

Enhancing intrusion detection performance in industrial internet of things using modified hyperparameter optimization

Arif Ullah¹, Javed Mansoori², Baber Akber³, Abdullah Altaf⁴, Abdul Rehman Altaf⁴, Aseel Smerat⁵

¹Department of Computer Science, Faculty of Computing and Artificial Intelligence, Air University, Islamabad, Pakistan

²Department of Computer Science, Vinayaka Mission Research Foundation University, Salem, India

³Department of Computer Science, University of Greater Manchester, Bolton, United Kingdom

⁴Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Batu Pahat, Malaysia

⁵Hourani Center for Applied Scientific Research, Al-Ahliyya Amman University, Amman, Jordan

Article Info

Article history:

Received Jan 17, 2025

Revised Jul 31, 2026

Accepted Aug 12, 2026

Keywords:

Algorithm

Cyberattacks

Industrial internet of things

Internet of things

Networking

Optimization

ABSTRACT

Many sectors have seen significant improvements in operational efficiency and modern connection due to the increasing usage of industrial internet of things (IIoT) devices, a phenomenon known as IIoT. However, efficient intrusion detection systems (IDS) are essential for IIoT security because this quick growth also makes the network more susceptible to sophisticated cyberattacks. The high dimensionality and dynamic nature of IIoT data frequently cause traditional IDS algorithms to struggle, which results in insufficient threat detection and response. This paper uses a novel technique called Bayesian hyperparameter optimization with decision trees to enhance IDS performance in complex IIoT scenarios. Using the large IIoT-23 dataset, the method achieved an excellent 96.07% accuracy rate and a weighted average F1-score of 96.03%, in addition to demonstrating a significant increase in identifying a range of attack scenarios. In direction to growth the precision and robustness of our intrusion detection algorithms, this invention emphasizes how important it is to carefully modify complex hyperparameters and combine decision trees with ensemble methods like genetic algorithms and Bayesian optimization. The results show how successfully the approach adapts to budding threat landscape, expressively lessens false positives, and efficiently handles the enormous volumes of data that are a part of IIoT networks.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Arif Ullah

Department of Computer Science, Faculty of Computing and Artificial Intelligence, Air University

Islamabad, Pakistan

Email: arifullahms88@gmail.com

1. INTRODUCTION

One of the fastest growing fields within the field of internet of things (IoT), the industrial internet of things (IIoT), the latter being the backbone for the industry of the next level i.e., Industry 4.0, have exploded with rapid growth. The industrial revolution is changing the industrial world at an alarming rate, bringing in revolutionary findings and advances [1]. The IIoT is helping us entering the era of automate yet connected, transformed the way industries do work. Nevertheless, as the networks of this are growing, they also become more prone to attacks. It is a paramount part for intrusion detection systems (IDS) to spot and remedy them [2].

Nevertheless, it requires constant evolution in order for it to be efficient on practical purposes to adapt the ever-changed nature of hackers. It might take advantage of a “hyperactive change in settings” when considering the parameters applied, can be considered when it comes to increasing efficiency. In this work,

some variables for IDS performance were tuned in order to improved ability for known as well as for zero-day exploit [3]. The performance and adaptability of the network system was explored when varying the parameters mentioned to discover how the accuracy of the system was influenced by the hyperactive variable change approach [4]. Although the intent was to increase the precision classification of normal cyber-attacks used k-means cluster to indicate deviations of the norm which can show the threat.

This work aimed to develop an IDS that was more reliable and resilient to ever the ever-changing face of cybercrime and developed IDS which could outperform other system when taking in account true and false positives [5]. A significant performance gain of the IDS system in the detection rate (DR) has been reported when applying the hyperparameter tuning, this is likely to pave the way towards comprehensive cybersecurity for IIoT. Future work exploring and defining a machine learning (ML)-based parameter tuning protocol may guide the path forward for efficient IDS for industrial-based systems [6].

2. RELATED WORK

According Shahin *et al.* [7], the IIoT is getting used fast, and it has made industrial automation and monitoring a lot better. The IIoT has a lot of devices connected to it, and they all use altered announcement rules, which makes it hard to keep them safe from cyberattacks. So, people have been working on IDS that use ML and deep learning (DL). These systems are getting better at finding attacks. They also need to be good at picking the right features and making sure they are working well.

Ferrag *et al.* [8] made a dataset called Edge-IIoTset, which's a collection of traffic from lots of devices and protocols. This dataset has lots of types of attacks like denial-of-service (DoS) and malware attacks. It is a good dataset for testing IIoT intrusion detection models because it has lots of real-life attack scenarios.

