, transportation, farming etc. Using this robust technology improves efficiency, mobility and cost reduction. But due to heterogeneous nature of this IoT network, it has many security issues. The devices in IoT network are generally attacked by intruders. Hence risk of security is high in IoT network than other computing paradigm. This is the reason why traditional security techniques are not useful in these IoT network. A holistic solution is required for fulfilling security requirement of IoT network. The existing security issues like authentication, access control, network security are not fulfilling challenges in large IoT system having number of smart devices. In this communication of Cloud based IoT network sensor data is transmitted from IoT network to cloud. This path is vulnerable. The objective of this work is to secure this path by proposed Attack Detection and Mitigation using ML approach for Cloud Internet of Things (IoT) network. For this proposed work, license software NetSim Standard v13.3 is used for identification of malicious node in Cloud based IoT network. The work was tested with ML approaches used for Attack Detection and Mitigation and efficiency is calculated to improve the performance. Performance of proposed model is improved using Decision Tree(Train Score 100%,Test Score 99.39%) comparing with K-Nearest Neighbors (Train Score 98.52% and Test Score 98.24%) and Logistic Regression algorithms(Train Score 92.87% and Test Score 92.31%).

Keywords: *Attack Detection and Mitigation, IoT, KNN, Lightweight Cryptography, Machine Learning.*

1. INTRODUCTION

Recent developments in IoT Technology have greatly make advances in lifestyle. About 75 billion smart devices will get connect in IoT by end of 2025[1]. IoT has done revolution in technology in many areas of life. IoT architecture aims to connect us to everything, anywhere and at any time. IoT offers us more and more benefits but at the same time issues in security and privacy also arise. Top priorities in IoT architecture is its security and privacy. Security issues like attack on IoT network, attack at the time of sensor data transmission of IoT devices are important. To deal with this problems this research provides protection to IoT network.To avoid this security issues, Cloud based IoT network can be designed and tested using simulation. This can develop solutions to different vulnerabilities in IoT network. In this research paper we have use license software NetSim Standard v13.3 to simulate Cloud based IoT network for identification of malicious node in network. Here IoT anomalies can be detected with the help of machine learning algorithm as Machine Learning is used for training and solving complex problems based on previous experience. ML can be used here for attack detection and mitigation in IoT network. Hence we have used ML algorithms like Decision Tree, K Nearest Neighbors and Logistic Regression for identification of "normal", "abnormal" behavior of IoT network. Another security issue arises with generation of large amount of data in Internet of Things network. IoT devices generates large amount of data and that is the reason IoT system requires cloud to store this big data. IoT device generates big data and

transmitted to gateway and further through this gateway transferred to cloud for storage using wireless channels. This path of sensor data transmission is vulnerable and security issues arise. To protect this end to end communication of sensor data from IoT network to cloud cryptography is a solution. But due to resource constrained devices cryptographic algorithms are not functioning well for IoT. Hence Lightweight cryptography can be useful. The communication from such devices can be secured by a mean of lightweight cryptography, a lighter version of cryptography [2].

Motivation

Things in IoT is nothing but devices used in IoT network. Devices having internet capability, sensors and actuators, some embedded software can collect data which is nothing but sensors data. These devices are able to continuously sense data from environment and transmitted to the cloud for storage purpose and further for analysis purpose which will be used for the prediction of different applications. IoT devices consist of sensors for collecting the data and actuators for actually performing the activity which will be required at that time for IoT network. Internet connectivity with this things or devices connect all these devices with the external network which will be useful for communicating of these devices to external world and can possible sensors big data to be stored on cloud for further analysis purpose. IoT device collect data from external environment such as humidity, light intensity or temperature etc. This sensor data can be communicated either to other devices in the network or for cloud base server or storage for analysis purpose. Various IoT devices are available which can be useful depending on different applications of IoT. Smart wearable for health monitoring like smart watch. For smart automobile application smart Car is the example. Smart irrigation system devices like soil moisture monitoring devices smart water motor. So this devices are smart in the sense consist of different interfaces sensors memory storage internet connectivity to make it smart. This smart devices in IoT network can communicate with each other and can communicate with external world through the internet connectivity. It requires different protocols for communication purpose. As devices are generally integrated to the information network. IoT devices can have the capability to describe themselves and communicate with the information network. To this integration into the information network IoT system get smarter and the data from large number of connected with the monitoring IoT node can we aggregated into a single location which can be further use for the prediction which requires cloud. But by referring different literature it is found that different security issues are there in IoT network.

