WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Using Machine Learning to Detect Cyber Attacks

Ravi B Prakash[1], Prof Rajeshwari K[2]

[1]Undergraduate, Dept of Information Science, BMS College of Engineering, Bangalore, India ravib.is20@bmsce.ac.in
[2]Assistant Professor, Dept of Information Science, BMS College Of Engineering, Bangalore, India rajeshwarik.ise@bmsce.ac.in
DOI: https://doi.org/10.55248/gengpi.5.0224.0555

ABSTRACT—

With the relentless growth in cyber threats, the imperative to fortify digital systems against malicious activities has become paramount. Leveraging the capabilities of machine learning (ML) has emerged as a pivotal strategy for bolstering cybersecurity defenses. This paper provides an in-depth exploration of the application of ML techniques in the realm of cyber attack detection. The study delves into the intricacies of feature selection, data preprocessing, and model evaluation techniques, pivotal components in refining the accuracy and efficiency of ML-based cybersecurity systems. The paper illustrates the practical implementation of these ML models across diverse cyber attack scenarios, showcasing their effectiveness in identifying and mitigating threats.

Keywords—Intrusion Detection Systems, machine learning, deep learning, cyber attacks

I. Introduction

In the contemporary digital landscape, the surge in cyber threats has propelled the integration of machine learning (ML) into cybersecurity as an innovative approach to fortify defenses. The efficacy of such a fusion hinges on a comprehensive understanding of both machine learning principles and the intricacies of cybersecurity. This paper delves into the domain knowledge required for effectively navigating the convergence of these two dynamic fields.

At the core of cybersecurity is a profound comprehension of the diverse threats that assail digital systems. Cybersecurity professionals must be well-versed in identifying and categorizing threats such as malware, phishing attacks, ransomware, and the stealthy advanced persistent threats (APTs). A nuanced understanding of vulnerabilities in both systems and networks is indispensable to preemptively address potential points of exploitation.

Simultaneously, a solid grasp of machine learning concepts forms the bedrock for deploying ML techniques in cybersecurity. Supervised learning, where models are trained on labeled datasets, allows for the recognition of known patterns associated with cyber threats. Unsupervised learning, on the other hand, plays a pivotal role in anomaly detection, identifying deviations from established norms that may signify a potential threat. Deep learning architectures, including neural networks, provide the capability for complex pattern recognition essential in tackling the sophisticated nature of modern cyber attacks.

II. Literature Survey

This paper[1] proposes an ensemble model which enhances the performance of IDS. The chi-squared feature selection method selects the attribute of the NSL-KDD dataset which are more dependent on the class label. Performance parameters such as Accuracy, Precision, Recall, and F1-Measure for evaluating the performance of the models are used. The experiment result reveals that the ensemble model which is AdaBoost with Logistic Regression performs better than all other models.

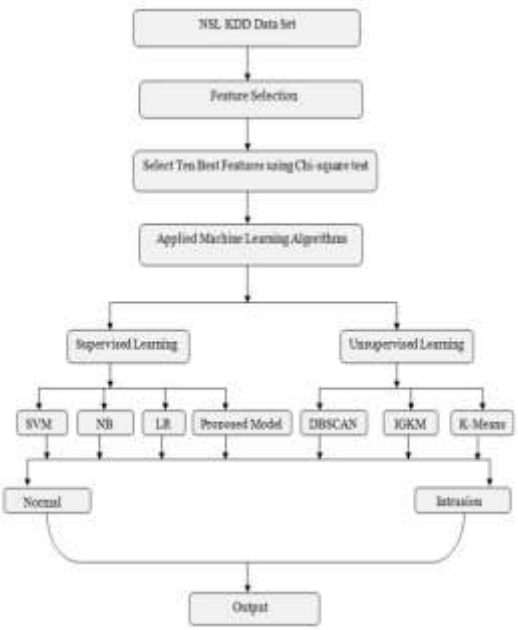

Fig 1. Structure of Intrusion Detection Model

Model	Attack	Accuracy
B.N (B. Selvakumar et al.)	DOS	99.95%
	Probe	93.42%
	R2L	97.83%
	U2R	68.97%
C4.5 (B. Selvakumar et al.)	DOS	99.98%
	Probe	63.85%
	R2L	98.73%
	U2R	17.24%
Proposed Model	DOS	99.91%
	Probe	99.6%
	R2L	99.90%
	U2R	98.15%

Table 1. Comparison with state of art model

Supervised Learning					
Algorithm	Attack	Accuracy	Precision	Recall	F-Score
SVM	DOS	91.18%	87%	91.8%	89.3%
	Probe	81.33%	42.7%	95.2%	58.9%
	R2L	85.57%	63%	64.4%	11.4%
	U2R	84.98%	34.2%	96.4%	50.5%
NB	DOS	93.9%	89.8%	95.8%	92.7%
	Probe	93.40%	69.2%	95.8%	80.4%
	R2L	97.8%	38.1%	76.3%	50.8%
	U2R	86.1%	35.8%	94.6%	52%
LR	DOS	98.4%	98.7%	97.4%	98%
	Probe	98.19%	93.8%	93.4%	93.6%
	R2L	98.95%	75%	40.7%	52.7%
	U2R	97.8%	90.2%	82.1%	86%
Proposed Model	DOS	99.91%	99.80%	99.99%	99.99%
	Probe	99.6%	99.4%	98.2%	98.8%
	R2L	99.90%	98.2%	94.9%	96.6%
	U2R	98.15%	87.7%	89.3%	88.50%

Table 2. Experiment results of supervised learning models

In this paper[2], a transfer learning and ensemble learning-based IDS is proposed for IoV systems using convolutional neural networks (CNNs) and hyper-parameter optimization techniques. In the experiments, the proposed IDS has demonstrated over 99.25% detection rates and F1-scores on two well-known public benchmark IoV security datasets: the Car-Hacking dataset and the CICIDS2017 dataset. This shows the effectiveness of the proposed IDS for cyber-attack detection in both intra-vehicle and external vehicular networks.

