A Machine Learning Framework for Automatic Detection and Classification of Cyber Attacks in IoT Use Cases

Hussam Aleem Mohammed Amar Yusof Jaffar

Department: Computer Engineering Department, College: College of Computer and Information Systems University: Umm Al-Qura University, Saudi Arabia Department: Computer Engineering Department College: College of Computer and Information Systems, University: Umm Al-Qura University, Saudi Arabia

ABSTRACT

Internet of Things (IoT) use cases are vulnerable to cyber-attacks due to lack of global standards and involvement of heterogeneous devices, protocols and platforms. Traditional methods are found inadequate safeguard IoT applications. With the emergence of Artificial Intelligence (AI), machine learning (ML) and deep learning techniques are widely used to solve security problems in different applications. Learning capability of AI models paves way for intelligent solutions. In this paper, we proposed a ML framework for automatic detection and classification of cyber-attacks in IoT use cases. We proposed a hyperparameter optimization method, designed for optimization of parameters of four ML techniques in tune with the dataset, used in the proposed framework. An algorithm named Learning based Optimal Machine Learning for Cyber Attack Detection and Classification (LbOML-CADC) is also proposed. This algorithm exploits hyperparameter tuning method for efficient detection and classification of cyber-attacks. We evaluated our framework using UNSW-NB15 dataset. Our empirical study reveals that highest accuracy achieved is 97.59%.

Keywords

Security, Machine Learning, Cyber Attack Detection, Hyperparameter Optimization, Internet of Things

1. INTRODUCTION

Internet of Things (IoT) technology have brought significant changes in the real world application scenarios. It led to smart applications that were never made possible. IoT applications include smart agriculture, smart transportation, smart city and smart home to mention few. Since IoT enables integration between things of any kind and also digital devices, its use cases are very complex and diversified in nature. Thousands of connected devices participate in IoT applications. Moreover, there is heterogeneity in protocols, devices and platforms. Thus, IoT use cases are vulnerable to various kinds of attacks. In addition to this, there are no globally acceptable standards yet. This is another reason why IoT applications are prone to cyberattacks. With the emergence of AI enabled methods, there is chance of improving security of IoT applications as they learn from time to time from historical labelled instances.

Many researchers contributed in cyber-attack detection using ML techniques. The literature also includes attack detection in IoT use cases. Elsisi *et al*. [2] stated that IoT-based architecture detects and visualizes induction motor faults. Hasan *et al*. [4] found that the rising IoT security threats demand robust anomaly detection. RF proves effective in identifying various attacks and anomalies accurately. Maluleke *et al*. [10] compared ML and statistical models for DDoS detection in CPS-IoT, highlighting effective supervised and semi-supervised techniques. Thilagam *et al*. [15] focused on ML and DL methods that offer solutions to cyber security issues. Sikdar *et al*. [22] found that IoT integration is crucial in the evolving healthcare sector. This paper reviews ML algorithms enhancing H-IoT applications, highlighting challenges. Williams *et al*. [29] discussed about the vulnerability of machine learning-based IDS in IoT networks to Adversarial Machine Learning attacks. From the literature, it was observed that the existing ML methods needs further improvement in terms of parameter optimization. Our contributions in this paper are as follows.

1. We proposed a ML framework for automatic detection and classification of cyber-attacks in IoT use cases.
2. We proposed a hyperparameter optimization method based on random search. This is used to tune hyperparameters of ML models for the UNSW-NB15 dataset.
3. We proposed an algorithm named Learning based Optimal Machine Learning for Cyber

Manuscript received January 5, 2025
Manuscript revised January 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.1.17

Attack Detection and Classification (LbOML-CADC).
4. We evaluated our framework using UNSW-NB15 dataset and found that the performance of ML models is greater than 97% with hyperparameter tuning.

The remainder of the paper is structured as follows. Section 2 reviews literature on diversified methods used for attack detection. Section 3 presents our methodology used for efficient detection of cyberattacks. Section 4 presents results of our experiments. Section 5 concludes the paper and gives directions for future scope.

2. RELATED WORK

This section reviews literature on existing methods based on ML for cyber-attack detection in IoT applications. Tran *et al*. [1] observed the IoT role in digitized power stations includes real-time monitoring and cybersecurity. Novel architecture detects GIS defects and cyber-attacks efficiently. Elsisi *et al*. [2] stated that IoT-based architecture detects and visualizes induction motor faults and cyber-attacks accurately, enhancing industrial decision-making and cybersecurity. Kaur *et al*. [3] opined that the Industrial IoT facilitates Industry 4.0, yet increases cyber threats. ML models efficiently identify and detect attacks in SCADA systems. In Hasan *et al*. [4] found that the rising IoT security threats demand robust anomaly detection. RF proves effective in identifying various attacks and anomalies accurately. Gidlund *et al*. [5] stated that the rising IIoT vulnerabilities include the sophisticated "False Data Injection" attack. Autoencoders effectively detect and recover from such attacks. According to Saheed *et al*. [6] the ICT advancements lead to the IoT's emergence, especially in healthcare. The study emphasizes using ML models for efficient IDS. Alarif *et al*. [7] observed that the healthcare cyber-physical system demands robust security. A proposed cognitive ML model achieves high accuracy and efficiency. Shafiq *et al*. [8] focused on the Efficient IoT security demands and accurate malicious traffic detection. A new CorrAUC-based feature selection model achieves over 96% accuracy.

Asyharia *et al*. [9] enhanced IDS for IoT involves implementing semi-distributed and distributed architectures. Experimentation shows promising results with comparable accuracies. Maluleke *et al*. [10] compared ML and statistical models for DDoS detection in CPS-IoT, highlighting effective supervised and semi-supervised techniques. Ranga *et al*. [11] assessed ML classifiers for IoT DoS defence. It recommends classification and regression trees and extreme gradient boosting for building anomaly-based IDS. Gupta *et al*. [12] stated that IIoT security is crucial due to potential damages.

