Proposal of a Machine Learning-based Model to Optimize the Detection of Cyber-attacks in the Internet of Things

Cheikhane Seyed, Jeanne roux BILONG NGO, Mbaye KEBE
Laboratory LIRT- Polytechnic Superior School, University Cheikh Anta DIOP (UCAD), Dakar, 10200, Senegal

***Abstract*—In this article, we propose a model to optimize the detection of attacks in IoT. IoT network is a promising technology that connects living and non-living things around the world. Despite the increased development of these technologies, cyber-attacks remains a weakness, making it vulnerable to numerous cyber-attacks. Of course, automatic computer intrusion detection systems are deployed. However, it does not make it possible to mobilize the full potential of Machine Learning. Our approach in this maneuver consists of offering a means to select the least expensive ML method in terms of learning in order to optimize the prediction of threats to introduce IoT objects. To do this, we make modular design based on two layers. The first module is a canvas containing the different methods most used in ML such as supervised learning method, unsupervised learning method and reinforcement learning method. The second module introduces a mechanism to measure the learning cost linked to each of these methods in order to choose the least expensive one in order to quickly and efficiently detect intrusions in IoT objects. To prove the validity of the proposed model, we simulated it using the Weka tool. The results obtained illustrate the following behaviors: The classification quality rate is 93.66%. This last result is supported by a classification consistency rate of 0.882 (close to unity 1) demonstrating a trend towards convergence between observation and prediction.**

***Keywords*—IoT; Machine learning; cyber-security; detection of attacks; weka tool; classification quality and consistency**

I. INTRODUCTION

IoT refers to a network of smart objects around the world via the Internet, allowing them to collect and exchange data without any human interference [1]. However, security in the Internet of Things (IoT) is a major concern because it is susceptible to cyber-attacks like any other network given the proliferation of connected devices and the massive data collection they perform [2].

Intrusion Detection System (IDS) is an effective technique for detecting cyber-attacks in any network. IDS detects cyber-attacks efficiently and quickly at fog nodes compared to the cloud [3]. The IoT network consists of connections between different types of smart objects, ranging from supercomputers to tiny devices that may have very little computing power. It is therefore difficult to secure this type of network and cyber security is therefore a major challenge.

Faced with this new mode of operation of the strike chain, traditional network security is no longer suitable. Certainly, computer systems for automatic intrusion detection are deployed [4, 5]. Most of the latest IDS are based on machine learning algorithm for training and detection of cyber-attacks on the network. However, their conceptual deficiency does not make it possible to mobilize the full potential of Machine Learning.

The problem that arises is that these IDS do not emphasize the impact linked to the learning cost for the ML method used. This can slow down the attack prediction process by choosing an ML method that is inappropriate for the context and environment of IoT objects.

In this context, we propose an approach to boost the detection of attacks by choosing the optimal method in terms of learning cost to provide a prediction of attacks that is fast, efficient and reflects reality.

The contribution consists of proposing a new process framework for integrating ML techniques. This process is based on three pillars. The first is the dynamic dimension of the cyber-attacks chain. This problem is addressed by proposing an updatable dataset in terms of sampling and scoring of variables. The second is the competition process of different existing ML methods. The third is the introduction of cost-sensitive learning using a risk-based cost matrix.

The remainder of this article is organized as follows: Related work is given in Section II, Section III delves into Approach and method, then Section III deals with the proposed modeling, then Section V deals with the methods and materials. Section VI dedicated to the results and discussions and finally we present the conclusion and the perspectives of our work in Section VII.

II. RELATED WORK

Intrusion detection systems are built based on data collected and trained using supervised, semi-supervised and unsupervised learning methods [6]. This article proposes to evaluate the performance of intrusion detection systems over the long term. The objective is to be able to detect still unknown zero-day attacks.

On the other hand, a summary on the analysis of security threats, issues and solutions for Cloud computing uses machine learning algorithms [7]. They are used to overcome security issues of cloud computing in supervised, unsupervised, semi-supervised and hardened modes.