Device Vulnerabilities: Many IoT devices may have inadequate security measures due to poor design or cost constraints, making them vulnerable to attacks.

Data Privacy: Data Interception: Attackers may intercept and eavesdrop on data transmitted between IoT devices, leading to privacy breaches. Unauthorized access: Unauthorized access to sensitive data collected by IoT devices poses a significant privacy risk.

Authentication and Authorization Issues: Weak Credentials: Devices with default or weak credentials can be easily compromised, allowing unauthorized access. Insufficient Authorization controls: Inadequate authorization mechanism may enable attackers to gain unauthorized control over IoT devices.

Network Security: Denial of Service (DoS) attacks: Overloading IoT devices or networks with excessive traffic can disturb normal operations.

Compromised Supply Chain: Insecure manufacturing process or compromised supply chains can introduce vulnerabilities in IoT devices before they even reach end user.

IoT protocol vulnerabilities: Weakness in communication protocols used by IoT devices may be exploited for unauthorized access or data manipulation. Also attackers may impersonate legitimate devices by exploiting weakness in communication protocols.

Cloud Security: IoT devices often relay on cloud services for data storage and processing. Insecure connection to the cloud can expose sensitive data.

To resolve this issues robust solution is required and hence we have implemented attack detection and mitigation with end to end secure cloud communication framework for cloud based IoT network.

2. RELATED WORK

A number of researchers from all around the world have worked on different security problems and their solutions using different techniques. Some related research articles are considered here for implementation of secure framework.

In [3], the author presented analysis of existing mechanisms in three concepts like IDS, IPS and also IRS for IoT security as a second line defence mechanism. Also presented IDS with IPS and also

IRS which is used for classifying their deployment, data pre-processing methods, evaluation metrics, attacks, and datasets. Different IoT security issues and solutions are reviewed and gaps are identified that Machine Learning can address security services in IoT network [4]. Hence ML can be used for attack detection and Mitigation in IoT network.

In [5], the author presented identification of attacks on network. Also how to identify anomalies and defend attacks is presented. Utilization of DDoS attack and different approaches were used to defend attack.

In [6], author proposed a technique for IoT sensor data transmission in secure manner and efficient way. Three phases are proposed for providing security at the time of data transmission i) registration ii) authentication and iii) data transfer phase. Information obtained at the receiver using Euclidean parameter which is shared by IoT sensor. This technique will definitely improve the data transmission security in IoT network.

In [7], author analyzed different techniques of Lightweight cryptographic algorithms for IoT network secure communication. Also analyzed different threats at different layers of IoT architecture. Merits and demerits of this algorithms in terms of ensuring security. As attack patterns on IoT are growing day by day, it demands improvement in Lightweight Cipher.

Table 1: ML and DL Techniques used for Detection of different Attacks

References	Machine Learning Techiniques	Target Attack	Performance
Ref.8	Q-Learning	Denial of Service	Solved the associated optimality equations
Ref.9	Support Vector Machine and Naïve Bayes	Intrusion Detection	Detect Wireless Sensor Network attack successfully
Ref.10	ML approach	Detection of Cyber attacks	Survey of ML techniques for detection of cyber attacks
Ref.11	Q-Learning	Detection of Malware	Accuracy in Detection is improved
Ref.12	RF, K-Nearest Neighbors	Detection of Malware	Improved TP rate
Ref.13	Deep Transfer Learning (DTL)	Cyber attack	Accuracy is improved for detecting IoT Cyber attack

In this related work, literature is studied regarding IoT network security issues. Depending on that some issues are identified as shown in Table 1, that IoT network can prone to different types of attacks and ML techniques can be a solution for various types of attacks detection on IoT network. End to End communication of IoT devices is insecure in IoT network. All these issues required a robust solution to improve the performance.

3. PROPOSED METHODOLOGY

After doing this literature survey it is found that different security issues are exits in Cloud based IoT architecture which requires secure framework consists of attack detection and mitigation techniques as well as end to end secure cloud communication. Hence we are proposing robust solution for securing cloud based IoT network.

3.1 IoT architecture

IoT Architecture system consist of following layers. Figure.1 shows IoT architecture.

Perception Layer**:** It consist of physical object that can sense environment and able to collect information from outside world. This layer consists of devices which are nothing but things to collect data from the outside world. After that this data can be transmitted to network layer.