Gaber *et al.* [9] came up with a way to detect IIoT intrusions that uses optimization and ML. They used something called particle swarm optimization (PSO) to pick the features and then used random forest to classify attacks. They tested their method using the Washington University in St. Louis (WUSTL)-IIOT-2021 dataset. It worked really well. Ahmad *et al.* [10] made a model called deep random neural network (DRaNN)_PSO, which's a deep neural network that uses PSO to find the best parameters. They tested their model on a few datasets, and it was able to detect attacks really well.

Huang *et al.* [11] up with a way to optimize neural network construction and hyperparameters at the time. They used algorithms to find the best parameters and it worked really well. Sezgin and Boyacı [12] made a framework called AID4I, which's an automated ML framework for IIoT intrusion detection. It can do lots of things on its own, like picking features and tuning parameters. Gopi *et al.* [13] worked on elevating hyperparameters for IIoT intrusion detection. They used something called the Archimedes optimization algorithm to find the parameters, and it made their model work really well. The IIoT is an important area of research, and people are working hard to make sure it is safe.

According to Babayigit and Abubaker [14], the IIoT needs to be safe because it is used in lots of areas like factories and power plants. So, people are working on making IDS that use ML and DL. The IIoT intrusion detection models need to be good at finding attacks. They also need to be able to work well in real-time. The IIoT has lots of devices connected to it. They all use different protocols, which makes it hard to keep them safe. People is working on making the IIoT by using optimization and ML. They are also working on making. The IIoT intrusion detection models that can work well in time.

According to Alsarhan *et al.* [15], the IIoT is an important area of research and people are making good progress. The IIoT needs to be safe because it is used in lots of areas. The IIoT intrusion detection models need to be good at finding attacks. They also need to be able to work well in real-time. The IIoT has lots of devices connected to it.

Maghrabi *et al.* [16] use different protocols, which make it hard to keep them safe. People are working hard to make the IIoT safer. They are using optimization and ML to make the IIoT intrusion detection models that can work well in time. The IIoT is an important area of research, and people are making good progress. Table 1 presents the summary of related work with details.

2.1. Research gap

Conventional hyperparameter tuning is frequently used by current IIoT IDS, which may restrict their ability to handle complex and dynamic network traffic. To increase detection accuracy and lower false positives, a small number of studies have integrated decision tree-based IDS models with Bayesian and evolutionary optimization. Therefore, to accomplish more reliable and accurate intrusion detection in IIoT contexts, a changed hyperparameter optimization strategy is required. This underscores the importance of adaptive optimization frameworks that can ensure scalability and resilience of IDS in rapidly evolving IIoT environments.

Table 1. The summary of selected papers

Reference	Technique	Dataset	Main findings	Limitation/research gap
[8]	Edge-IIoTset with ML/DL-based IDS	Edge-IIoTset	Introduced a comprehensive and realistic IIoT cybersecurity dataset containing multiple devices, protocols, and attack types.	Dataset diversity is high, but IDS performance can still depend strongly on model configuration and hyperparameter selection.
[17]	PSO and Bat algorithm with random forest	WUSTL-IIoT-2021	Optimization-based feature selection improved intrusion detection while reducing irrelevant features.	Focuses mainly on feature selection; limited investigation of advanced hyperparameter optimization.
[10]	DRaNN with PSO	DS2OS, UNSW-NB15, ToN-IoT	Combining DL with PSO improved intrusion detection for binary and multiclass attacks.	Metaheuristic optimization can increase computational complexity and optimization time.
[11]	Synchronous optimization of parameters and architectures (SOPA)-genetic algorithm-convolutional neural network (CNN) using genetic algorithm	IIoT security datasets	Genetic algorithms was used to optimize CNN architecture and hyperparameters, improving automated model configuration.	Joint architecture and hyperparameter optimization may require considerable computational resources.
[12]	AID4I / automated ML	IIoT datasets	Automated feature selection, model selection, and hyperparameter tuning reduced manual model configuration.	AutoML approaches can be computationally expensive and may not be optimized specifically for resource-constrained IIoT environments.
[16]	Golden Jackal optimization + DL	IIoT dataset	Optimization combined with DL improved cyberattack detection and classification.	Multiple optimization stages can increase computational complexity and may affect real-time deployment.
[18]	Enhanced firefly algorithm for hyperparameter tuning	Edge-IIoT	Enhanced firefly algorithm-based hyperparameter optimization improved accuracy, precision, recall, and F1-score compared with conventional approaches.	Further modification of optimization strategies is needed to improve convergence, computational efficiency, and generalization.

