Attack and Anomaly Detection in IoT Sensors

Madhur Tatiya - 191IT227
Dept. of Information Technology
NITK Surathkal
Mangaluru, India
mowgli.191it227@nitk.edu.in

Kiran Kumar J M - 191IT126
Dept. of Information Technology
NITK Surathkal
Mangaluru, India
kirankumarjm.191it126@nitk.edu.in

Sparsh Agarwal - 191IT150
Dept. of Information Technology
NITK Surathkal
Mangaluru, India
ishu.191it150@nitk.edu.in

***Abstract*—Smart devices and sensors are getting increasingly common, promising to form life simpler for his or her owners. If the web of Things (IoT) grows in popularity, so does the amount of malicious attacks that cause a serious hazard to exposed IoT applications. the speed of success in infecting IoT devices is dependent on the devices' exposure to the web . A high infection rate is observed in networks where users are regularly allocated public-facing internet IP addresses. an increase in disturbances within the IoT environment can cause system sensor faults or unintended disturbances, also as provide opportunities for criminals to realize access. due to the features of the underlying hardware, vulnerabilities to IoT systems and applications translate to higher privacy issues. These features make IoT environments practical and effective, however malicious hackers are likely to require advantage of them.As a consequence, unexpected sensor signal accidents must be investigated. Implementation of varied machine learning and neural network models and performance evaluation using different metrics on the DS2oS traffic traces dataset for attack and anomaly detection in IoT devices is that the context of this paper. We also compare the results with the bottom paper. The novelty is to implement some new models which aren't implemented in base paper and determine the foremost optimal solution for this problem.**

***Index Terms*—IoT, Machine Learning, DoS, Cybersecurity , Anomaly detection**

I. Introduction

IoT encompasses a good range of domains and markets. Over the previous couple of years, there has been a big increase within the production and application of IoT products. because of advancements in IoT technology, tens of thousands of latest jobs are developed.The main reason behind it's development of the new and advanced IoT hardware features, which permit applications across multiple domains and industries. The health sector uses IoT to trace and regulate human activities; industry uses IoT to power lighting, smart homes use IoT to deal with incoming threats; and transportation uses smart lightning devices to analyse temperature, global climate change , and hazard prediction. Similarly there are more uses of Iot devices in various fields. Any of the sensors mentioned in each of the examples above sends signal data periodically to relay the present state of the environment. Different attacks and threats on particular IoT devices or a set of IoT devices in sensor networks are the origins of imbalanced data. The sources of attacks are often Intrusion detection, Fraud detection, Data Leakage etc. When the amount of smart devices on the market grows, so does the likelihood of security breaches. When a source of anomaly joins the environment, it triggers widespread data disruption before time mitigating actions are implemented. Unavoidable tracking and anomaly identification are a number of the key goals of IoT technology. Therefore, Anomaly identification in IoT systems may be a comparatively recent topic of research that's getting popular and in demand nowadays. It also can be wont to detect data entry errors, which may then be resolved instantly. There are many sorts of anomalies in IoT systems which permit an attacker to compromise the user's security and privacy during a smart home. Among those, we glance at seven differing types of anomalies during a smart home system, including scanning, distributed denial of service, data probing,spying, wrong setup, malicious control and malicious operations during this paper. The solution we evaluated for this problem uses both ML fundamentals and innovative deep learning (DL) approaches for this multi-class classification problem. we've used the DS2oS traffic dataset for this project. This contains the The traces reported within the IoT environment DS2OS. These are collected using different simulated IoT locations that provide a spread of facilities. The dataset contains 8 classes out of which seven are anomalous attacks and one is normal class. To classify activities and discern between predicted and abnormal activity, our proposal employs a spread of ML and deep learning principles. The approaches we use include Support Vector Machines, k-Nearest Neighbors, Naive Bayes, Decision Tree, Random Forest, Logistic Regression, Multi-Layer Perceptron - Artificial Neural Network, and Convolutional Neural Network. We compare the results of of these approaches using different measures of evaluation to urge the precise idea how accurately the classification is completed by these models. After analysis of results we discover the optimal solution for this multi-class classification problem. The remainder of this paper is split into the various sections which debate the study of comparable works on anomaly detection techniques, the project's goals and priorities, the outline of various assessment models utilized in our frame-add depth and therefore the recommended solution.

