ISSN:2229-6107

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY

E-mail :
editor.ijpast@gmail.com
editor@ijpast.in

www.ijpast.in

INTERNATIONAL JOURNAL OF PURE AND APPLIED SCIENCE & TECHNOLOGY
IJPAST

ISSN 2229-6107
www.ijpast.in
Vol 14 Issue 1 Jan 2024

Trustworthy and reliable machine learning based cyberattack detection in IOT

Ms.Supriya Belkar[1], G.Akshitha[2],I.Nikitha[3],G.Manasa[4]

ABSTRACT

A fundamental expectation of the stakeholders from the Industrial Internet of Things (IIoT) is its trustworthiness and sustainability to avoid the loss of human lives in performing a critical task. A trustworthy IIoT-enabled network encompasses fundamental security characteristics, such as trust, privacy, security, reliability, resilience, and safety. The traditional security mechanisms and procedures are insufficient to protect these networks owing to protocol differences, limited update options, and older adaptations of the security mechanisms. As a result, these networks require novel approaches to increase trust level and enhance security and privacy mechanisms. Therefore, in this article, we propose a novel approach to improve the trustworthiness of IIoT-enabled networks. We propose an accurate and reliable supervisory control and data acquisition (SCADA) network-based cyberattack detection in these networks. The proposed scheme combines the deep learning- based pyramidal recurrent units (PRU) and decision tree (DT) with SCADA-based IIoT networks. We also use an ensemble-learning method to detect cyberattacks in SCADA-based IIoT networks. The nonlinear learning ability of PRU and the ensemble DT address the sensitivity of irrelevant features, allowing high detection rates. The proposed scheme is evaluated on 15 datasets generated from

SCADA-based networks. The experimental results show that the proposed scheme outperforms traditional methods and machine learning-based detection approaches. The proposed scheme improves the security and associated measure of trustworthiness in IIoT-enabled networks.

I. INTRODUCTION

The Industrial Internet of Things (IIOT) is a pervasive network that connects a diverse set of smart appliances in the industrial environment to deliver various intelligent services. In IIOT networks, a significant amount of industrial control systems (ICSs) premised on supervisory control and data acquisition(SCADA) are linked to the corporate network through the Internet [1]. Typically, these SCADA-based IIOT networks consist of a large number of field devices [2], for instance, intelligent electronic devices, sensors, and actuators, connected to an enterprise network via heterogeneous communications [3]. This integration provides the industrial networks and systems with supervision and a lot of flexibility and agility [2]–[4], resulting in greater production and resource efficiency. On the other hand, this integration exposes SCADA-based IIOT networks to serious security threats and vulnerabilities, posing a significant

[1]Assistant Professor, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad,supriyabelkar27@gmail.com

[2,3,4]UG Students, Department of CSE, Malla Reddy Engineering College for Women, Hyderabad, TS, India.

danger to these networks and the trustworthiness of the systems [5]. The trustworthiness of an IIOT-enabled system ensures that it performs as expected while meeting a variety of security requirements, including trust, security, safety, reliability, resilience, and privacy [6]–[8]. Fig. 1 depicts the fundamental aspects of trustworthiness in an IIoT-enabled network. The basic goal of the IIOT-enabled system is to increase trustworthiness by safeguarding identities, data, and services, and therefore to secure SCADA-based IIOT networks from cybercriminals [8], [9].

Several protocol updates have been proposed to meet this purpose, including the distributed network protocol (DNP 3.0) [10]. However, it covers authentication and data integrity aspects only, leaving numerous holes for attackers to use known flaws like hash collision to carry out serious attacks [11]. Information Technology and Industrial Operational technology bodies build a typical risk management plan utilizing ISO 27005:2018 [10] to recognize, rank, and implement alleviation techniques in automated or semi automated enterprises. A comprehensive risk management plan and adequate preventive measures may not ensure absolute security against growing risks and attacks. This consequently offers a difficult research challenge for industrial and cyber security control researchers to 1) obtain the maximum degree of attack detection, 2) report malicious behavior as soon as it appears, and 3) isolate the afflicted subsystems as soon as possible. In recent years, there has been a surge toward the utility of artificial intelligence (AI) methods in evolving cyber security approaches, including attack prediction [12], privacy preservation [13], forensic exploration [14], and malware disclosure [15]. Deep learning (DL) is an AI approach that incorporates better learning models with considerable success in various disciplines [16]. However, designing a reliable and trustworthy AI, particularly a DL-based cyber attack detection model for the IIOT platforms, remains a research problem.