The Internet of Connected Things in the industrial domain (I-IoT) is also an active area of research and is the subject of several studies. The problem of low detection rates and high proportions of false alarms is addressed in this article [7]. The sole objective of this work is to detect and stop cyber-attacks. Concerns about the costs and impact of this detection are not the focus.

The article in [8] makes an important contribution to solving the problem of security of connected objects. An in-depth analysis of the literature is assigned to them. The articles cited in this study certainly differ in their aims and objectives. Some of them approach the question from the reasonable angle of the technical constraints intrinsic to the IoT, notably storage, memory and energy.

Other authors in [9, 10] introduce the notions of layered architecture with or without integration of techniques such as machine learning, artificial intelligence and cryptography. The contextualization of the security issue of connected objects remains reactive and corrective. However, the proposed solutions do not seem to be part of an innovative and proactive methodology.

In the article [11], the authors have access to a review of the typology of anomalies, detection layers, context and methodology. What emerges is an overly simplistic view of anomaly classification. All attacks are classified into a single anomaly category, resulting in only four anomaly types. This represents more than half of the population. In addition, the type of attack is not well specified. More than 90% of articles do not consider context. This further weakens the robustness of the proposed solutions.

The articles in [12,13] shows the need to focus on learning methods for Cyber security in IoT Networks, the quality of the data used and the importance of security issues in free decision-making. This last point is crucial with regard to the cognitive dimension of the proposed solution.

In the paper [14], the authors proposed a cyber-attack detection framework for IoT using the voting-based ensemble learning approach. This idea of ensemble learning like Random Forest (RF) is good, but the process does not include risk-based thinking although it achieves over 97% accuracy.

The authors in [15] proposed several approaches based on recurrent neural networks (RNN) using long short-term memory (LSTM), auto encoders and multi-layer perceptron. For the authors [16], deep learning LSTM is applied with the resampling of an imbalanced dataset. Here again, no risk prioritization or cost discrimination was applied. The overall accuracy rate of 99% did not resolve the impact of individual cyber-attacks.

In the work [17], it is recognized that the IoT cyberspace is like an “unsecured Internet of Things” and that emerging technologies (machine learning, block chain) are key solutions. This survey reveals that there are many problems associated with the use of machine learning techniques. Topics include dataset accuracy and versioning.

However, these articles do not seem to draw attention to the innovative approach of modular analysis and security segregation based on learning costs which prompted us to focus in this research study on the impact of learning cost of ML methods thus influencing the effectiveness of attack predication in IoT.

III. Approach and Methodology

The majority of detection systems are based on classical linear structure learning models (see Fig. 1). That is, we draw a dataset S from an operational IoT network. This data set and the underlying variables describe a particular state of a functional system. Critical security factors may constantly change over time horizon t, with respect to the dynamics of cyber threats. The resulting M-model becomes inappropriate for tracking cyber-attacks due to short-term mutations in the threat process called block chain.

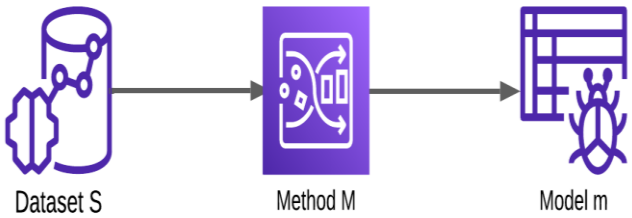

Fig. 1. Classic intrusion detection model.

Viable, reliable and agile machine learning that streamlines operations and strengthens businesses is a very serious and time-consuming task [18]. Indeed, this approach to cyber security modeling does not call into question the improvement in algorithmic performance delivered by a one-way learning method. As a result, we will not be able to capitalize on the differential advantage offered by a range of different learning methods. Additionally, it should be noted that omitting the impact of the learning process and attack detection would reduce the quality of the model. The reason is that cyber-attacks differ in terms of their impact on the entire company and in terms of the resources used to neutralize them. These conceptual cognitions constitute the very foundation of our motivation to propose a new type of approach to modeling cyber security issues. We seek to achieve essentially the following objectives.