Network Layer: It is responsible for communication of objects with network devices, communicating and processing of sensor data can be possible with this. The IoT gateway is between devices and the cloud for communication purpose.

Application Layer: This layer is for development and application of IoT.This layer classifies different services to a user. At this layer the services for users, such as the smart homes applications, health care applications, etc which make user life easy are available. At this layer, security services like authentication integrity and confidentiality is maintained.

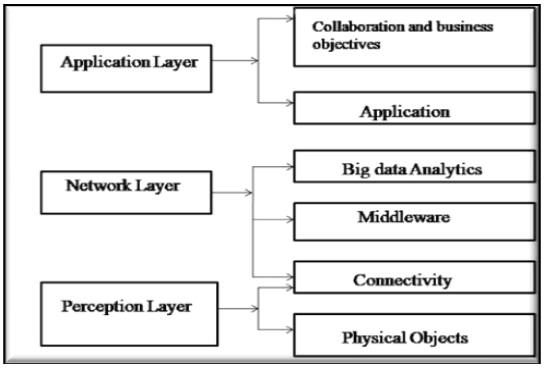

Figure. 1Three Layered Architecture of IoT

Due to this layered architecture of IoT network, it requires coordination of diverse technologies, distributed communication technologies and also

heterogeneous nature of devices prone it to different types of cyber-attacks. Hence for end to end security of IoT network requires robust solution. In IoT networks, devices involved are constrained in resources, this is the basic reason they are vulnerable and prone to attacks. Hence security is the issue in design and deployment of IoT network. So for securing a vulnerable IoT network, deployment of Attack Detection and Mitigation model can be used to defend against attacks. For this ML based defending model structure is to improve the consistency efficiency of identification and mitigation of attacks on IoT network. Big data generated by IoT devices requires Cloud for storage purpose. Again secure storage of sensors data on cloud is a big challenge. Authentication of users and data integrity must be maintained at the time of Cloud data storage. Hence to avoid misuse of data Cryptography is a solution. But in IoT network devices are resource constrained so cryptography is not suitable. Instead Lightweight cryptography can be used for resource constrained device secure communication. With the help of Lightweight Cryptography secure transmission of sensors data from IoT network to cloud can be possible.

3.2 ML for Attack Detection and Mitigation

ML is for detecting and mitigating security threats in IoT networks. The dynamic and complex nature of IoT ecosystems along with the sheer volume of data generated by connected devices makes traditional rule base approaches less effective. ML algorithms on the other hand can analyze large data sets identify patterns and adapt to evolving threats. Here are ways in which machine learning can be useful for attack detection in IoT networks. Implementing machine learning for attack detection in IoT network requires careful consideration of data privacy, model interpretability and the unique challenges pose by the IoT environment. Additionally ongoing monitoring and update to the machine learning model are essential to ensure their effectiveness against new and evolving threats. Machine learning techniques are increasingly being employed for attack detection in IoT networks due to their ability to analyze large data sets, identify patterns and adapt to evolving threats. ML models can learn the normal behavior of IoT devices and network traffic. Any deviation from the learned patterns can be flag as anomalous potentially indicating a security threat.

3.3 Proposed Design of Attack Detection and Mitigation for Securing Cloud based IoT network

Malicious activity or intrusion can be monitor identified and mitigated with the help of attack detection and mitigation module. When sensor data is transferred from IoT devices it will pass from this path to reach to cloud storage. This path is vulnerable. Different malicious activities can be happened in the communication path. Hence to avoid this attack of IoT network it must have one attack detection and mitigation module.

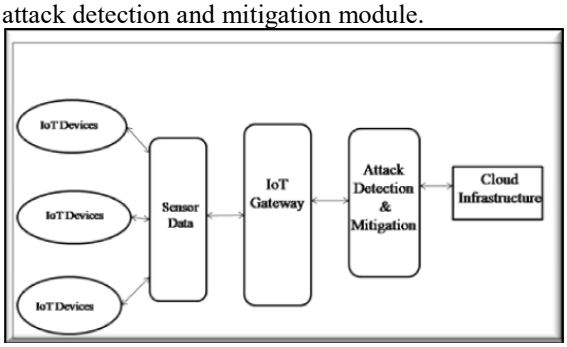

Figure.2 Design of Attack Detection & Mitigation for Cloud based IoT Network

This Secure Cloud based IoT architecture consists of **IoT Devices:**IoT devices can sense data, communicate data and also process data with the help of sensors. Also it generates big data and transfer this data to gateway.