By considering the limitations of previous techniques, we employ network attributes of industrial protocols and propose a pyramidal recurrent unit (PRUs)- and decision tree (DT)-based ensemble detection mechanism. The proposed mechanism has the potential to detect cyber attacks in any extensive industrial network. The interoperability with other detection engines and expandability for a wider industrial network with multiple areas distinguishes the proposed mechanism from previous studies. The proposed detection method is disseminable across many IIOT domains. Furthermore, our model is straightforward to implement and deploy and can improve efficiency and accuracy while overcoming the shortcomings of previous efforts. The following capabilities can characterize the novelty and contribution of our article.

1) We propose a scalable and efficient DL- and DT-based ensemble cyber-attack detection framework to resolve trustworthiness issues in the SCADA-based IIOT networks.

2) We present an efficient probing approach by the SCADA based network data to solve the protocol mismatch limitations of traditional security solutions for the IIOT platform. Fig. 2 . SCADA-based industrial IOT network .

3) A statistical analytic approach for ensuring the trustworthiness and reliability of the proposed model for SCADA based IIOT networks.

The rest of the article is organized as follows. In Section II, we have discussed the basics of problem formulation. In Section III, we have given details of our proposed work, followed by the results and discussion in Section IV. Finally, Section V concludes this article.

II. LITERATURE REVIEW:

Trustworthy and Reliable Deep-Learning-Based Cyberattack Detection in Industrial IoT, Fazlullah Khan, Md Arafatur Rahman, Imran Razzak,A fundamental expectation of the stakeholders from the Industrial Internet of Things (IIoT) is its trustworthiness and sustainability to avoid the loss of human lives in performing a critical task. A trustworthy IIoT-enabled network encompasses fundamental security characteristics, such as trust, privacy, security, reliability, resilience, and safety. The traditional security mechanisms and procedures are insufficient to protect these networks owing to protocol differences, limited update options, and older adaptations of the security mechanisms. As a result, these networks require novel approaches to increase trust-level and enhance security and privacy mechanisms. Therefore, in this article, we propose a novel approach to improve the trustworthiness of IIoT-enabled networks. We propose an accurate and reliable supervisory control and data acquisition (SCADA) network-based cyberattack detection in these networks. The proposed scheme combines the deep-learning-based pyramidal recurrent units (PRU) and decision tree (DT) with SCADA-based IIoT networks. We also use an ensemble-learning method to detect cyberattacks in SCADA-based IIoT networks. The nonlinear learning ability of PRU and the ensemble DT address the sensitivity of irrelevant features, allowing high detection rates. The proposed scheme is evaluated on 15 datasets generated from SCADA-based networks. The experimental results show that the proposed scheme outperforms traditional methods and machine learning-based detection approaches. The proposed scheme improves the security and associated measure of trustworthiness in IIoT-enabled networks.

III.EXISTING SYSTEM :

The Internet of Things (IoT) has revolutionized modern tech with interconnected smart devices. While these innovations offer unprecedented opportunities, they also introduce complex security challenges. Cybersecurity is a pivotal concern for intrusion detection systems (IDS). Deep Learning has shown promise in effectively detecting and preventing cyberattacks on IoT devices. Although IDS is vital for safeguarding sensitive information by identifying and mitigating suspicious activities, conventional IDS solutions grapple with challenges in the IoT context. This paper delves into the cutting-edge intrusion detection methods for IoT security, anchored in Deep Learning.

We review recent advancements in IDS for IoT, highlighting the underlying deep learning algorithms, associated datasets, types of attacks, and evaluation metrics. Further, we discuss the challenges faced in deploying Deep Learning for IoT security and suggest potential areas for future research. This survey will guide researchers and industry experts in adopting Deep Learning techniques in IoT security and intrusion detection.

