Cyber-Attack Detection Using Artificial Intelligence

[1]V. Yamuna, [2]P. Harika, [3]Sk. Javeed, [4]S. Manindra, [5]V. Saradhi

[1]Assistant Professor, [2,3,4,5]Student
Electronics and Communication Engineering
N.B.K.R Institute of Science and Technology, Andhra Pradesh, India

Abstract: Cyber-Physical Systems have made momentous evolution in many effective applications cause of the integration between physical entities, computational resources, and communication potentialities. Although, cyber-attacks are dominant intimidation to these systems. Cyber-attacks occur brilliantly and stealthy. A few of these attacks which are specifically called malware, deception attacks, Denial-of-service (DoS) attacks and also by compromising with some cyber components, manipulate data, or entering false information into the system. If the system is oblivious of the existence of those attacks, systems were unable to detect them, and performance of the systems may be disrupted or disabled completely. Hence, it is decisive to adapt algorithms to pinpoint these kind of attacks in these systems. It should be remembered that the information generated in these systems is produced in very large number, with so much variety, and high speed, thus it is essential to use machine learning algorithms to ease the analysis and evaluation of data and to identify hidden patterns. The proposed method in this study is to use various machine learning algorithms such as Support Vector, Decision Tree, Random Forest, Extra Tree Classifier, ad boost and Neural networks, Gradient boosting, K-means clustering, and Logistic regression techniques. After uploading the dataset, pre-processing by using will be done on the unstructured data to convert it to the structured data and then data is trained using the algorithms. Based on the accuracy of these algorithms, the cyber-attack is detected

Keywords: Artificial Intelligence, Extra Trees Classifier, Cyber-Attack, Gradient Boosting, Random Forest Classifier.

1. INTRODUCTION

Latest upgrades in technology leads to introduction of cyber-physical systems. These systems connect physical infrastructure and things to the internet and to one another by integrating sensing, computation, control, and networking. The improvement in cyber-physical systems comes at a cost of being exposed to cyber-attacks. Physical components including sensors, which gets data from the physical environment, maybe attacked and be infused erroneous data into the system. One of the crucial challenges of a cyber-physical system is its physical part, which handles large number of sensors in the environment, which collect large amount of data, with so much heterogeneity, and at high speed. Therefore, one of the most salient features of a cyber-physical system is to communicate between these sensors, compute and control the system.

An essential concern with these systems is the security of cyber-physical systems to identify cyber-attacks. It should be noted that cyber-attacks occurs in irregular ways, and it is not possible to describe these attacks in a regular and orderly manner. The cyber-attacks in cyber-physical systems are classified into two types: denial of service (Dos)and deception attacks. These attacks can corrupt data or enter false information into the system and cause misbehaving.

System monitoring in the system can find these attacks. These attacks can be called as stealthy deception attacks.

In this project, some of the machine learning algorithms are used to detect the cyber-attacks. This project mainly focuses on accuracy and time complexity of the detection.

2. LITERATURE SURVEY

[1] Kwon, Cheolhyeon, Weiyi Liu, and Inseok Hwang. "Security study against stealthy deception attacks for cyber-physical systems." American Control Conference, 2013, IEEE, 3344–3349

For a networked control system, the security issue in the state estimation problem is investigated (NCS). The NCS's remote estimator and sensors' communication channels are open to intrusions from nefarious enemies. Attacks that inject bogus data are taken into account. The purpose of this study is to identify the so-called insecurity criteria that make the estimate system insecure in the sense that malicious attacks can still cause unbounded estimation mistakes even when they manage to get past the anomaly detector.

. In particular, when all communication channels are compromised by the adversary, a new necessary and sufficient condition for the vulnerability is developed. Also, a specific algorithm is suggested for creating attacks that can compromise the estimating system. Also, a system security plan for the insecure system is provided, where only a few communication channels (rather than all of them) need to be protected against fake data injection assaults. The usefulness of the suggested criteria and techniques in solving the secure estimation problem for a flight vehicle is shown using a simulated scenario. [2] George J. Pappas, Oleg Sokolsky, Nicola Bezzo, Miroslav Pajic, and Insup Lee. With a focus on attack-resilient state estimators, design and implementation of attack-resilient cyberphysical systems. 66–81 in IEEE Control Systems Magazine, Vol. 37, No. 2, 2017.

The frequency of security-related incidents using control systems has significantly increased in recent years. These include high-profile attacks across a variety of application domains, from attacks on critical infrastructure, as in the case of the Maroochy Water breach [1], and industrial systems, to assaults on modern automobiles [6]–[8]. Examples include the cyberattack on the German Steel Plant and the StuxNet virus attack on an industrial supervisory control and data acquisition system [2–5]. Even high-assurance military systems were shown to be vulnerable to attacks, as demonstrated by the widely reported downing of the US drone RQ-170

Sentinel [9]–[11]. These mishaps have significantly enhanced the need for security in cyberphysical systems (CPSs), which tightly combine computation and communication substrates with sensing and actuation components.
. However, the next generation of safety-critical, networked, and embedded control systems' complexity and heterogeneity have presented challenges to the established design methodologies, where security is typically considered as an afterthought.