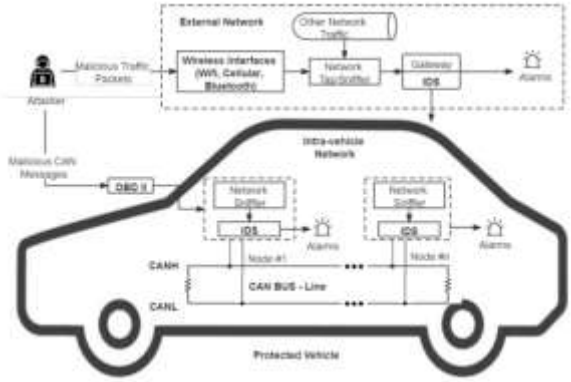

Fig 2. The IDS-protected vehicle architecture

Method	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)	Training Time (s)	Test Time Per Packet (ms)
P-LeNet [1]	98.10	98.14	98.04	97.83	-	-
1D-CNN [5]	99.96	99.94	99.63	99.80	-	-
DCNN [7]	99.93	99.84	99.84	99.91	-	-
VGG16-PSO	99.97	99.97	99.97	99.97	384.9	0.2
VGG19-PSO	100.0	100.0	100.0	100.0	417.9	0.2
Xception-PSO	100.0	100.0	100.0	100.0	529.2	0.3
Inception-PSO	100.0	100.0	100.0	100.0	733.6	0.6
InceptionResnet -PSO	100.0	100.0	100.0	100.0	970.4	1.3
Concatenation (Proposed)	**100.0**	**100.0**	**100.0**	**100.0**	**2490.5**	**3.2**
Confidence Averaging (Proposed)	**100.0**	**100.0**	**100.0**	**100.0**	**1680.7**	**2.7**

Table 3. Performance evaluation of models on car-hacking dataset

Method	Accuracy (%)	Precision (%)	Recall (%)	F1 (%)	Training Time (s)	Test Time Per Packet (ms)
KNN [12]	96.3	96.2	93.7	96.3	15243.6	0.2
RF [12]	98.82	98.8	99.955	98.8	1848.3	0.3
MLP [4]	99.46	99.52	99.40	99.46	-	1.1
VGG16-PSO	99.724	99.625	99.724	99.674	436.5	0.1
VGG19-PSO	99.849	99.850	99.849	99.850	688.1	0.1
Xception-PSO	99.699	99.700	99.699	99.697	655.5	0.2
Inception-PSO	99.750	99.725	99.750	99.729	782.8	0.3
InceptionResnet -PSO	99.849	99.850	99.849	99.850	1187.2	0.7
Concatenation (Proposed)	**99.899**	**99.900**	**99.899**	**99.898**	**3598.7**	**1.8**
Confidence Averaging (Proposed)	**99.925**	**99.925**	**99.924**	**99.925**	**2658.1**	**1.5**

Table 4. Performance evaluation of models on CICIDS2017 dataset

As the rapid progress in honeypot detection using machine learning technologies, this paper[3] proposes a new automatic identification model based on random forest algorithm with three group features: application-layer feature, network-layer feature, and other system-layer feature. The experiment datasets are collected from public known platforms and designed to prove the effectiveness of the proposed model. The experiment results showed that the presented model achieved a high area under curve (AUC) value with 0.93 (area under the receiver operating characteristic curve), which is better than other machine learning algorithms.