Disadvantages

- The complexity of data: Most of the existing machine learning models must be able to accurately interpret large and complex datasets to detect Cyber Attacks.
- Data availability: Most machine learning models require large amounts of data to create accurate predictions. If data is unavailable in sufficient

quantities, then model accuracy may suffer.

• Incorrect labeling: The existing machine learning models are only as accurate as the data trained using the input dataset. If the data has been incorrectly labeled, the model cannot make accurate predictions.

IV. PROPOSED SYSTEM

By considering the limitations of previous techniques, we employ network attributes of industrial protocols and propose a pyramidal recurrent unit (PRUs)- and decision tree (DT)-based ensemble detection mechanism. The proposed mechanism has the potential to detect cyberattacks in any extensive industrial network. The interoperability with other detection engines and expandability for a wider industrial network with multiple areas distinguishes the proposed mechanism from previous studies. The proposed detection method is disseminable across many IIoT domains. Furthermore, our model is straightforward to implement and deploy and can improve efficiency and accuracy while overcoming the shortcomings of previous efforts.

Advantages

1) We propose a scalable and efficient DL- and DT-based ensemble cyber-attack detection framework to resolve trustworthiness issues in the SCADA-based IIoT networks.

2) We present an efficient probing approach by the SCADAbased network data to solve the protocol mismatch limitations of traditional security solutions for the IIoT platform.

3) A statistical analytic approach for ensuring the trustworthiness and reliability of the proposed model for SCADA based IIoT networks.

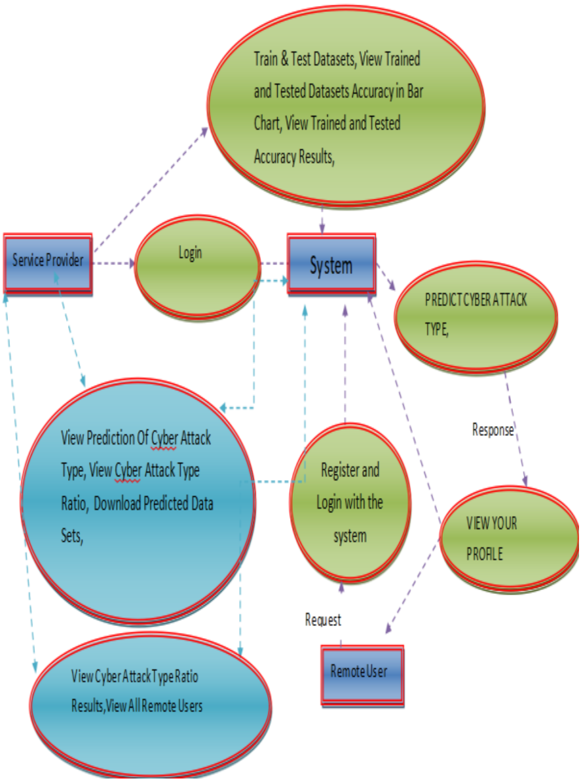
Train & Test Datasets, View Trained and Tested Datasets Accuracy in Bar Chart, View Trained and Tested Accuracy Results,
Service Provider
Login
System
PREDICT CYBER ATTACK TYPE,
Response
View Prediction Of Cyber Attack Type, View Cyber Attack Type Ratio, Download Predicted Data Sets,
Register and Login with the system
VIEW YOUR PROFILE
Request
View Cyber Attack Type Ratio Results,View All Remote Users
Remote User

Fig1:flow diagram **V. MODULES**

Service provider

In this module, the service provider has to login by using valid user name and password. After login successful he can do some operations such as train & test datasets, view trained and tested datasets accuracy in bar chart, view trained and tested accuracy results, view prediction of cyber attack type, view cyber attack type ratio, download predicted data sets, view cyber attack type ratio results, view all remote users.

View and authorize users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote user

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once login is successful user will do some operations like register and login, predict cyber attack type, view your profile.