II. Literature Survey

Here, we briefly introduce previous work on Anomaly detection and classification in IoT Sensors. Several works have been done in the field of IoT. Still, researchers are working in this area.

Mahmudul et al. [1] analysed several machine learning models to classify and predict the attacks based on IoT sensors. The different methods used in this paper include SVM, Decision Tree, Random Forest and Logistic Regression. The models are tested on different evaluation metrics and Random Forest Model performs the best out of all with around 99.4% accuracy. Pahl et al.

[2] described an experimental setup and development of a firewall and its detector at various IoT sites. The methods which are used in this paper include KMeans Clustering and BIRCH. The Clustering based algorithm performs well with around 96% accuracy.

Lingjuan et al. [3] proposed a method of using hyper ellipsoidal clustering algorithm which works on Fog computing platform. Their approach is tested on fog-to-things computing. Fog architecture was preferred because it reduces the latency and energy in recognizing anomalies and the entire process is tested on the fog-to-things computing.

To cater to the issue of safety and preservation of data being transferred between the Logical, Physical and Virtual components, Usmonov et al. [4] developed an embedded system for IoT.

A research in the field of Healthcare analytics was carried out by Ukil et al. [5] which discussed the role of IoT sensors for the detection of anomalies in the cardio-vascular system.

Anthi et al. [6] in his novel research, developed an intrusion detection system for the IoT. Data was gathered from Wireshark by generating the network traces for four days. Various Machine Learning classifiers were used to scan the traces and detect the different forms of Denial of Service attacks.

X.Liu. et al. [7] proposed an automated system for detecting On and Off attacks in an Industrial IoT site due to malicious and corrupted network nodes.The hypothesis was reached because the IoT network is vulnerable to attack when the infected node is turned on, but not when it is turned off or inactive.

In the above mentioned analysis of various papers and studies we inferred that Anomalies were mostly characterized by the minority samples in the pool of majority even data. However in case of IoT data, using a supervised learning approach, we must study continuous categorical datasets of IoT traffic traces in a smart home simulation with several forms of attacks and anomalies.

III. Methodology

A. *Obtaining the Data*

The challenge is solved using an open-source dataset of traffic traces during a virtual IoT environment. the info we used was generated by practically replicating the IoT environment. This was accomplished with the assistance of the Distributed Smart Space Orchestration System (DS2OS).

The dataset contains 357,952 samples and 13 features. The features along with their types are mentioned as follows: 1) Source ID: Nominal
2) Source Address: Nominal
3) Source Type: Nominal
4) Source Location Nominal
5) Destination Service Address: Nominal
6) Destination Service Type: Nominal
7) Destination Location: Nominal
8) Accessed Node Address: Nominal
9) Accessed Node Type: Nominal
10) Operation: Nominal
11) Value: Continuous
12) Timestamp: Discrete
13) Normality: Nominal

The dataset contains 347,935 Normal data and 10,017 anomalous data and eight classes which were classified.Among the mentioned features "Accessed Node Type" contains 148 missing values and the feature "Value" contains 2050 missing data. The class label is Normality and the data is divided into 8 different classes according to Normality:
1) Denial of Service (Dos): The attacker sends a large number of obscure packets flooding the target and rendering its services unavailable to other services.
2) Data Type Probing (D.P): A different datatype other than the intended data type is written by the malicious node.
3) Malicious Control (M.C): The attacker can gain a valid session key and capture network traffic.
4) Malicious Operation (M.O): Affects the original operation negatively by distraction from original task using decoy activity.
5) Scan(SC): Corruption of data in the process of scanning it from hardware.
6) Spying (SP): Attacker gains knowledge of the vulnerabilities in a system and uses it to manipulate the whole system.
7) Wrong Setup (W.S): the data is corrupted because of the wrong system setup.
8) Normal(NL): non anomalous data without any disruption.

B. *Pre-Processing the Data*

We evaluate the subsequent statistics on the amount of instances of every Class within the data after processing the info and extracting the essential information from it. The

TABLE I
Number of instances of each Class

Attacks Type/Class Label	Number of Instances
Dos	57800
Data type Probing	342
Malicious Control	889
Malicious Operation	805
Scan	1547
Spying	532
Wrong Setup	122
Normal	347935

timestamp column has been eliminated because it's a coffee association with the dataset's variable normalcy.