On the one hand, the goal of our approach is to define what represents an acceptable algorithmic methodology. It allows the learning engine to have access to a set of machine learning methods to increase the algorithmic space. The reason is to match the most salient issues that need to be resolved. This will increase the quality of intrusion detection and the cyber security of connected objects. Additionally, the outcome of this expected performance depends on the raw data sampling process. The quality criteria for this sampling include not only the size of the data set but also the relationship between the descriptive variables called inter-correlation. This last parameter should ideally be reduced to zero. In addition, the delay in capturing network data has a great advantage. This will keep the dataset up to date and consistent with threat level and complexity.

On the other hand, the objective is to follow a risk-based approach when analyzing the cyber-security attack chain or kill chain. This means that cyber risk must be identified first. Then,

the assessment of this risk is based on its probability and its total impact on the system. The end goal of this process is to prioritize each risk category in terms of cost weighting. This will lead to a framework enabling the integration of security objectives, taking into account the risk tolerance level of security councils, and at the same time reduce the costs induced by security and insecurity related to the Internet of Things.

The ultimate goal of this approach is to develop an optimized model that recovers all the drawbacks linked to the state of the art of cyber-security and ensures enhanced cyber-security of connected objects. This model should compensate for the shortcomings of the approaches discussed in the state of the art.

IV. Proposed Modeling

The motivation for proposing a new intrusion detector optimization model lies in the fact that NIDS attempts to apply the same intrusion filters regardless of the risk policies in place. Since zero risk is unrealistic, it is essential to control its assessment and level of acceptance.

The ultimate goal of this approach is to develop a model allowing you to choose among Machine Learning methods (supervised, unsupervised and reinforcement), the optimal method to effectively detect intrusions in IoT objects. This choice is essentially based on the cost-sensitive technique thus minimizing the learning impact of attacks and intrusions in IoT objects.

Upgrading the generic classification and detection model involves redefining the methodology. To do this, we imagined the creation of two functional layers at the conceptual level (see Fig. 2). This brings us to modular programming of the detection engine. On the one hand, the first module serves to design the algorithmic component of the methodology in order to integrate a wide range of learning methods. On the other hand, the second module models the security-cost component of the methodology. This allows the security manager to control the acceptable level of risk in relation to the typology of cyber-attacks. In this way, the most optimal classification method will be chosen. This is the least expensive method in terms of negative impact.

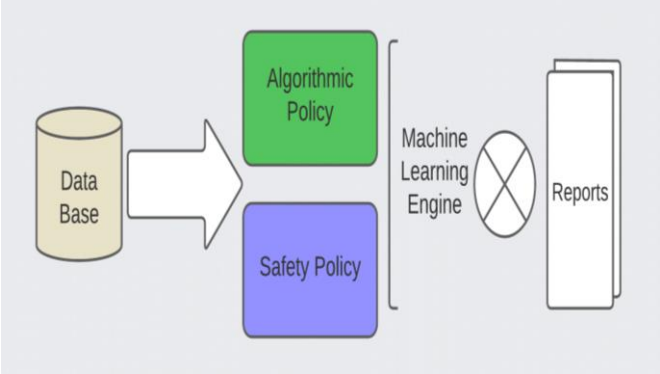

Fig. 2. Macro-learning optimization method for cyber-attacks.

We find ourselves in an optimization automation process with the possibility of acting on the algorithmic parameters and the security cost.

Achieving the previously set optimization goals will be a prerequisite for achieving the optimized cyber security logic model (see Fig. 3).