3. PROBLEMS STATEMENT

The IIoT is rapidly transforming industries by enabling connected equipment to collect, distribute, and process data. However, this interdependence also increases the risk of cyberattacks, making effective IDS necessary [18]. Traditional IDS techniques might occasionally fail in dynamic IIoT scenarios because to their limited flexibility, scalability, and efficiency in handling big and diverse datasets. Moreover, conventional hyperparameter optimization methods are used by ML-based IDS models, which are computationally intensive and rarely yield ideal outcomes. To enhance IIoT systems' intrusion detection [19]. This, work proposes a modified hyperparameter optimization method in [20]. By refining hyperparameter tuning methods, the goal is to improve detection accuracy, reduce false positives, and provide a more efficient and scalable IDS system. Especially created to satisfy the complex requirements of IIoT networks. Research objectives: i) to develop a modified hyperparameter optimization approach for enhancing intrusion detection performance in IIoT networks; ii) to optimize a decision tree-based IDS using Bayesian and evolutionary optimization techniques for accurate detection of diverse cyberattacks; and iii) to evaluate and compare the proposed approach using the datasets network security laboratory (NSL) and knowledge discovery in databases (KDD) based on accuracy, precision, recall, F1-score, and false-positive rate.

4. PROPOSED MODEL

Sensors, actuators, programmable logic controller (PLCs), control systems, and other interconnected industrial devices that operate in smart factories and vital infrastructures make up the IIoT environment. Large amounts of diverse network traffic and system logs are consistently produced by these devices. IIoT systems are extremely susceptible to cyberattacks because of their limited computational resources and stringent real-time requirements; hence, effective intrusion detection is crucial [21]. Figure 1 presents the proposed model framework.

4.1. Data preprocessing module

Compile network traffic data from IIoT devices. Conduct feature selection, data cleaning, and normalization to extract relevant characteristics for intrusion detection. Use techniques like synthetic minority oversampling technique (SMOTE) to manage unbalanced datasets in order to ensure balanced learning [22].

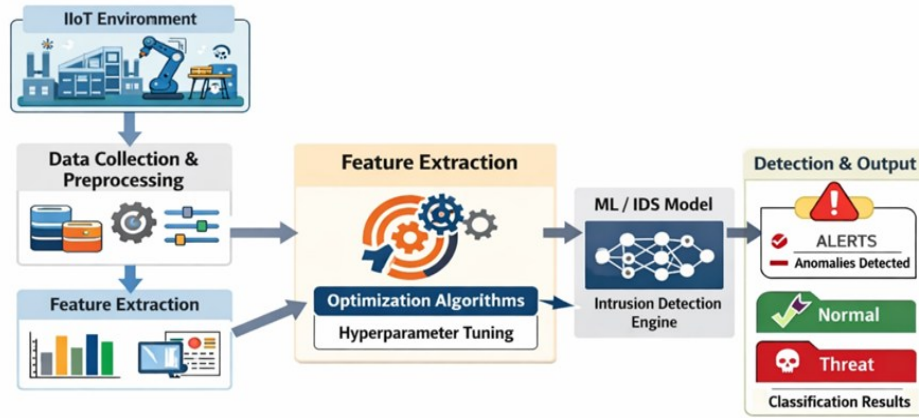


Figure 1. The proposed model framework

4.2. Modified mathematical model for hyperparameter optimization framework

To improve detection accuracy and overall classification performance in IIoT contexts, the modified hyperparameter optimization framework is designed. It aims to find an ideal collection of hyperparameters (θ) for ML and DL-based intrusion detection models [23]. The optimization algorithm, objective function, hyperparameter search space, and performance evaluation criteria are some of the essential elements of the mathematical formulation [24].