Gateway: Gateway devices is between IoT devices and cloud server. It is worked as relay node. It receives IoT data from sensor devices and this sensor data forwarded to cloud.

Attack Detection and Mitigation: In Figur.2 attack on IoT network can be defended using Attack Detection and Mitigation is demonstrated. This module is placed in between IoT network and Cloud infrastructure. Packet Capturing of IoT devices data is done and this captured data which is live sensor data then transferred through IoT Gateway to Attack Detection and Mitigation Module. This module will predict normal and abnormal network traffic using ML approach. Normal and Abnormal Traffic can be identified using trained Machine Learning model. Finally normal traffic sensors data is stored on Cloud infrastructure.

Cloud Server: This data is transmitted from gateway it will be received on cloud for storage purpose. IoT devices huge amount of data requires cloud to storage it. It may be public or private cloud.We have used License software NetSim

Journal of Theoretical and Applied Information Technology
15th May 2024. Vol.102. No 9
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Standard v13.3 for this proposed architecture. Proposed design consists of following components.

Table 2: Components involved in Designing Cloud based IoT network

Sr.No	Device	Count
1.	IoT Sensor	16
2.	6LoWPAN Gateway	1
3.	Routers	2
4.	Cloud Server	1

Design of Cloud based IoT Network Scenario using license software NetSim Standard v13.3

Step 1. Creating a Cloud based IoT Network Scenario using sensor nodes, 6LoWPAN gateway, routers and Cloud Server as shown in Figure.3. Configuring Devices and Links can be possible by setting properties to devices as well as links. Modeling Application Traffic is done by establishing application between Sensor node 1 and Cloud Server.

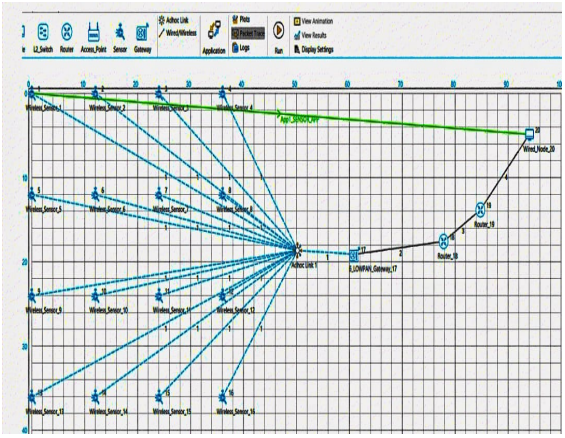

Figure.3 Design of Cloud Based IoT network

Step2. Run Simulation for capturing live traffic between sensor nodes like Wireless _Sensor_1 upto Wireless_Sensor_16 of Cloud based IoT network and also between Application_1 which is for capturing live traffic from Wireless_Sensor_1 to Wired_Node_20 is shown in Figure.4.

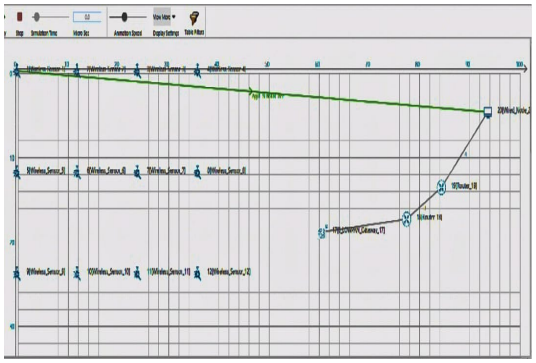

Figure.4 NetSim Packet Animation

Step 3. Enabling Plots and Traces can be made enabled for generating it after completion of simulation. Following metrics are generated after simulation is completed which consists of Application_Matrics_Table, TCP_Metrics_Table, Link_Metrics_Table, Queue_Mterics_Table as shown in Figure.5.

Figure.5 NetSim Simulation Results

Step 4. Packet Trace option is available for generating log of Sensor data.Captured Live Sensor data is now can be analysed for attack detection and mitigation as shown in Figure.6.

