Towards Machine Learning Based IoT Intrusion Detection Service

TagyAldeen Mohamed(✉), Takanobu Otsuka(✉), and Takayuki Ito(✉)

Department of Computer Science, Nagoya Institute of Technology,
Gokiso, Showa-ku, Nagoya, Japan
tagy.mohamed@itolab.nitech.ac.jp,
{otsuka.takanobu,ito.takayuki}@nitech.ac.jp
http://itolab.nitech.ac.jp

Abstract. IoT Security is one of the most critical issues when developing, implementing and deploying IoT platforms. IoT refers to the ability of communication, monitoring and remote control of automated devices through the internet. Due to low computational capabilities, less power, and constrained technologies, IoT is vulnerable to various cyber attacks. Security mechanisms such as cryptography and authentication are hard to apply due to the aforementioned constraints on IoT devices. To overcome this issue Intrusion Detection Systems (IDSs) play main role as a high-security solution. This paper shows a proposed IDS based on machine learning techniques to be implemented into IoT platforms as a service. We used Random forest as a classifier to detect intrusions, then we applied neural network classifier to detect the categorization of the detected intrusion. The experimental results showed the proposed model can effectively detect intrusions, yet categorization of the intrusion suffers from low accuracy and high bias.

Keywords: Anomaly detection · Neural network · IoT security · IDS

1 Introduction

With the recent revolution of low-cost computing devices along with technological advancement in communication, the next generation of internet services, which touch every aspect of our life has been developed. Internet-of-Things (IoT) concept is used as a multitude of objects interconnected to each other and to the internet allowing people and objects to interact and create smart environments for transportation systems, cities, health, energy and any other possible objects.

Since Internet Of Things operate in completely isolated environments and was never designed to handle security threats, (IoT) is vulnerable to malicious attacks, furthermore because of it's opening development, deployment and limited resources. Its heterogeneous and distributed character make it difficult to apply standard security mechanism [2], causing systems to take wrong and dangerous actions.

M. Mouhoub et al. (Eds.): IEA/AIE 2018, LNAI 10868, pp. 580–585, 2018.
https://doi.org/10.1007/978-3-319-92058-0_56

Intrusion Detection System is one of the techniques which helps to determine network security, by alarming when an intrusion is detected. Security vulnerabilities are both technically difficult and economically costly. Hence, the role of Intrusion Detection System (IDS), as special-purpose devices to detect anomalies and attacks in the network, is important.

We propose using cloud computing for anomaly detection, to use it as a robust and scalable security solution for IoT platforms. Our proposed solution is based on neural network and random forest. We perform all the analysis in the cloud, so that, IoT performance isn't affected.

The remaining of the paper is organized as follows, in Sect. 2 we present the IoT structure and it's security issues, the used machine learning algorithms, and the IDS detection methods. In Sect. 3, we show the detailed design of our proposed solution, In Sect. 4, we present results discussion and Future work.

1.1 IoT Security Challenges

IoT traditional network security solutions may not be directly applicable due to the differences in IoT structure and behavior. We consider the following issues as the main reasons for that lack [3]. (1) IoT design focuses mainly on functionality with tradeoff to security. Manufacture companies seek new functions working at lowest cost. (2) Low operating energy and minimal computational capabilities. Therefore security mechanism such as encryption protocols and authentication can not be directly applied. (3) The lack of a single standard for IoT architecture. IoT may have different policies, and connectivity domains. Therefore, security law and regulations are not applied yet [6]. These Given challenges along with the use of hacking software, vulnerabilities can be easily discovered. Penetration testing tools, which are able to automate attacks against IoT systems, are easily accessible. Such tools [4] are convenient enough to enable even low-skilled exploiters to cause huge damage to IoT platforms in several ways. According to [5] IoT testing guidance issues can be described with 10 different security domains.

1.2 Intrusion Detection System

Intrusion detection systems are strategically placed on a network in order to detect threats and monitor network traffic. The IDS take either network or host based approachs for recognizing attacks. The IDS achieves this mission by collecting data from systems and network sources and perform analysis on it for possible [6] threats. The IDS main functions are offering information on threats, perform actions when threat is detected and record important events within the network [6].

Detection techniques fall into several classes:

1. **Signature based Detection** are based on set of rules used to match patterns in the network traffic. It has the advantage of detecting well known attacks, but it fails to detect novel attacks that aren't known to the database.