VI. ALGORITHMS:

Decision tree classifiers

Decision tree classifiers are used successfully in many diverse areas. Their most important feature is the capability of capturing descriptive decision making knowledge from the supplied data. Decision tree can be generated from training sets. The procedure for such generation based on the set of objects (S), each belonging to one of the classes C1, C2, …, Ck is as follows:

Step 1. If all the objects in S belong to the same class, for example Ci, the decision tree for S consists of a leaf labeled with this class

Step 2. Otherwise, let T be some test with possible outcomes O1, O2,…, On. Each object in S has one outcome for T so the test partitions S into subsets S1, S2,… Sn where each object in Si has outcome Oi for T. T becomes the root of the decision tree and for each outcome Oi we build a subsidiary decision tree by invoking the same procedure recursively on the set Si.

Gradient boosting

Gradient boosting is a machine learning technique used in regression and classification tasks, among others. It gives a prediction model in the form of an ensemble of weak prediction models, which are typically decision trees.[1][2] When a decision tree is the weak learner, the resulting algorithm is called gradient-boosted trees; it usually outperforms random forest.A gradient-boosted trees model is built in a stage-wise fashion as in other boosting methods, but it generalizes the other methods by allowing optimization of an arbitrary differentiable loss function.

K-Nearest Neighbors (KNN)

- ➢ Simple, but a very powerful classification algorithm
- ➢ Classifies based on a similarity measure
- ➢ Non-parametric
- ➢ Lazy learning
- ➢ Does not “learn” until the test example is given
- ➢ Whenever we have a new data to classify, we find its K-nearest neighbors from the training data

Example

- ➢ Training dataset consists of k-closest examples in feature space
- ➢ Feature space means, space with categorization variables (non-metric variables)
- ➢ Learning based on instances, and thus also works lazily because instance close to the input vector for test or prediction may take time to occur in the training dataset

Logistic regression Classifiers

Logistic regression analysis studies the association between a categorical dependent variable and a set of independent (explanatory) variables. The name *logistic regression* is used when the dependent variable has only two values, such as 0 and 1 or Yes and No. The name *multinomial logistic regression* is usually reserved for the case when the dependent variable has three or more unique values, such as Married, Single, Divorced, or Widowed. Although the type of data used for the dependent variable is different from that of multiple regression, the practical use of the procedure is similar.

Logistic regression competes with discriminant analysis as a method for analyzing categorical-response variables. Many statisticians feel that logistic regression is more versatile and better suited for modeling most situations than is discriminant analysis. This is because logistic regression does not assume that the independent variables are normally distributed, as discriminant analysis does.

This program computes binary logistic regression and multinomial logistic regression on both numeric and categorical independent variables. It reports on the regression equation as well as the goodness of fit, odds ratios, confidence limits, likelihood, and deviance. It performs a comprehensive residual analysis including diagnostic residual reports and plots. It can perform an independent variable subset selection search, looking for the best regression model with the fewest independent variables. It provides confidence intervals on predicted values and provides ROC curves to help determine the best cutoff point for classification. It allows you to validate your results by automatically classifying rows that are not used during the analysis.

Naïve Bayes

The naive bayes approach is a supervised learning method which is based on a simplistic hypothesis: it assumes that the presence (or absence) of a particular feature of a class is unrelated to the presence (or absence) of any other feature .

Yet, despite this, it appears robust and efficient. Its performance is comparable to other supervised learning techniques. Various reasons have been advanced in the literature. In this tutorial, we highlight an explanation based on the representation bias. The naive bayes classifier is a linear classifier, as well as linear discriminant analysis, logistic regression or linear SVM (support vector machine). The difference lies on the method of estimating the parameters of the classifier (the learning bias).

While the Naive Bayes classifier is widely used in the research world, it is not widespread among practitioners which want to obtain usable results. On the one hand, the researchers found especially it is very easy to program and implement it, its parameters are easy to estimate, learning is very fast even on very large databases, its accuracy is reasonably good in comparison to the other approaches. On the other hand, the final users do not obtain a model easy to interpret and deploy, they does not understand the interest of such a technique.