Machine learning aids vulnerability analysis. A case study illustrates effective anomaly detection. Baig *et al*. [13] found that IoT's exponential growth poses challenges, but a proposed adaptable framework enables machine learning integration for intelligent IoT solutions. Salem *et al*. [14] observed that a cognitive radio network utilizes relay nodes for improved transmission, proposing an overlapped spectrum sensing strategy for efficient access. Thilagam *et al*. [15] focused on ML and DL methods that offer solutions to cyber security issues. This paper discusses their classifications and implementations. Gao *et al*. [16] observed that the IoT's evolution empowers automation and data collection. Machine learning's potential in cybersecurity is praised, yet its vulnerabilities and malicious uses are also scrutinized. Jena*et al*. [17] stated that IoT's widespread adoption poses security challenges. The survey delves into ML, AI, and Blockchain integration for enhanced security. Munoz *et al*. [18] found growing concerns about computer network security necessitate advanced intrusion detection techniques. Focus on ML and IoT for robust security solutions.

Reza *et al*. [19] found that the WSNs face cyber threats; ML-based multi-layer detection system with a mobile robot detects and mitigates internal attacks effectively. Alsolami *et al*. [20] observed that the IoT's widespread use enhances life, but security challenges persist. AI, particularly ML and deep learning, fortify IoT security effectively. Cao *et al*. [21] found that IoT security concerns prompt advanced intrusion detection. A data-driven approach with improved dataset balance achieves 99.7% accuracy. Sikdar *et al*. [22] found that IoT integration is crucial in the evolving healthcare sector. This paper reviews ML algorithms enhancing H-IoT applications, highlighting challenges. According to Gupta *et al*. [23] IoT's ubiquity raises concerns; tailored security is essential. Cloud integration heightens vulnerabilities. ML-based approach enhances edge IoT security. Hameed *et al*. [25] stated that the Rapid cyber expansion demands enhanced security. ML aids cyber defence, yet challenges persist, including dataset availability and evasion. Gupta *et al* [26] found that IoT's vulnerability to cyber threats demands effective intrusion detection systems. A hybrid feature selection approach enhances detection accuracy. Janicki *et al*. [27] investigated privacy risks in IoT, focusing on traffic fingerprinting attacks and ML's role in device identification and activity tracking. Singh *et al*. [28] introduced a scalable forensic framework for IoT data analysis using Google's MapReduce, emphasizing evidence reliability. Williams *et al*. [29] discussed about the vulnerability of machine learning-based IDS in IoT networks to Adversarial Machine Learning attacks. It proposes a rule-based approach to generate attack samples and demonstrates the impact on classifier performance. It highlights the need for more sophisticated defence mechanisms. Shi *et al*. [30] addressed IoT security challenges and proposes a statistical learning-based anomaly detection framework. It highlights the suitability of simple machine learning models for IoT security. From the literature, it was observed that the existing ML methods needs further improvement in terms of parameter optimization.

3. PROPOSED FRAMEWORK

We proposed a ML framework as presented in Figure 1 for automatic detection of cyber-attacks and classifying the same. It is a learning based approach which has ability to scale and gain knowledge incrementally. Attack detection methods based on ML are widely used of late. However, hyperparameter tuning is found important as the dataset used in learning differs in each domain. Unlike some of the existing attack detection models found in [31], [32] and [33], we proposed a parameter optimization technique, described in Section 3.2, that tunes parameters of ML models based on the dataset named UNSW-NB15. As explored in [34], [35] and [36] parameter tuning has its impact on the efficiency of ML models.

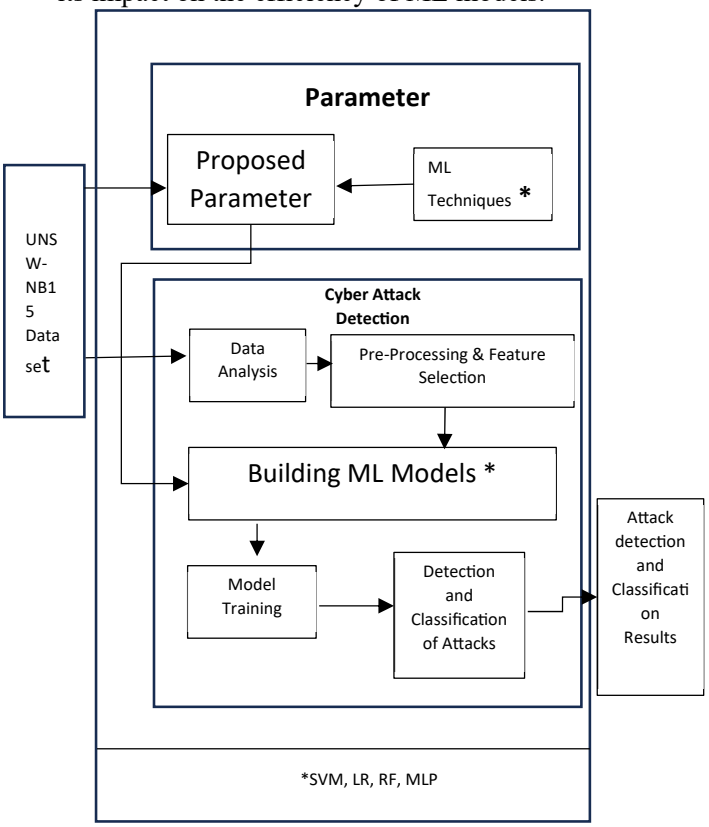

Figure 1: Our framework for attack detection and classification

The given dataset UNSW-NB15 is used for hyperparameter tuning of the ML models such as Support Vector Machine (SVM), Logistic Regression (LR), Random Forest (RF) and Multilayer Perceptron (MLP). Then the data is subjected analysis to understand attack distribution and know whether data has any sort of imbalance. Afterwards, treating null values and one hot encoding are carried out as part of pre-processing.

