INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Hybrid Enhanced Intrusion Detection Frameworks for Cyber-Physical Systems via Optimal Features Selection

Ram Ji[1]*, **Neerendra Kumar**[2], **Devanand Padha**[3]

1 Research Scholar, Department of Computer Science & IT, Central University of Jammu, 181143, (J&K), India
2 Associate Professor, Department of Computer Science & IT, Central University of Jammu, 181143, (J&K), India
3 Professor, Department of Computer Science & Engineering, Model Institute of Engineering & Technology, Kotbhalwal, 181142, Jammu (J&K), India

OPEN ACCESS

Received: 26-05-2024

Accepted: 19-07-2024

Published: 31-07-2024

Citation: Ji R, Kumar N, Padha D (2024) Hybrid Enhanced Intrusion Detection Frameworks for Cyber-Physical Systems via Optimal Features Selection. Indian Journal of Science and Technology 17(30): 3069-3079. https://doi.org/10.17485/IJST/v17i30.1794

* **Corresponding author**.

ramji.adm@cujammu.ac.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Background/Objectives: Cyber-physical systems (CPSs) form the critical infrastructure for many nations like smart grids, home automation, smart cities, smart health care, smart automobiles, etc. These systems are susceptible to various attacks due to their wider surface area. Cyber-attacks on these systems can interrupt the critical services provided by them. Thus, intrusion detection frameworks (IDFs) are needed to identify the attacks on CPSs so that countermeasures can be taken to minimize the harm of such attacks. Limitations of existing IDFs are poor detection rate, high detection time, high false alarm rate, and large space and time complexities. The objective of this study is to design hybrid-enhanced IDFs to overcome these issues. **Methods:** Two enhanced IDFs are proposed in this research work. SelectKBest-MI (mutual information), framework fuses two filter-based feature selection techniques namely SelectKBest and mutual information for selecting optimal features, and the Random Forest (RF) is utilized as a classifier. The second proposed IDF is named CNN-SVM-GWO. Convolutional Neural Network (CNN) is used for extraction of attributes, Support Vector Machine (SVM) and Gray Wolf Optimizer (GWO) are used for the optimal number of feature selection, RF and Extreme Gradient Boosting (XGB) classifiers are used for intrusion detection. Two datasets have been used: CICIDS2017 and CIC-IoT-2023. Parameters considered for comparison with existing techniques are accuracy, precision, recall, F1-score, and prediction time. **Findings:** Implementation of SelectKBest-MI framework using the CICIDS2017 dataset, results in better accuracy of 99.99%, precision of 0.99, recall of 0.99, F1-score 0.99 for binary classification. Implementation of CNN-SVM-GWO framework using CIC-IoT-2023 dataset results in accuracy 99.60%(RF), 99.49(XGB), precision 0.99, recall 0.99, F1-score 0.99. **Novelty:** CNN-SVM-GWO IDF prediction time is 0.75 seconds (RF) and 0.078 seconds (XGB). The proposed model has reduced time complexity. Novel hybrid IDFs for optimal feature selection are proposed with enhanced efficiency.

Keywords: Cyber-physical systems; Intrusion detection system; Optimal feature selection; Gray wolf optimizer; Convolutional neural network

1 Introduction

Cyber-physical systems (CPSs) have become integral to various aspects of our daily lives, including applications in automotive technology, medical monitoring, smart grids, and industrial control systems. Since CPSs have a wider surface area, these systems are susceptible to various kinds of attacks/threats. Developing a robust intrusion detection system presents a significant challenge due to the complexity of sophisticated attacks. Although numerous IDFs for CPSs exist, they have limitations like poor identification rate, high false positive rate, elevated time and space complexities, etc. Hence, there arises a necessity to formulate enhanced hybrid IDFs capable of proficiently detecting various types of attacks on CPSs and overcoming the limitations of the existing frameworks.

1.1 Related Work

Hybrid IDFs for CPS are crucial for enhancing network security(1). Feature selection plays a vital role in optimizing intrusion detection systems by reducing redundant features and improving performance(1,2). Various techniques like Boruta feature selection and improved grey wolf optimizations (IGWO) have been proposed to efficiently select relevant features for detecting cyber threats in datasets like CICIDS-2017 and CIC-IOT-2023 (2). Additionally, hybrid optimization approaches combining ABC and Grasshopper optimization techniques have been utilized to enhance feature selection efficiency and overall system performance in detecting network intrusions(3). By integrating these advanced feature selection methods with machine learning algorithms like XGBoost and support vector machines (SVM), intrusion detection frameworks can achieve high accuracy rates, crucial for securing CPS environments against evolving cyber-attacks. Tables 1 and 2 and Table 3 represent the recent existing hybrid IDFs.

