MANTECH Publications

Journal of Internet of Things and Information Technology
Volume 4 Issue 3

AI and Machine Learning Based Network Anomaly Detections

M Naga Triveni[1], G Y Vybhavi[2], Eswar Poluri[3]

Assistant Professor[1, 2], Assistant Manager[3]

Dept. of Computer Science Engineering[1, 2], Dept. of Automation[3]

SMEC, Hyderabad[1], GCET, Hyderabad[2], LNT, Hyderabad[3]

Corresponding Authors' Email id: *3venipoluri@gmail.com[1], gy.vaibhavi@gmail.com[2], eswarpoluri@gmail.com[3]*

Abstract

It is possible that someday the Industrial Internet of Things will alter the planet. It is the amount of knowledge so far that lets the universe spin quicker. Detecting unexpected occurrences, adjustments or transitions in databases is one way to process data quickly and more effectively. Anomaly detection, a technique that focuses on Artificial Intelligence to recognise irregular behaviour inside the data collection pool, has since become one of the Industrial IoT's key goals. Anomaly detection relates to the discovery of objects or occurrences in a dataset that are normally undetectable by a human specialist that do not adhere to a predicted trend or to other items. Typically, those irregularities may be converted into concerns such as design flaws, mistakes, or theft. We recommend a two-phase model in this paper to identify and categorise irregularities. First, out of eleven widely used algorithms tested for the same data collection, we chose Random Forest based on the maximum accuracy-score. The RF is used to identify irregularities and create a "attack-or-not" additional function. We supplied the Neural Network with the "attack-or- not" data function to distinguish attack types, which will help to handle each form accordingly.

Keywords: *Machine Learning, Neural Network, Cyber Security, Network Anomaly Detection and UNSW-NB15*

INTRODUCTION

In order to get the full image of their business, modern corporations recognise the value of interconnected activities. In addition, they need to respond swiftly to fast-moving data shifts, especially in the event of cyber security threats. Detection of abnormalities may be a key to overcoming certain intrusions, since disturbances of regular behaviour signify the existence of expected or unintentionally triggered threats, errors, flaws, and so on while detecting anomalies.

Unfortunately, there is no reliable way to manually manage and interpret continuously increasing datasets. They require a modern constructive approach to recognising anomalous behaviour with the complex structures having multiple components in continuous motion where the "natural" behaviour is continuously redefined. Statistical Process Control, or SPC, is a gold-standard technique for consistency assessment and control during output.

During the manufacturing phase, they gather quality data as product or process measurements in real-time and plotted on a graph with preset control limits that represent the process capacity. Data that comes beyond the boundaries of regulation implies that it operates as expected. Any deviation beyond the boundaries of regulation is likely to be attributed to a common source, the normal variation expected as part of the process.

If data goes below the control limits, this means that the root of the product variation may be an assignable factor, and everything inside the procedure has to be resolved and changed to correct the problem before errors arise. SPC is a powerful tool for promoting quality development in this manner. We ensure it performs at its maximum capacity by tracking and regulating a mechanism and identifying irregularities at an early level.

Introduced in 1924, the method is likely to live permanently in the core of industrial quality assurance. Its interaction of Artificial Intelligence technology, though, could render things more detailed and reliable and offer more information into the development process and the existence of irregularities.

One of the significant aspects about AI systems and ML-based solutions is that, for each iteration, they will improve on the produce more and more reliable outcomes. For any device, the pipeline of the learning phase is exactly the same and includes the

following automated and human-assisted steps:

- Datasets are fed to an AI system
- Data models are developed based on the datasets
- A potential anomaly is raised each time a transaction deviates from the model
- A domain expert approves the deviation as an anomaly
- The system learns from the action and builds upon the data model for future predictions
- The system continues to accumulate patterns based on the preset conditions

Learning Process of AI Systems: As elsewhere in AI-powered solutions, the algorithms to detect anomalies are built on supervised or unsupervised machine learning techniques.

Supervised Machine Learning for Anomaly Detection: For developing a predictive model, the supervised approach needs a classified training set of regular and anomalous samples. Supervised neural networks, help vector machines, k- nearest neighbours, Bayesian networks and decision trees are the most popular supervised approaches. K-nearest neighbour (k-NN), which calculates the estimated distances between different points on the input vectors and assigns the unlabeled point to the class of its K-nearest neighbours, is possibly the most common nonparametric technique. The Bayesian network that encodes probabilistic relationships between variables of interest is another powerful model. Because of their capacity to encode interdependencies between variables, coupled with their ability to combine all previous information and data and to return a trust score with the model performance, supervised they assume models to have a better detection rate than unsupervised approaches.