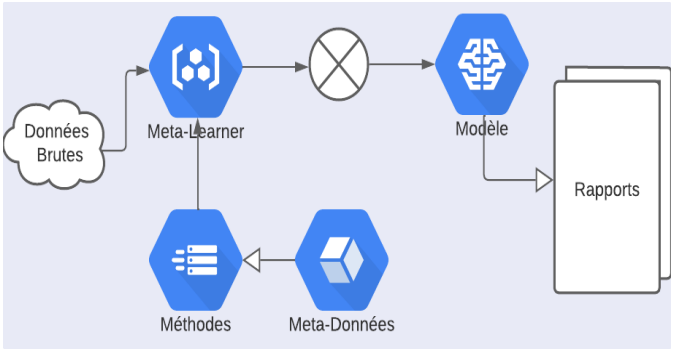

Fig. 3. Optimized cyber-security logic model (olm).

This process takes place in two successive phases. First, we introduce the concept of Meta-Learning on which algorithmic policy is based. Next, we present the cost-aware learning technique. This will make it possible to implement the entity's security policy in terms of intrusion detection and cost control.

Meta-learning corresponds to what we could call macro learning. This involves understanding the behavior of multiple learning methods. The objective is to collect metadata consisting of performance values and algorithmic parameters associated with the methods.

This approach makes it possible to nest or encompass several learning methods within a single Canvas. We know that the quality of an algorithm includes not only how well it predicts reality, but also how quickly it is executed. This is the basic principle of the meta-learning process.

In the second block dedicated to security policy, we propose to introduce the notion of learning costs (impacts). The goal of classical learning is to minimize the errors generated by the difference between prediction and observation. Since not all errors have the same cost or impact, we will use the cost-sensitive learning technique. The fundamental principle of cost-aware learning is that the learning engine is informed about the cost or impact of intrusion detection scenarios.

At the formal level of the description of the proposed model, we are faced with an operational research problem. On the one hand, it involves defining an objective function, which takes into account the resource constraint and aims to maintain a level of algorithmic performance and to reduce the expression of costs.

Let n be the bisquare dimension matrix, the confusion matrix M (Mij) and the cost matrix C (Cij). The objective function F should be the aggregation of all effects that trigger resource consumption. This includes the cost of detection training and the cost of missed detection of an intrusion. F will be the scalar product of M and C:

$$F = (M * C) = \sum_{\substack{i=1 \\ j=1}}^{n} \left((M_{i,j} * C_{i,j}) \right)$$

Since the first diagonal corresponds to well-classified items, their cost is identical and can be normalized to Cij=1:

$$F = \sum (\mathrm{M_{i,j}} * \mathrm{C_{i,j}}) + \sum (M_{i,i}) \ , \qquad i \neq j$$

The cost of well-classified elements related to correct detection is $\sum(\mathrm{M_{i,i}})$. This is simply a computational cost. Thus, the remaining quantity $\sum(\mathrm{M_{i,j}} * \mathrm{C_{i,j}})$ of F corresponds to the cost linked to the impact of cyber-security. The linear optimization of the objective function is obtained by:

$$min \sum (M_{i,j} * C_{i,j}), \qquad i \neq j$$

V. Methods and Materials

A. Dataset

To conduct the proposed work, we used the latest DDoS attack dataset CICIDS2018 [19]. Most DDoS attack datasets have many limitations, such as missing relevant data and redundancy, which are unreliable. The CICIDS2018 datasets contain up-to-date real-world working network like data. This dataset was collected for five consecutive days with many different cyber-attacks as well as normal data. This dataset contains the latest network data with and without attack, very close to real network data. This dataset is unbalanced, so we balanced it using a duplication method because it seriously affects the training of the deep learning method and therefore testing. This work is applied in an environment containing a 32-bit Intel Core-i5 processor with 8 GB of RAM in a Windows 10 environment.

B. Confusion Matrix

The confusion matrix is a predictive analysis tool in machine learning. It is also known as an error matrix, and is used to evaluate the performance of a machine-learning model based on classification, which aim to predict a categorical label for each input instance [20].