While processing the info we observed that the dataset contains 148 tuples of knowledge during which the worth within the column "Accessed Node Type" isn't variety or NaN. this might cause a problem within the further processing as our Machine Learning Pipeline only considers the Numerical Inputs.We have replaced the 'NaN' values within the "Accessed Node Type" with 'Malicious', to avoid loss of valuable data. Similarly, we will also find some non continuous unexpected data within the "Value" column. These unexpected values were converted to real values that might help the classifiers to possess better accuracy. just in case of "Value" feature, unexpected observations "True", "Twenty", "False" and "none" are replaced by values "1.0", "20.0", "0.0" and "0.0", respectively.

Another crucial task was converting the nominal categorical data into vectors. There are some ways to rework Categorical data into vectors. Among them one hot encoding and label encoding are hottest . One hot encoding can increase total count of features within the dataset by a big amount, resulting in dataset with tons of dimensions. Hence we've used label encoding technique to avoid increasing the dimension of the dataset. Besides, label encoding is simpler to suit within the machine learning model and also takes lesser time interval than one hot encoded features.

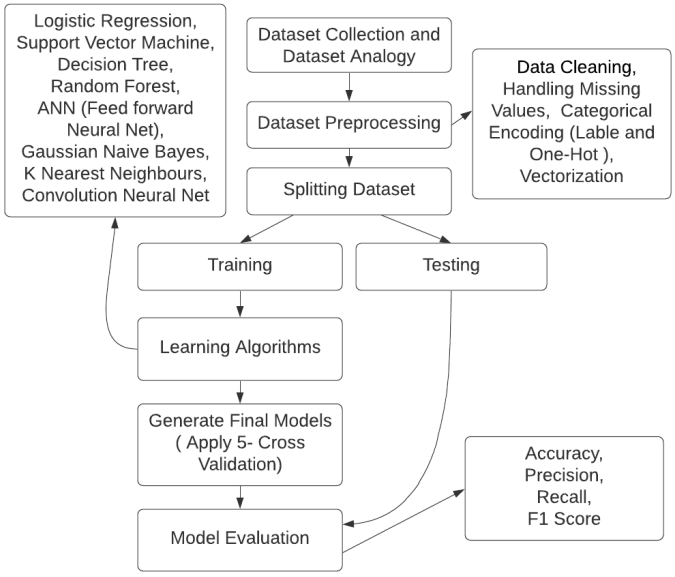


Fig. 1. Overview of Methodology

C. *Applying the Algorithms*

*1) **Logistic Regression(LR)**:* Logistic Regression (LR) may be a supervised model which is employed to map a given set of observations to a discrete set of classes.In this problem we've used the concept of multi-class Logistic Regression which classifies our tuples into the various classes supported the Normality of IoT Operation.

*2) **Support Vector Machine(SVM)**:* SVM - Support Vector Machine is additionally a supervised model like Logistic regression. And is employed to interpret data for classification and therefore the analysis of outliers. within the case of non-linear data, support vector machines are often one among the foremost effective models. Weight vector theta are often computed using the subsequent equation given input X, class or label C, and LaGrange multipliers alpha:

$$\Theta = \sum_{i=1}^{m} \alpha_i c_i x_i$$

Fig. 2. Weight Vector equation

The Support Vector Machine's aim is to find the best solution to the following equation:

$$\text{Maximize}_{\alpha_i} \sum_{i=1}^{m} \alpha_i - \sum_{i=1}^{m} \sum_{j=1}^{m} \alpha_i \alpha_j c_i c_j < x_i x_j >$$

Fig. 3. Support vector machine equation

Here,vector ¡ x i , x j ¿ can be achieved using kernels like polynomial kernel, Radial Basis Function kernel and Sigmoid Kernel.