4.3. Goal function

To find the ideal set of hyperparameters that enhances the overall intrusion detection performance, the optimization strategy aims to optimize performance metrics like accuracy, precision, and recall while reducing the loss function L [25]. In (1), the hyperparameter optimization process is represented.

$$\min L(\theta) = N \sum_{i=1}^n L(y_i, f(x_i; \theta)) \quad (1)$$

During the optimization process, a variety of hyperparameters are taken into account, including the number of layers, batch size, learning rate, and other model configuration parameters [26]. The difference between the genuine labels y_i is measured by the loss function $L(y_i, f(x_i; \theta))$ and the forecasts $f(x_i; \theta)$, where N is the total number of data samples [27]. The issue is described as a supervised learning challenge where a dataset $D = \{(x_i, y_i)\}_{i=1}^n$ includes n samples with feature vectors x_i . R^d and labels $y_i \in \{0, 1\}$, signifying, for instance, normal and incursion classes. The goal is to maximize a performance metric M , such as accuracy, precision, recall, or F1-score, by optimizing the hyperparameters θ of the chosen model $f(x; \theta)$ [28]. For (2) to (5), we can use the following formulation to represent maximizing IDS performance.

$$\max M(D; f(x; \theta)) \quad (2)$$

Define the search space for the proposed model as (3).

$$\theta = [\alpha_{min}, \alpha_{max}] \times [\lambda_{min}, \lambda_{max}] \times \{L_1, L_2, \dots, L_k\} \times \{U_1, U_2, \dots, U_m\} \times \Gamma \quad (3)$$

Combine exploration (global search) and exploitation (local refinement).

$$\begin{aligned} \theta_{new} &= \text{Crossover}(\theta_p, \theta_q) + \text{Mutation}(\theta_{new}) \\ f(x; \theta) &= \text{argmax}_P(y | x; \theta) \end{aligned} \quad (4)$$

The model that has been optimized which is mention below, with the details.

$$f^*(x) = "f"(x; "\theta") \quad (5)$$

The formula $f^*(x) = f(x; \theta^*)$, where the ideal set of hyperparameters is represented by θ^* . The hyperparameters used to modify the given solution in term of local search with global parameters [29].

4.4. Experiments and evaluation metrics

In this part, a variety of tests were conducted on several publicly available datasets to confirm the effectiveness of the proposed model. The results of the experiment were then thoroughly examined and discussed. Two types of datasets NSL and KDD are used for the experiment, and various systems which are detailed in Table 2, are used and the environment where they system are developed.

Table 2. Experimental environment

Simulation tools	Simulation environment	Simulation environment
Operating system	Windows 10	Python 3.9
ML library	Scikit-learn 1.13	RTX 3070

5. RESULT AND DISCUSSION

A sweep-based method was used to optimize the hyperparameters W and B . To find the optimal configuration, the sweep iteratively investigated the parameter space. The F1-score was maximized and parameters like max_depth were optimized using Bayesian optimization. Figure 2 and Table 3 provide information on the NSL dataset result with details.