We can also say that the confusion matrix is a summer table of the number of correct and incorrect predictions produced by a classifier for binary classification tasks.

The matrix displays the number of true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) produced by the model on the test data (see Table I).

- True Positive (TP): when the actual value is Positive and predicted is positive.
- True Negative (TN): when the actual value is Negative and prediction is Negative.
- False Positive (FP): When the actual is negative but prediction is Positive. Also known as the Type 1 error
- False Negative (FN): When the actual is Positive but the prediction is Negative. Also known as the Type two errors.

TABLE I. Confusion Matrix Basic Metrics

Techniques	Observation	
Learning (Predicted Class)	(True Positives) TP	(False Positive) FP
	(False Negative) FN	(True Negative) TN

C. Performance Metrics

The performance of proposed deep learning models for the detection of DDoS attack is measured by standard matrices as Accuracy, Recall and Precision. The definition and the equation for the same is given below:

Accuracy: An indicator makes it possible to measure the proportion of well-classified individuals relative to the entire population examined. It is obtained using the following equation:

$$Accuracy = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FN} + \mathrm{TN} + \mathrm{FP}}$$

Precision: An indicator of false alarms. It allows us to answer the following question. What proportions of positive identifications were actually correct? It is obtained using the following equation:

$$Precision = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}}$$

Recall: A metric that characterizes detection failures. This failure results in the presence of false negatives. It is obtained using the following equation:

$$Recall = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}}$$

D. Weka Tool

The physical implementation of the IoT cyber-security model requires the use of hardware and software resources. In order to produce an Optimized Physical Cyber-security Model (OPCM), we opted for open source software that is well known in the scientific research community. This is Weka and its applications.

WEKA provides implementations of learning algorithms that you can easily apply to your database. It also includes a variety of tools for transforming datasets. These include algorithms for discretization and sampling. It can also be used to pre-process a dataset, integrate it into a learning scheme, and analyze the resulting classifier and its performance [21].

In this article, we use the tool for apply learning methods to a dataset and analyze its output to learn more about the data. The objective is to verify the performance of our cyber security mechanism in effectively predicting attacks hitting the IoT.

VI. Results and Discussions

The evaluation study of the proposed model is based on a set of tests obtained after simulating the model in the Weka tool. These data will be provided as input values to the prediction function. The results of this operation will be compared with the corresponding observation values.

Fig. 4. Prediction (star series) of cyberattacks using confusion matrix.

As these results show in Fig. 4, we notice that almost 2863 packets are denial of service (see DINAIL*). This prediction is confirmed by the observations of the test set. In addition there are 1928 packets recognized as benevolent (see Normal*) both in prediction and in observation. We find the errors made by the model for a column of observations outside the first diagonal. There were 1628 predictions ARP spoofing (see SPOOF*). The curves show that the prediction (star series) of cyber-attacks is very close to the values from observation.

To assess the validity of the model, several indicators can measure these objectives at the same time. We have the holistic statistical estimates, which evaluate the overall performance of the model. These indicators reflect the quality, shortcomings and consistency of the learning process.

Correctly Classified Instances	29306	93.6623 %
Incorrectly Classified Instances	1983	6.3377 %
Kappa statistic	0.882	
Mean absolute error	0.0254	
Root mean squared error	0.1592	
Relative absolute error	12.0258 %	
Root relative squared error	49.0447 %	
Total Number of Instances	31289	

Fig. 5. Performance statistics.

In Fig. 5, the results obtained illustrate the following behaviors: The classification quality rate is 93.66%. This rate shows a high level of conformity between predictions and observations. This result is supported by a classification consistency rate of 0.882 (close to unity 1), demonstrating a trend towards convergence between observation and prediction. This deduces the accuracy and performance of the model evaluated.

We then proceed to deepen our assessment of the model's validity using other metrics such as the model's sensitivity, specificity and precision.