Thus, we introduce in a new presentation of the results of the learning process. The classifier is easier to understand, and its deployment is also made easier. In the first part of this tutorial, we present some theoretical aspects of the naive bayes classifier. Then, we implement the approach on a dataset with Tanagra. We compare the obtained results (the parameters of the model) to those obtained with other linear approaches such as the logistic regression, the linear discriminant analysis and the linear SVM. We note that the results are highly consistent. This largely explains the good performance of the method in comparison to others. In the second part, we use various tools on the same dataset (Weka 3.6.0, R 2.9.2, Knime 2.1.1, Orange 2.0b and RapidMiner 4.6.0). We try above all to understand the obtained results.

Random Forest

Random forests or random decision forests are an ensemble learning method for classification, regression and other tasks that operates by constructing a multitude of decision trees at training time. For classification tasks, the output of the random forest is the class selected by most trees. For regression tasks, the mean or average prediction of the individual trees is returned. Random decision forests correct for decision trees' habit of overfitting to their training set. Random forests generally outperform decision trees, but their accuracy is lower than gradient boosted trees. However, data characteristics can affect their performance.

The first algorithm for random decision forests was created in 1995 by Tin Kam Ho[1] using the random subspace method, which, in Ho's formulation, is a way to implement the "stochastic discrimination" approach to classification proposed by Eugene Kleinberg.

An extension of the algorithm was developed by Leo Breiman and Adele Cutler, who registered "Random Forests" as a trademark in 2006 (as of 2019, owned by Minitab, Inc.).The extension combines Breiman's "bagging" idea and random selection of features, introduced first by Ho[1] and later independently by Amit and Geman[13] in order to construct a collection of decision trees with controlled variance.

Random forests are frequently used as "blackbox" models in businesses, as they generate reasonable predictions across a wide range of data while requiring little configuration.

SVM

In classification tasks a discriminant machine learning technique aims at finding, based on an *independent and identically distributed* (*iid*) training dataset, a discriminant function that can correctly predict labels for newly acquired instances. Unlike generative machine learning approaches, which require computations of conditional probability distributions, a discriminant classification function takes a data point *x* and assigns it to one of the different classes that are a part of the classification task. Less powerful than generative approaches, which are mostly used when prediction involves outlier detection, discriminant approaches require fewer computational resources and less training data, especially for a multidimensional feature space and when only posterior probabilities are needed. From a geometric perspective, learning a classifier is equivalent to finding the equation for a multidimensional surface that best separates the different classes in the feature space.

SVM is a discriminant technique, and, because it solves the convex optimization problem analytically, it always returns the same optimal hyperplane parameter—in contrast to *genetic algorithms* (*GAs*) or *perceptrons*, both of which are widely used for classification in machine learning. For perceptrons, solutions are highly dependent on the initialization and termination criteria. For a specific kernel that transforms the data from the input space to the feature space, training returns uniquely defined SVM model parameters for a given training set, whereas the perceptron and GA classifier models are different each time training is initialized. The aim of GAs and perceptrons is only to minimize error during training, which will translate into several hyperplanes' meeting this requirement.

VI. CONCLUSION

The ability to protect SCADA-based IIOT networks against cyber attacks increases their trustworthiness. The existing security methods along with machine learning algorithms were inefficient and inaccurate for protecting IIOT networks. In this article, we proposed a cyber attacks detection mechanism using enhanced deep and ensemble learning in a SCADA-based IIOT network. The proposed mechanism is reliable and accurate because an ensemble detection model was built using a combination of the PRU and the DT. The proposed method was evaluated across 15 datasets generated from a SCADA-based network, and a considerable increase in terms of classification accuracy was obtained. Compared to state-of-the-art techniques, the obtained outcomes of our method exhibited a good balance between reliability, trustworthiness, classification accuracy, and model complexity, resulting in improved performance.

In the future, we will employ more powerful deep learning models to further improve trustworthiness by detecting cyber attacks accurately. In addition, we will try to formulate and assess its performance in real-world scenarios. Also, we will work on the selection of optimal features in scenarios when the features are not sufficient.

VII. REFERENCES

[1] Y. Luo, Y. Duan, W. Li, P. Pace, and G. Fortino, "A novel mobile and hierarchical data transmission architecture for smart factories," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3534–3546, Aug. 2018.

[2] C. Gavriluta, C. Boudinet, F. Kupzog, A. Gomez-Exposito, and R. Caire, "Cyber-physical framework for emulating distributed control systems in smart grids," *Int. J. Elect. Power Energy Syst.*, vol. 114, 2020,Art. no. 105375.

