International Research Journal of Parroha (IRJP)
Volume 02, Issue 02, 2023. pp. 93-104
https://doi.org/10.61916/prmn.2023.v02i01.009
Research Article

An Artificial Intelligence (AI) Enabled Framework for Cyber Security Using Machine Learning Techniques

Syed Shabbeer Ahmad[1], Krishna Prasad K[2]

[1]*Post-Doctoral Research Scholar, Srinivas University, Mangalore, India*

[2]Professor, Institute of Engineering and Technology, Srinivas University, Mangalore, India

ARTICLE INFO

Corresponding Author
Krishna Prasad K

Email
krishnaprasadkcci@srinivasuniversity.edu.in

Article History
Received: 18 September 2023
Accepted: 20 October 2023

Orcid
https://orcid.org/0009-0000-9728-8474

Cite
Ahmad, S.S. & Krishna Prasad, K. (2023). Madheshi Contribution in Nepali Education: Empowering Minds and Transforming Communities. *International Research Journal of Parroha (IRJP), 2*(1), 93-104. https://doi.org/ 10.5281/zenodo.10250960

ABSTRACT

Cyber security has become very important aspect with respect to security in the contemporary era. The rationale behind this is that, with the emergence of Internet of Things (IoT) use cases, there are millions of connected devices that play crucial role in different applications. Cyber-attacks have been increasing due to the benefits to attackers or adversaries in different means. Therefore, there is need for continuous effort to safeguard cyber space. With respect to different IoT use cases, it is essential to have better solution that is based on machine learning techniques. In this paper an Artificial Intelligence (AI) enabled framework is built for cyber security. The framework is extendible in nature which can support future developments in classifiers. The framework also supports machine learning (ML) models along with feature selection towards cyber security. In other words, it provides support for an AI approach towards safeguarding cyber security. The proposed system is made up of both ML models so as to leverage protection from time to time. It is a generic framework that can be used for any IoT use case provided the inputs from that network of IoT application. The proposed system is made up of both ML models so as to leverage protection from time to time. It is a generic framework that can be used for any IoT use case provided the inputs from that network of IoT application. We proposed an algorithm known as Machine Learning Pipeline for Cyber Attack Detection (MLP-CAD). Experimental results showed that the ML pipeline with underlying techniques could provide better performance. Highest accuracy is achieved by Random Forest with 95.97% accuracy.

Keywords: *Machine learning, Cyber security, AI, IoT, Random forest, Framework, Intrusion detection*

Introduction

Cyber security if found an important security requirement in the contemporary era. Moreover, network traffics are ever increasing and in the IoT use cases, it is more so, therefore, there is need for machine learning and automated approaches rather than other alternatives. When there is an associated system that learns from the network traffics, over a period of time, the learning will have sufficient training samples so as to detect attacks accurately and with automated system. Another important observation in the literature is that different IoT use cases exist in the real world without sufficient security in place. Yet another observation in the literature is that the existing solutions are based on particular techniques and there is need for a comprehensive cyber security framework that leverages AI in the form of ML and deep learning techniques. Different AI enabled approaches have

Copyright (c) 2023: Author(s). Published by Parroha Multiple Campus

been studied from the literature. It is understood that there is need for reusable framework that leverages cyber security in IoT use cases. Literature (Said et al., 2020: Buczak at al., 2015: Diro et al., 2018: H.I. Kure, et al. 2022: Manikandan et al., 2021: Sivanathan et al., 2028: V.G. Promyslov et al., 2019: Z. Li., 2021: R.C. Nunes et al., 2019: T. Saha et al., 2021: S.M. de Lima et al., 2021: Kelton et al, 2019: M. Almiani et al., 2021: T. Sawik et al., 2022 & Ahmad Ali Al Zubi et al., 2021) is rich in providing different machine learning based approaches to detect different kinds of attacks. However, a comprehensive framework that is holistic in nature with supervised learning methods and ability to analyse live network flows from IoT use cases is highly desired.

Problem Statement

The study of the literature from has provided very useful insights. The insights are summarized here. Cyber security if found an important security requirement in the contemporary era. Moreover, network traffics are ever increasing and in the IoT use cases, it is more so, therefore, there is need for machine learning and automated approaches rather than other alternatives. When there is an associated system that learns from the network traffics, over a period of time, the learning will have sufficient training samples so as to detect attacks accurately and with automated system. Another important observation in the literature is that different IoT use cases exist in the real world without sufficient security in place. Yet another observation in the literature is that the existing solutions are based on particular techniques. It is understood that there is need for reusable framework that leverages cyber security in IoT use cases.

Research Objective

Our contributions in this paper are as follows.

1. To construct a framework for improving cyber security using machine learning techniques.
2. To design an algorithm known as Machine Learning Pipeline for Cyber Attack Detection (MLP- CAD) for automatic detection of cyber-attacks on IoT use case.

We made comparative study of different ML models and found their performance dynamics. The remainder of the paper is structured as follows. Section 2 reviews literature on existing ML models for cyber security. Section 3 presents the proposed framework with underlying algorithm. Section 4 presents results of our empirical study. Section 5 concludes our work besides giving scope for future research.

Literature Review

This section reviews important literature on different existing methods used for cyber security. Said et al. (2020) explored the need for machine learning techniques for cyber security enhancement. Their work includes both ML and deep learning models towards improving cybersecurity. Ibitoye et al. (2015) proposed a deep learning technique for intrusion detection. It was designed to have a defence model for IoT networks. Diro et al. (2018) studied a distributed approach using ML for automatic detection of attacks. Alrashdi et al. (2022) proposed a methodology for IoT security using ML techniques. It is based on the use case of IoT pertaining to smart city where there are several vulnerabilities. Bahs et al. (2021) focused on IoT botnet detection using ML techniques. It is supported by their proposed approach towards dimensionality reduction process. Ge et al. (2018) explored an intrusion detection model for cyber security. They studied IoT networks, their vulnerabilities besides proposing an intrusion detection framework. Hussain et al. (2019) found that IoT security can be enhanced using ML models. Their research has revealed state of the art and directions for future scope of the research.