Unsupervised Machine Learning for Anomaly Detection: Unsupervised techniques do not need manually labelled training details. They believe that most network links are regular traffic and that only a limited amount of traffic is irregular and expect that malicious traffic varies statistically from normal traffic. Based on these two hypotheses, it is presumed that groups with regular comparable events are common and that they classify the infrequent data groups as malicious. K-means, Auto-encoders, GMMs, PCAs, and hypothesis tests-based research are the most common unsupervised algorithms.

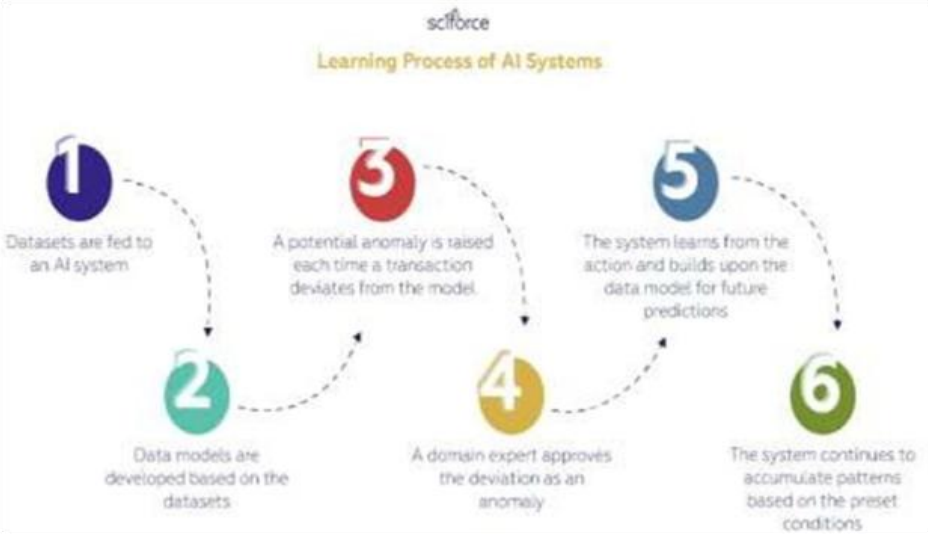

Figure 1: AI-powered solutions

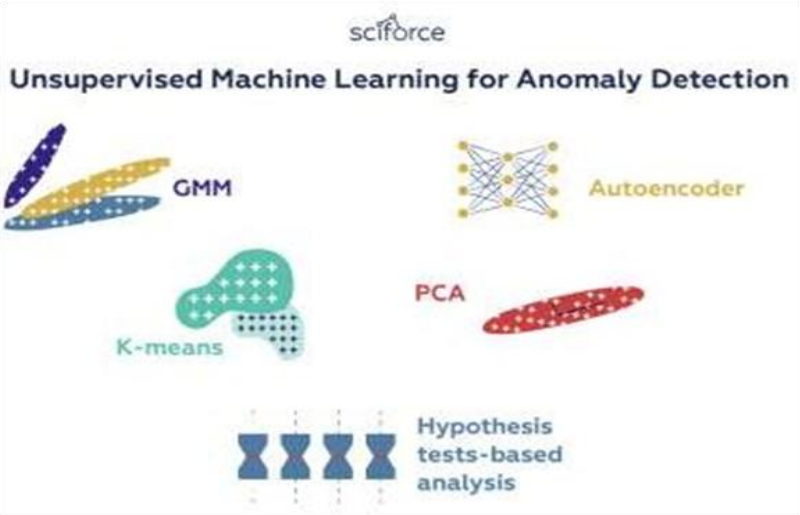

Figure 2: The most popular unsupervised algorithms

A fundamental method in Network Intrusion Detection Systems (NIDSs), Network Anomaly Detection (NAD) has played a key role in the discovery of novel threats in the last three decades and is domain-specific [1]. Despite several studies carried out in the area, it is strongly recommended to build robust models to cope with rapid data shifts in terms of attack rates, forms and existence of attacks (existing/zero-day-attack). One of the outstanding problems for Intrusion Detection Systems is the detection of irregularities with high precision and lower computational costs from vast quantities of data (IDSs). With the aid of data mining techniques and machine learning algorithms, choosing powerful data

features can minimise computing costs and eventually enhance anomaly detection with greater precision.

RELATED WORK

In [2], the authors researched victim-end DoS detection on an artificial neural network, utilising algorithms for feed forward and back propagation learning in this research. To pick functions, the unsupervised correlation-based approach was implemented. They carried the experiment out in three stages, first data collection of incoming traffic, second function selection for DoS identification, and third grouping into regular traffic and DoS attack. On the two well-known data sets such as NSL-KDD and UNSW-NB15, output assessment was checked, as they recorded feature collection reduced data dimensionality and increased training time and detection time satisfactory compared to other DoS detection methods. In [3], the authors built a hybrid approach feature selection algorithm focused on core points of attribute values, accompanied by an ARM (association rule mining).