1.2 Drawbacks of existing work

In(1), only one feature selection technique i.e. information gain is used to select the features; whereas if combined two or more techniques for feature selection, then the best features can be selected. In(4) , the model proposed can identify only one type of attack i.e. (DDoS). So, there is a need to develop the IDS which can identify multiple types of attacks on CPS. In(5) , proposed model but it does not perform well with infrequent traffic. In(6), testing time can further be improved.

In(7) accuracy can further be improved. In(8) research gaps have been identified as improving the machine learning robustness, identifying zero-day attacks, and improving security measures for CPS. In(9) the proper utilization of nature-inspired metaheuristic algorithms has been specified as a research gap. In(10) handling high dimensionality, data imbalance, and missing data effectively has been identified as gaps.

From the literature review, we have concluded that although there exist multiple IDFs they have certain limitations like high false positive rate, high space, and time complexities, need to improve accuracy, high prediction time, high training time, unable to deal with class imbalance problem, unable to identify zero-day attacks.

1.3 Overcoming limitations through the proposed frameworks

A reliable and effective method for choosing features in the detection of intrusion for CPS is provided by the CNN-SelectKBest technique. It's the ideal option for creating dependable and efficient IDS in contemporary CPS contexts because of its capacity to ensure scalability, increase feature representation, decrease dimensionality, boost detection accuracy, and adapt to complex data. Secondly, The CNN-SVM-GWO technique is the ideal option for choosing features in the detection of intrusion for CPS because of its better feature extraction, accurate feature evaluation, optimized selection procedure, enhanced reliability of detection, adaptability, and scalability. Through the combination of CNN, SVM, and GWO strengths, this method offers a strong, effective, and all-encompassing defense against cyberattacks, guaranteeing the safe and dependable functioning of CPS. The proposed frameworks address the following issues detection rate is improved, false alarm rate is minimized, space and time complexities are minimized.

Table 1. Hybrid IDFs for intrusion detection in CPSs

Reference	Year	Technique used for feature selection	Description	Dataset	PerformanceAccuracy %(Acc) Detection Rate (DR)False Alarm Rate (FAR)Precision (Pr)F1-score(F1)Recall (Re) Time Cost (Tc)	Merits/Demerits
[11]	2024	Mutual information and subspace clustering algorithms	Logistic regression is utilized with NB, LGBM, and XGB for classification.	UNSWNB15	Acc = 97.05 Pr = 96.33 Re = 96.55 F1 = 96.45 FPR = 0.029	The model can detect both known and unknown attacks. Mutual information may ignore nonlinear dependencies. Financial and operational costs are reduced thereby reducing the false alarms.
[12]	2024	Optimized extreme learning machine with genetic algorithm and wrapper method	The classifier in use is SVM.	IoT_ToN UNSWNB15	Acc = 99 Pr = 1 Re = 1 Acc = 86 Pr = 0.95 Re = 0.84	One disadvantage is that, even if a feature doesn't add anything to the model, once it is selected, it cannot be removed. Furthermore, because open-source tools are used in this model, its output might not be replicable in a real-world environment.
[13]	2023	Heterogenous Ensemble Feature Section method (HEFS)	They use union operation to merge an outcome attribute subset of five filtered selection techniques.	NSL-KDD	Acc = 99.61 Pr = 0.996 Re = 0.996 F1 = 0.996 ROC = 1.0 DR = 0.996	The best features have been determined by applying a merit-based evaluation that makes use of feature-feature and feature-class correlation.

Table 2. Hybrid IDFs for intrusion detection in CPSs

Reference	Year	Technique used for feature selection	Description	Dataset	Performance	Merits/Demerits
(14)	2023	Shapely values and genetic algorithm.	The importance of the features is evaluated using shapely values while genetic algorithm-based preprocessing is used for feature selection optimization.	X-IIOTID Kdd-Cup99 NSL-KDD	Acc = 99.72 Acc = 99.98 Acc = 99.94 Pr = 0.99 Re = 0.99 F1 = 0.99	Computational and communication costs have been reduced. Median imputation and standard scaling results in the highest accuracy.
(15)	2022	To find the most appropriate features, union, and intersection operations are applied to the features that were chosen based on information gain and gain ratio.	Using the Bagging, Multi-layered Perceptron, J48, and IBK methods, the model is trained and tested.	IoTID20 NSL-KDD	Acc = 99.81 FPR = 0.027 Pr = 0.99 Re = 0.99 F1 = 0.99 AUC = 98.50 Acc = 99.66 FPR = 0.004 Pr = 0.99 Re = 0.99 F1 = 0.99 AUC = 99.6	To overcome the limitations of each, two entropy-based choice of features techniques are used.
(5)	2022	Forest Penalised Attributes integrated with Correlation Feature Selection (CFS-FPA)	Ada boosting and bagging ensemble learning algorithms have been exploited to modify base classifiers	CCIDS 2017	Acc = 99.7 FNR = 0.053 FAR = 0.004 F1 = 1 DR = 99 Pr = 0.99	Does not perform well with infrequent traffic.