Kelton et al. (2021) investigated on different methodologies in which ML approach is used for intrusion detection. It was made to provide valuable insights on cyber security dynamics. Doshi et al. (2019) proposed ML based framework for detection of DDoS attacks that threaten cyber security in distributed applications. Kilincer et al. (2021) explored different datasets and ML models existing for cyber-attack detection. AlZubi et al. (2021) considered cyber-physical system in healthcare domain to perform research on cyber security. They proposed an attack detection model based on ML techniques. Strecker et al. (2019) also focused on ML-driven solution to cyber-attacks. Abdallah et al. (2021) used supervised learning

mechanisms to deal with intrusion detection in network systems. Leon et al. (2022) made a comparative study of different ML model used for intrusion detection. Mishra and Tyag (2021) studied the importance and role of ML models in security of IoT based cloud assisted applications. From the literature, it is understood the importance of ML models and need for further improvement of the state of the art for cyber security.

Proposed Framework

Methodology

This section throws light into different aspects involved in the project and its implementation. It focuses on the modus operandi of its functionality. It illustrates an extendible AI framework based on ML techniques to have cyber security to IoT use cases. The conceptual framework of the proposed system includes extensive literature review to arrive at the present state of the art. Based on the insights, it is possible to fine tune requirements further. The implementation of project is based on ML techniques used with an extendible framework that supports future innovations as well. After prototype is built and tested, it is evaluated and improved it further to have a product with commercial value. Figure 1 shows the broad overview of the approach used in the system prior to elaborating it further more minute details.

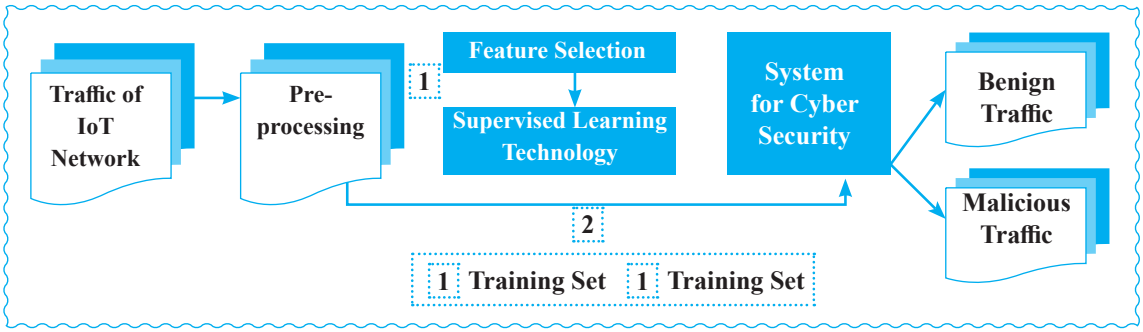

Figure 1: Shows the Broad Overview of the Proposed System for AI based Cyber Security

The system overall architecture shows a simple and effective phenomenon for detection of malicious traffic (due to attacks) in IoT use cases. The traffic is examined for any malicious patterns. Based on this malicious traffic is identified and such data will be used, as the time elapses, as training data. The training data is subjected to feature selection in order to have better performance. The feature selection process identifies the features, out of all available features, that can contribute to the determination of class labels in the supervised learning process. After training with a machine leaning or deal learning classifier, it results a knowledge model that enables AI based cyber security. More details of the proposed framework are given in Figure 2.

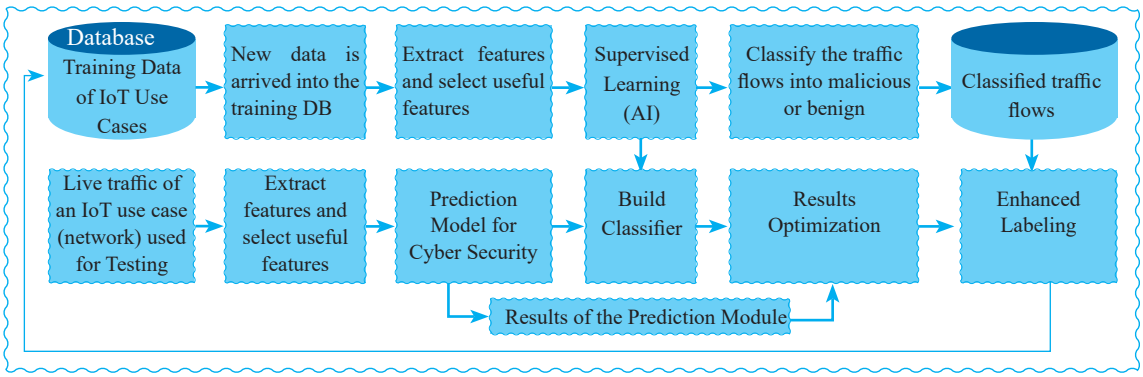

Figure 2: The AI Framework for Cyber Security with More Details

The network traffic of IoT use case is continuously monitored by the framework and the results of classification are used to increase training dataset so as to leverage performance as time elapses. It is gradually overcome any data insufficiency problem with training dataset, often known as cold start issue. The results of testing phase are evaluated and sent to training database so as to increase number of training samples (network flows). As the training data increased, it results in quality of training and thus testing accuracy gets improved as well. When new training samples arrive, they are evaluated and when live traffic data comes from an IoT use case, the data is continuously monitored and the traffic patterns are classified. The system supports any classifier that is based on supervised learning approach. It is extendible so as to support future classifiers as well. Once the samples are classified, they are optimized in terms of validating class labels and then the training database gets updated. Thus, there are two procedures running one for online and one for offline. Online means when new test data (live network traffic arrives) and offline means that is a continuous process irrespective of new traffic to enhance its database. It may be supported by human experts to add samples continuously to database to get validated and increase training samples from time to time.