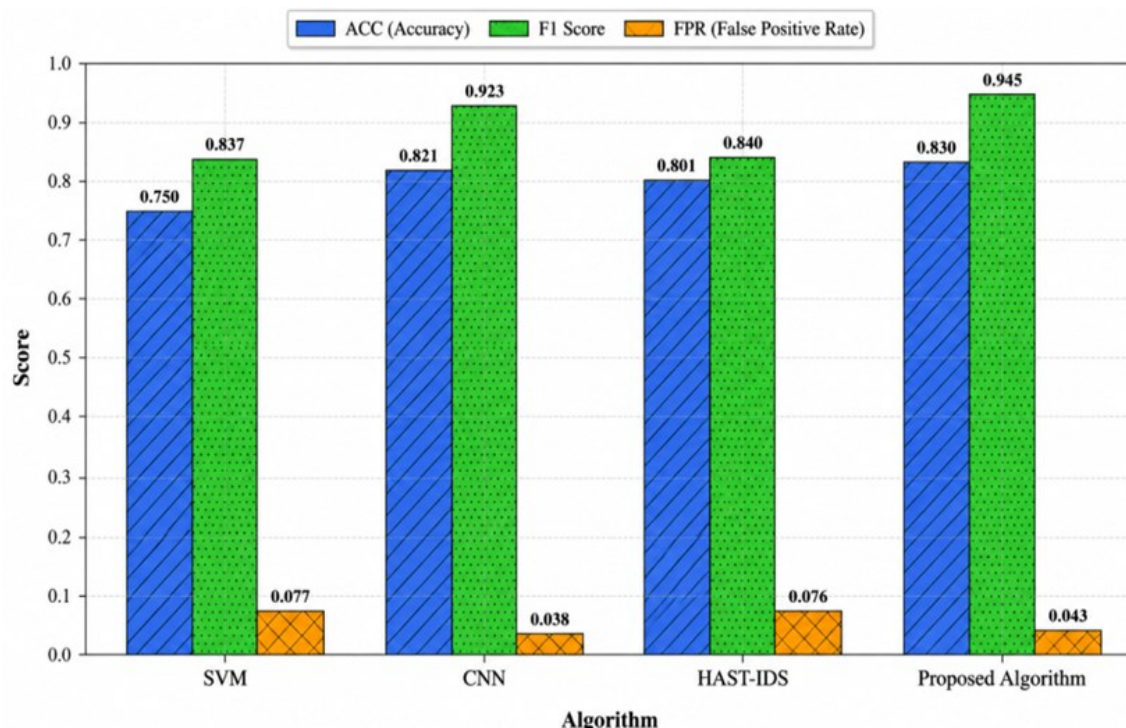


Figure 2. Performance comparison of the proposed model on the NSL dataset

Table 3. The result of NSL dataset

Algorithm name	Accuracy	F1-score	False positive rate (FPR)
SVM	0.750	0.837	0.077
CNN	0.821	0.923	0.038
Hierarchical spatial-temporal features (HAST) based-IDS	0.801	0.840	0.076
Proposed algorithm	0.830	0.945	0.043

This proposed model shows a strong prediction result. The proposed model of the decision tree achieves an accuracy value of 96.07% for the test set, which is an amazing accuracy. Moreover, for the F1-score, this model reached 96.03% in average weighted scores, which are indeed very efficient in identifying abnormal traffic for the specific IIoT environment. All results illustrate a successful application of

the Bayesian optimization technique for tuning the parameters for the decision tree model so as to make the models have better predictive capability. Table 4 and Figures 3 and 4 reveal that, compared with other methods, the suggested model surpasses in multiple aspects, like the confusion matrix, accuracy, and correlation analysis and the result is better than other models.

Table 4. The result of KDD dataset

Algorithm name	Accuracy	DR	FPR
SVM	0.648	0.737	0.075
CNN	0.760	0.820	0.042
HAST-IDS	0.756	0.836	0.066
Proposed algorithm	0.867	0.950	0.040

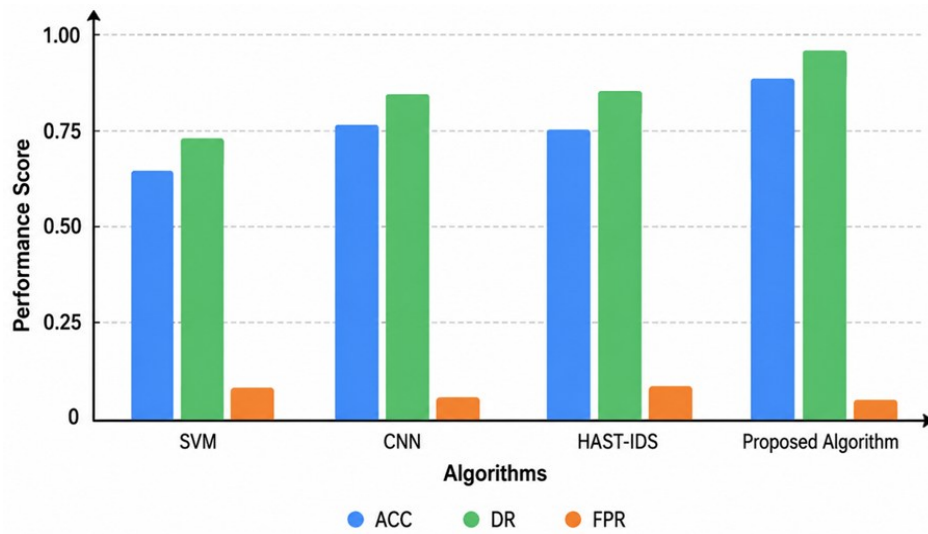


Figure 3. Performance comparison of the proposed model on the KDD dataset

Model consistency and performance: the scores from the test and the cross-validation are nearly the same; this proves the model is not overfitting and has a relatively good degree of generalization. The model is overfitting if there is good prediction performance on the training set and the new set-test score is high and near to the cross-validation score. The slight increased on the score also proves that by providing more training data the model prediction is getting better. The described approach has given better results for accuracy, F1-score, and FPR, considering two kinds of datasets available. Figure 5 presents the confusion matrix result, Figure 6 illustrates the accuracy result, and Figure 7 presents all the obtained results based on different approaches using the KDD sorts of datasets.