Table 3. Hybrid IDFs for intrusion

Reference	Year	Technique used for feature selection	Description	Dataset	Performance	Merits/Demerits
(16)	2020	Relationship-based Combining the BAT algorithm with feature selection (CFS-BAT)	Combining the C4.5, RF, and Forest by Penalising Attributes algorithms, a novel ensemble approach has been presented.	NSL-KDD AWID CCIDS 2017	Acc = 99.8 Pr = 0.987 DR = 0.998 F1 = 0.998 FAR = 0.001 Acc = 99.5 Pr = 0.995 DR = 0.995 F1 = 0.995 FAR = 0.001 Acc = 99.9 Pr = 0.99 DR = 0.99 F1 = 0.99 FAR = 0.001	Testing time has been reduced from 997.94s to 98.42s on the CICIDS-2017 dataset
(17)	2020	Mutual information of GA, PSO, GWO, Fire fly optimization	SVM and J48 as classifier.	UNSW-NB15	Acc=90.484(J48) Pr =0.84 TPR = 0.97 FNR = .0.28 FPR = 0.014 TNR =0.85 F1 = 0.90 Acc =90.119(SVM) Pr = 0.83 TPR = .096 FNR = 0.031 FPR = 0.015 TNR = 0.84 F1 = 0.89	GA results better FNR and TPR. PSO results in better precision and TNR.

Continued on next page

Table 3 continued

[18]	2019	A majority voting system is proposed for selecting features.	IDS using a decision tree classifier is proposed.	NSL-KDD	Acc = 80.6 Pr = 0.96 Re = 0.69 F1 = 0.80	Although the efficiency is not increased, the number of features is dropped which makes the model simpler.

In Segment 1, we give a brief introduction to CPSs, the limitations of existing intrusion detection frameworks, need for an enhanced framework for intrusion detection in CPSs. In section 2 we have discussed the proposed frameworks, by implementing the proposed frameworks we concluded that proposed frameworks have better performance in comparison to the existing frameworks for intrusion detection in CPSs. In section 3 we discuss the results. In section 4 we have concluded this work.

2 Methodology

2.1 Development of SelectKBest-MI-based intrusion detection framework for CPSs

An enhanced intrusion detection framework for CPSs via optimal feature selection using Min-Max Normalization, SelectKBest, and Mutual information for feature selection and Random Forest for binary classification has been proposed.

In this proposed framework we have used the publicly available dataset CCIDS2017. First, we preprocessed the dataset by using Min-Max normalization, then we replaced the missing values in the dataset with zero, and next, we converted the object values to numerical values. In step 2 split the data set into two ratios 80% for training and 20% for testing. In step 3 we have used a fusion of SelectKBest and mutual information features selection for choosing the best number of attributes and dimensionality reduction. Through intensive experiments, we have found that by choosing the value of K=30 in the SelectKBest feature selection technique, we get better performance, for the proposed model using RF as the classifier. Figure 1 represents the proposed framework named SelectKBest-MI for the optimal choice of features and RF as the classifier.

2.2 CNN-SVM-GWO an Enhanced Metaheuristic technique-based intrusion detection framework for CPSs

In this framework we have first preprocessed the dataset (CIC-IoT-2023) by using Min-Max normalization then we have replaced the NaN values with mode. CNN is used for feature extraction, GWO, and SVM are utilized for the optimal number of feature selection, and RF and XGB classifiers are used for intrusion detection. Figure 2 shows the proposed framework CNN-SVM-GWO for intrusion detection in CPSs.

Implementation of this framework using CIC-IoT-2023 dataset results in accuracy 99.53%(RF), 99.42(XGB), precision 0.99, recall 0.99, F1-score 0.99. Model prediction time is 0.69 seconds (RF) and 0.078 seconds (XGB). The proposed model has reduced time complexity in comparison to the existing models for IDS. By doing intensive experiments we have found that by fixing the number of optimal features to be selected as 30(thirty) proposed model gives the best result.

3 Results and Discussion

3.1 Results of SelectKBest-MI based intrusion detection framework for CPSs

Within this segment, we have presented the various results and functionality analyses of the suggested SelectKBest-MI framework for IDS in CPSs. Table 4 shows the implementation results.