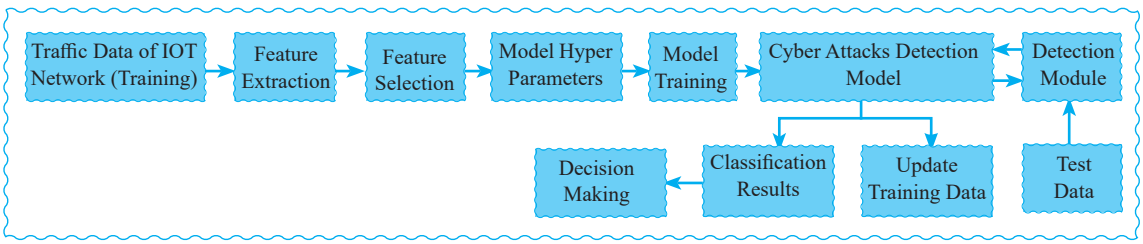

Figure 3: Technical Details Pertaining to the Proposed System

Figure 3 shows the technical details of the proposed system. It shows that there is training data pertaining to IoT network traffic given as input to the system. Then the system extracts feature from the training data. As all features may not be suitable for class label selection, there is feature selection module that takes the extracted features and selects features that are useful for determination of class labels. The framework supports any classification model (supervised learning) which may have different hyper parameters. Such hyper parameters are tuned in order to have better outcomes. Then the training is given to the selected model (classifier). The results of training are the cyber-attacks detection model. When live data arrives from IoT network, that is given to the detection module which consults the cyber-attacks detection model in order to classify traffic. After classification, the training data is updated with new labeled samples. The classification results can be used to make well informed decisions.

Algorithm: Machine Learning Pipeline for Cyber Attack Detection (MLP-CAD)
Input: UNSW-NB15 dataset D, ML models for cyber security M
Output: Results R

1. Start
2. T1 ← Get Data For Training(D)
3. T2 ← Get Data For Testing(D)
4. F ← Find Featuress (T1)
5. For each ML model m in pipeline of models M
6. m ← Train Model (F)
7. For each network flow in T2
8. R ← Test Model (m, T2)
9. Display R
10. Evaluate performance
11. Display performance statistics
12. End For
13. End For

Algorithm 1: Machine Learning Pipeline for Cyber Attack Detection (MLP-CAD)

As presented in Algorithm 1, it takes different ML models as pipeline along with dataset used for experiments. It performs pre-process in order to differentiate training and testing data for further supervised learning process. It extracts features from the training dataset referred to as T1. Afterwards, there is an iterative process in which each model is trained with the extracted features and the learned model is used to detect intrusions or cyber-attacks. After completion of the algorithm, the output includes attack detection for each test instance and overall performance of different ML models.

Results and Discussion

This section presents experimental results in terms of data dynamics, feature importance, partial dependence of features on class labels and cyber-attack detection performance among different ML models. UNSW-NB15 dataset [16] is used for empirical study.

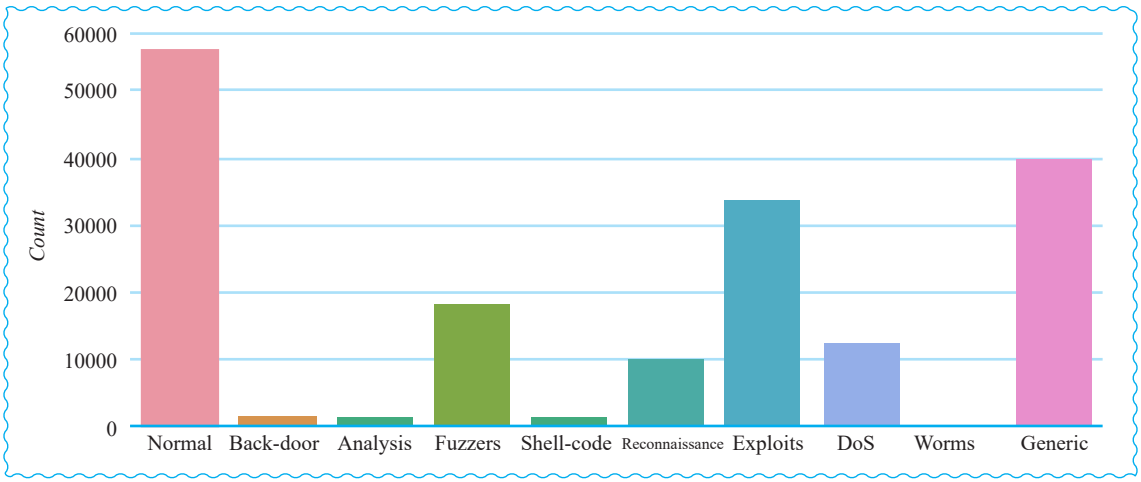

Figure 4: Shows attack distribution in the dataset

As presented in Figure 4, there are different kinds of attacks found in the dataset used for experiments. For each attack, number of instances is provided.

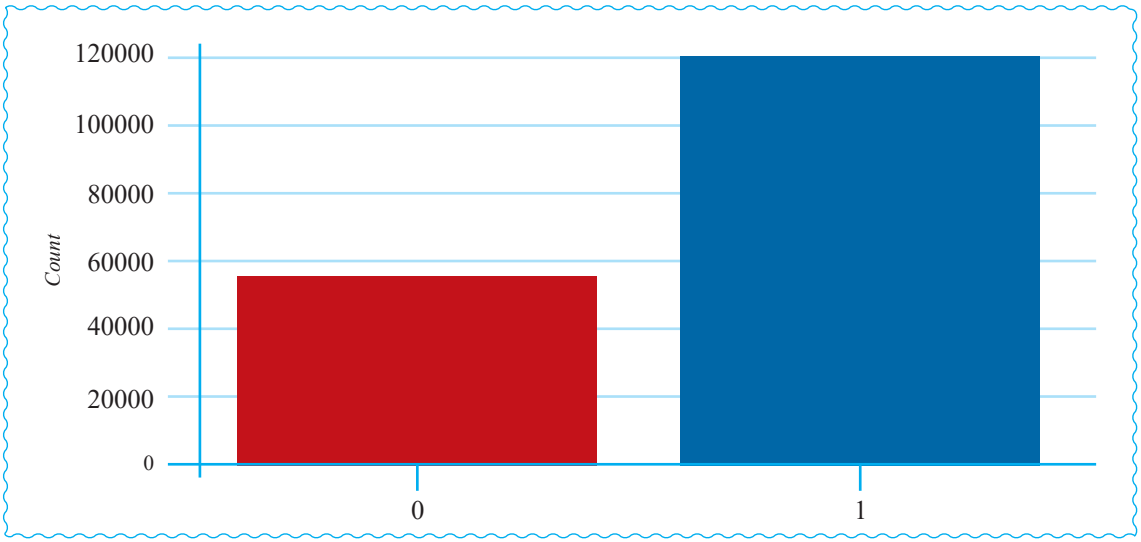

Figure 5: Shows Attack and Normal Traffic Flows Distribution in the Dataset

As presented in Figure 5, it shows number of attack instance and normal instances provided in the given dataset. Attack instance and normal instance are denoted by 1 and 0 respectively.