3. PROPOSED METHOD

Here several proposed machine learning models to classify whether there will be a cyber-attack or not. But in the existing method, it has methods like Network Intrusion Detection and Prevention systems (IDS/IPS) monitors malicious activities. Both the methods, though effective, have some weaknesses. To address this, researchers have presented models for performance classification evaluation that, for the most part, do not take the heterogeneity and amount of the data into account. Hence, we propose a Support Vector, Decision Tree, Random Forest, Extra Tree Classifier and ad boost and Neural network classifier, Gradient boosting, K-means clustering, Logistic regression techniques
The main advantages of the proposed system are: High accuracy and Reduction of time complexity.

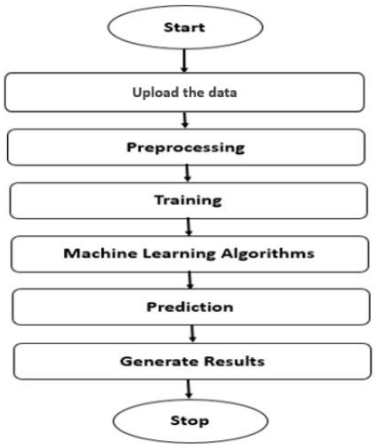

Fig.1 Block Diagram

4. ALGORITHMS

3.1. Decision Tree

Decision tree is a supervised learning model that can be preferred for solving classification problems. It is a tree-structured classifier, with internal nodes denoting dataset features, branches suggesting decision-making steps, and specific leaf nodes denoting results. The features of the raw dataset have been employed to conduct the decisions.
The basic idea behind any decision tree algorithm is shown in below fig.2

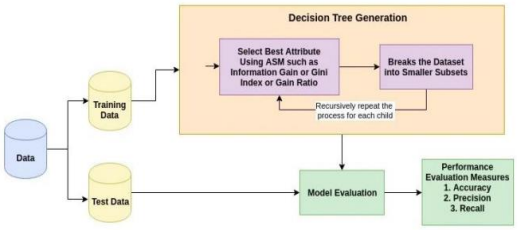

Fig.2 Decision tree block diagram

3.2 Random Forest Classifier:

Random Forest is an algorithm that makes use of supervised learning. It is founded on the notion of transfer learning, a mechanism for merging different classifiers to resolve a broad range of issues and improve model performance.
Instead of depending on a single decision tree, Random Forest is a classifier that uses many decision trees on different sets of a given dataset and averages the results to increase predicted accuracy. The random forest forecasts the result based on the average of all guesses for a single decision by using the prediction from each tree.
Increased accuracy and a reduction in the overfitting problem are produced by more trees in the forest. Also, compared to other algorithms, it requires less training time.

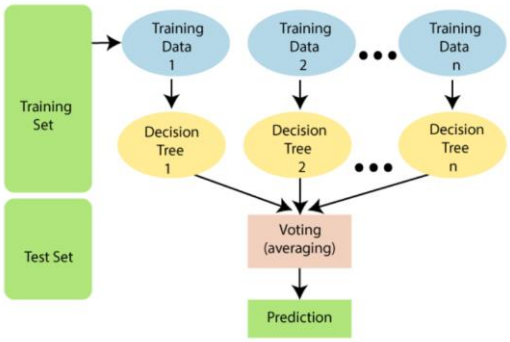

Fig.3 Random forest classifier block diagram

3.3 Extra Trees Classifier

An ensemble learning technique called Extra Trees Classifier is mostly founded on decision trees. Similar to Random Forest, Extra Trees Classifier encounters various some assessments and subsets of information to avoid over-learning from the data and overfitting. We'll examine a few ensemble techniques in the following order: Extra Trees Classifier comes last, from high to low variance.

Decision Tree (High Variance):

- Because there is merely one feasible decision-making pathway that even a single decision tree has ever encountered, often this overfits the data it is learning from. Normally, predictions made from a single decision tree are inaccurate when applied to new data.
- Random forest (medium variance): To counteract overfitting, randomness is integrated into random forest models. building multiple trees (n_estimators)
- drawing observations with replacement (i.e., a bootstrapped sample)
- splitting nodes on the best split among a random subset of the features selected at every node

Extra trees (low variance):

Similar to Random Forest in that it constructs multiple trees and splits nodes using random subsets of features, Extra Trees differs from that algorithm in two significant ways: first, it does not bootstrap observations (i.e., it samples without replacement), and second, nodes are split on random splits rather than the best splits.

3.4 Gradient Boosting

The approach calculates the gradient of the loss function with respect to the current ensemble of predictions in each iteration, and then iteratively trains a new weak model to minimise this gradient. A formidable boosting process called gradient boosting turns a number of weak learners into especially conducive. Each new model is trained to minimise the loss function, such as mean squared error or cross-entropy of the prior model using gradient descent.