By analyzing Table 4 we can conclude that the model achieves an accuracy of 99.99%, with a precision of 0.99, recall of 0.99, and an F1-score of 0.99. Table 3 lists the names of selected optimal features for intrusion detection in CPSs. Figure 3 depicts the relationship between the true positive rate and the false positive rate.

3.2 Results of CNN-SVM-GWO an Enhanced Metaheuristic technique-based intrusion detection framework for CPSs

In this section, we have presented the various results and performance analyses of the proposed CNN-SVM-GWO framework for IDS in CPSs. Table 5 lists the names of optimal selected features, we are getting after the execution of CNN for the extraction

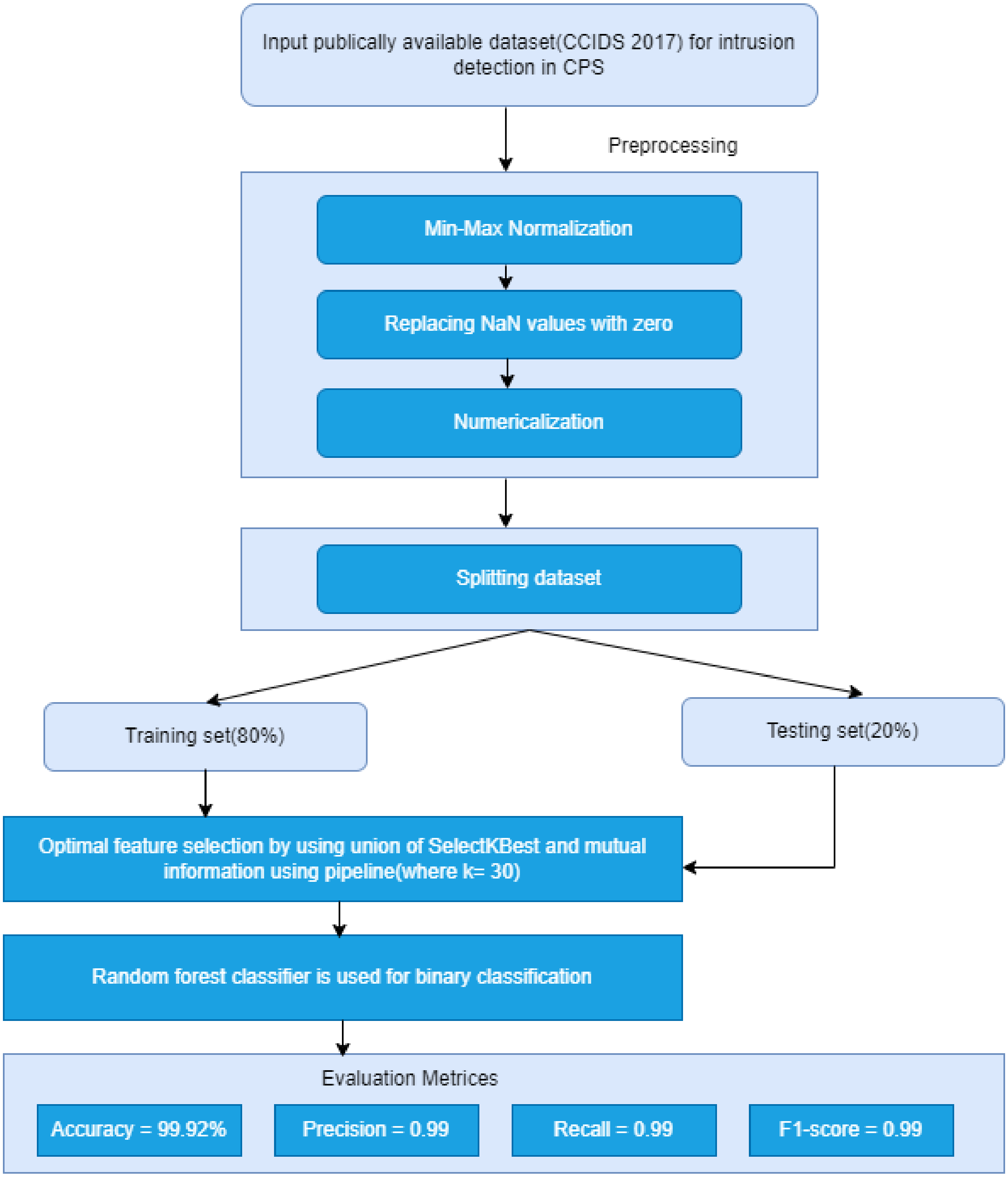
Input publically available dataset(CCIDS 2017) for intrusion detection in CPS
Preprocessing
Min-Max Normalization
Replacing NaN values with zero
Numericalization
Splitting dataset
Training set(80%)
Testing set(20%)
Optimal feature selection by using union of SelectKBest and mutual information using pipeline(where k= 30)
Random forest classifier is used for binary classification
Evaluation Metrices
Accuracy = 99.92%
Precision = 0.99
Recall = 0.99
F1-score = 0.99