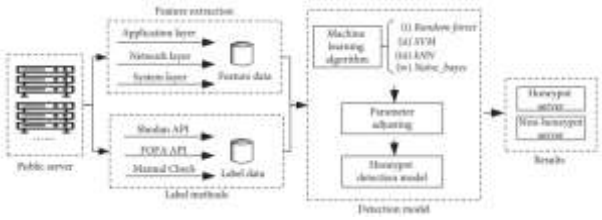

Fig 3. The framework of proposed automatic identification methods

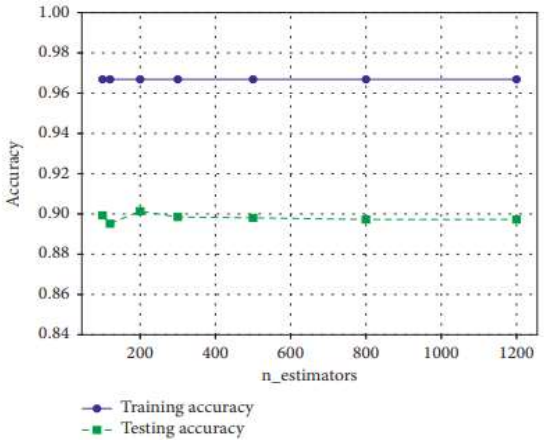

Fig 4. The effect of different values of 'n_estimators' on the accuracy

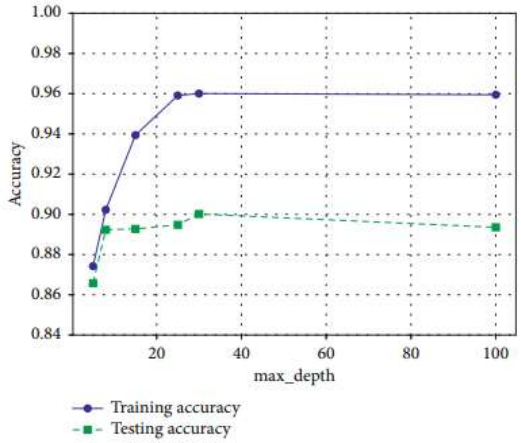

Fig 5. The effect of different values of 'max_depth' on the accuracy

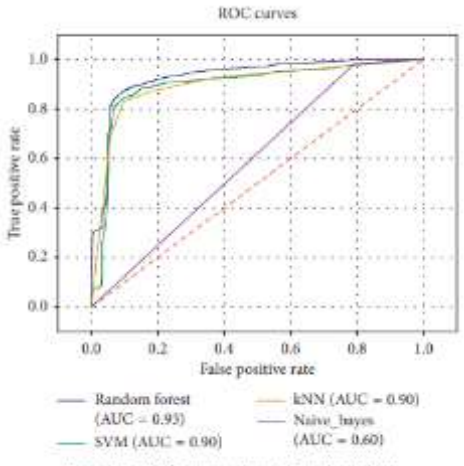

Fig 6. ROC curves about four algorithms

In this paper[4], the Network Security Laboratory Knowledge Discovery and Data Mining benchmark data set has been used to evaluate Network Intrusion Detection Systems (NIDS) by using different machine learning algorithms such as Support Vector Machine, J48, Random Forest, and Naïve Bytes with both binary and multiclass classification. The results of the application of those techniques are discussed in detail and outperformed previous works. The performance of these classifiers was tested on 13 features of the dataset for first, detections if the network flow is normal or attacks, and second if the detections show if there are any type of attacks on this flow.

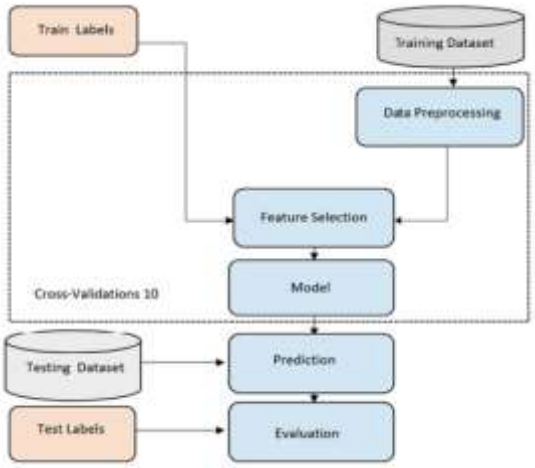

Fig 7. Flowchart sequence of steps for build IDS models

Classifier	Test options	Accuracy (%)	Precision (%)	Recall (%)	F- measures (%)	MCC (%)	Roc area (%)
RF	Cross Validation	98.02	98.0	98.0	98.0	97.8	99.9
	NSL-KDD Test	98.77	98.8	98.8	98.8	97.5	99.9
J48	Cross Validation	98.00	98.0	98.0	98.0	95.9	99.1
	NSL-KDD Test	98.20	98.2	98.2	98.2	96.3	99.6
SVM	Cross Validation	97.26	97.3	97.3	97.3	94.4	97.2
	NSL-KDD Test	97.79	97.8	97.8	97.8	95.5	97.8
Bayesian	Cross Validation	94.12	94.1	94.1	94.1	88.1	98.6
	NSL-KDD Test	94.97	95.0	95.0	95.0	89.7	98.7

Table 5. Cross-validation and test result of binary classification

Classifier	Test options	Accuracy (%)	Precision (%)	Recall (%)	F- measures (%)	MCC (%)	Roc area (%)
RF	Cross Validation	98.0	97.2	97.3	97.3	97.3	85.3
	NSL-KDD Test	97.9	98.0	98.0	98.0	98.8	99.9
J48	Cross Validation	98.0	97.0	97.0	97.0	95.3	99.6
	NSL-KDD Test	97.4	97.5	97.4	97.4	95.8	99.9
SVM	Cross Validation	96.2	96.3	96.2	96.2	94.0	98.4
	NSL-KDD Test	96.4	96.5	96.5	96.5	94.3	98.4
Bayesian	Cross Validation	86.2	89.0	86.3	86.7	77.2	97.2
	NSL-KDD Test	87.4	89.8	87.4	87.8	79.0	98.0

Table 6. Cross-validation and test result of multi-classification

Due to the dynamic nature of malware with continuously changing attacking methods, the malware datasets available publicly are to be updated systematically and benchmarked. In this paper[5], a deep neural network (DNN), a type of deep learning model, is explored to develop a flexible and effective IDS to detect and classify unforeseen and unpredictable cyber attacks. The continuous change in network behavior and rapid evolution of attacks makes it necessary to evaluate various datasets which are generated over the years through static and dynamic approaches. This type of study facilitates identifying the best algorithm which can effectively work in detecting future cyber attacks. A comprehensive evaluation of experiments of DNNs and other classical machine learning classifiers are shown in various publicly available benchmark malware datasets.