Feature selection follows it to improve quality of training. Feature importance is computed and features with more than 0.3 correlation with corresponding attack label are considered for training process. Afterwards, the ML models are built and trained. The trained models are further used to evaluate test data to arrive at attack detection and classification results.

3.1 Machine Leaning Models

LR is one of the statistical models used in the empirical study. Its functionality is based on logistic function and sigmoid function as expressed in Eq. 1. Logistic function is used by the model to get values for classification purpose. The probability of the linear function is denoted as p and its values can be between 0 and 1.

$$F(x) = \frac{1}{1+e^{-x}} = \frac{e^{x}}{e^{x}+1} \quad (1)$$

Considering a linear function log p(x) it can be solved as given in Eq. 2.

$$\text{Log}\frac{p(x)}{1-p(x)} = \alpha_0 + \alpha.x \quad (2)$$

After obtaining solution for p(x), it can be further computed as in Eq. 3.

$$P(x) = \frac{e^{\alpha_0+\alpha}}{e^{\alpha_0+\alpha}+1} \quad (3)$$

In order to minimize rate of misclassification, threshold of linear function is set to 0.5. SVM is another widely used model used in our framework. It is used to achieved multi-class classification. RF model on the other hand makes use of number of Decision Tree (DT) models internally using ensemble approach. It makes use of majority voting, given in Eq. 4, for final class determination.

$$C_{RF}(s) = majority\ vote\{C_n(s)\}_1^N \quad (4)$$

Here N denotes number of DTs. MLP is yet another ML model used in our framework. It is a variant of ANN model with three layers such as input, hidden and output layers. It involves computations expressed in Eq. 5 and Eq. 6.

$$h^1 = step(z^1) = step(w^1.x + b^1) \quad (5)$$

$$y = step(z^2) = step(w^2.h^1 + b^2) \quad (6)$$

MLP is trained in batches where each input is a vector X. It generates k new instances from available instances as expressed in Eq. 7.

$$x_1 = \begin{pmatrix} x_{1,1} \\ \vdots \\ x_{1,n} \end{pmatrix}, \ldots\ldots, x_k = \begin{pmatrix} x_{k,1} \\ \vdots \\ x_{k,n} \end{pmatrix} \quad (7)$$

After generating k instances, they are combined as given in Eq. 8.

$$X = \begin{pmatrix} x_1^T \\ \vdots \\ x_k^T \end{pmatrix} = \begin{pmatrix} x_{1,1} \ldots\ldots x_{1,n} \\ \vdots \\ x_{k,1}, \ldots\ldots\ldots, x_{k,n} \end{pmatrix} \quad (8)$$

Afterwards, the y is computed as in Eq. 9.

$$y = step(z) = step(X.W+b) \quad (9)$$

where X denotes input consisting of shape (k,n) denoting input values and instances. A matrix is used in the computation which is denoted as W.

3.2 Random Search based Hyperparameter Optimization

Considering a ML model *A,* it is indispensable to minimize loss, denoted as L(x;*f*), for efficiency. The learning process is associated with ground truth, denoted as G_x, of training data denoted as $x^{(train)}$. ML model has number of hyperparameters denoted as λ. With optimization of λ, f =$A_\lambda(x^{(train)})$ denotes algorithm with optimized parameters. It is also important to minimize error denoted as $E_{x\sim G_x}$[L(x; $A_\lambda(x^{(train)})$)]. The optimization process is thus expressed in Eq. 10.

$$\lambda^{(*)} = \text{argmin}_{\lambda\in\Lambda} E_{x\sim G_x}[L(x; A_\lambda(X^{(train)}))] \quad (10)$$

Optimization has influence on the performance of A. Based on ground truth G_x, it is a difficult problem to optimize parameters. In this regard, grid based search is found a poor choice. In this paper, our optimization method is based on random search which finds optimal values for λ. Cross validation is used as in Eq. 11 for hyperparameter optimization.

$$\lambda^{(*)} \approx \text{argmin}_{\lambda\in\Lambda}\text{mean}_{\text{x}\in\text{X(valid)}} \text{L(x; } A_\lambda(X^{(train)})) \quad (11)$$

$$\equiv \text{argmin}_{\lambda\in\Lambda}\Psi(\lambda) \quad (12)$$

$$\approx \text{argmin}_{\lambda\in\{\lambda^{(1)},\ldots\ldots\lambda^{(S)}\}}\Psi(\lambda) \equiv \hat{}\lambda \quad (13)$$

The optimization is expressed in Eq. 11, Eq. 12 and Eq. 13. The response function is denoted as Ψ. Its optimization is achieved by reducing Ψ(λ) such that $\lambda \in \Lambda$. In the process a set of trials is used as expressed in $\{\lambda^{(1)}, \ldots\ldots\lambda^{(S)}\}$. Unlike the grid search methods found in [34], [35] and [36] our methodology based on random search is found more efficient in presence of high dimensional space. In spite of optimizing λ, it is important to compute validation and test errors as in Eq. 14 and Eq. 15.

$$\Psi^{(valid)}(\lambda) = mean_{x\epsilon\text{x}^{(valid)}} l(\text{x; } A_\lambda(X^{(train)})) \quad (14)$$

$$\Psi^{(test)}(\lambda) = mean_{x\epsilon\text{x}^{(test)}} l(\text{x; } A_\lambda(X^{(train)})) \quad (15)$$

Similarly, Bernoulli variance is computed on those sets as in Eq. 16 and Eq. 17.

$$\mathbb{V}^{(valid)}(\lambda) = \frac{\Psi^{(valid)}(\lambda)(1-\Psi^{(valid)}(\lambda))}{|\text{x}^{(valid)}|-1} \quad (16)$$

$$\mathbb{V}^{(test)}(\lambda) = \frac{\Psi^{(test)}(\lambda)(1-\Psi^{(test)}(\lambda))}{|\text{x}^{(test)}|-1} \quad (17)$$

The estimation of variance often depends on loss function. Our empirical study showed that the proposed hyper-parameter optimization method is better than grid based methods.