Fig 1. Proposed enhanced SelectKBest-MI intrusion detection framework for CPS

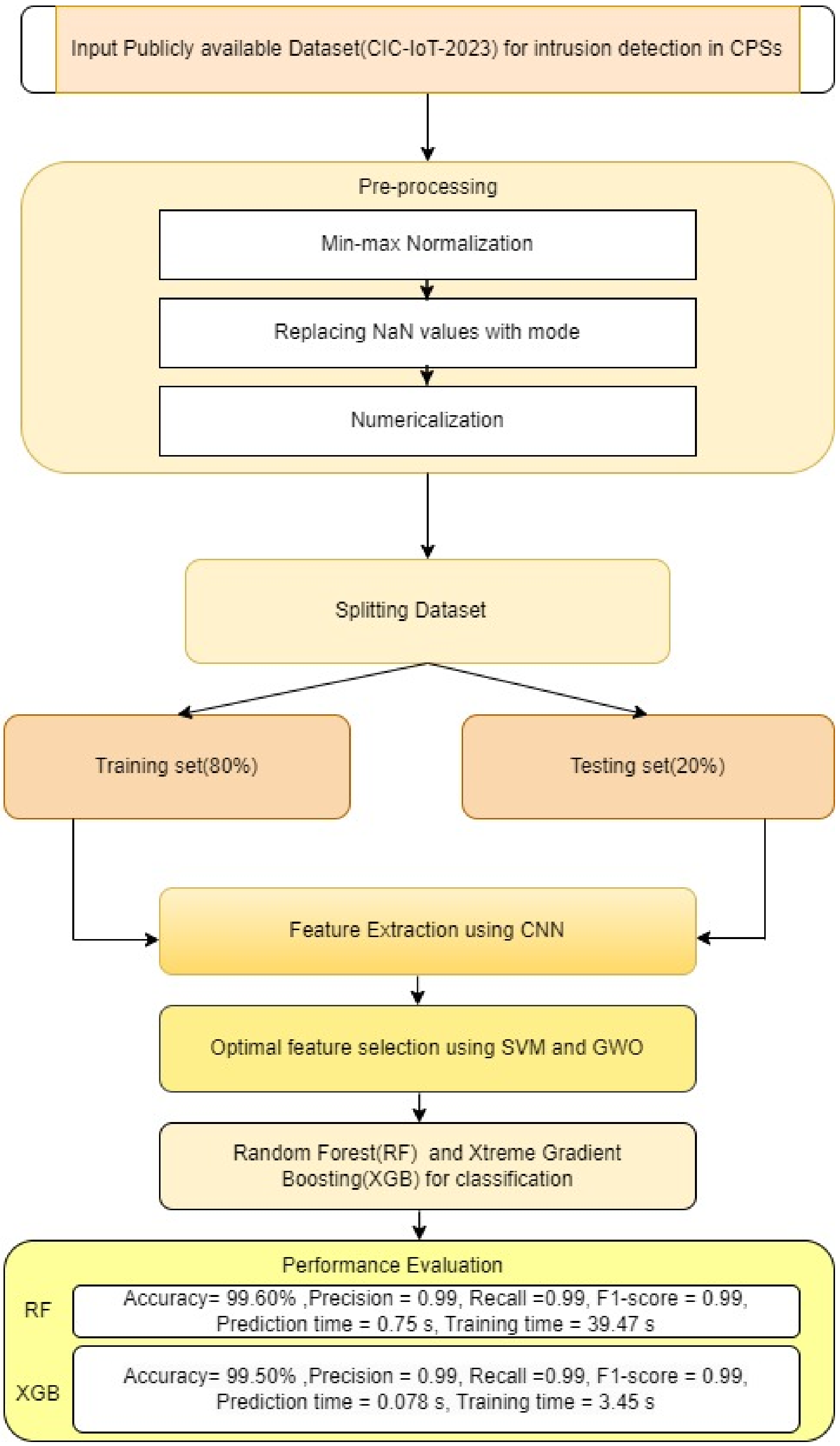
Input Publicly available Dataset(CIC-IoT-2023) for intrusion detection in CPSs
Pre-processing
Min-max Normalization
Replacing NaN values with mode
Numericalization
Splitting Dataset
Training set(80%)
Testing set(20%)
Feature Extraction using CNN
Optimal feature selection using SVM and GWO
Random Forest(RF) and Xtreme Gradient Boosting(XGB) for classification
Performance Evaluation
RF
Accuracy= 99.60% ,Precision = 0.99, Recall =0.99, F1-score = 0.99, Prediction time = 0.75 s, Training time = 39.47 s
XGB
Accuracy= 99.50% ,Precision = 0.99, Recall =0.99, F1-score = 0.99, Prediction time = 0.078 s, Training time = 3.45 s