Layers	Type	Output shape	Number of units	Activation function	Parameters
0-1	fully-connected	(None, 1,024)	1,024	ReLU	43,008
1-2	Batch Normalization	(None, 1,024)			4,096
2-3	Dropout (0.01)	(None, 1,024)			0
3-4	fully-connected	(None, 768)	768	ReLU	7,87,200
4-5	Batch Normalization	(None, 768)			3,072
5-6	Dropout (0.01)	(None, 768)			0
6-7	fully-connected	(None, 512)	512	ReLU	3,93,728
7-8	Batch Normalization	(None, 512)			2,048
8-9	Dropout (0.01)	(None, 512)			0
9-10	fully-connected	(None, 256)	256	ReLU	1,31,328
10-11	Batch Normalization	(None, 256)			1,024
11-12	Dropout (0.01)	(None, 256)			0
12-13	fully-connected	(None, 128)	128	ReLU	32,896
13-14	Batch Normalization	(None, 128)			512
14-15	Dropout (0.01)	(None, 128)			0
15-16	fully-connected	KDDCup 99- NSL-KDD- UNSW-NB15- Kyoto- WSN-DS- CICIDS 2017-	Binary, Multi-class 1, 5- 1, 5- 1, 10- 1- 1, 5 1, 6	Sigmoid for Binary and Softmax for Multi-class classification	

Table 7. Configuration of proposed DNN model

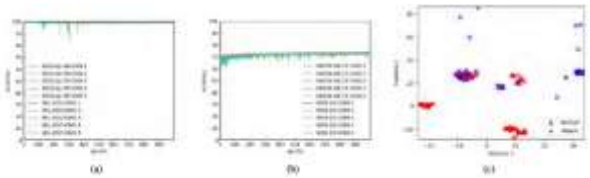

Fig 8. Train accuracy. (a)KDDCup 99 and NSL-KDD. (b) UNSW-NB-15 and WSN-DS. c. Visualization of 100 connection records with their corresponding activation values of the last hidden layer neurons from Kyoto

In this study[6], the CPS is modeled as a network of agents that move in unison with one another, with one agent acting as a leader and commanding the other agents. The proposed strategy in this study is to employ the structure of deep neural networks for the detection phase, which should tell the system of the attack's existence in the early stages of the attack. The use of robust control algorithms in the network to isolate the misbehaving agent in the leader-follower mechanism has been researched. Following the attack detection phase with a deep neural network, the control system uses the reputation algorithm to isolate the misbehaving agent in the presented control method. Experiment results show that deep learning algorithms can detect attacks more effectively than traditional methods, making cyber security simpler, more proactive, and less expensive.

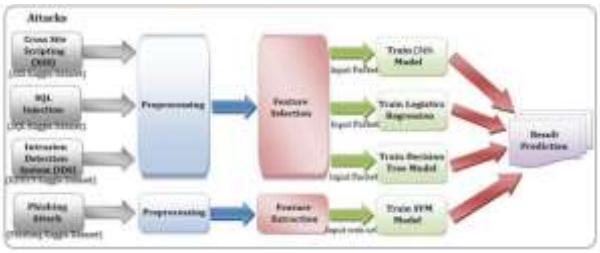

Fig 9. System architecture

Attack	Algorithm	Accuracy
Intrusion Detection	Decision Tree	99.47%
	KNN Classifier	99.16%
	BNB Classifier	90.67%
SQL Injection Attack	Logistic Regression	92.85%
Cross Site Scripting Attack (XSS)	Convolutional Neural Network	98.59%
Phishing Attack	Support Vector Machine	82.63%

Table 8. Comparative analysis

The proposed transformer-based system outperforms traditional machine learning methods and existing deep learning approaches in terms of accuracy, precision, and recall, demonstrating the effectiveness of deep learning for intrusion detection in Industry 5.0. This study's[7] findings showcased the superiority of the proposed transformer-based system, outperforming previous approaches in accuracy, precision, and recall. This highlights the significant contribution of deep learning in addressing cybersecurity challenges in Industry 5.0 environments.

Layer (type)	Output Shape	Param. No.
conv2d (Conv2D)	(None, 126, 126, 32)	896
max_pooling2d (MaxPooling2D)	(None, 63, 63, 32)	0
conv2d_1 (Conv2D)	(None, 61, 61, 64)	18,496
max_pooling2d_1 (MaxPooling2D)	(None, 30, 30, 64)	0
conv2d_2 (Conv2D)	(None, 28, 28, 128)	73,856
max_pooling2d_1 (MaxPooling2D)	(None, 14, 14, 128)	0
flatten (Flatten)	(None, 25,088)	0
dense (Dense)	(None, 128)	3,211,392
dense_1 (Dense)	(None, 2)	258

Table 9. Model architecture and parameters

Model	Accuracy	Precision	Recall	F1 Score
CNNs	0.94	0.92	0.91	0.92
RNNs	0.95	0.93	0.92	0.93
Transformer model	0.96	0.94	0.94	0.94

Table 10. Performance of deep learning models

This paper[8] has proposed a cloud intrusion detection system (IDS) that is focused on boosting the classification accuracy by improving feature selection and weighing the ensemble model with the crow search algorithm (CSA). The feature selection is handled by combining both filter and automated models to obtain improved feature sets. The ensemble classifier is made up of machine and deep learning models such as long short-term memory (LSTM), support vector machine (SVM), XGBoost, and a fast learning network (FLN). The proposed ensemble model's weights are generated with the CSA to obtain better prediction results. Experiments are executed on the NSL-KDD, Kyoto, and CSE-CIC-IDS-2018 datasets. The simulation shows that the suggested system attained more satisfactory results in terms of accuracy, recall, precision, and F-measure than conventional approaches.