3.3 Algorithm Design

We proposed an algorithm known as Learning based Optimal Machine Learning for Cyber Attack Detection and Classification (LbOML-CADC). This algorithm exploits hyperparameter tuning method for efficient detection and classification of cyber-attacks.

Algorithm: Learning based Optimal Machine Learning for Cyber Attack Detection and Classification
Inputs: UNSW-NB15 dataset D, ML models M
Output: Results of prediction P

1. Begin
2. *D'*←PreProcess(*D*)
3. (*T1*, *T2*)←DataSplitting(*D'*)
4. For each model m in M
5. λ ← HyperParameterTuning(T1)
6. Update m with λ
7. End For
8. F←FeatureSelection(T1)
9. For each *m* in *M*
10. Train m with F
11. predictionResults←Predict(m, T2)
12. Add predictionResults to P
13. End For
14. Return P
15. End

Algorithm 1: Learning based Optimal Machine Learning for Cyber Attack Detection and Classification

As presented in Algorithm 1, it takes UNSW-NB15 dataset D and ML models M as inputs. Then the data subjected pre-processing as in step 2. The pre-processing involves treating null values and normalization. Afterwards, the data is split into 70% training (T1) and 30% testing (T2). From step 4 through step 7 there is an iterative process to optimize hyperparameters of all ML models. In step 8 feature selection is carried out to identify features whose importance is greater than 0.3. Afterwards, from step 9 through step 13, there is another iterative process which takes care of training each ML model with selected features F and then perform multi-class attack classification using T2. Finally, the algorithm returns detection and classification results of various cyberattacks.

3.4 Performance Measures

Different performance metrics are used in this study to evaluate our proposed algorithm with underlying ML models. The metrics used in the evaluation include accuracy as in Eq. 18, mean squared error (MSE) as in Eq. 19, mean absolute error (MAE) as in Eq. 20, root mean squared error (RMSE) as in Eq. 21 and R2 score as in Eq. 22.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (18)$$

$$\text{MSE} = (1/n)^{*}\sum(actual - forecast)^2 \quad (19)$$

$$\text{MAE} = \frac{1}{n}\sum_{i=1}^{n}|x_i - x| \quad (20)$$

$$\text{RMSE} = \sqrt{\sum(P_i - O_i)^2/n} \quad (21)$$

$$R - Suared = \frac{SS_{regression}}{SS_{total}} \quad (22)$$

These metrics are comuted for each ML model used in the empirical study. Table 1 shows the notations used in the performance metrics.

Table 1: Notations used in the evaluation metrics

Notation	Description
$\|x_i - x\|$	Denotes absolute errors
O_i	The actual value for i^{th} instance
P_i	Denotes predicted value for i^{th} instance
$SS_{regression}$	Denotes sum of squares due to regression
SS_{total}	Denotes total sum of squares
$\sum$	Denotes summation
actual	Denotes the original value
Forecast	Denotes forecasted value
N	Size of sample
N	Denotes number of errors / items

Experiments are made and performance of the ML models are observed. The experimental results are presented in Section 4.

4. EXPERIMENTAL RESULTS

We built an application realize our framework and used it for performance evaluation. The execution environment includes a Dell PC with Windows 11 OS, Intel i5 -1335U processor and 16 GB RAM. We collected IoT use case related dataset known as UNSW-NB15 from [37]. Each ML model used in our study is subjected to the proposed hyperparameter tuning for leveraging its prediction performance. Each model is designed to achieve multi-class classification.

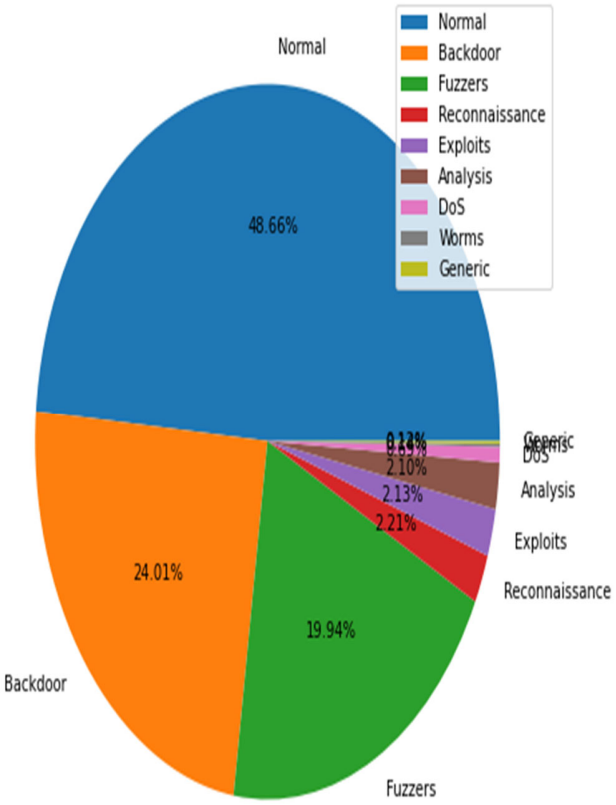

Figure 2: Distribution of attack labels in the UNSW-NB15 dataset

As presented in Figure 2, the dataset has 9 class labels. The percentage of data distribution pertaining various attack categories is visualized.