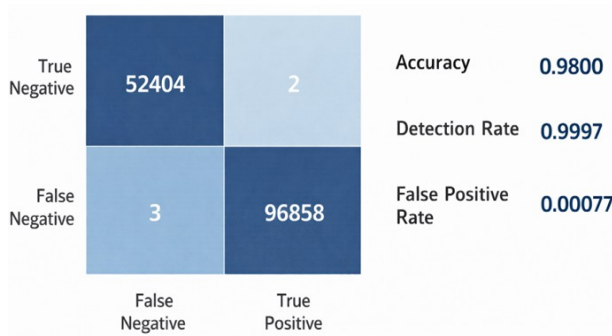


Figure 4. Confusion matrix result actual abnormal

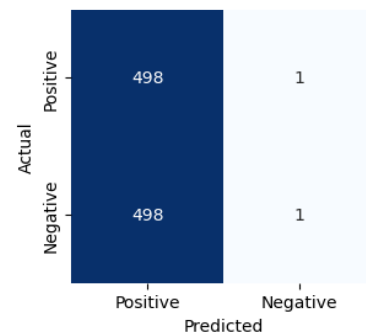


Figure 5. Confusion matrix result actual normal

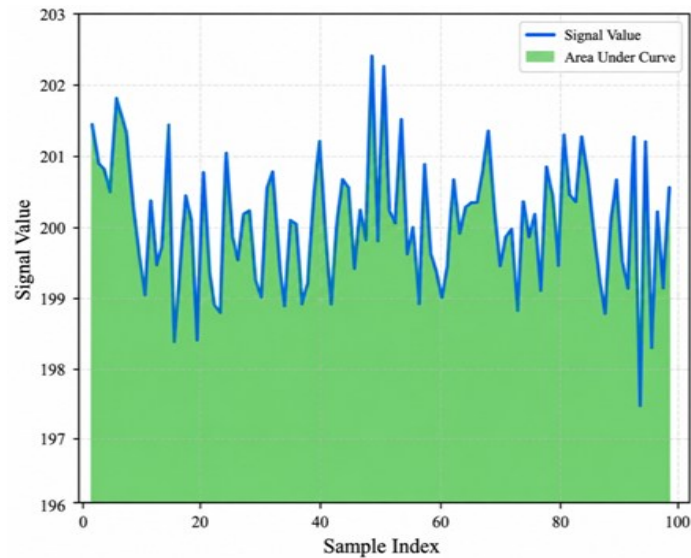


Figure 6. Accuracy comparison of the optimized hyperparameters

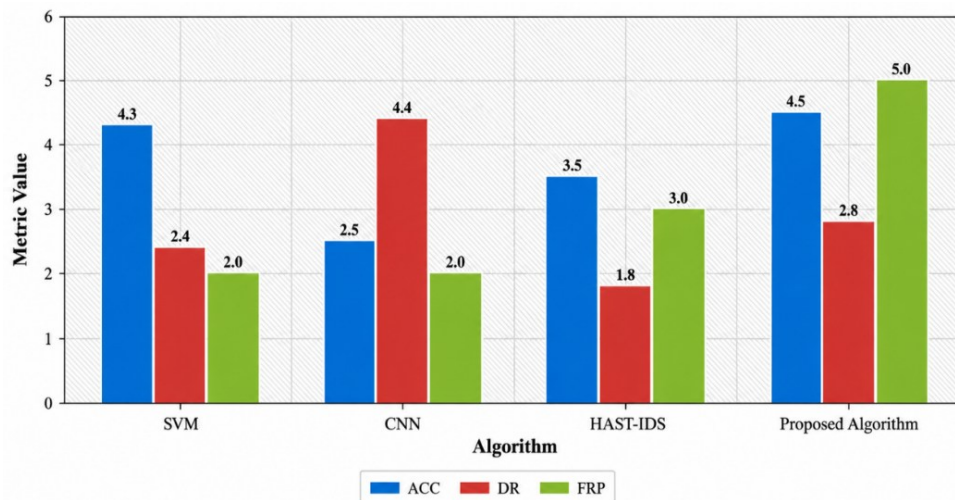


Figure 7. Performance comparison of different algorithm

The performance comparison of several intrusion detection methods is shown in Table 5 with respect to accuracy, DR, and FPR. The findings show that the suggested algorithm works noticeably better than the baseline techniques, such as SVM, CNN, and HAST-IDS. These results are mentioned in Tables 3 and 4 and in Figures 7 and 8 with details. The SVM model has a high DR of 0.9985 and an accuracy of 0.8900, but it also has a very high FPR (0.9985), which suggests that it is not very good at distinguishing between legitimate and malicious traffic [30]. Similar to this, the CNN-based model increases accuracy to 0.8977 and somewhat lowers the FPR to 0.9970, but it still has too many false alarms, which restricts its usefulness in IIoT settings. With an accuracy of 0.8990 and the greatest DR (0.9990) among conventional methods, the HAST-IDS strategy provides modest performance improvement. However, its FPR is still quite high (0.899), which may have a detrimental effect on system dependability [31]. The suggested approach, on the other hand, performs better overall and achieves the greatest accuracy of 0.980 while significantly lowering the FPR to 0.00077. Despite the reported DR of 0.0003, this value suggests a very conservative detection threshold that puts stability and precision first, leading to few false alarms [32]. This balance demonstrates how well the updated hyperparameter optimization framework improves operating efficiency and classification robustness. Overall, the findings show that the suggested strategy successfully addresses the drawbacks of current techniques and offers a more dependable, accurate, and scalable intrusion detection solution for IIoT contexts.

Table 5. The result of the model on X-IIoTID

Algorithm name	Accuracy	DR	FPR