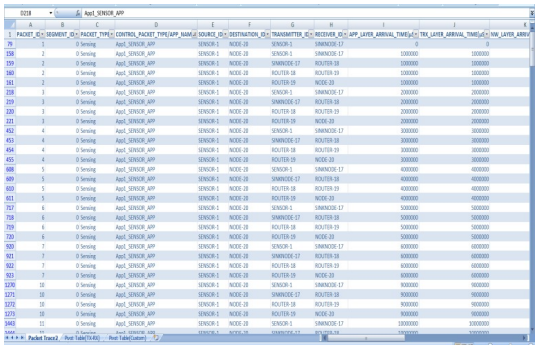

Figure 6:NetSim Packet Trace Window

We have created this Cloud based IoT network in which Sinkhole attack detection can be possible. It will identify malicious node and stop receiving and transmitting data through this malicious node. When we run the simulation broadcasting of message is done and all sensors starts transmitting packets. After malicious activity identified by some node, attack is identified and malicious nodes are declared. Immediately transmission and receiving of packet are stopped from this node. This can be

identified in Packet Trace File after completing this simulation. Packet Trace file consists of Transmitter ID and Receiver ID column in which this malicious node not found. It means packet transmission is stopped from this malicious nodes. In this architecture Sensor Node 6 and Sensor Node 8 is found to be malicious. In this malicious node advertise a fake rank.This will form fake routes. After receiving message packet, it drops the packet information. This attack affects the performance of IoT network protocol such as RPL.

3.4 Proposed End to End Secure Cloud IoT Communication

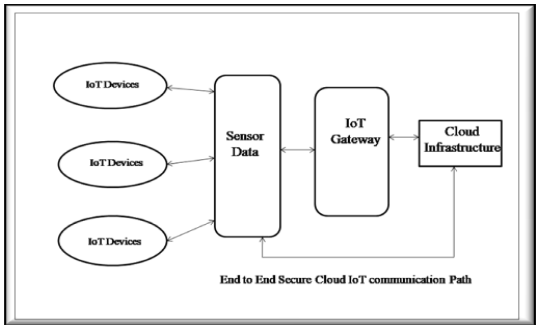

Figure.7 End to End secure Cloud IoT communication

In Figure. 7 end to end secure Cloud IoT communication path is shown. When sensor data from this devices is transmitted to IoT gateway it is encrypted and encrypted sensor data is generated with the help of Lightweight cryptography. This encrypted sensor data then can be transmitted though gateway for storage purpose on cloud. So end to end communication between this devices and cloud is secured as data is transmitted through wireless channel but it is in encrypted format. So no one is able to hack this information and communication path becomes secure.

4. RESULTS AND DISCUSSION

Implementation of Attack Detection and Mitigation is successfully done. Also using three types of ML techniques, performance analysis can be done. Here Machines learning approaches are used to detect "Normal" and "Anomaly" in IoT network traffic. Based on Train and Test Scores, best suited algorithm is found.

4.1 Logistic Regression

Logistic regression is used for predicting of Instance belonging to the class. The input to this is a output taken from linear regression. For the purpose of estimating probability for the class sigmoid function is used. After training a Machine Learning model using Logistic Regression Algorithm, Train Score is found 92.87% and Test Score is found 92.31% as shown in Figure 8.

```
In [30]: lg_model = LogisticRegression(random_state = 42)
         lg_model.fit(x_train, y_train)
Out[30]: LogisticRegression(random_state=42)

In [31]: lg_train, lg_test = lg_model.score(x_train , y_train), lg_model.score(x_test , y_test)

         print(f"Training Score: {lg_train}")
         print(f"Test Score: {lg_test}")

         Training Score: 0.9287739593966202
         Test Score: 0.9231278115903678
```

Figure.8 Logistic Regression

4.2 K NearestNeighbors (KNN)

In KNN non-parametric approach used for classification of data samples. Sample of unknown class are decided according to the majority number I its nearest neighbor. KNN is also used for intrusion and anomaly detection. It can be used for classifying both normal and abnormal system behavior. After training a Machine Learning model using K Nearest Neighbors Algorithm, Train Score is found 98.52% and Test Score is found 98.24% as shown in Figure 9.

```
In [36]: KNN_model = KNeighborsClassifier(n_neighbors=study_KNN.best_trial.params['KNN_n_neighbors'])
         KNN_model.fit(x_train, y_train)

         KNN_train, KNN_test = KNN_model.score(x_train, y_train), KNN_model.score(x_test, y_test)

         print(f"Train Score: {KNN_train}")
         print(f"Test Score: {KNN_test}")

         Train Score: 0.985255755926052
         Test Score: 0.9824027520508071
```

Figure.9 K Nearest Neighbors (KNN)

4.3 Decision Tree

Decision Tree is used for classification by sorting feature values. Decision Tree has two main approaches i) Building ii) Classification. Decision Tree is constructed in building phase. Classification is for constructing tree. Decision Tree is a approach to ensure security to detect malicious traffic sources in a network. After training a Machine Learning model using Decision Tree Algorithm, Train Score is found 100% and Test Score is found 99.39% as shown in Figure 10.