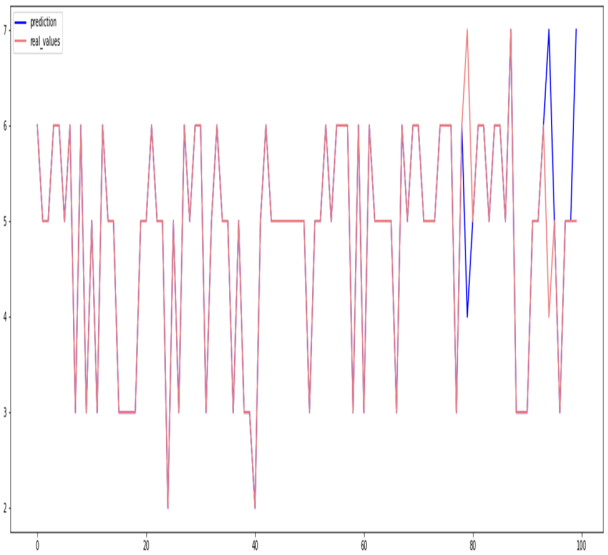

Figure 3: Real and predicted values visualized for RF model

As presented in Figure 3, the performance of RF model in the proposed framework is provided in terms of real and predicted values visualized.

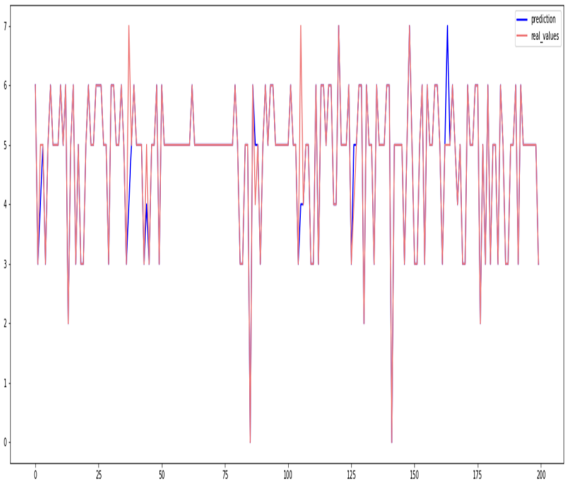

Figure 4: Real and predicted values visualized for MLP model

As presented in Figure 4, the performance of MLP model in the proposed framework is provided in terms of real and predicted values visualized.

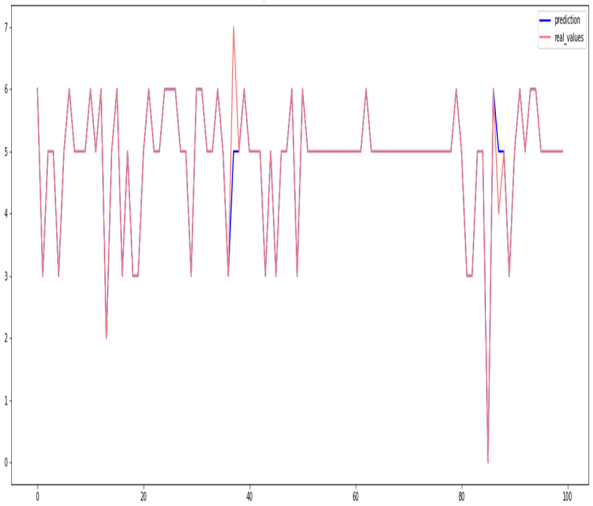

Figure 5: Real and predicted values visualized for LR model

As presented in Figure 5, the performance of LR model in the proposed framework is provided in terms of real and predicted values visualized.

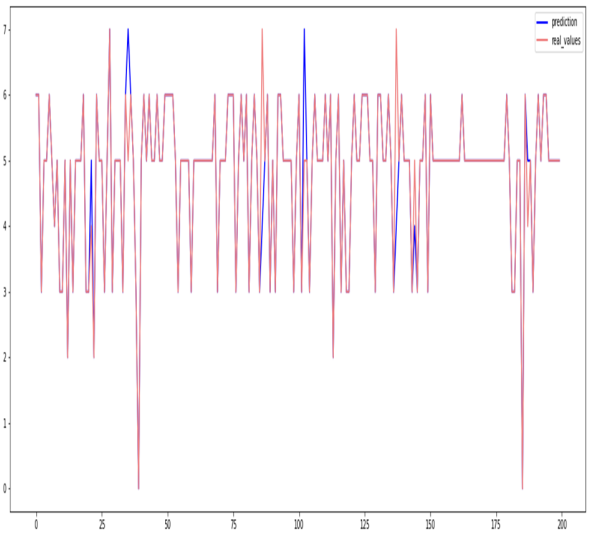

Figure 6: Real and predicted values visualized for SVM model

As presented in Figure 6, the performance of SVM model in the proposed framework is provided in terms of real and predicted values visualized.

Table 2: Performance comparison among attack detection models

Attack Detection Model	Performance				
	MAE	MSE	RMSE	R2 Score	Accuracy
Linear Support Vector Machine	0.0599	0.1794	0.4236	87.93	97.59
Logistic Regression	0.0601	0.1805	0.4249	87.88	97.59
Multi-Layer Perceptron	0.0606	0.1785	0.4225	87.98	97.54
Random Forest	0.0661	0.1985	0.4455	86.63	97.32

As presented in Table 2, the performance of the ML models used in the proposed framework is provided in terms of MSE, MAE, RMSE, R2 score and accuracy.

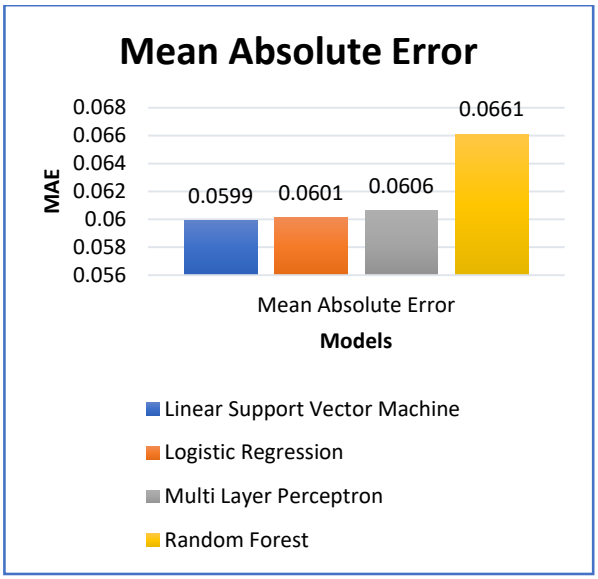

Figure 7: Performance of ML models in attack detection and classification in terms of MAE

As presented in Figure 7, MAE is the measure used to compare performance of different ML models in attack detection and classification. Lesser MAE indicates better performance. SVM exhibited 0.0599 MAE, LR 0.0601, MLP 0.0606 and RF showed 0.0661 MAE. From the results it is observed that least MAE is achieved by SVM model.