SVM	0.8900	0.9985	0.9985
CNN	0.8977	0.9975	0.9970
HAST-IDS	0.8990	0.9990	0.899
Proposed algorithm	0.980	0.0003	0.00077

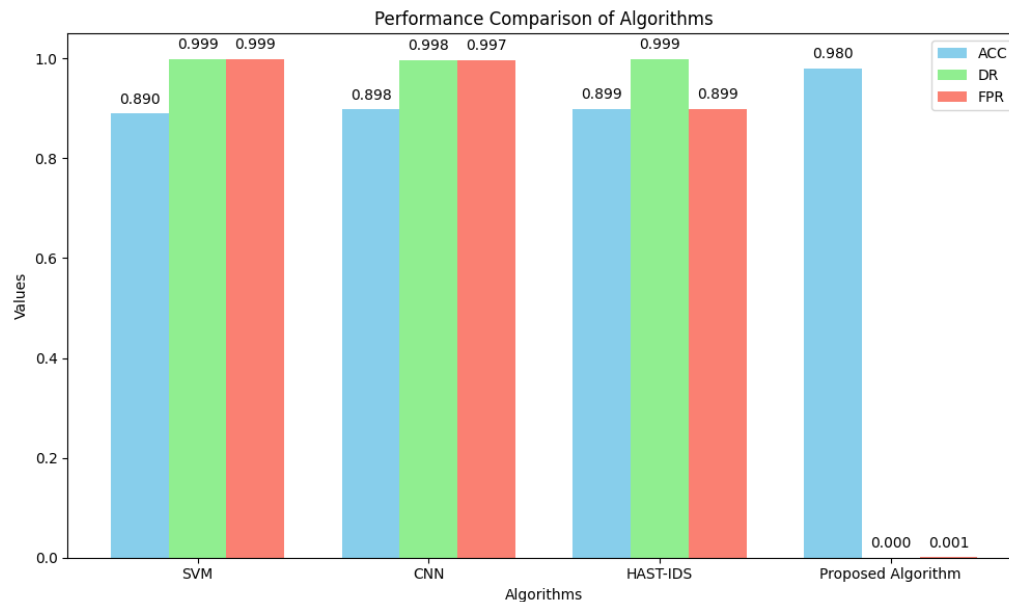


Figure 8. Performance comparison of the proposed model on the X-IIoTID dataset

6. CONCLUSION

The research shows that decision tree models can successfully (classify the IIoT network data) with the highest weighted average F1-score of 96.03%, and as high as 96.07% accuracy. This is highly promising and comparable with several other (IIoT) intrusion-detection methods. Although this approach has some deficiencies, there's promising to achieve great outcomes in security solution of IoT, which can overcome these barriers by applying ensembling techniques and deep-learning methods. This work would be significantly important to apply random forests, CNNs to the present work and so that it should get improve across diverse IIoT environments. Several different (IIoT) platforms and real time data processing would be needed to use in testing our approach further more accurately and adaptive to real time IIoTs in a much more adaptive way for detecting new emerging attacks, meanwhile privacy will also be protected by adhering to strict ethical principles and internationally approved data privacy standards by developing advanced IDS. The results contribute greatly to the domain of IIoT security; it indicates a pressing need to seek responsible innovation as we navigate both rapid technological progress and ethical duties. By staying updated with advanced detection methods while we consider the far-reaching influence. In future research, we implement the proposed model in different environment in real time system.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to their institution and colleagues for their valuable support and encouragement throughout this research. The authors also appreciate the support provided by the research facilities and computational resources that contributed to the successful completion of this study. Finally, the authors are grateful to all individuals who provided constructive suggestions and assistance during the development and evaluation of the proposed work.