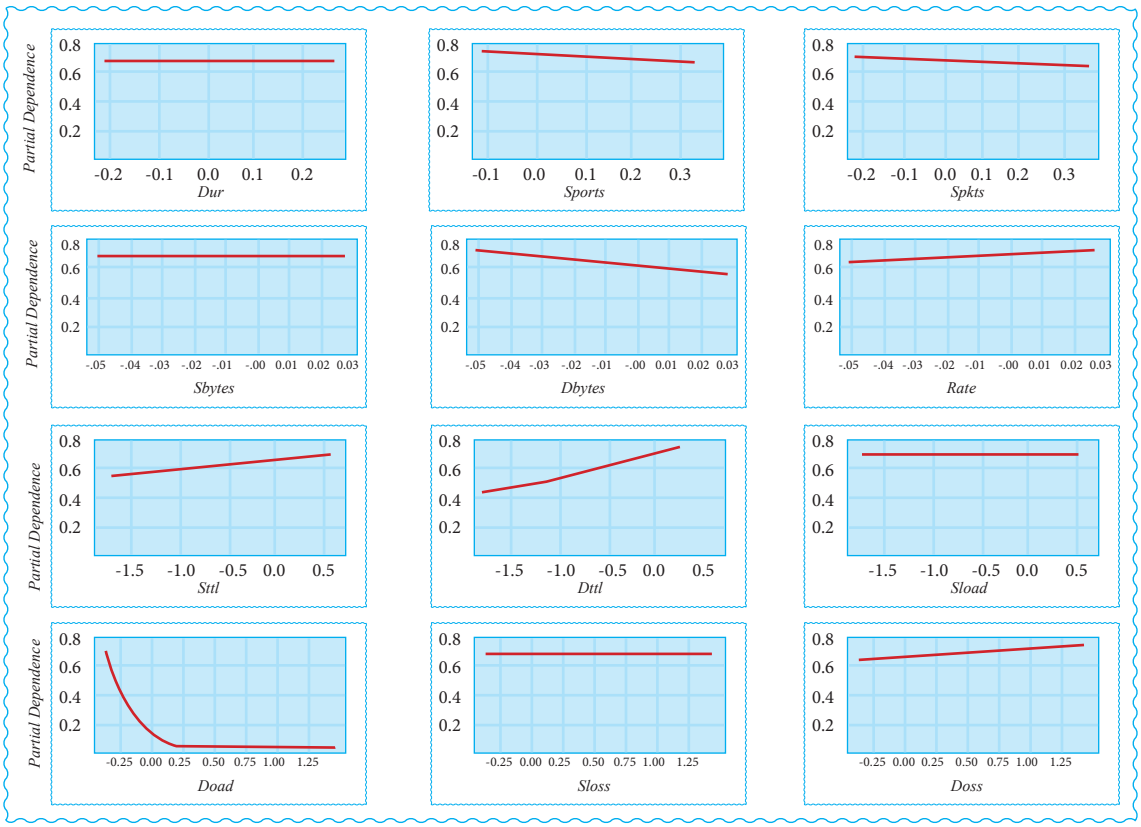

Figure 6: Shows Partial Dependence on Class Labels on Different Features Using Logistic Regression model

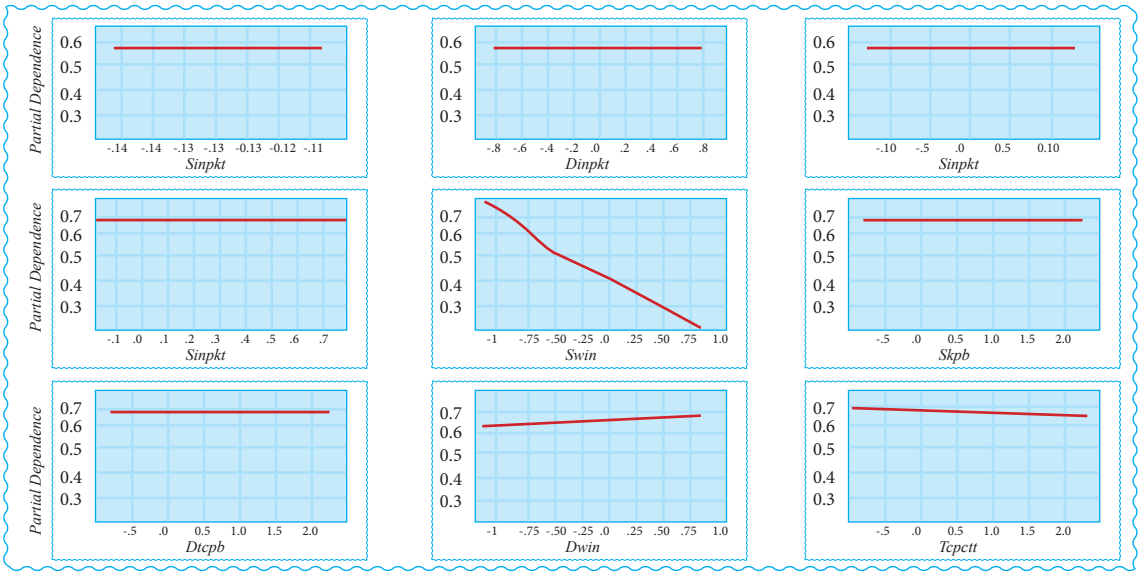

Figure 7: Shows Partial Dependence on Class Labels on Different Features Using Logistic Regression Model

As presented in Figure 7, partial dependence on class labels on different features using Logistic Regression model is provided.