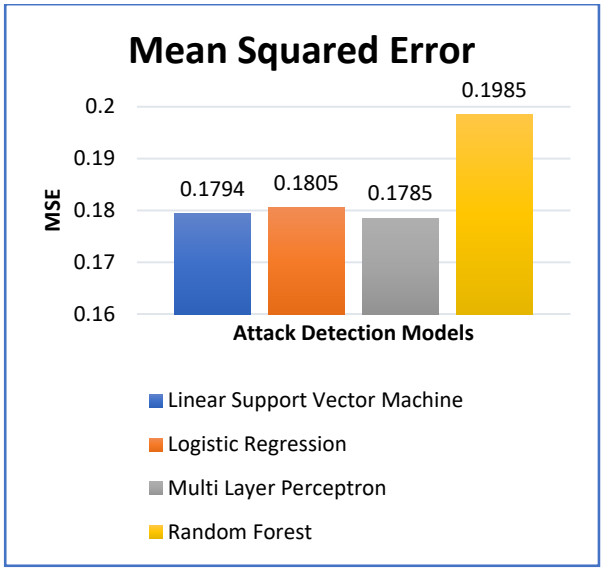

Figure 8: Performance of ML models in attack detection and classification in terms of MSE

As presented in Figure 8, MSE is the measure used to compare performance of different ML models in attack detection and classification. Lesser MSE indicates better performance. SVM exhibited 0.1794 MAE, LR 0.1805, MLP 0.1785 and RF showed 0.1985 MSE. From the results it is observed that least MSE is achieved by MLP model.

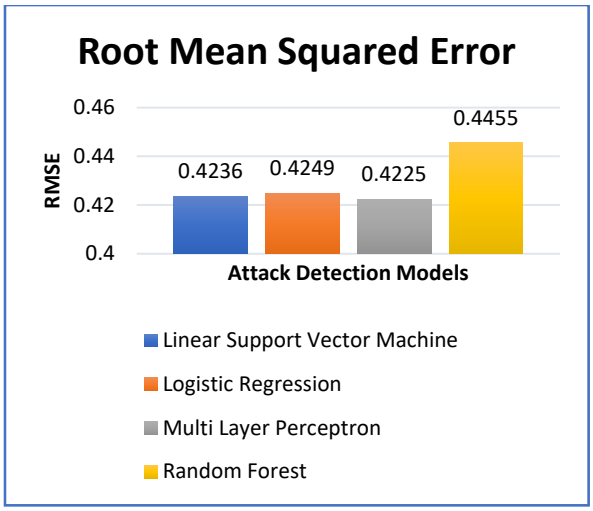

Figure 9: Performance of ML models in attack detection and classification in terms of RMSE

As presented in Figure 9, RMSE is the measure used to compare performance of different ML models in attack detection and classification. Lesser RMSE indicates better performance. SVM exhibited 0.4236 RMAE, LR 0.4249, MLP 0.4225 and RF showed 0.4455 RMSE. From the results it is observed that least RMSE is achieved by MLP model.

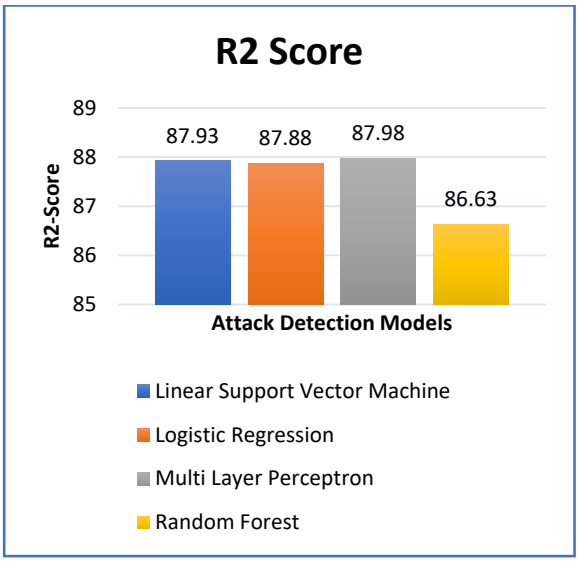

Figure 10: Performance of ML models in attack detection and classification in terms of R2 score

As presented in Figure 9, R2 score is the measure used to compare performance of different ML models in attack detection and classification. Higher R2 score indicates better performance. SVM exhibited 87.93% R2 score, LR 87.88%, MLP 87.98 and RF showed 86.63% R2 score. From the results it is observed that highest R2 score is achieved by MLP model.