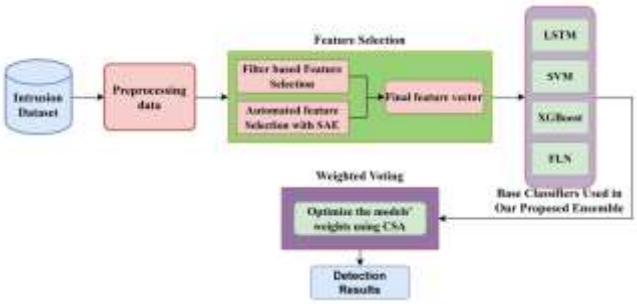

Fig 10. Proposed block diagram

Methodology	ACC	R	P	F
SMOTE-LSTM+AM	96.20	96.00	96.00	-
CNN	95.14	-	-	-
DSSTE+miniVGGNet	96.99	96.97	97.46	97.04
IBM	96.55	94.00	-	-
DNN+PSO	95.00	98.20	-	-
DNN	90.25	59.00	65.00	-
PTDAE+DNN	95.79	95.79	95.38	95.11
HCRNN	97.75	97.12	96.33	97.60
ABC-BWO-CONV-LSTM	98.25	98.67	97.48	98.18
IG+GR+CS-SVM	99.89	92.93	93.02	92.97
Our Proposed Ensemble	**99.99**	**99.87**	**99.96**	**99.91**

Table 11. Comparison of the proposed ensemble with recent methods on the CSF-CIC-IDS 2018 dataset

This paper[9] proposes an alternate approach inspired by honeypots to detect adversaries. The approach yields learned models with an embedded watermark. When an adversary initiates an interaction with the model, attacks are encouraged to add this predetermined watermark stimulating detection of adversarial examples. It is shown that HoneyModels can reveal 69.5% of adversaries attempting to attack a Neural Network while preserving the original functionality of the model. HoneyModels offer an alternate direction to secure Machine Learning that slightly affects the accuracy while encouraging the creation of watermarked adversarial samples detectable by the HoneyModel but indistinguishable from others for the adversary.

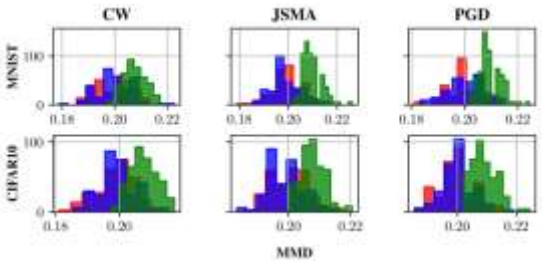

Fig 11. Distribution of maximum mean discrepancy scores from adversarial samples from benign model and honeypot model compared among themselves.

This research[10] aims to introduce a study on ML-based IDS in IoT, considering different feature extraction algorithms with several ML models. This study evaluated several feature extractors, including image filters and transfer learning models, such as VGG-16 and DenseNet. Additionally, several machine learning algorithms, including random forest, K-nearest neighbors, SVM, and different stacked models were assessed considering all the explored feature extraction algorithms. The study presented a detailed evaluation of all combined models using the IEEE Dataport dataset. Results showed that VGG-16 combined with stacking resulted in the highest accuracy of 98.3%.

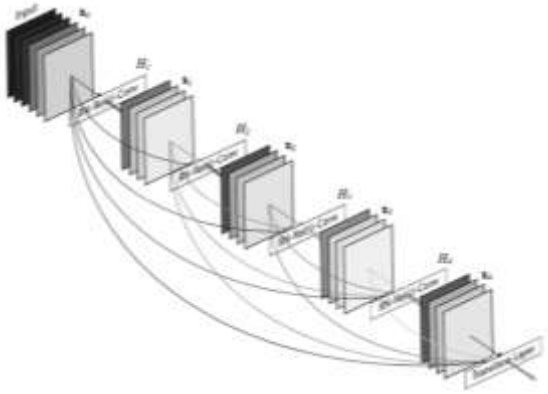

Fig 12. DenseNet architecture

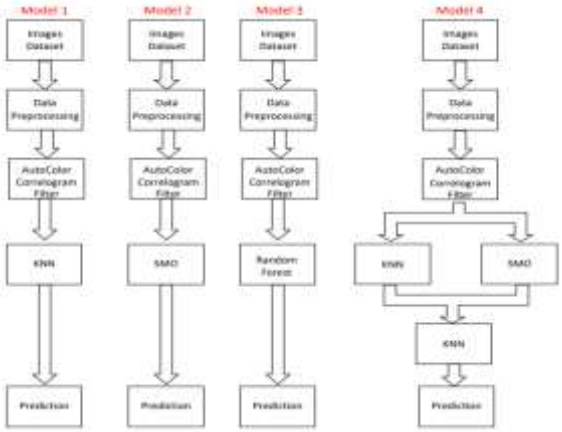

Fig 13. Four models with auto-color correlogram filter

This paper[11] has used an advanced intrusion detection system with high network performance to detect the unknown attack package, by using a deep neural network algorithm, also in this model, the attack detection is done by two ways (binary classification and multiclass classification). The proposed system has shown encouraging results in terms of the high accuracy (99.98% with multiclass classification and with binary classification). The proposed intrusion detection system discover the attacks by using a deep neural network algorithm with anomaly detection techniques without accessing information in the packet payload to avoid a breach of data privacy.