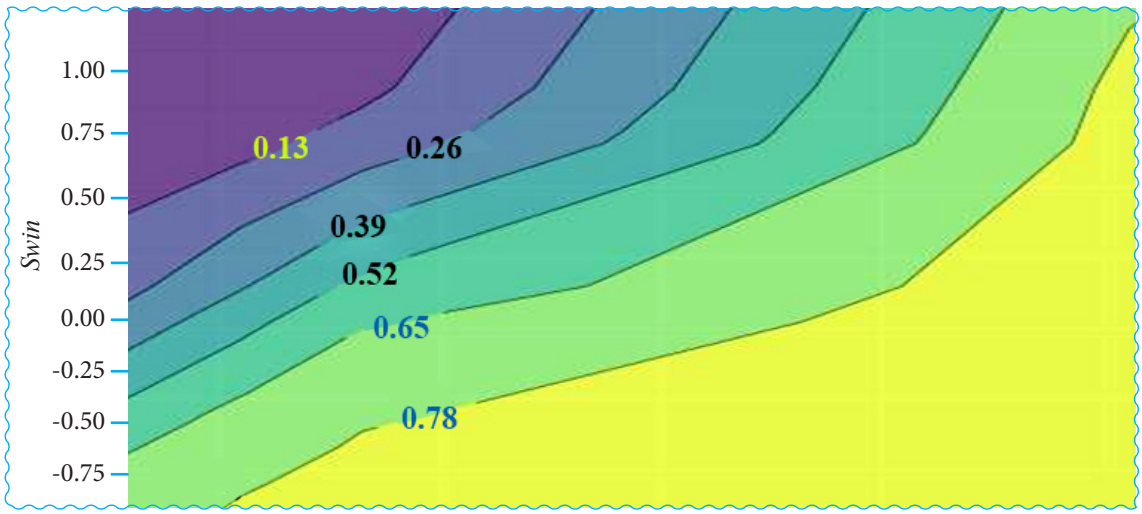

Figure 8: Shows Partial Dependence on Class Labels on dttl vs. Swin Features Using Logistic Regression Model

As presented in Figure 8, partial dependence on class labels on dttl vs. swin features using Logistic Regression model is provided.

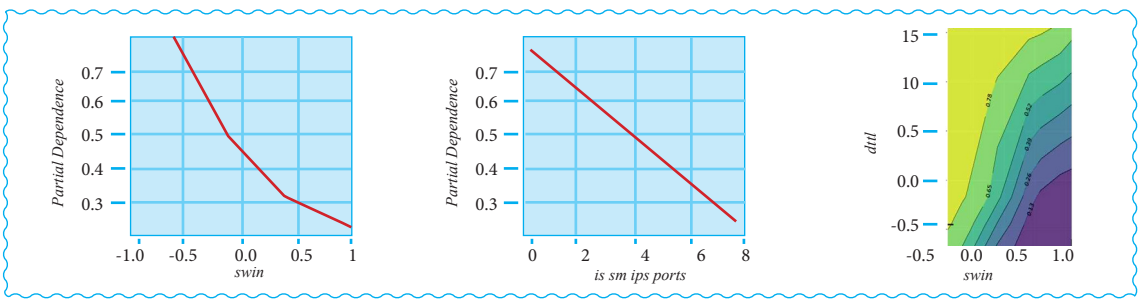

Figure 9: Shows Partial Dependence on Class Labels on dttl vs. Swin Features Using Logistic Regression Model Reflecting one Way and Two Way Approaches

As presented in Figure 9, partial dependence on class labels on dttl vs. swin features using Logistic Regression model is provided reflecting one way and two way approaches.

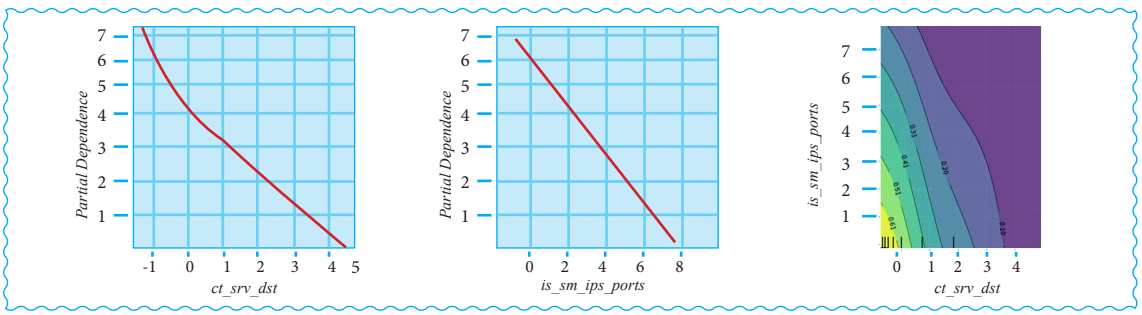

Figure 10: Shows Partial Dependence on Class Labels on ct_srv_dst vs. is_sm_ips_ports Features Using Logistic Regression Model Reflecting One Way and Two Way Approaches

As presented in Figure 10, partial dependence on class labels on ct_srv_dst vs. is_sm_ips_ports features using Logistic Regression model is provided reflecting one way and two way approaches.

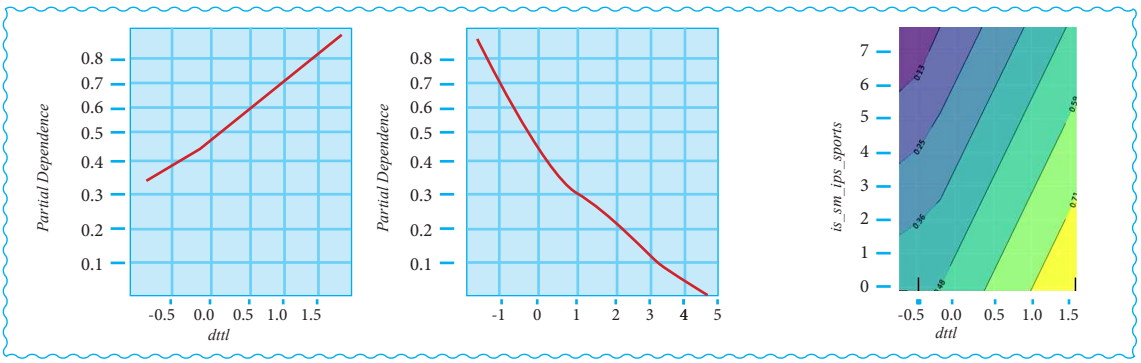

Figure 11: Shows Partial Dependence on Class Labels on ct_srv_dst vs. dttl Features Using Logistic Regression Model Reflecting one Way and Two Way Approaches

As presented in Figure 11, partial dependence on class labels on ct_srv_dst vs. dttl features using Logistic Regression model is provided reflecting one way and two way approaches.