Journal of Theoretical and Applied Information Technology
15th May 2024. Vol.102. No 9
© Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

```
In [41]: dt = DecisionTreeClassifier(max_features = study_dt.best_trial.params['dt_max_features'], max_depth = study_dt.best_trial.params
         dt.fit(x_train, y_train)

         dt_train, dt_test = dt.score(x_train, y_train), dt.score(x_test, y_test)

         print(f"Train Score: {dt_train}")
         print(f"Test Score: {dt_test}")

Train Score: 1.0
Test Score: 0.9939137337920884
```

Figure. 10 Decision Tree

4.4 Comparison of Train and Test Scores of Machine Learning Models

Machine Learning models are trained using KNN, Logistic Regression and Decision Tree algorithms also Train and Test Scores are calculated are as shown below Table. 1. Amongst all three Machine Learning Algorithms Decision Tree has highest Train Score and Test Score found hence performance of Decision tree is best comparing with other algorithms.

Table 3: Comparison of Train and Test Scores of Machine Learning Models

Model	Train Score	Test Score
KNN	0.985256	0.982403
Logistic Regression	0.928774	0.923128
Decision Tree	1	0.993914

4.5 Precision and Recall for Machine Learning Algorithms

Comparison of Precision and Recall for KNN, Logistic Regression and Decision Tree Classifier is found that is shown in below Figure. 11. Comparing with all algorithms Decision Tree is having best values found for Mean Precision and Mean Recall.

```
************** KNeighborsClassifier Model Validation **************
Mean precision:
 98.45 % +- 0.48

Mean recall:
 98.24 % +- 0.54

*************** LogisticRegression Model Validation ***************
Mean precision:
 91.35 % +- 0.57

Mean recall:
 95.72 % +- 0.67

************* DecisionTreeClassifier Model Validation *************
Mean precision:
 99.54 % +- 0.18

Mean recall:
 99.51 % +- 0.16
```

Figure.11 Comparison of Precision and Recall for Machine Learning Algorithms

4.6 Graph representing Precision and Recall for Machine Learning Algorithms

Following Figure.12 shows Graphical representation comparison of Precision and Recall for KNN, Logistic Regression and Decision Tree.

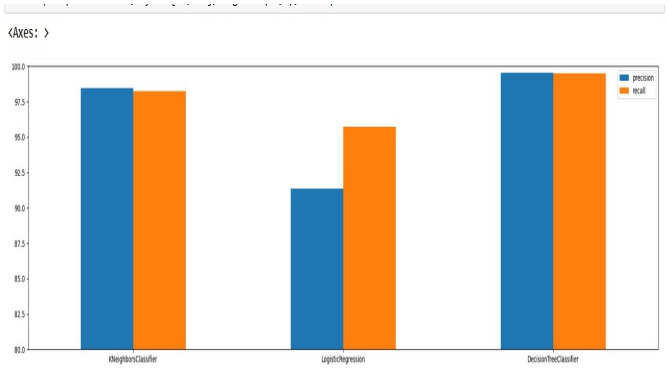

Fig.12 Graph representing Precision and Recall for Machine Learning Algorithms

In Figure.13 F1 Score for KNN,Logistic Regression and Decision Tree are represented. F1 Score is found to be highest for Decision Tree Classifier.