*3) **Decision Trees(DT)**:* a choice Tree starts with one node then it branches into possible outcomes. These outcomes further branch off into other nodes which successively further cause more nodes and instances. With x features, I(data), the amount of samples within the parent node Pn, the amount of samples within the left child LCn, and therefore the number of samples within the right child RCn;Information Gain are often maximized as:

$$\text{Information Gain}(P_d, x) = I(P_d) - \frac{LC_n}{P_n} I(LC_d) - \frac{RC_n}{P_n} I(RC_d)$$

Fig. 4. Information Gain in Decision Tree

Gini Index IG, Entropy IH and Classification Error IE can be used to calculate I(data) as:

$$I_H(n) = -\sum_{i=1}^{c} p(c|n) log_2 p(c|n)$$

$$I_G(n) = 1 - \sum_{i=1}^{c} p(c|n)^2$$

$$I_E(n) = 1 - max\{p(c|n)\}$$

Fig. 5. Impurity Measure in Decision Tree

*4) **Random Forest(RF)**:* Multiple decision trees are used together to make a forest of trees.The speed of random forest is basically fast thereby making it an optimal choice in classification problems. because the random forest is formed by ensembling many decision trees together, the ultimate predictions are given by averaging the predictions of all the constituent decision trees. due to this the info is correctly covered and an honest predictive score is obtained as accuracy.

*5) **Artificial Neural Network(ANN)**:* Artificial Neural Network (ANN) may be a deep learning method which trains the model supported data . the amount of parameters in ANN is extremely large as compared to other classification methods. thanks to this ANN takes an extended time in training. Also because the complexity and size increases, the time to backpropagate error and fine tuning the parameters becomes larger.

*6) **Naive Bayes Classifier**:* The supervised machine learning algorithm Naive Bayes is predicated on Bayes' theorem of probability. The algorithm assumes that each one the input variables are independent of every other hence it's called "Naive". After the consideration of independence, the bayes' theorem is applied on the dataset. the ultimate predictive score is given as probability of what proportion a tuple is associated to a given class label.

*7) **K-Nearest Neighbour Classifier**:* K-nearest neighbours or KNN for brief , may be a specialised sort of supervised ML algorithm. it's used for both regression and classification problems. KNN works by assigning the new datum on the idea of how closely it matches the info points within the training set. It doesn't have any distinct training phase, rather it uses the entire data for training while classifying and not assuming anything about the underlying data.

*8) **Convolutional Neural Network (CNN)**:* The convolutional neural network, (CNN) may be a sort of neural network model specially designed for working with two-dimensional image data. It also can be applied on one dimensional and three dimensional data. because the name suggests, convolution operation is central to the present model. Convolution is multiplication is performed between an array of input file and a two- dimensional array of weights, called a filter or a kernel. The filter is systematically applied to the input file which is captured by the feature map.

IV. Results and Analysis

We applied various machine learning and deep learning techniques and performed Five-fold cross-validation in each of those techniques. It are often deduced from Tables II and III that RF and ANN have had better results than all other models. performed best and have produced 99.40% accuracy. within the case of coaching , DT gave approximately similar results thereto of RF and ANN. For the primary two folds, DT outperformed other approaches, but within the last three folds of 5-fold cross validation, it had been like RF and ANN. In terms of precision, CNN and KNN had almost identical scores, with 99.34% and 99.37% accuracy, respectively. On the other hand, SVM, LR and Gaussian Naive Bayes performed weaker than other techniques. As we made several trial and error attempts, tuning the hyper parameters of the ANN model used in the base paper, we obtained little improvement. the amount of hidden layers within the base papers are 50. Upon several trials, we observed that upon increasing the hidden layers did not give any improvement. In fact, we got a touch improvement upon reducing the amount of hidden layers 35. A probable reason for this will be that if we add the hidden layers excessively, the model trains itself for more parameters than are required to repair the difficulty.

TABLE II
Evaluation Metrics for Training Data

	KNN	NB	LR	SVM	DT	RF	ANN (base paper)	CNN	ANN
Accuracy	0.9931	0.9872	0.9881	0.9828	0.9933	0.9942	0.9941	0.9934	0.9942
Precision	1.00	0.98	0.99	0.99	0.99	0.99	0.99	0.99	0.99
Recall	0.99	0.02	0.99	0.98	0.99	0.99	0.99	0.99	0.99
F1 Score	0.99	0.01	0.99	0.98	0.99	0.99	0.99	0.99	0.99