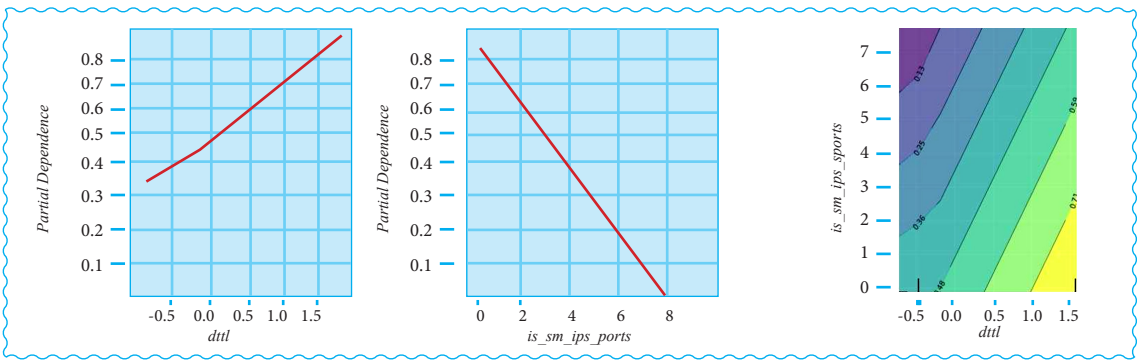

Figure 12: Shows Partial Dependence on Class Labels on is_sm_ips_ports vs. dttl Features Using Logistic Regression Model Reflecting One Way and Two Way Approaches

As presented in Figure 12, partial dependence on class labels on is_sm_ips_ports vs. dttl features using Logistic Regression model is provided reflecting one way and two way approaches.

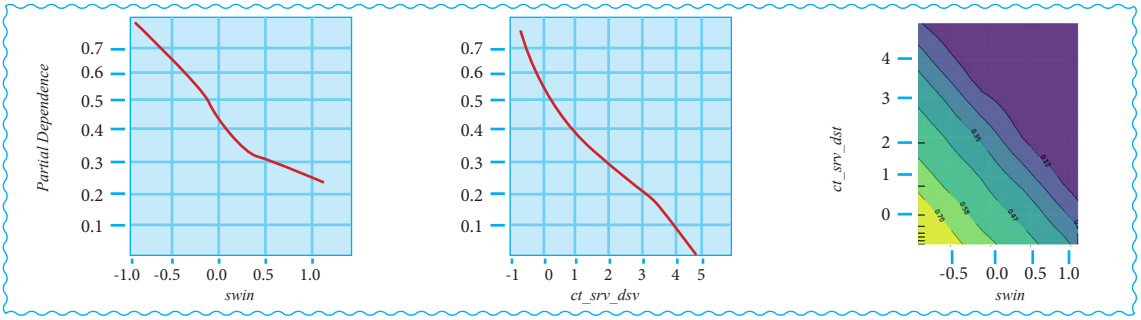

Figure 13: Shows Partial Dependence on Class Labels on ct_srv_dst vs. swin Features Using Logistic Regression Model Reflecting One Way and Two Way Approaches

As presented in Figure 13, partial dependence on class labels on ct_srv_dst vs. swin features using

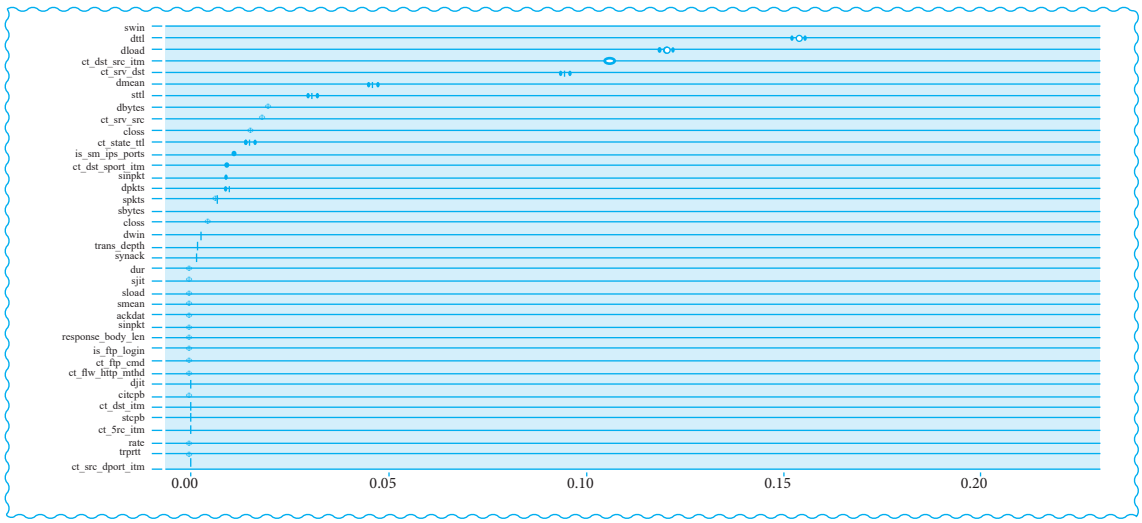

Figure 14: Feature importance of training dataset

Logistic Regression model is provided reflecting one way and two way approaches. As presented in Figure 14, feature importance is computed and visualized for different features in the dataset. Higher importance indicates more capability of feature in predicting class labels on training data.