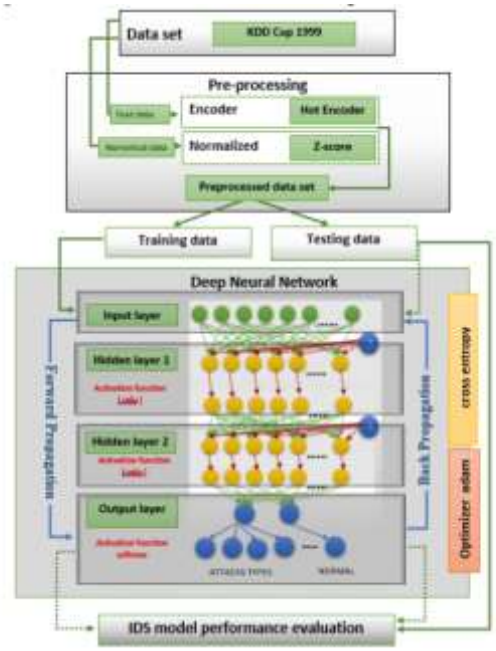

Fig 14. Block diagram of the proposed DNN-NIDS

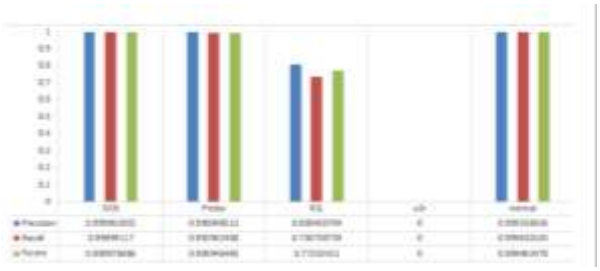

Fig 15. Evaluation results for multiclass classification

This paper[12] proposes the use of deep learning architectures to develop an adaptive and resilient network intrusion detection system (IDS) to detect and classify network attacks. The emphasis is how deep learning or deep neural networks (DNNs) can facilitate flexible IDS with learning capability to detect recognized and new or zero-day network behavioral features, consequently ejecting the systems intruder and reducing the risk of compromise. To demonstrate the model's effectiveness, we used the UNSW-NB15 dataset, reflecting real modern network communication behavior with synthetically generated attack activities.

Optimization Functions: $F_k(f_1,\ldots f_k)$
Gradient Descent Optimization Algorithm: $G_a(g_1,\ldots g_a)$
Dropout Rate: $D_r(d_1,\ldots dr)$
Batch Size: $B_s(b_1,\ldots b_s)$ each consecutive $b_i = 2^*b_{i-1}$
Learning Rate: $L_j(l_1,\ldots l_j)$ each consecutive $l_j = .8\ l_{j-1}$

```
Assign a midway dropout rate, batch size and learning rate from given sample space
  for i =1 to k (Fk)
    for j=1 to a (Ga)
      run models, save as baseline models (deploy EarlyStopping, ModelCheckpoint)
      increment dropout rate, batch size, learning rate one at a time
        if (new_model < baseline) switch sample space direction else update baseline
    end for
  end for
```

Fig 16. A semi-dynamic hyperparameter optimization approach

Fig 17. Learning curve accuracy for the multiclass classification model

This study[13] proposes a hybrid intrusion detection software architecture for IDS using machine learning algorithms. By placing appropriate machine learning algorithms in the existing detection systems, improvements in attack detection and classification can be obtained. This paper has also attempted to compare the machine learning algorithms by testing them in a simulated environment to make performance evaluations. The approach provides indicators in selecting machine learning algorithms that can be used for a generic intrusion detection system in the context of industrial control applications.