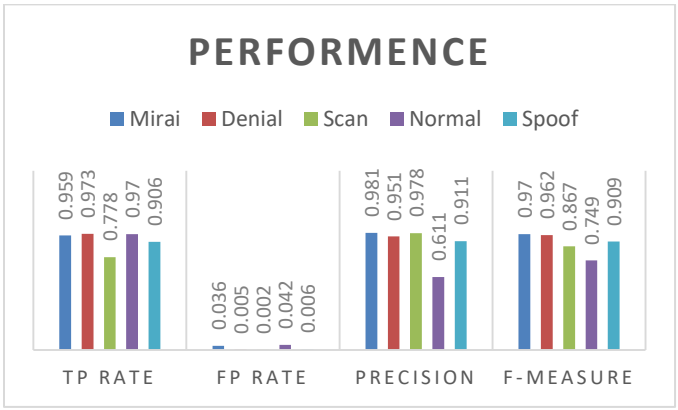

Fig. 6. Learning assessment metrics.

From these test results (see Fig. 6), we deduce that the sensitivity varies between 74% and 97%, while the specificity of the model is between 95.8% and 99.8%. The false alarm rate (false positives) is therefore between 0.2% and 4.2%.

VII. Conclusion

Our exploration has revealed major IoT security risks. The physical security of IoT is challenged in remote sites. Hardware and software upgrades and updates are critical. This is a major constraint to the scale of the threat.

This threat is accentuated by the availability of tools for researching and exploiting vulnerabilities in the IoT system. This represents obvious cyber security challenges.

In this design, special attention is paid to the cybernetic strike chain. To adapt to this, we opted for an optimized detection model. This optimization is based on algorithmic and security policies.

This integrates the potential of algorithmic methods and the reduction of learning costs. To implement it, macro-learning (Meta learning) and discriminated cost methods are used. The programming is carried out on the Weka of the machine-learning platform.

References

[1] B. Mazon-Olivo and A. Pan, (2022) "Internet of Things: State-of-the-art, Computing Paradigms and Reference Architectures," in IEEE Latin America Transactions, vol. 20, no. 1, pp. 49-63, Jan. 2022, doi: 10.1109/TLA.2022.9662173.

[2] K. Yang, Y. Zhang, X. Lin, Z. Li and L. Sun, (2022) "Characterizing Heterogeneous Internet of Things Devices at Internet Scale Using Semantic Extraction," in IEEE Internet of Things Journal, vol. 9, no. 7, pp. 5434-5446, 1 April1, 2022, doi: 10.1109/JIOT.2021.3110757.

[3] I. Dutt, S. Borah and I. K. Maitra, "Immune System Based Intrusion Detection System (IS-IDS): A Proposed Model," in IEEE Access, vol. 8, pp. 34929-34941, 2020, doi: 10.1109/ACCESS.2020.2973608.

[4] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf and Y. A. Bangash, (2020) "An In-Depth Analysis of IoT Security Requirements,

Challenges, and Their Countermeasures via Software-Defined Security," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10250-10276, Oct. 2020, doi: 10.1109/JIOT.2020.299765.

[5] Z. Shi, S. He, J. Sun, T. Chen, J. Chen and H. Dong, (2023) "An Efficient Multi-Task Network for Pedestrian Intrusion Detection," in IEEE Transactions on Intelligent Vehicles, vol. 8, no. 1, pp. 649-660, Jan. 2023, doi: 10.1109/TIV.2022.3166911.

[6] S. Yao et al., "Deep Learning for the Internet of Things," in Computer, vol. 51, no. 5, pp. 32-41, May 2018, doi: 10.1109/MC.2018.2381131. T.-H. Chua et I. Salam (2022), « Evaluation of Machine Learning Algorithms in Network-Based Intrusion Detection System », p. 31 symmetry 2023, https://doi.org/10.3390/sym15061251.

[7] U. A. Butt et al., (2020) « A Review of Machine Learning Algorithms for Cloud Computing Security », Electronics, vol. 9, no 9, Art. no 9, sept. 2020, doi: 10.3390/electronics9091379.