Fig 2. CNN-SVM-GWO framework for intrusion detection in CPSs

Table 4. Performance Analysis of SelectKBest-MI framework using CICIDS2017 dataset

Metrics	Random Forest Classifier
Accuracy	99.99%
Precision	0.99
Recall	0.99
F1-Score	0.99
Prediction time	4.4s

Table 5. List of selected optimal features using the SelectKBest-MI framework

S.No	Name of Selected features	S.No	Name of Selected features
1.	Port of Destination	23.	Forward header length
2.	Duration of Flow	24.	Bwd header length
3.	Length of all forward packets	25.	Forward packets/s
4.	The entire BWD packet length	26.	Backward packets/s
5.	Fwd Maximum packet length	27.	Minimum length of packet
6.	Fwd Minimum packet length	28.	The maximum length of the packet
7.	Fwd Mean packet length	29.	Mean of Packet length
8.	Fwd Standard packet length	30.	Packet length std
9.	Maximum Bwd length of packets	31.	Variance of Packet length
10.	Minimum Bwd length of packets	32.	Synchronous Flag Counter
11.	Mean Bwd length of packet	33.	Push flag counter
12.	Standard Bwd length of packet	34.	Flag counter for URG
13.	Flow IAT mean	35.	Average Packet size
14.	Flow IAT max	36.	Average Forward size of the segment
15.	Total Forward IAT	37.	Average Backward size of Segment
16.	Mean Forward IAT	38.	Forward header length.1
17.	Max Forward IAT	39.	Forward Subflow Bytes
18.	Total Backward IAT	40.	Backward Subflow Bytes
19.	Mean Backward IAT	41.	Winbytes_Init_forward
20.	Standard Backward IAT	42.	Initial Win Bytes Forward
21.	Maximum Backward IAT	43.	win_size_minimum forward
22.	Fwd PSH flags	44.	Idle_Std

of attributes.

Table 6 shows the results we are getting after implementing the proposed model. By analyzing Table 7 we can conclude that the model achieves an accuracy of 99.60%, with a precision of 0.99, recall of 0.99, and an F1-score of 0.99. Selecting only 21 out of 46 features improves the response time for intrusion detection and reduces the framework's space complexity. In Table 8 we have compared the results of the proposed techniques with the other similar techniques available in literature.

4 Discussion

From Table 8, it is concluded that the proposed approaches for intrusion detection in CPS perform better compared to the other related techniques. In[19], a lightweight IDS has been proposed using the CIC-IoT-2023 dataset, getting an accuracy of 97.65%, precision of 0.98, recall of 1.0, F1-score of 0.99; whereas the proposed IDF CNN-SVM-GWO results in better performance accuracy (99.60% & 99.49%) in case of RF and XGB classifiers, respectively. Also, prediction time is very less i.e. (0.75s (RF) & 0.078s (XGB)). In[6], CFS-BA has been used for feature selection then an ensemble of RF-C4.5-Forest PA is proposed as the classifier using the CCIDS2017 dataset, getting accuracy (99.90%) and prediction time 98.42s; whereas our proposed IDF Select-KBest-MI results in accuracy (99.99%) and prediction time 4.4s using CCIDS2017 dataset. SelectKBest-MI performs better for intrusion detection in CPS because it effectively identifies and selects the most informative features, handles diverse and noisy data, and adapts to evolving threats, all of which are critical for maintaining robust and efficient intrusion detection