In order to minimise processing time, they split the first data set into equivalent partitions, and they fed CP output as input to ARM to choose highly rated functions. For Network Intrusion Detection, Expectation-Maximization clustering and Naïve Bayes techniques were used in the Logistic Regression decision engine to compare and test the performance. On the UNSW-NB15 and NSL- KDD data sets, they tested the model. They discovered the model could improve precision, decrease the false alarm rate and shorten the processing time.

In [4], the authors proposed a cyber-system detection method focused on Multimodal Artificial Neural Network (MANN). The Genetic Algorithm has an algorithm for feature collection. The clustering algorithm K-means and Convolutionary Neural Network (CNN) are used to approximate the states in the cyber environment and to thoroughly learn the characteristics. They added two attack detection systems, i.e., attack detection for fully observable and attack detection was used for the analysis to approximate the form of states in partly observable cyber systems, NSL-KDD and UNSW-NB15.

In [5], the writers applied two step classifiers, the RepTree algorithm and the IDS subset of protocols. To test the efficacy of their methods, they used UNSW-NB15 and NSL-KDD datasets. First, incoming network traffic flow was categorised into TCP, UDP and OTHER,

then categorised into regular and anomaly. They used a multiclass algorithm in the second stage to identify observed irregularities into groups in order to choose adequate intervention accordingly. By balancing data gain and accuracy via the evolutionary search process, they decreased the number of features from 40 to 20.

The identification accuracy for the full datasets of UNSW-NB15 and NSL-KDD was 88.95% and 89.85%, respectively. In [6], the authors suggested an architectural scheme to design a network attack threat intelligence strategy, utilising a method so that, first, web data was gathered through crawling websites they extracted the essential data features using the algorithm of Association Rule Mining (ARM). Simulated network attack data utilising these derived features and suggesting a modern Outlier Gaussian Mixture (OGM) strategy to identify documented and zero-day attacks focused on anomaly detection method.

The outcome of the experiment revealed that, relative to four other machine learning mechanisms, the suggested method was superior in terms of increasing detection rate and decreasing FAR. UNSW-NB15 and network attack data were the data collection that was used for the experiment. In [7], the authors proposed a Deep Feature Embedding Learning (DFEL) system for detecting intrusions in the IoT setting, the experiment outcome highlights that DFEL improved the accuracy of classifiers for cyber-attack predictions and substantially saves detection time as well. In [8], the authors suggested an IDS model based on an exception.

With additional modern function selection techniques, the algorithms applied for the analysis were SVM and Genetic Algorithm. This latest paradigm invoked Genetic Algorithm-based feature selection strategies with a fitness function breakthrough to decrease data dimensions and at the same time improve true positive identification. The outcome shows that preparation period was shortened and accuracy was improved and there was a smaller false positive rate.

PROPOSED WORK

UNSW-NB15 (University of NewSouth Wale Network Based 2015) and many others. KDD98, KDDCUP99 and NSLKDD were generated decade(s) ago, so they do not reflect modern low footprint attacks. Based on UNSW-NB15 data set was created by the IXIA Perfect Storm

tool in the ACCS. ACCS is Cyber Range Lab of the Australian Centre for Cyber Security.

A. Data Pre-processing

We use full UNSW-NB15 CSV data. It has different feature types i.e., nominal, integer, binary, float and timestamp, we slice the data based on different feature types, then each type is converted to numeric accordingly, NaN values are replaced with zero if possible, removed data points otherwise because small in number. Nominal values are unified by trimming and changing to lower case and subsequently vectorized and encoded, for example a feature with four possible nominal values was converted to four features, where value 1 means that the data point belongs to that category. We did not consider timestamp features for time being in our study. After all these operations, data are merged back and normalized between (0, 1).

B. Splitting The Data

The data is very unbalanced, we under-sample the data by taking much smaller sets of data per category. As we have two-phase model i.e., binary classifier and multi-classifier, so the data has to be split for each one separately, either of the step must not be trained with each other's test set, otherwise it can't proof anything.

C. Feature Reduction

We have 47 features in the data set, further it increases while we apply encoding and vectorization. The features were ranked based on their importance and then top 10 were selected for the first phase of the model.

D. Training Binary Classifiers

In this step we train, test and compare accuracy of some commonly used classifiers, then select the best classifier and generate additional "attack-or-not" feature. The algorithms are Random Forest Classifier (RFC), Decision Tree Classifier (DTC), Gradient Boosting Classifier (GBC), K-Neighbors Classifier (KNN), Multinomial NB (MNB), SVC (SVM), Linear SVC (LSVC), Linear Discriminant Analysis (LDA), Logistic Regression (LGR), CART and Gaussian NB (GNB).