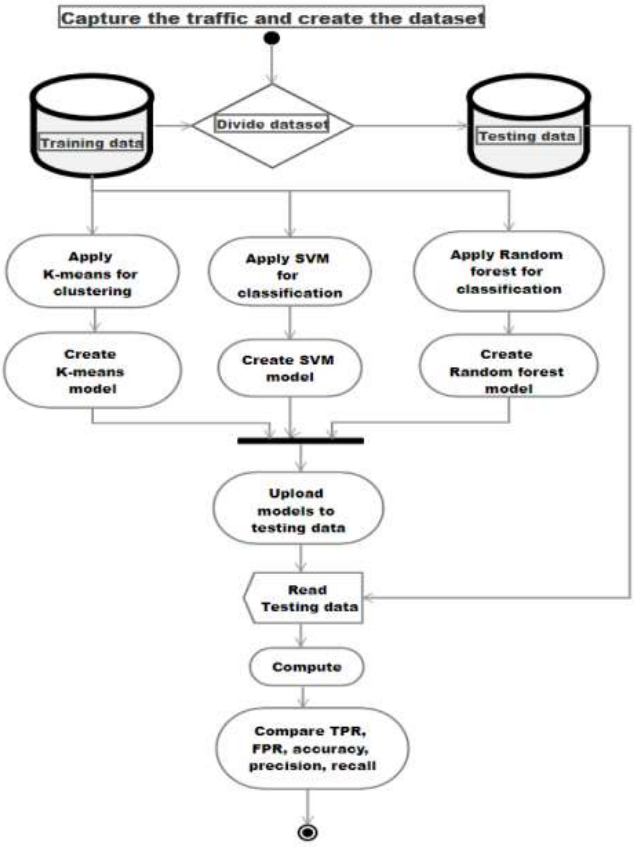

Fig 18. Process followed in experiments

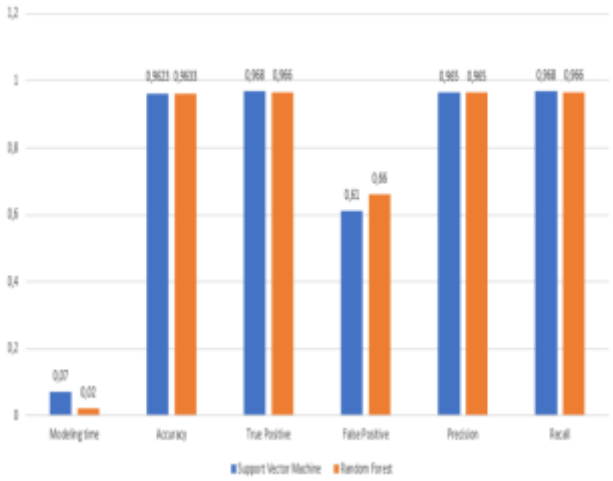

Fig 19. Metrics comparison

This paper[14] investigates the possibility of training an ML-based NIDS for an ICS (specifically, the well-known Secure Water Treatment testbed) by combining network traffic data and physical process data. In the supplied dataset, data had already been labeled "according to normal and abnormal behaviors"; the labeling of data collected around the start and end of each attack was scrutinized and, where found to be problematic, labeled data were excluded in order to improve the effectiveness of supervised learning. The ML technique of "Learning using Privileged Information" was evaluated and found to be superior to six baseline ML algorithms trained on network traffic data alone.

In this paper[15], a model is being proposed, where the data is preprocessed before training with the algorithms. A study done by comparing with other models shows that, the current model built with Random Forest can outperform other existing models built with ANN when the data is preprocessed. After building model after data pre-processing and feature extraction, we are able to achieve 98.71% accuracy on the NSL-KDD dataset.

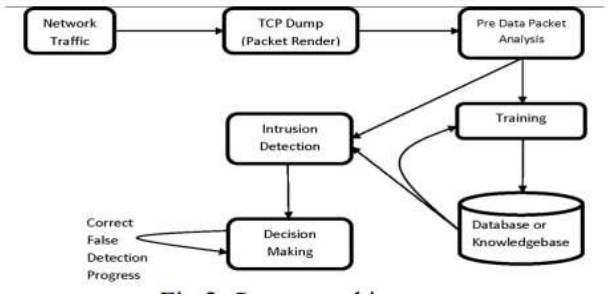

Fig 20. System architecture

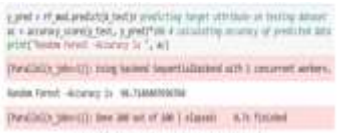

Fig.5: Random forest accuracy

Random Forest accuracy achieved is 98.71409%

Fig.6: MLP accuracy

MLP accuracy achieved is 97.7487%

Conclusion

The integration of machine learning into cybersecurity for the detection of cyber attacks represents a paradigm shift in fortifying digital defenses against an ever-evolving threat landscape. The applications of machine learning in this domain, ranging from malware detection and anomaly identification to phishing detection and incident response automation, showcase the versatility and potential of this innovative approach.

The inherent adaptability of machine learning models to learn from historical data and dynamically adjust to emerging threats positions them as valuable assets in the ongoing battle against cyber adversaries. The efficiency gained through automation allows for real-time analysis of vast datasets, significantly reducing response times and enhancing the overall security posture.

However, the deployment of machine learning in cybersecurity is not without its challenges. Issues such as false positives and negatives, data privacy concerns, model interpretability, and the need for constant maintenance underscore the importance of a nuanced and responsible approach to implementation. Two of the most important metrics we need to keep in mind are response time and false negatives. The response time should be as low as possible for detecting and stopping cyber attacks and the false negative rate should be as low as possible. Since the false negative rate is inversely proportional to recall, the recall score should be as high as possible. Striking a balance between the benefits of automation and the necessity for human oversight is imperative to ensure the reliability and ethical use of machine learning in cybersecurity operations.

As the field continues to evolve, the collaboration between cybersecurity professionals, data scientists, and policymakers becomes increasingly crucial. Addressing legal and ethical considerations, understanding the limitations of machine learning models, and fostering a culture of continuous learning and adaptation will be key to staying ahead of sophisticated cyber threats.

Summary

Author name/ year of publication	**Methodology/ Technique/ Algorithms**	**Dataset**	**Findings**
Mukesh Kumar Yadav , Mahaiyo Ningshen, 2023	Ensemble model, chi-squared feature selection method	NSL-KDD dataset	AdaBoost with Logistic Regression performs better than all other models.
Yang, Li, and Abdallah Shami, 2022	Transfer learning and ensemble learning-based IDS, using CNNs	Car-Hacking dataset and the CICIDS2017 dataset	Over 99.25% detection rates and F1-scores.
Huang, Cheng, 2019	Random forest algorithm with three group features: application-layer feature, network-layer feature, and other system-layer feature.	IP addresses from Shodan and Fofa.	Model achieved a high AUC value (0.93)
Almutairi, Yasmeen, 2022	Support Vector Machine, J48, Random Forest, and Naïve Bytes with both binary and multiclass classification.	Network Security Laboratory Knowledge Discovery and Data Mining benchmark dataset.	In both binary and multi-classifications, the RF classifier achieves the highest score.
R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat and S. Venkatraman, 2019	A deep neural network (DNN), a type of deep learning model.	KDDCup99, NSL- KDD:NS, Kyoto dataset, UNSW- NB15, CICIDS2017.	The classifiers gives less preference for these attack categories, the performance of the DNN is clearly superior to that of classical machine learning algorithms, often by a large margin.
Sumeet Babasaheb Suryawanshi, Tejas Shital katkar, Yash Rajiv Ghute, Prof. Nikita Kawase, Prof. Deepak K. Sharma, 2023	Employ the structure of deep neural networks for the detection phase.	Kaggle datasets	Machine learning techniques can result in higher detection rates, lower false alarm rates, and cheaper computing and transmission costs.
Salam, A.; Ullah, F.; Amin, F.; Abrar, M, 2023	Transformer-based system	KDD Cup 1999, CICIDS2017.	Superiority of the proposed transformer-based system, outperforming previous approaches in accuracy, precision, and recall.
Bakro, M.; Kumar, R.R.; Alabrah, A.A.; Ashraf, Z.; Bisoy, S.K.; Parveen, N.;	Ensemble model with the crow search algorithm (CSA)	NSL-KDD, Kyoto, and CSE-CIC-IDS-2018.	System attained more satisfactory results in terms of accuracy, recall,