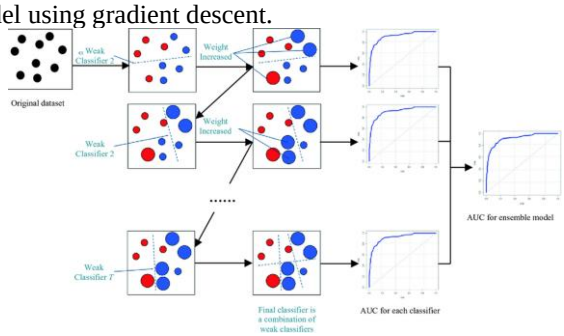

Fig.4 Gradient Boosting block diagram

5. RESULTS AND DISCUSSION

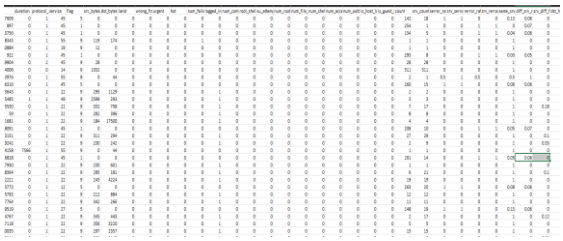

Fig. 5(a) Collected Dataset

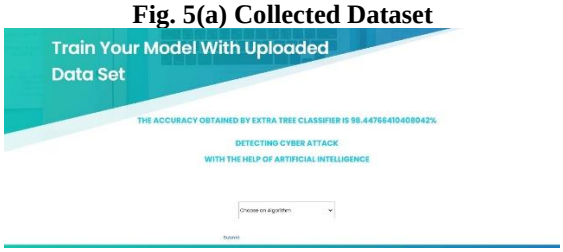

Fig. 5(b) Algorithm selection based on the Accuracy

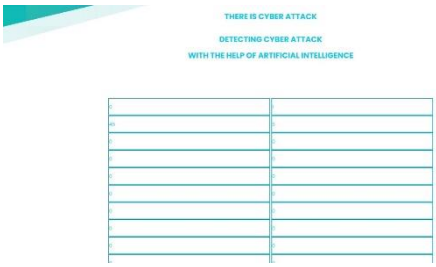

Fig. 5(c) Predicted Output for the given The training of the data model by choosing each algorithm and evaluating its accuracy is shown in Fig. 5(b). Based on the highest level of accuracy, we moved on to the following step, which is prediction. Here, the output of the trained data was produced as depicted in Fig. 5. (c).

6. CONCLUSION:

In order to address the shortcomings of the existing method, such as its low accuracy, time-consuming nature, inefficient handling of larger datasets, and high complexity, this work proposes the cyber-attack detection strategy utilising artificial intelligence. We gathered a dataset made up of unstructured data and used several pre-processing methods and machine learning algorithms. The data output, or whether a cyberattack has occurred or not, was anticipated based on the algorithms' greatest level of accuracy.

REFERENCES

1. Kwon, Cheolhyeon, Weiyi Liu, and Inseok Hwang. ”Security analysis for cyber-physical systems against stealthy deception attacks.” In 2013 American control conference, IEEE (2013): 3344-3349.
2. Pajic, Miroslav, James Weimer, Nicola Bezzo, Oleg Sokolsky, George J. Pappas, and Insup Lee. ”Design and implementation of attack-resilient cyberphysical systems: With a focus on attack-resilient state estimators.” IEEE Control Systems Magazine 37, no. 2 (2017): 66-81.
3. Sheng, Long, Ya-Jun Pan, and Xiang Gong. ”Consensus formation control for a class of networked multiple mobile robot systems.” Journal of Control Science and Engineering 2012 (2012).
4. Zeng, Wente, and Mo-Yuen Chow. ”Resilient distributed control in the presence of misbehaving agents in networked control systems.” IEEE transactions on cybernetics 44, no. 11 (2014): 2038-2049.
5. Sun, Hongtao, Chen Peng, Taicheng Yang, Hao Zhang, and Wangli He. ”Resilient control of networked control systems with stochastic denial of service attacks.” Neurocomputing 270 (2017): 170-177.
6. Zhang, Haotian, and Shreyas Sundaram. ”Robustness of information diffusion algorithms to locally bounded adversaries.” In 2012 American Control Conference (ACC), IEEE (2012): 5855- 5861.
7. Fu, Weiming, Jiahu Qin, Yang Shi, Wei Xing Zheng, and Yu Kang. ”Resilient Consensus of Discrete-Time Complex Cyber-Physical Networks under Deception Attacks.” IEEE Transactions on Industrial Informatics (2019).
8. Ozay, Mete, Inaki Esnaola, Fatos Tunay Yarman Vural, Sanjeev R. Kulkarni, and H. Vincent Poor. ”Machine learning methods for attack detection in the smart grid.” IEEE transactions on neural networks and learning systems 27, no. 8 (2015): 1773-1786.
9. Tianfield, Huaglory. ”Data mining based cyber-attack detection.” System simulation technology 13, no. 2 (2017): 90-104.
10. Pasqualetti, Fabio, Florian Dorfler, and Francesco Bullo. ”Attack detection and ¨ identification in cyber-physical systems.” IEEE Transactions on Automatic Control 58, no. 11 (2013): 2715-2729.