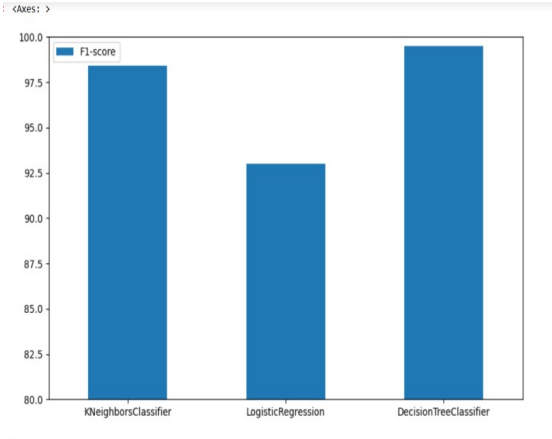

Figure.13 Graph representing F1 Score for Machine Learning Algorithms

In proposed Attack Detection and Mitigation module, output is a value "1" for "anomaly" or "0" for "normal" and value for prediction is correct or incorrect. So there are four relationships between prediction and labels are as shown in Table.2: True positive (TP), False positive (FP), True negative (TN) and False negative (FN).TP: network found anomaly and prediction is also anomaly .FP: network found normal but prediction is anomaly.
TN: network found normal and prediction is normal. FN: network found anomaly and prediction is normal. Following equations shows True positive rate, True Negative rate, Accuracy and precision of Machine Learning Model. True positive rate= True positive/ (True positive + False negative)
True Negative rate= True negative / (True negative + False positive) Accuracy= (True positive + True negative)/ (True positive + True negative + False positive + False negative)

Precision= True positive / (True positive + False positive)

Table 4: Relationships between labels and predictions

Results	Labels	Predictions
TP	Anomaly	Anomaly
FP	Normal	Anomaly
TN	Normal	Normal
FN	Anomaly	Normal

5. CONCLUSION AND FUTURE SCOPE

In this proposed research, Simulation design using licence software NetSim Standard v13.3, Machine Learning approach and Lightweight Cryptographic algorithm are used for implementation of secure Cloud based IoT network which will resolve the problem of IoT security to larger extent. This research paper demonstrated that for the purpose of design of Cloud based IoT network simulation is used which can identify Malicious Node in network, Machine Learning approach can be used for IoT network Attack Detection and Mitigation and Lightweight Cryptography is used for End to End secure communication. The performance analysis of this model can be identified by calculating Train Score and Test Score for different Machine Learning models based on true positive rate, true negative rate, accuracy and precision. In this research work comparison of performance of Logistic Regression, KNN, and Decision Tree algorithms is done for Attack Detection and Mitigation of cloud based IoT network. It is found that Performance of proposed model is improved using Decision Tree(Train Score 100%,Test Score 99.39%) as compare to K Nearest Neighbors (Train Score 98.52% and Test Score 98.24%) and Logistic Regression algorithms(Train Score 92.87% and Test Score 92.31%). In the future, Deep Learning algorithms can be applied to improvised Attack Detection and Mitigation for getting better accuracy in prediction of type of attacks on IoT networks.

REFERENCES:

[1] Abbas, Ghulam, AmjadMehmood, Maple Carsten, Gregory Epiphaniou, and Jaime Lloret. "Safety, Security and Privacy in Machine Learning Based Internet of Things" *Journal of Sensor and Actuator Networks* 11, no. 3: 38, 2022,doi.org/10.3390/jsan11030038.

[2] V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," in IEEE Access, vol. 9, pp. 28177-28193, 2021, doi: 10.1109/ACCESS.2021.3052867.

[3] Kamaldeep, M. Dutta and J. Granjal, "Towards a Secure Internet of Things: A Comprehensive Study of Second Line Defense Mechanisms," in IEEE Access, vol. 8, pp. 127272-127312, 2020, doi: 10.1109/ACCESS.2020.3005643.

[4] F. Hussain, R. Hussain, S. A. Hassan and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686-1721, thirdquarter 2020, doi: 10.1109/COMST.2020.2986444.

[5] Mishra, S.; Albarakati, A.; Sharma, S.K.," Cyber Threat Intelligence for IoT Using Machine Learning", Journal Processes, Vol.10, pp.2673doi. 10.3390/pr10122673.

[6] Sharma, R., Arya, R. Secure transmission technique for data in IoT edge computing infrastructure. Complex Intell. Syst. **8**, 3817–3832 (2022). https://doi.org/10.1007/s40747-021-00576-7

[7] Muhammad Rana,QuaziMamun,RafiqulIslam"Lightweight cryptography in IoT networks: A survey", Journal Future Generation Computer Systems,Vol.129,pp.77-89,2022,doi.org/10.1016/j.future.2021.11.011

[8] Y.Li,D.E.Quevedo, S. Dey, andL. Shi, "SINR-based dos attack on remotestate estimation: A game-theoretic approach," *IEEE Trans. Control Netw.Syst.*, vol. 4, no. 3, pp. 632–642, Sep. 2016.

[9] M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learningin wireless sensor networks: Algorithms, strategies, and applications,"*IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1996–2018,Oct.–Dec. 2014.

[10] A.L.BuczakandE.Guven, "Asurvey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Commun. SurveysTuts.*, vol. 18, no. 2, pp. 1153–1176, Apr.–Jun. 2015.