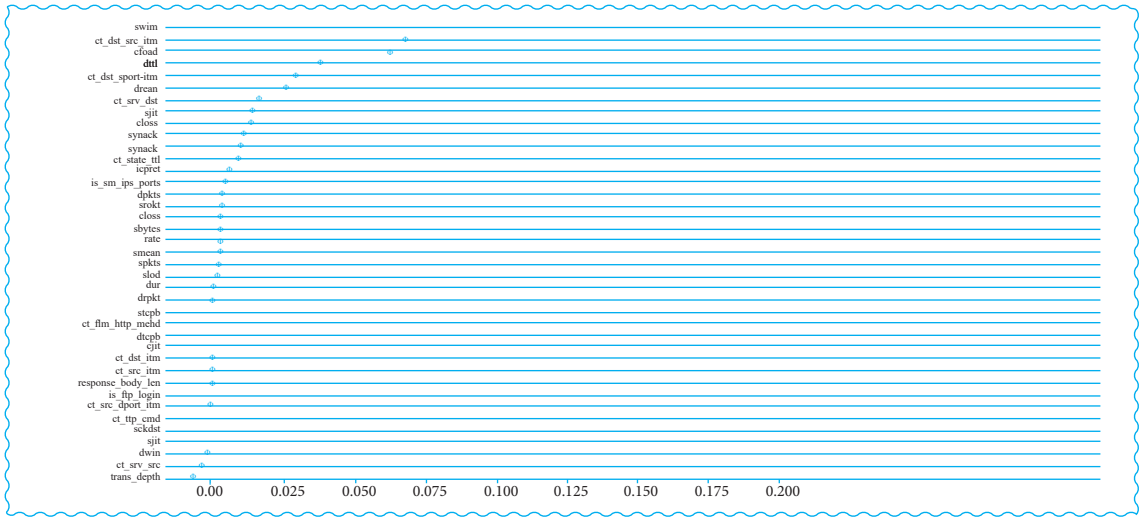

Figure 15: Feature importance of testing dataset

Table 1: Shows performance comparison

Prediction Model	Performance (%)			
	Accuracy	Precision	Recall	F1-Score
Random Forest	0.9597	0.963	0.9783	0.9706
Decision Tree	0.9485	0.9629	0.9614	0.9621
Multi Layer Perception	0.9472	0.9555	0.9676	0.9614
Logistic Regression	0.9274	0.9129	0.9874	0.9487

ML models is provided with different metrics.

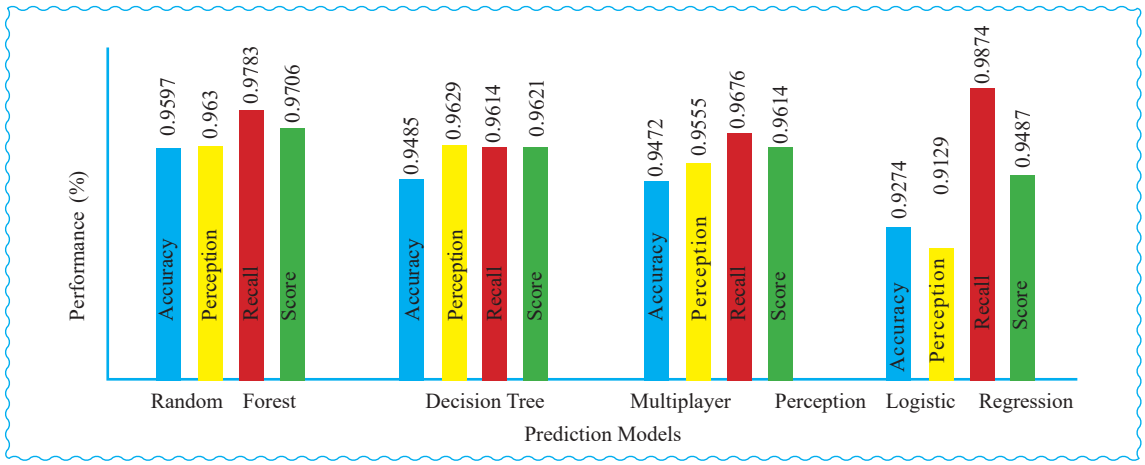

Figure 16: Cyber-attack detection performance of different models

As presented in Figure 16, the proposed framework is evaluated. The proposed algorithm exploits 4 ML models in pipeline. Each model is found to have different performance due to its internal mechanisms. The accuracy of Logistic Regression is least with 92.74% accuracy. Performance of MLP is 94.72% while Decision Tree exhibited 94.85% accuracy. Highest performance is exhibited by Random Forest model with 95.97%.

Recommendations

1. In future we incorporate Deep learning models in the proposed framework for improving its performance further.
2. In future research may use this present work as a reference to address AI-based cyber security issues in the context of Industry 4.0.
3. Future work in this area, there is a need for constant updating of the requirements to implement cyber security actions, arising from the cybernetic technological evolution applied for both defense and attack in the context of the Industry 4.0 ecosystem.

Conclusion

In this paper an Artificial Intelligence (AI) enabled framework is built for cyber security. The framework is extendible in nature which can support future developments in classifiers. The framework also supports machine learning (ML) models along with feature selection towards cyber security. In other words, it provides support for an AI approach towards safeguarding cyber security. The proposed system is made up of both ML models so as to leverage protection from time to time. It is a generic framework that can be used for any IoT use case provided the inputs from that network of IoT application. We proposed an algorithm known as Machine Learning Pipeline for Cyber Attack Detection (MLP-CAD). Experimental results showed that the ML pipeline with underlying techniques could provide better performance. Highest accuracy is achieved by Random Forest with 95.97% accuracy.

Reference

A. Shah., R. Ganesan., S. Jajodia., H. Cam. (2018). Dynamic optimization of the level of operational effectiveness of a CSOC under adverse conditions: ACM Trans. Intell. Syst. Technol, 9 (5) , 1–20. Google Scholar

Ahmad Ali Al Zubi., Mohammed Al- Maitah., Abdul aziz Alarifi. (2021). Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques: Soft Computing, 25(18), 12319-12332. Google Scholar

Buczak, A.L., Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection: IEEE Commun. *Surv. Tutor*, 18(2), 1153–1176 . Google Scholar

C. Iwendi., S.U. Rehman., A.R. Javed., S. Khan., G. Srivastava.(2021). Sustainable security for the internet of things using artificial intelligence architectures: ACM Trans. *Internet Technol*, 21 (3), 1–22. Google Scholar

Chandrasekhar, G., Sahin, F. A survey on feature selection methods. Comput. *Electr. Eng*. 40(1),. Google Scholar

Diro, A. A., Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, 82(6), 761–768. Google Scholar

Emad E., Abdallah., Wafa Eleisah., Ahmed Fawzi Otoom. (2022). Intrusion Detection Systems using Supervised Machine Learning Techniques: A survey. *Procedia Computer Science* ,201 (2022) 205–212. Google Scholar