[3] M. S. Mahmoud, M. M. Hamdan, and U. A. Baroudi, "Modeling and control of cyber-physical systems subject to cyber attacks: A survey of recent advances and challenges," *Neurocomputing*, vol. 338, pp. 101–115, 2019.

[4] T. Wang, G. Zhang, M. Z. A. Bhuiyan, A. Liu, W. Jia, and M. Xie, "A novel trust mechanism based on fog computing in sensor–cloud system," *Future Gener. Comput. Syst.*, vol. 109, pp. 573–582, 2020.

[5] K. Guo et al., "MDMaaS: Medical-assisted diagnosis model as a service with artificial intelligence and trust," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2102–2114, Mar. 2020.

[6] M. Al-Hawawreh and E. Sitnikova, "Developing a security testbed for industrial Internet of Things," *IEEE Internet of Things J.*, vol. 8, no. 7, pp. 5558–5573, Apr. 2021.

[7] M. A. Shahriar et al., "Modelling attacks in blockchain systems using petri nets," in *Proc. IEEE 19th Int. Conf. Trust Secur. Privacy Comput. Commun.*, 2020, pp. 1069–1078.

[8] M. Abdel-Basset, V. Chang, H. Hawash, R. K. Chakrabortty, and M. Ryan, "Deep-IFS: Intrusion detection approach for IIoT traffic in fog environment," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7704–7715, Nov. 2021.

[9] S. Huda, J. Abawajy, B. Al-Rubaie, L. Pan, and M. M. Hassan, "Automatic

extraction and integration of behavioural indicators of malware for protection of cyber–physical networks," *Future Gener. Comput. Syst.*, vol. 101, pp. 1247–1258, 2019.

[10] Information Technology-Security Techniques-Information Security Risk Management, ISO/IEC 27005:2018, 2018.

[11] X. Yan, Y. Xu, X. Xing, B. Cui, Z. Guo, and T. Guo, "Trustworthy network anomaly detection based on an adaptive learning rate and momentum in IIoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6182–6192, Sep. 2020.

[12] D. Wu, Z. Jiang, X. Xie, X. Wei, W. Yu, and R. Li, "LSTM learning with Bayesian and Gaussian processing for anomaly detection in industrial IoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 8, pp. 5244–5253, Aug. 2020.

[13] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in *Proc. Mil. Commun. Inf. Syst. Conf.*, 2015, pp. 1–6.

[14] M. M. Hassan, A. Gumaei, S. Huda, and A. Almogren, "Increasing the trustworthiness in the industrial IoT networks through a reliable cyberattack detection model," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6154–6162, Sep. 2020.

[15] A. N. Jahromi et al., "An improved two-hidden-layer extreme learning machine for malware hunting," *Comput. Secur.*, vol. 89, 2020, Art. no. 101655.

[16] S. T. U. Shah, J. Li, Z. Guo, G. Li, and Q. Zhou, "DDFL: A deep dual function learning-based model for recommender systems," in *Proc. Int. Conf. Database Syst. Adv. Appl.*, 2020, pp. 590–606.

[17] R. C. B. Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyberattack discrimination," in *Proc. 7th Int. Symp. Resilient Control Syst.*, 2014, pp. 1–8.

[18] A. Derhab et al., "Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security," *Sensors*, vol. 19, no. 14, 2019, Art. no. 3119.

[19] S. Mehta, R. Koncel-Kedziorski, M. Rastegari, and H. Hajishirzi, "Pyramidal recurrent unit for language modeling," in *Proc. Conf. Empirical Methods Natural Lang. Process.*, 2018, pp. 4620–4630.

[20] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," 2014, *arXiv:1412.6980*.

[21] P. Refaeilzadeh, L. Tang, and H. Liu, "Cross-validation," *Encyclopedia*

Database Syst., vol. 5, pp. 532–538, 2009.

[22] G.W. Zeoli and T. S. Fong, “Performance of a two-sample Mann-Whitney nonparametric detector in a radar application,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-7, no. 5, pp. 951–959, Sep. 1971.