[11] L. Xiao, Y. Li, X. Huang, and X. Du, "Cloud-based malware detection game for mobile devices with offloading," *IEEE Trans. Mobile Comput.*, vol. 16, no. 10, pp. 2742–2750, Oct. 2017

[12] F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," *Soft Comput.*,vol. 20, no. 1, pp. 343–357, 2016.

[13] Ly Vu,QuangUy Nguyen,Diep Nguyen,Dinh Thai Hoang,ErykDutkiwicz,"DeepTransferLearning forIoTAttackDetection",IEEEAccess, Vol.8,June 18,2020.

[14] Hsing-Chung Chen and Ilsun You and Chien-ErhWeng and Chia-Hsin Cheng and Yung-Fa Huang,"A security gateway application for End-to-End M2M communications", Computer Standards & Interfaces,Vol.44,pp.8593,2016,doi.org/10.1016/j.csi.2015.09.001.

[15] Xuezhi Zeng and Saurabh Kumar Garg and Peter Strazdins and Prem Prakash Jayaraman and DimitriosGeorgakopoulos and Rajiv Ranjan,"IOTSim: A simulator for analysing IoT applications", Journal of Systems Architecture,Vol.72,pp.93-107,2017,doi.org/10.1016/j.sysarc.2016.06.008

[16] M. S. A. Muthanna, R. Alkanhel, A. Muthanna, A. Rafiq and W. A. M. Abdullah, "Towards SDN-Enabled, Intelligent Intrusion Detection System for Internet of Things (IoT)," in IEEE Access, vol. 10, pp. 22756-22768, 2022, doi: 10.1109/ACCESS.2022.3153716.

[17] M. Chernyshev, Z. Baig, O. Bello and S. Zeadally, "Internet of Things (IoT): Research, Simulators, and Testbeds," in IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1637-1647, June 2018, doi: 10.1109/JIOT.2017.2786639.

[18] M. Khoda, T. Imam, J. Kamruzzaman, I. Gondal and A. Rahman, "Robust Malware Defense in Industrial IoT Applications Using Machine Learning With Selective Adversarial Samples," in IEEE Transactions on Industry Applications, vol. 56, no. 4, pp. 4415-4424, July-Aug. 2020, doi: 10.1109/TIA.2019.2958530.

[19] A. Makkar, S. Garg, N. Kumar, M. S. Hossain, A. Ghoneim and M. Alrashoud, "An Efficient Spam Detection Technique for IoT Devices Using Machine Learning," in IEEE Transactions on Industrial Informatics, vol. 17, no. 2, pp. 903-912, Feb. 2021, doi: 10.1109/TII.2020.2968927.

[20] N. Ravi and S. M. Shalinie, "Semisupervised-Learning-Based Security to Detect and Mitigate Intrusions in IoT Network," in IEEE Internet of Things Journal, vol. 7, no. 11, pp. 11041-11052, Nov. 2020, doi: 10.1109/JIOT.2020.2993410.

[21] M. Shafiq, Z. Tian, A. K. Bashir, X. Du and M. Guizani, "CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques," in IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3242-3254, 1 March1, 2021, doi: 10.1109/JIOT.2020.3002255.

[22] C. Liu, Y. Zhang, J. Xu, J. Zhao and S. Xiang, "Ensuring the Security and Performance of IoT Communication by Improving Encryption and Decryption With the Lightweight Cipher uBlock," in IEEE Systems Journal, vol. 16, no. 4, pp. 5489-5500, Dec. 2022, doi: 10.1109/JSYST.2022.3140850.

[23] K. -Y. Lam, S. Mitra, F. Gondesen and X. Yi, "ANT-Centric IoT Security Reference Architecture—Security-by-Design for Satellite-Enabled Smart Cities," in IEEE Internet of Things Journal, vol. 9, no. 8, pp. 5895-5908, 15 April15, 2022, doi: 10.1109/JIOT.2021.3073734.

[24] A. Jamalipour and S. Murali, "A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9444-9466, 15 June15, 2022, doi: 10.1109/JIOT.2021.3126811.

[25] A. K. Pathak, S. Saguna, K. Mitra and C. Åhlund, "Anomaly Detection using Machine Learning to Discover Sensor Tampering in IoT Systems," ICC 2021 - IEEE International Conference on Communications, Montreal, QC, Canada, 2021, pp. 1-6, doi: 10.1109/ICC42927.2021.9500825.