Khawatmi, S.; Abdelsalam, A, 2023			precision, and F-measure than conventional approaches.
Abdou, Ahmed, 2021	Approach yields learned models with an embedded watermark	MNIST and CIFAR10.	HoneyModels can reveal 69.5% of adversaries attempting to attack a Neural Network.
Musleh, D.; Alotaibi, M.; Alhaidari, F.; Rahman, A.; Mohammad, R.M, 2023	VGG-16 and DenseNet	IEEE Dataport	VGG-16 combined with stacking resulted in the highest accuracy of 98.3%.
Mohammed Maithem and Ghadaa A. Al-sultany, 2021	deep neural network algorithm with binary classification and multiclass classification	KDD CUP 1999	99.98% accuracy with multiclass classification and with binary classification
Lirim Ashiku, Cihan Dagli, 2021	CNN with regularized multi-layer perceptron,	UNSW-NB15	95.6% accuracy
Plaka, R, 2021	SVM and RF algorithms.	BATADAL.	This algorithm classified 96.8% of the data correctly.
M. Pordelkhaki, S. Fouad and M. Josephs,2021	ML technique of “Learning using Privileged Information	Supplied dataset	This technique evaluated and found to be superior to six baseline ML algorithms
Pallepati, Manvith, 2022	data is preprocessed before training with the RF algorithm.	NSL-KDD	98.71% accuracy

References

[1] Mukesh Kumar Yadav , Mahaiyo Ningshen, 2023, Enhancement of Intrusion Detection System using Machine Learning, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 12, Issue 01 (January 2023)

[2] Yang, Li, and Abdallah Shami. "A transfer learning and optimized CNN based intrusion detection system for Internet of Vehicles." ICC 2022-IEEE International Conference on Communications. IEEE, 2022.

[3] Huang, Cheng et al. “Automatic Identification of Honeypot Server Using Machine Learning Techniques.” Secur. Commun. Networks 2019 (2019): 2627608:1-2627608:8.

[4] Almutairi, Yasmeen et al. "Network Intrusion Detection Using Machine Learning Techniques." Advances in Science and Technology Research Journal, vol. 16, no. 3, 2022, pp. 193-206. doi:10.12913/22998624/149934.

[5] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," in IEEE Access, vol. 7, pp. 41525-41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[6] Detection of Cyber Attacks and Network Attacks using Machine Learning Algorithms - Sumeet Babasaheb Suryawanshi, Tejas Shital katkar, Yash Rajiv Ghute, Prof. Nikita Kawase, Prof. Deepak K. Sharma - IJFMR Volume 5, Issue 6, November-December 2023. DOI 10.36948/ijfmr.2023.v05i06.8900.

[7] Salam, A.; Ullah, F.; Amin, F.; Abrar, M. Deep Learning Techniques for Web-Based Attack Detection in Industry 5.0: A Novel Approach. Technologies 2023, 11, 107. https://doi.org/10.3390/technologies11040107.

[8] Bakro, M.; Kumar, R.R.; Alabrah, A.A.; Ashraf, Z.; Bisoy, S.K.; Parveen, N.; Khawatmi, S.; Abdelsalam, A. Efficient Intrusion Detection System in the Cloud Using Fusion Feature Selection Approaches and an Ensemble Classifier. Electronics 2023, 12, 2427. https://doi.org/10.3390/electronics12112427.

[9] Abdou, Ahmed, et al. "HoneyModels: Machine Learning Honeypots." MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM). IEEE, 2021.

[10] Musleh, D.; Alotaibi, M.; Alhaidari, F.; Rahman, A.; Mohammad, R.M. Intrusion Detection System Using Feature Extraction with Machine Learning Algorithms in IoT. J. Sens. Actuator Netw. 2023, 12, 29. https://doi.org/10.3390/jsan12020029.

[11] Mohammed Maithem and Ghadaa A. Al-sultany, Network intrusion detection system using deep neural networks, 2021 J. Phys.: Conf. Ser. 1804012138.

[12] Lirim Ashiku, Cihan Dagli, Network Intrusion Detection System using Deep Learning, Procedia Computer Science, Volume 185, 2021, Pages 239-247, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2021.05.025.

[13] Plaka, R. (2021). INTRUSION DETECTION USING MACHINE LEARNING FOR INDUSTRIAL CONTROL SYSTEMS (Dissertation).

[14] M. Pordelkhaki, S. Fouad and M. Josephs, "Intrusion Detection for Industrial Control Systems by Machine Learning using Privileged Information," 2021 IEEE International Conference on Intelligence and Security Informatics (ISI), San Antonio, TX, USA, 2021, pp. 1-6, doi: 10.1109/ISI53945.2021.9624757.

[15] Pallepati, Manvith. (2022). Network Intrusion Detection System Using Machine Learning with Data Preprocessing and Feature Extraction. International Journal for Research in Applied Science and Engineering Technology. 10. 2360-2365. 10.22214/ijraset.2022.44326.