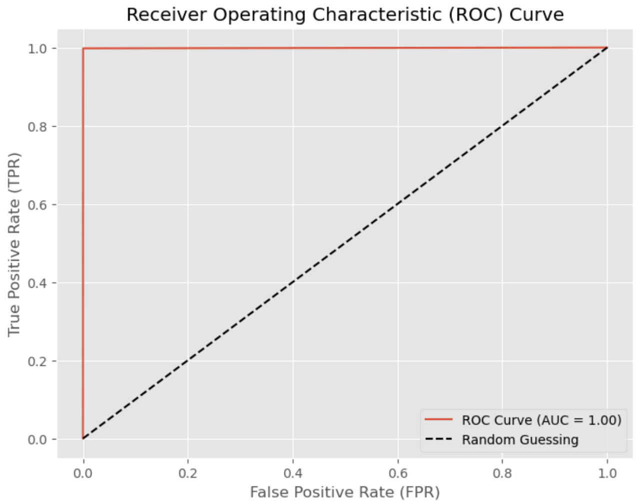

Fig 3. Receiver operating curve

Table 6. List of selected optimal features from the CIC-IoT-2023 dataset

S.No	Name of Selected features
1.	Flow duration
2.	Header Length
3.	Duration
4.	Strate
5.	Syn_flag_number
6.	Rst_flag_number
7.	Ece_flag_number
8.	fin_count
9.	Rst_count
10.	HTTP
11.	HTTPS
12.	SMTP
13.	SSH
14.	IRC
15.	ICMP
16.	Totsum
17.	Min
18.	Max
19.	AVG
20.	IAT
21.	Radius
22.	Covariance

Table 7. Performance analysis of CNN-SVM-GWO framework using data set CIC-IoT-2023

Performance	Random Forest Classifier	XGB Classifier
Accuracy	99.60%	99.49%
Precision	0.99	0.99
Recall	0.99	0.99
F1-Score	0.99	0.99
Training time	39.47s	3.45s
Prediction time	0.75s	0.078s

Table 8. Comparison of the proposed approaches with the state-of-the-art approaches

Author	Year	Approach	Accuracy	Dataset	Precision	Recall	F1-score	Prediction time
[6]	2020	CFS-BAT	99.90%	CICIDS2017	0.99	0.99	0.99	98.42s
[19]	2024	Lightweight IDS	97.65%	CIC-IoT-2023	0.98	1.0	0.99	-
[7]	2022	Coyote optimization algorithm	99.13%	CICIDS2017	0.99	0.99	0.99	-
Proposed approach	**2024**	**Proposed Framework (SelectKBest-MI)**	**99.99%**	**CICIDS2017**	**0.99**	**0.99**	**0.99**	**4.4 s**

Proposed approach	**2024**	**Proposed framework (CNN-SVM-GWO)**	**99.60(RF)
			99.50(XGB)**
				CIC-IoT-2023	**0.99**	**0.99**	**0.99**	**0.75 s(RF)
								0.078s(XGB)**

in complex CPS environments. CNN-SVM-GWO IDF leverages the strengths of deep learning for feature extraction, robust classification capabilities of SVM, and efficient optimization from GWO. This combination results in a powerful and adaptive IDS that performs well in the complex and dynamic environments characteristics of CPS.

5 Conclusion

This research work has found that there is a need for dimensionality reduction of dataset features to enhance the overall efficacy of the intrusion detection models; because all the features of the dataset need not contribute to intrusion detection. This study has analyzed the various recent techniques for the selection of the optimal number of features for intrusion detection deployed by different researchers. Two enhanced IDFs namely SelectKBest-MI and CNN-SVM-GWO have been proposed. After implementing these frameworks, it is concluded that these proposed IDFs for intrusion detection in CPSs perform better than the various existing frameworks. CNN-SVM-GWO frameworks select only 22 features out of 46 features from the CIC-IoT-2023 dataset. It aids in lowering the suggested framework's complexity in terms of time and space. Also, the prediction time of the proposed model is improved. These models are implemented only for binary classification i.e. these models can only identify whether an intrusion has occurred or not. In the future, these models can be extended for multiclassification of intrusions. Proposed techniques can be extended for the multiclassification of intrusions by using the concept of mapping and converting the different types of labels (attacks) into numeric format. Experimental code can be found at the following link: SelectKBest-MI/CNN4.ipynb at main · RAMJI1984/SelectKBest-MI (github.com).

References

1) Farhan BI, Jasim AD. Improving detection for intrusion using deep LSTM with hybrid feature selection method. *Iraqi J Inf Commun Technol*. 2024;6(1):40–50. Available from: https://doi.org/10.31987/ijict.6.1.213.
2) Yuvaraja M, Arunkumar S, Kumar PV, Sheela LMI. Improved Grey Wolf Optimization- (IGWO-) Based Feature Selection on Multiview Features and Enhanced Multimodal-Sequential Network Intrusion Detection Approach. *Wirel Commun Mob Comput*. 2023;2023:1–13. Available from: https://doi.org/10.1155/2023/8478457.
3) Goswami PK, Baruah S, Thakuria L. Identifying the Features of the Various Cyber ataset for Ensuring Cyber Security using Hybrid Optimization Techniques and Machine Learning (ML). *2023 International Conference on Emerging Smart Computing and Informatics (ESCI) IEEE*. 2023;p. 1–6. Available from: https://doi.org/10.1109/ESCI56872.2023.10100207.