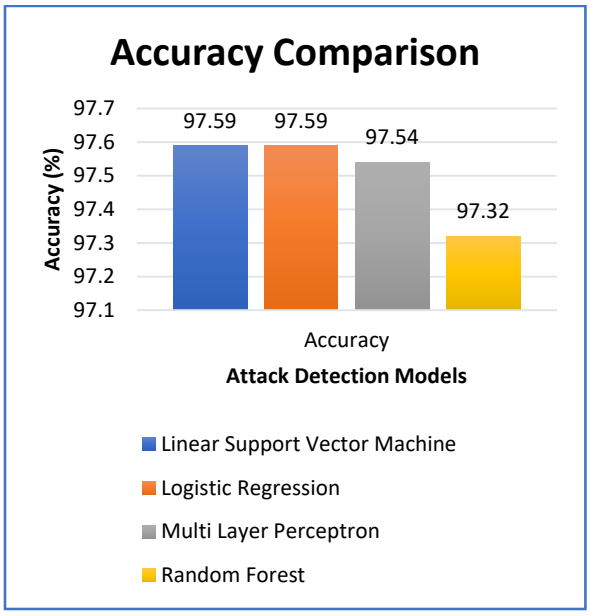

Figure 11: Performance of ML models in attack detection and classification in terms of accuracy

As presented in Figure 9, accuracy is the measure used to compare performance of different ML models in attack detection and classification. Higher accuracy indicates better performance. SVM exhibited 97.59% accuracy, LR 97.59%, MLP 97.54%and RF showed 97.32% accuracy. From the results it is observed that highest accuracy is achieved by SVM and LR models with 97.59% accuracy.

The observations form the empirical study provided many valuable insights. First, the proposed parameter optimization method has its influence on the prediction of performance of ML models. The random search based hyperparameter optimization is found more efficient than grid based models found in the literature. The underlying ML models in the proposed framework are able to achieve more than 97% accuracy with the underlying hyperparameter optimization technique.

5. CONCLUSION AND FUTURE WORK

In this paper, we proposed a ML framework for automatic detection and classification of cyber-attacks in IoT use cases. Our framework takes dataset as input. Then the data is subjected analysis to

understand attack distribution and know whether data has any sort of imbalance. Afterwards, treating null values and one hot encoding are carried out as part of pre-processing. Feature selection follows it to improve quality of training. Feature importance is computed and features with more than 0.3 correlation with corresponding attack label are considered for training process. Afterwards, the ML models are built and trained. The trained models are further used to evaluate test data to arrive at attack detection and classification results. We proposed a hyperparameter optimization method, designed for optimization of parameters of four ML techniques in tune with the dataset, used in the proposed framework. An algorithm named Learning based Optimal Machine Learning for Cyber Attack Detection and Classification (LbOML-CADC) is also proposed. This algorithm exploits hyperparameter tuning method for efficient detection and classification of cyber-attacks. We evaluated our framework using UNSW-NB15 dataset. Our empirical study reveals that highest accuracy achieved is 97.59%.

References

[1] Mahmoud Elsisi; Minh-Quang Tran; Karar Mahmoud; Diaa-Eldin A. Mansour; Matti Lehtonen and Mohamed M. F. Darwish; (2021). Towards Secured Online Monitoring for Digitalized GIS Against Cyber-Attacks Based on IoT and Machine Learning . IEEE Access. http://doi:10.1109/ACCESS.2021.3083499

[2] MINH-QUANG TRAN, MAHMOUD ELSISI, KARAR MAHMOUD , MENG-KUN LIU, MATTI LEHTONEN AND MOHAMED M. F. DARWISH. (2021). Experimental Setup for Online Fault Diagnosis of Induction Machines via Promising IoT and Machine Learning: Towards Industry 4.0 Empowerment. *IEEE*. 9, pp.115429-115441. http://doi:10.1109/ACCESS.2021.3105297

[3] Pallavi Arora; Baljeet Kaur and Marcio Andrey Teixeira; (2021). Evaluation of Machine Learning Algorithms Used on Attacks Detection in Industrial Control Systems . Journal of The Institution of Engineers (India): Series B. http://doi:10.1007/s40031-021-00563-z

[4] Hasan, Mahmudul; Milon Islam, Md.; Islam, Ishrak and Hashem, M.M.A. (2019). Attack and Anomaly Detection in IoT Sensors in IoT Sites Using Machine Learning Approaches. Internet of Things, 100059–. http://doi:10.1016/j.iot.2019.100059

[5] Aboelwafa, Mariam M. N.; Seddik, Karim G.; Eldefrawy, Mohamed H.; Gadallah, Yasser and Gidlund, Mikael (2020). A Machine Learning-Based Technique for False Data Injection Attacks Detection in Industrial IoT. IEEE Internet of Things Journal, 1–1. http://doi:10.1109/JIOT.2020.2991693

[6] YAKUB KAYODE SAHEED and AND MICHEAL OLAOLU AROWOLO. (2021). Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Netw. *IEEE*. 9, pp.161546-161554. http://doi:10.1109/ACCESS.2021.3128837

[7] Ahmad Ali AlZubi; Mohammed Al-Maitah and Abdulaziz Alarifi; (2021). Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques . Soft Computing. http://doi:10.1007/s00500-021-05926-8

[8] Shafiq, Muhammad; Tian, Zhihong; Bashir, Ali Kashif; Du, Xiaojiang and Guizani, Mohsen (2020). CorrAUC: a Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine Learning Techniques. IEEE Internet of Things Journal, 1–1. http://doi:10.1109/JIOT.2020.3002255

[9] Rahman, Md Arafatur; Asyharia, A. Taufiq; Leong, L.S.; Satrya, G.B.; Tao, M. Hai and Zolkipli, M.F. (2020). Scalable Machine Learning-Based Intrusion Detection System for IoT-Enabled Smart Cities. Sustainable Cities and Society, 102324–. http://doi:10.1016/j.scs.2020.102324

[10] Pheeha Machaka, Olasupo Ajayi, Hloniphani Maluleke, Ferdinand Kahenga, Antoine Bagula, Kyandoghere Kyamakya. (2022). Modelling DDoS Attacks in IoT Networks Using Machine Learning. *Springer*., pp.1-20.