E. Training Multi-classifier

Here we train Neural Network with training set having "attack-or-not" feature in addition to previous features used in binary classification, to predict attack categories with the testing data (with generated attack-or-not feature) and apply

performance metrics to measure how well the model perform in the second phase**.**

F. Classification Metrics Used

IDSs performance depends on conducting a confusion matrix, it shows classification problem and the size of table depends on the number of classes included in a particular data set. Confusion matrix helps us to compare actual and predicted labels. The terms True Positive and True Negative implies correctly predicted conditions and similarly False Positive and False Negative denote misclassified ones.

RESULTS AND DISCUSSION

We trained and tested commonly used classifiers such as RFC, DTC, CART, GBC, KNN, MNB, SVM, LSVC, LDA, LGR and GNB with the same set of data and compared their accuracy. Random Forest scored the highest (98%) among all followed by Decision Tree Classifier (97%), the result is shown in Table-1. As the RF scored the highest accuracy, so it was chosen for anomaly detection phase in the model.

Table 1: Accuracy Comparison of Binary Classifier

No.	Classifier	Accuracy	No.	Classifier	Accuracy
1	RFC	98 %	7	SVM	76 %
2	DTC	97 %	8	LSVC	76 %
3	CART	97 %	9	LDA	76 %
4	GBC	93 %	10	LGR	76 %
5	KNN	89 %	11	GNB	52 %
6	MNB	76 %			

In this step we predict anomalies and calculate Precision, Recall and F1-Score of RF. We found that the weighted average of Precision, Recall and F1-score is 0.99. The result is given in Table-2, class 1 means that the sample is attack and class 0 means normal.

Table 2: Anomaly Detection Results

Class	Precision	Recall	F1-Score	Support
0	1.00	0.98	0.99	2,187,456
1	0.89	1.00	0.94	290,263
Avg./Total	0.99	0.99	0.99	2,477,719

To find types of attacks, we have used neural network with sigmoid function, the result of classification is shown in Table-3

Table 3: Attack Categorization Results

Class	Name	Precision	Recall	F1-Score	Support
0	analysis	0.00	0.00	0.00	268
1	backdoor	0.00	0.01	0.00	233
2	dos	0.16	0.07	0.10	11,353
3	exploits	0.07	0.41	0.11	39,525
4	fuzzers	0.15	0.49	0.23	19,246
5	generic	0.59	0.00	0.00	210,481
6	normal	1.00	0.98	0.99	2,187,456
7	reconn.	0.04	0.00	0.00	8,987
8	shellcode	0.00	0.00	0.00	152
9	worms	0.00	0.00	0.00	18
Avg.		0.93	0.88	0.88	2,477,719

CONCLUSION

Detection of deviations alone or combined with the prediction feature may be a successful way of detecting fraud and finding strange behaviour in large and complex datasets. It could be essential for the smooth operations of banking security, pharmacy, marketing, natural sciences, and manufacturing industries. Businesses will improve the productivity and protection of their automated operations through Artificial Intelligence.

In order to divide the UNSW-NB15 data set into regular and attack in the first step and two separate attack forms in the second phase, a two-phase model was developed: utilising Random Forest and Neural Network. The overall performance of the model was strong, particularly in the identification of abnormalities, but we require some improvements in attack differentiation.

REFERENCES

1. M. Ahmed, A. N. Mahmood, and J. Hu, “A survey of network anomaly

detection techniques," Journal of Network and Computer Applications, vol. 60, pp. 19–31, 2016.

2. M. Idhammad, K. Afdel, and M. Belouch, "Dos detection method based on artificial neural networks," Int J Adv Comput Sci Appl (ijacsa), vol. 8 no. 4, pp. 465–471, 2017.
3. N. Moustafa and J. Slay, "A hybrid feature selection for network intrusion detection systems: central points and association rules," in Australian Information Warfare Conference, 2015.
4. S. Guha, Attack detection for cyber systems and probabilistic state estimation in partially observable cyber environments. Arizona State University, 2016.
5. M. Belouch, S. El Hadaj, and M. Idhammad, "A two-stage classifier approach using reptree algorithm for network intrusion detection, "International Journal of Advanced Computer Science and Applications (ijacsa), vol. 8, no. 6, pp. 389–394, 2017.
6. N. Moustafa, G. Misra, and J. Slay, "Generalized outlier Gaussian mixture technique based on automated association features for simulating and detecting web application attacks," IEEE Transactions on Sustainable Computing, 2018.
7. Y. Zhou, M. Han, L. Liu, J. S. He, and Y. Wang, "Deep learning approach for cyber attack detection," in IEEE INFOCOM 2018-IEEEConference on Computer Communications Workshops (INFOCOMWKSHPS). IEEE, 2018, pp. 262–267.
8. H. Gharaee and H. Hosseinvand, "A new feature selection id basedon genetic algorithm and svm," in Telecommunications (IST), 2016 8thInternational Symposium on. IEEE, 2016, pp. 139–144.