4) Sharma A, Rani S, Shah SH, Sharma R, Yu F, Hassan MM. An Efficient Hybrid Deep Learning Model for Denial of Service Detection in Cyber Physical Systems. *IEEE Transactions on Network Science and Engineering*. 2023;10(5):2419–2428. Available from: https://dx.doi.org/10.1109/tnse.2023.3273301.

5) Mhawi DN, Aldallal A, Hassan S. Advanced feature-selection-based hybrid ensemble learning algorithms for network intrusion detection systems. *Symmetry (Basel)*. 2022;14:1461–1461. Available from: https://doi.org/10.3390/sym14071461.

6) Zhou Y, Cheng G, Jiang S, Dai M. Building an efficient intrusion detection system based on feature selection and ensemble classifier. *Comput Networks*. 2020;174. Available from: https://doi.org/10.1016/j.comnet.2020.107247.

7) Alqaralleh AY, Aldhaban B, Alqaralleh EA, Al-Omari AH. Optimal Machine Learning Enabled Intrusion Detection in Cyber-Physical System Environment. *Comput Mater Contin*. 2022;72(3):4691–707. Available from: https://doi.org/10.32604/cmc.2022.026556.

8) Sharma DM, Shandilya SK. Attack Detection Based on Machine Learning Techniques to Safe and Secure for CPS—A Review. *Lecture Notes in Electrical Engineering*. 2023;p. 273–286. Available from: https://doi.org/10.1007/978-981-19-8136-4_23.

9) Malik MI, Ibrahim A, Hannay P, Sikos LF. Developing Resilient Cyber-Physical Systems: A Review of State-of-the-Art Malware Detection Approaches, Gaps, and Future Directions. *Computers*. 2023;12(4):79–79. Available from: https://dx.doi.org/10.3390/computers12040079.

10) Yuan H, Li H. Time series intrusion warning with GAN for missing data in CPS. *Proceedings of the 2023 11th International Conference on Communications and Broadband Networking*. 2023;p. 59–64. Available from: TimeseriesintrusionwarningwithGANformissingdatainCPS.

11) Zhu J, Liu X. An integrated intrusion detection framework based on subspace clustering and ensemble learning. *Comput Electr Eng*. 2024;115:109113–109113. Available from: https://doi.org/10.1016/j.compeleceng.2024.109113.

12) Maseno EM, Wang Z. Hybrid wrapper feature selection method based on genetic algorithm and extreme learning machine for intrusion detection. *J Big Data*. 2024;11(1):24–24. Available from: https://doi.org/10.1186/s40537-024-00887-9.

13) Damtew YG, Chen H, Yuan Z. Heterogeneous ensemble feature selection for network intrusion detection system. *Int J Comput Intell Syst*. 2023;16(1):9–9. Available from: https://doi.org/10.1007/s44196-022-00174-6.

14) Sezgin A, Boyacı A. Enhancing intrusion detection in industrial internet of things through automated preprocessing. *Adv Sci Technol Res J*. 2023;17(2):120–155. Available from: https://doi.org/10.12913/22998624/162004.

15) Albulayhi K, Al-Haija QA, Alsuhibany SA, Jillepalli AA, Ashrafuzzaman M, Sheldon FT. IoT intrusion detection using machine learning with a novel high-performing feature selection method. *Applied Sciences*. 2022;12(10):1–30. Available from: https://doi.org/10.3390/app12105015.

16) Zhou Y, Cheng G, Jiang S, Dai M. Building an efficient intrusion detection system based on feature selection and ensemble classifier. *Comput Networks*. 2020;174. Available from: https://doi.org/10.1016/j.comnet.2020.107247.

17) Almomani O. A feature selection model for network intrusion detection system based on PSO, GWO, FFA, and GA algorithms. . *Symmetry (Basel)*. 2020;12. Available from: https://doi.org/10.3390/sym12061046.

18) Ahmadi SS, Rashad S, Elgazzar H. Efficient feature selection for intrusion detection systems. *2019 IEEE 10th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2019*. 2019. Available from: https://doi.org/10.1109/UEMCON47517.2019.8992960.

19) Wardana AA, Kołaczek G, Sukarno P, Lightweight. Trust-Managing, and Privacy-Preserving Collaborative Intrusion Detection for Internet of Things. *Appl Sci*. 2024;14(10):4109–4109. Available from: https://doi.org/10.3390/app14104109.