2. **Anomaly based** is a behavior based detection. It observes changes in normal activity through profiling the objects which are being monitored. This technique is efficient in identifying new malicious activities, but sometimes it fails to identify popular attacks or provides false positive alarms.
3. **Hybrid IDS** is a hybrid of signature-based and anomaly-based techniques. This technique consumes energy and resources, but is efficient in terms of detection and for identifying attacks and threats. With this mixed technique IDS is able to identify well known attacks along with novel attacks.

1.3 Artificial Neural Network

Neural networks are a set of tools that can automatically detect patterns to classify new data [10]. While there is a large number of machine learning algorithms, the main performance of all of them relies on optimal features selection An artificial neural network consists of a collection layered of processing elements that are interconnected and transform a set of inputs into a set of outputs [11]. In all anomaly detection approaches learning and testing phases are used in order to differentiate data generated from IoT systems are anomalous or not. The main challenge is in disputing whether are all anomalies in IoT datasets are considered as intrusions. However, the most important advantage of neural networks is the ability to "learn" the characteristics of novel attacks, and to identify instances that are unlike any of which has been observed.

1.4 Random Forest

A random forest is a meta estimator that fits a number of decision tree classifiers on various sub-samples of the dataset and use averaging to improve the predictive accuracy and control over-fitting. It is a supervised classification algorithm which creates forest with a number of decision trees [7]. Random forests are a way of averaging multiple deep decision trees, trained on different parts of the same training set, with the goal of reducing the variance. A tree classification algorithm is used to construct a tree with a different bootstrap sample from the original data. When the formation of a forest is completed, a new object which is to be classified is taken from each of the trees in the forest.

1.5 Network Features

We propose using dataset UNSW-NB15 [1] to employ a customized machine learning algorithm for learning general behaviors in the dataset in order to differentiate between normal and malicious activities. Dataset UNSW-NB15 is a modren labeled dataset for evaluating NIDSs, created by cyber security research group at ACCS. The dataset contains over 2.5 million records as CSV format along with 49 features. Categories are 9 types of modern attacks and 1 normal traffic patterns. The features type are different: Integer, Float, Binary, Nominal and Timestamp. We think this dataset has different attack families which may reflect real world and modern attacks.

2 Intrusion Detection Service

Our solution is divided into two parts. A device collects end nodes traffic and sends it to the cloud analyzer. In this solution, we propose using Raspberry Pi 3 as the main device for all the implementations of our proposed solution. The device acts as an interface between the application layer in the top level and the end nodes layer. Since sensors usually have low (or no) computational power, this service is a more suitable approach to secure the end nodes in IoT network by watch and monitor abnormal behaviors.

The second part is a cloud-based intrusion detector based on Random Forests and Neural Network. It receives IoT traffic from the aforementioned device, performs features extraction, and classification on the extracted features. Random Forest is used to detect if the data point is classified as intrusion or not. The Neural Network is used to categorize the detected intrusion

Our solution is divided into three modules: (1) Data collection Module, (2) Data processing and (3) Detection module and alerting.

2.1 Traffic Gathering Module

We propose using Tshark. Tshark is a network protocol analyzer. It is capable of capturing packet data from a live network connection, for a particular time window or read packets from a previously saved capture file. Our idea is to capture IoT network traffic and save it as pcap files. Then we upload these files to the cloud analyzer. Our proposed traffic capture algorithm is based on traffic capture time and the size of pcap file. Tshark configuration allow capture specific features of the network traffic along with of deep inspection. Since the proposed model handles only numerical features, pcap files are processed by Bro-IDS and other scripts to mine the features, Bro-IDS is an open-source traffic analyzer, considered as a security monitor and malicious activities inspector. MySQL technology is used to store the extracted features. The extracted features are then passed to the processing module to be analyzed.

2.2 Detection Module

Random Forest Classifier: Scikit-Learn' ExtraTreesClassifier are used to classify intrusions with 31 estimators (decision trees). Measurement of decision tree's quality was done with Information gain ratio. Other settings were left default, Number of estimators and criterion were selected by hand.

Neural Network architecture was selected by trial and error. The input layer has the same number as the dataset features. Sigmoid activation function $h_\theta(x) = \frac{1}{1+e^{-\theta^T x}}$ gave better results than ReLU and tanh. Dense layers are fully connected. The output layer has softmax as activation function, $\text{softmax}(\mathbf{x})_i = \frac{e^{x_i}}{\sum_{j=1} e^{x_j}}$ output dimensions are dataset data categories: 9 are attacks and 1 is normal. Dropout regularization is used to prevent overfitting.