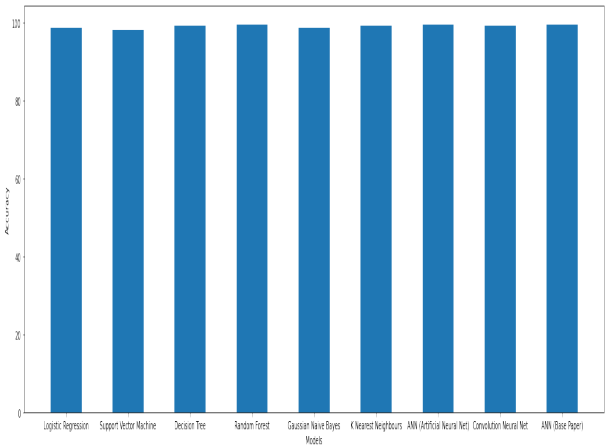
TABLE III
Evaluation Metrics for Testing Data

	KNN	NB	LR	SVM	DT	RF	ANN (base paper)	CNN	ANN
Accuracy	0.9931	0.9873	0.9881	0.9827	0.9931	0.9940	0.9940	0.9934	0.9940
Precision	1.00	0.98	0.99	0.99	0.99	0.99	0.99	0.99	0.99
Recall	0.99	0.02	0.99	0.98	0.99	0.99	0.99	0.99	0.99
F1 Score	0.99	0.01	0.99	0.98	0.99	0.99	0.99	0.99	0.99

The accuracies of all the implemented models as observed are mentioned in the Table IV below:

TABLE IV
Accuracy obtained from each of the models

Model Used	Accuracy Obtained
Logistic Regression	98.814%
Support Vector Machine	98.276%
Decision Tree	99.311%
Random Forest	99.409%
Gaussian Naive Bayes	98.737%
K Nearest Neighbours	99.378%
ANN (Artificial Neural Net)	99.409%
Convolution Neural Net	99.348%
ANN (Base Paper)	99.407%



V. Conclusions and Future Work

In this project we implemented the models from the bottom paper. We also experimented with new models like KNN, Naive Bayes, ANN and CNN .

If we glance from the purpose of view of Statistical Measures, all the models and techniques which we applied provided excellent results with a mean accuracy around 99% for every model. Among of these , we will conclude that RF and ANN are the foremost accurate and have rock bottom misclassification rate. Our System is fully automated and may be deployed to any IoT Networks or Enterprise Network where it can automatically detect the presence of any quite Malware or Anomalies without the utilization of any expensive hardware and may therefore save the network from threats.

As a part of future work, we decide to ensemble different models to unravel this problem and improve the results. We can also experiment with different IoT sensors and check out to urge real time data from them and thereby test and improve our work further.

Acknowledgments

We would like to thank Dr. Anand Kumar M, Dept. of Information Technology, NITK Surathkal who helped us shape the idea of our project.

References

[1] Mahmudul Hasan, Md. Milon Islam, Md Ishrak Islam Zarif, M.M.A. Hashem, Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches, in: Proceeding of the Internet of Things 7 Conference(2019)

[2] M.-O. Pahl, F.-X. Aubet, All eyes on you: distributed multi-dimensional IoT microservice anomalydetection, in: Proceedings of the 2018 Fourteenth International Conference on Network and Service Management (CNSM)(CNSM 2018), 2018. Rome, Italy

[3] Lingjuan Lyu, Jiong Jin, Sutharshan Rajasegarar, Xuanli He, n Marimuthu Palaniswami. Fog-empowered anomaly detection in Io-Tusing hyperellipsoidal clustering.IEEE Internet of Things Journal,4(5):1174–1184, oct 2017.

[4] B. Usmonov, O. Evsutin, A. Iskhakov, A. Shelupanov, A. Iskhakova, R. Meshcheryakov, The cybersecurity in development of IoT embedded technologies, in: Proceedings of the 2017 International Conference on Information Science and Communications Technologies (ICISCT), IEEE, 2017, pp. 1–4.

[5] A. Ukil, S. Bandyopadhyay, C. Puri, A. Pal, Iot healthcare analytics: The importance of anomaly detection, in: Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), IEEE, 2016, pp. 994–997.

[6] E. Anthi, L. Williams, P. Burnap, Pulse: an adaptive intrusion detection for the internet of things (2018).

[7] X. Liu, Y. Liu, A. Liu, L.T. Yang, Defending on–off attacks using light probing messages in smart sensors for industrial communication systems, IEEE Trans. Ind. Inf. 14 (9) (2018) 3801–3811.