[8] I. A. Khan, M. Keshk, D. Pi, N. Khan, Y. Hussain, et H. Soliman, (2022) « Enhancing IoT networks protection: A robust security model for attack detection in Internet Industrial Control Systems », Ad Hoc Networks, vol. 134, p. 102930, sept. 2022, doi: 10.1016/j.adhoc.2022.102930.

[9] P. Williams, I. K. Dutta, H. Daoud, et M. Bayoumi, (2022) « A survey on security in internet of things with a focus on the impact of emerging technologies », Internet of Things, vol. 19, p. 100564, août 2022, doi: 10.1016/j.iot.2022.100564.

[10] A. Kumar and A. Bansal, (2019) "Software Fault Proneness Prediction Using Genetic Based Machine Learning Techniques," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-5, doi: 10.1109/IoT-SIU.2019.8777494.

[11] F. H. Sifat, R. Mahzabin, S. Anjum, A. -A. Nayan and M. G. Kibria, (2022) "IoT and Machine Learning-Based Hypoglycemia Detection System," 2022 International Conference on Innovations in Science, Engineering and Technology (ICISET), Chittagong, Bangladesh, 2022, pp. 222-226, doi: 10.1109/ICISET54810.2022.9775890.

[12] M. R. Diana, P. Tobón, D. Múnera (2023) « Anomaly classification in industrial Internet of things: A review », In Intelligent Systems with Applications, vol. 18, p. 200232, mai 2023, doi: 10.1016/j.iswa.2023.200232.

[13] Naji, M., Zougagh, H. (2023). Deep Learning Models for Cybersecurity in IoT Networks. In: El Ayachi, R., Fakir, M., Baslam, M. (eds) Business Intelligence. CBI 2023. Lecture Notes in Business Information Processing, vol 484 . Springer, Cham. https://doi.org/10.1007/978-3-031-37872-0_3.

[14] A. Oseni et al., "An Explainable Deep Learning Framework for Resilient Intrusion Detection in IoT-Enabled Transportation Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 1, pp. 1000-1014, Jan. 2023, doi: 10.1109/TITS.2022.3188671.

[15] G. S. Mahara and S. Gangele, "Fake news detection: A RNN-LSTM, Bi-LSTM based deep learning approach," 2022 IEEE 1st International Conference on Data, Decision and Systems (ICDDS), Bangalore, India, 2022, pp. 01-06, doi: 10.1109/ICDDS56399.2022.10037403.

[16] K. Greff, R. K. Srivastava, J. Koutník, B. R. Steunebrink, and J. Schmidhuber, "LSTM: A search space odyssey," IEEE transactions on neural networks and learning systems, vol. 28, pp. 2222-2232, 2017.

[17] N. Ahmad, R. P. George, R. Jahan and S. Hussain, "Integrated IoT and Block chain for secured access and managing education data," 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), Kannur, India, 2022, pp. 1201-1204, doi: 10.1109/ICICICT54557.2022.9917643.

[18] A. Abeshu and N. Chilamkurti, "Deep learning: the frontier for distributed attack detection in Fog-to-Things computing," IEEE Communications Magazine, vol. 56, pp. 169- 175, 2018.

[19] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," in ICISSP, 2018, pp. 108- 116.

[20] J. L. Garcia-Balboa, M. V. Alba-Fernandez, F. J. Ariza-López and J. Rodriguez-Avi, "Homogeneity Test for Confusion Matrices: A Method and an Example," IGARSS 2018 - 2018 IEEE International Geoscience and Remote Sensing Symposium, Valencia, Spain, 2018, pp. 1203-1205, doi: 10.1109/IGARSS.2018.8517924.

[21] Ian H. Witten, Mark A. Hall, et Eibe Frank, « The WEKA workbench ». Consulté le: 20 Octobre 2023. [En ligne]. Disponible sur: https://waikato.github.io/weka-wiki/documentation.