3 Simulation Results

Normal or Intrusion Classification: In order to evaluate the aforementioned algorithms, we used UNSW-NB15 [1] as a simulation to real IoT traffic. The results show that Random Forest works fine with UNSW-NB15 [1].

Confusion matrix is used to evaluate performance. It also helped to identify which classes the algorithm didn't classify correctly. Precision, recall, and F1-score were calculated. Table 1 shows the results of metrics performance, 0 means the sample is classified as a normal data point, 1 represents an intrusion. Table 1 shows the classification result.

Table 1. Random forest classification results

Class	Precision	IRecall	F1-score
0	1.00	0.98	0.99
1	0.88	1.00	0.93
Avg/total	0.99	0.98	0.98

Intrusion Categorization: Intrusion classes represented with numbers 0–9 corresponding to the dataset labels. For example, the precision of the normal class which is represented by number 6 is approximately 1 and recall is 0.98. The results showed that mostly classes 2,4 and 6 were classified, Class 6 always classified correctly, which suggest differentiating features present in class 6. Predictions mostly fall under class 2 and 4. Therefore instances of the classes 2 and 4 have high recall score. Class 5 and 2 are similar, most data point predicted to be class 2, so the precision is low as Table 2 shows.

Table 2. Neural network categorization results

Class	Precision	IRecall	F1-score
0	0.00	0.00	0.00
1	0.00	0.00	0.00
2	0.04	0.81	0.07
3	0.02	0.00	0.00
4	0.16	0.60	0.25
5	0.06	0.00	0.00
6	1.00	0.98	0.99
7	0.00	0.00	0.00
8	0.00	0.00	0.00
9	0.00	0.00	0.00
Avg/total	0.89	0.87	0.88

We tried changing neural network architecture in order to get better performance, it made an impact on which classes the data points were classified to, but the overall classification accuracy stayed almost the same. Different residual layer techniques, bypasses between layers and other techniques were used but no positive impact on the accuracy.

4 Conclusion and Future Work

IoT's heterogeneous and distributed characters make traditional intrusion detection methodologies hard to deploy. To overcome this issue, we proposed Cloud computing service as an efficient mechanism to process data from different resources of IoT platforms. Effectivness in time and intrusion detection is a must for critical IoT applications. Towards verifying our hypothesis, we test the proposed model on UNSW-NB15 [1].

Algorithms and techniques [8] will be improved in future. Now we are working on IoT environment to test and deploy our proposed solution. In the future work, IoT network traffic features will be studied closely to provide high accuracy. Data collection and pre-processing along with detection algorithms will be presented from IoT test environment. We plan to extend this proposal in three manners. (1) IoT traffic Features selection regarding anomaly detection, (2) IPv6 and it's feature extraction, and (3) Performance of the proposed methods regards detecting anomalies as intrusions.

References

1. Moustafa, N., Slay, J.: UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In: 2015 Military Communications and Information Systems Conference (MilCIS). IEEE (2015)
2. Suo, H., Wan, J., Zou, C., Liu, J.: Security in the Internet of Things: a review. In: International Conference on Computer Science and Electronics Engineering (ICCSEE), vol. 3 (2012)
3. Pacheco, J., Hariri, S.: IoT security framework for smart cyber infrastructures. In: 1st International Workshops on Foundations and Applications of Self Systems (2016)
4. Aircrack-ng tools for Wifi network security. https://www.aircrack-ng.org/
5. OWASP IoT Testing Guidance. https://owasp.org
6. Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., Atkinson, R.: Shallow and deep networks intrusion detection system: a taxonomy and survey (2017)
7. Breiman, L.: Random forests. Mach. Learn. **45**(1), 5–32 (2001)
8. ITKST42: information security technology course. https://github.com/Moskari/ITKST42-network-data-classifier
9. Matthew, V., Philip, K.: PHAD: packet header anomaly detection for identifying hostile network traffic. Department of Computer Sciences Florida Institute of Technology Technical report CS-2001-04 (2001)
10. Witten, I.H., Frank, E.: Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann, San Francisco (2005)
11. de Lima, I.V.M., Degaspari, J.A., Sobral, J.B.M.: Intrusion detection through artificial neural networks. In: Network Operations and Management Symposium NOMS 2008, pp. 867–870. IEEE, 7–11 April 2008