H. Liu., C. Zhong., A. Alnusair., S.R. Islam.(2021). A framework for enhancing AI Explain ability of intrusion detection results using data cleaning techniques: J. *Netw. Syst. Manag*. 29 (4) 1–30. Google Scholar

H.I. Kure., S. Islam., M. Ghazanfar., A. Raza, M. Pasha.(2022). Asset criticality and risk prediction for an effective cyber security risk management of cyber-physical system Neural Comput. *App*., 34 (1) , 493-51. Google Scholar

H.K. Kim., K.H. Im., S.C. Park.(2010). DSS for computer security incident response applying CBR and collaborative response: Expert Syst. *Appl*, 37 (1) , 852–870. Google Scholar

Husak., T.Bajtoˇs.,J. Kaˇspar., E. Bou-Harb., P. Celeda.(2020). Predictive cyber situational awareness and personalized blacklisting: a sequential rule mining approach: ACM Trans. Manag. *Inf. Syst*, 11 (4) , 1–6. Google Scholar

Kelton A.P. da Costaa ., João P. Papaa. , Celso O. Lisboaa ., Roberto Munoz b ., Victor Hugo C., de Albuquerque. (2019). Internet of Things: A survey on machine learning-based intrusion detection approaches: *Elsevier*. Volume 151, 14 March 2019, Pages 147-157. Google Scholar

Krishna Prasad, K and Aithal, P. S. (2017) Two-Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(2), 51-65.

Krishna Prasad, K. & Aithal, P. S. (2017). A Conceptual Study on Fingerprint Thinning Process based on Edge Prediction. *International Journal of Applied Engineering and Management Letters (IJAEML*), 1(2), 98-111.

Krishna Prasad, K. (2016). An Empirical Study on Role of Vedic Mathematics in Improving the Speed of Basic Mathematical Operations. *International Journals of Management, IT & Engineering (IJMIE*), 6(1), 161-171.

Krishna Prasad, K. and Aithal, P. S. (2015). Mobile System for Customized and Ubiquitous Learning by 4G/5G. *International Journal of Management, IT and Engineering*, 5(7), 63-71.

Krishna Prasad, K. and Aithal, P. S. (2016). A Study on Enhancing Mobile Banking Services using Location based Authentication. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 1(1), 48-58.

Krishna Prasad, K. and Aithal, P. S. (2017). A Study on Fingerprint Hash Code Generation Using Euclidean Distance for Identifying a User. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(2), 116-126.

Krishna Prasad, K. and Aithal, P. S. (2017). A Study on Online Education Model Using Location Based Adaptive Mobile Learning. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(1), 36-44,

Krishna Prasad, K., Aithal, P. S. (2017). A Customized and Flexible Ideal Mobile Banking System using 5G Technology. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(1), 25-37.

M. Almiani., A. AbuGhazleh., Y. Jararweh., A. Razaque.(2021). DDoS detection in 5 Genabled IoT networks using deep Kalman back propagation neural network : *Int. J. Mach. Learn. Cybern*, 12 (11) ,3337–3349. Google Scholar

Manikandan, S., Dhanalakshmi, P., Priya, S., Mary Odilya Teena, A. (2021). Intelligent and Deep Learning Collaborative method for E-Learning Educational Platform using Tensor Flow: *Turkish Journal of Computer and Mathematics Education*, 12(10), 2669-2676. Google Scholar

Miguel Leon., Tijana Markovic., Sasikumar Punnekkat. (2022). Comparative Evaluation of Machine Learning Algorithms for Network Intrusion Detection and Attack Classification: *IEEE, IJCNN* 2022, 1-8. Google Scholar

R.C. Nunes., M. Colom´e., F.A. Barcelos., M. Garbin., G.B. Paulus., L.A. Silva.(2019). A case based reasoning approach for the cyber security incident recording and resolution: *Int. J. Softw. Eng. Knowl. Eng*, 11 (12) , 1607–1627. Google Scholar

R.C. Nunes., M. Colom´e., F.A. Barcelos., M. Garbin., G.B. Paulus., L.A. Silva.(2019). A case based reasoning approach for the cyber security incident recording and resolution: *Int. J. Softw. Eng. Know l. Eng*, 11 (12) , 1607–1627. Google Scholar

S.M. de Lima., H.K. Silva., J.H. Luz., H.J. Lima., S.L. Silva., A. de Andrade., A.M. da Silva. (2021). Artificial Intelligence-based antivirus in order to detect malware preventively: *Prog. Artif. Intell*. 10 (1) ,1–22. Google Scholar

Said A. Salloum., Muhammad Alshurideh., Ashraf Elnagar ., Khaled Shaalan. (2020). Machine Learning and Deep Learning Techniques for Cyber security: *A Review. Springer*, 2(11) , 50-57. Google Scholar

Sivanathan., H.H. Gharakheili., F. Loi., A. Radford., C. Wijenayake., A. Vishwanath., V. Sivaraman. (2018). Classifying IoT devices in smart environments using network traffic characteristics : IEEE Trans. *Mobile Comput,* 18 (8) , 1745-1759. Google Scholar

Sneh, M.S. and Krishna Prasad, K. (2018). Analysis of Business Strategies of Salesforce. Com Inc. Analysis of Business Strategies of Salesforce.com Inc. I*nternational Journal of Case Studies in Business, IT and Education (IJCSBE)*, 2(1), 37-44.

T. Saha., N. Aaraj., N. Ajjarapu., N.K. Jha. (2021). Smart hacking approaches for Risk scanning in internet-of-things and cyber-physical systems based on machine learning: I*EEE Trans. Emerg*, 10 (2), 1870–885. Google Scholar

T. Sawik., B. Sawik.(2022). A rough cut cyber security investment using portfolio of security controls with maximum cyber security value: *Int. J. Prod. Res*, 60 (21), 6556–6572. Google Scholar

UNSW-NB15 (UNSQ-NB15) dataset. https://paperswithcode.com/dataset/unsw-nb15

V.G. Promyslov., K.V. Semenkov., A.S. Shumov. (2019). A clustering method of asset cyber security classification: *IFAC-Papers On Line*, 52 (13) , 928–933. Google Scholar

Z. Li., A.L. Rios., L. Trajkovi´c. (2021). Machine learning for detecting anomalies and intrusions in communication networks: *IEEE J. Sel. Areas Commun* , 39 (7) , 2254–2264. Google Scholar