[11] Abhishek Verma and Virender Ranga. (2019). Machine Learning Based Intrusion Detection Systems for IoT Applications. *Springer*., pp.1-24. https://doi.org/10.1007/s11277-019-06986-8

[12] Maede Zolanvari, Marcio A. Teixeira, Lav Gupta, Khaled M. Khan and Raj Jain. (2019). Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things. *IEEE*. 6(4), pp.1-13. http://DOI:10.1109/JIOT.2019.2912022

[13] Adi, Erwin; Anwar, Adnan; Baig, Zubair and Zeadally, Sherali (2020). Machine learning and data analytics for the IoT. Neural Computing and Applications. http://doi:10.1007/s00521-020-04874-y

[14] Hussain, Fatima; Hussain, Rasheed; Hassan, Syed Ali and Hossain, Ekram (2020). Machine Learning in IoT Security: Current Solutions and Future Challenges. IEEE Communications Surveys & Tutorials, 1–1. http://doi:10.1109/COMST.2020.2986444

[15] Geetha, R. and Thilagam, T. (2020). A Review on the Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security. Archives of Computational Methods in Engineering,. http://doi:10.1007/s11831-020-09478-2

[16] Liang, Fan; Hatcher, William G.; Liao, Weixian; Gao, Weichao and Yu, Wei (2019). Machine Learning for Security and the Internet of Things: the Good, the Bad, and the Ugly. IEEE Access, 1–1. http://doi:10.1109/access.2019.2948912

[17] Mohanta, B. K., Jena, D., Satapathy, U., & Patnaik, S. (2020). Survey on IoT Security:Challenges and Solution using Machine Learning, Artificial Intelligence and Blockchain Technology. Internet of Things, 100227. http://doi:10.1016/j.iot.2020.100227

[18] da Costa, Kelton A.P.; Papa, João P.; Lisboa, Celso O.; Munoz, Roberto and de Albuquerque, Victor Hugo C. (2019). Internet of Things: A Survey on Machine Learning-based Intrusion Detection Approaches. Computer Networks, S1389128618308739–. http://doi:10.1016/j.comnet.2019.01.023

[19] Shereen Ismail, Diana Dawoud and Hassan Reza. (2022). Machine learning techniques for Detection of Cyber Attacks in IoT Use Cases. *IEEE*. .(.), pp.0481-0486.

[20] Iqbal H. Sarker,Asif Irshad Khan,Yoosef B. Abushark and Fawaz Alsolami. (2022). Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Direction. *Springer*, p.296–312. http://doi:10.20944/preprints202203.0087.v1

[21] Hao Xu, Zihan Sun, Yuan Cao and Hazrat Bilal. (2023). A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things. *Springer*, pp.1-13. https://doi.org/10.1007/s00500-023-09037-4

[22] Hemantha Krishna Bharadwaj; Aayush Agarwal;Vinay Chamola; Naga Rajiv Lakkaniga; Vikas Hassija; Mohsen Guizani and Biplab Sikdar; (2021). A Review on the Role of Machine Learning in Enabling IoT Based Healthcare Applications . IEEE Access. http://doi:10.1109/access.2021.3059858

[23] Elena Becker, Maanak Gupta and Kshitiz Aryal. (2023). Using Machine Learning for Detection and Classification of Cyber Attacks in Edge IoT. *IEEE*, pp.1-11. http://DOI:10.1109/EDGE60047.2023.00063

[24] Hao Xu, Zihan Sun, Yuan Cao and Hazrat Bilal. (2023). A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things. *Springer*., p.14469–14481. https://doi.org/10.1007/s00500-023-09037-4

[25] Shaukat, Kamran; Luo, Suhuai; Varadharajan, Vijay; Hameed, Ibrahim A. and Xu, Min (2020). A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. IEEE Access, 8, 222310–222354. http://doi:10.1109/access.2020.3041951

[26] Prabhat Kumar; Govind P. Gupta and Rakesh Tripathi; (2021). Toward Design of an Intelligent Cyber Attack Detection System using Hybrid Feature Reduced Approach for IoT Networks . Arabian Journal for Science and Engineering. http://doi:10.1007/s13369-020-05181-3

[27] Skowron, Monika; Janicki, Artur and Mazurczyk, Wojciech (2020). Traffic Fingerprinting Attacks on Internet of Things using Machine Learning. IEEE Access, 1–1. http://doi:10.1109/ACCESS.2020.2969015

[28] Chhabra, Gurpal Singh; Singh, Varinder Pal and Singh, Maninder (2018). Cyber forensics framework for big data analytics in IoT environment using machine learning. Multimedia Tools and Applications. http://doi:10.1007/s11042-018-6338-1

[29] Eirini Anthi; Lowri Williams; Amir Javed and Pete Burnap; (2021). Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks . Computers & Security. http://doi:10.1016/j.cose.2021.102352

[30] Li, Fangyu; Shinde, Aditya; Shi, Yang; Ye, Jin; Li, Xiang-Yang and Song, Wen Zhan (2019). System Statistics Learning-Based IoT Security: Feasibility and Suitability. IEEE Internet of Things Journal, 1–1. http://doi:10.1109/JIOT.2019.2897063

[31] Moustafa, Nour, and Jill Slay. "UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)." Military Communications and Information Systems Conference (MilCIS), 2015. IEEE, 2015.

[32] Moustafa, Nour, and Jill Slay. "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 dataset and the comparison with the KDD99 dataset." Information Security Journal: A Global Perspective (2016): 1-14.

[33] Moustafa, Nour, *et al*. . "Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks." IEEE Transactions on Big Data (2017).

[34] Nelder, J. A.; Mead, R. (1965). A Simplex Method for Function Minimization. The Computer Journal, 7(4), 308–313. http://doi:10.1093/comjnl/7.4.308.

[35] S. Kirkpatrick, C. D. Gelatt, and M. P. Vecchi. Optimization by simulated annealing. Science, 220 (4598):671–680, 1983.

[36] M. J. D. Powell. A direct search optimization method that models the objective and constraint functions by linear interpolation. Advances in Optimization and Numerical Analysis, pages 51– 67, 1994. http://doi:10.1007/978-94-015-8330-5_4.

[37] UNSW-NB dataset. Retrieved from https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15