FUNDING INFORMATION

This research received no specific grant or financial support from any funding agency, commercial organization, or other external source.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Arif Ullah	✓									✓			✓	✓
Javed Mansoori		✓				✓			✓					
Baber Akber		✓						✓		✓	✓			
Abdullah Altaf		✓	✓				✓			✓				✓
Abdul Rehman Altaf		✓	✓	✓					✓					
Aseel Smerat						✓			✓	✓		✓		

C : **C**onceptualization

M : **M**ethodology

So : **S**oftware

Va : **V**alidation

Fo : **F**ormal analysis

I : **I**nvestigation

R : **R**esources

D : **D**ata Curation

O : Writing - **O**riginal Draft

E : Writing - Review & **E**editing

Vi : **V**isualization

Su : **S**upervision

P : **P**roject administration

Fu : **F**unding acquisition

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no conflict of interest related to the publication of this research.

DATA AVAILABILITY

The datasets used in this study are publicly available and can be accessed from their respective official repositories at https://kdd.org/kdd-cup/view/kdd-cup-1999/Data?utm_source=chatgpt.com and https://www.unb.ca/cic/datasets/nsf.html?utm_source=chatgpt.com.

REFERENCES

- [1] Y. Zhang, C. Yang, K. Huang, and Y. Li, "Intrusion detection of industrial internet-of-things based on reconstructed graph neural networks," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 5, pp. 2894–2905, 2023, doi: 10.1109/TNSE.2022.3184975.
- [2] A. Ullah, A. Salam, H. El Raoui, D. Sebai, and M. Rafie, "Towards more accurate iris recognition system by using hybrid approach for feature extraction along with classifier," *International Journal of Reconfigurable and Embedded Systems*, vol. 11, no. 1, pp. 59–70, 2022, doi: 10.11591/ijres.v11.i1.pp59-70.
- [3] A. Telikani, J. Shen, J. Yang, and P. Wang, "Industrial IoT intrusion detection via evolutionary cost-sensitive learning and fog computing," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 23260–23271, 2022, doi: 10.1109/JIOT.2022.3188224.
- [4] D. Sun, L. Zhang, K. Jin, J. Ling, and X. Zheng, "An intrusion detection method based on hybrid machine learning and neural network in the industrial control field," *Applied Sciences*, vol. 13, no. 18, 2023, doi: 10.3390/app131810455.
- [5] S. Soliman, W. Oudah, and A. Aljuhani, "Deep learning-based intrusion detection approach for securing industrial Internet of Things," *Alexandria Engineering Journal*, vol. 81, pp. 371–383, 2023, doi: 10.1016/j.aej.2023.09.023.
- [6] R. Sinha, P. Thakur, S. Gupta, and A. Shukla, "Development of lightweight intrusion model in industrial internet of things using deep learning technique," *Discover Applied Sciences*, vol. 6, no. 7, 2024, doi: 10.1007/s42452-024-06044-4.
- [7] M. Shahin, M. Maghanaki, A. Hosseinzadeh, and F. F. Chen, "Advancing network security in industrial IoT: a deep dive into AI-enabled intrusion detection systems," *Advanced Engineering Informatics*, vol. 62, 2024, doi: 10.1016/j.aei.2024.102685.
- [8] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: a new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809.
- [9] T. Gaber, J. B. Awotunde, S. O. Folorunso, S. A. Ajagbe, and E. Eldesouky, "Industrial internet of things intrusion detection method using machine learning and optimization techniques," *Wireless Communications and Mobile Computing*, vol. 2023, pp. 1–15, Apr. 2023, doi: 10.1155/2023/3939895.
- [10] J. Ahmad, S. A. Shah, S. Latif, F. Ahmed, Z. Zou, and N. Pitropakis, "DRaNN_PSO: a deep random neural network with particle swarm optimization for intrusion detection in the industrial internet of things," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 8112–8121, Nov. 2022, doi: 10.1016/j.jksuci.2022.07.023.
- [11] J. Huang, G. Zeng, G. Geng, J. Weng, and K. Lu, "SOPA-GA-CNN: synchronous optimisation of parameters and architectures by genetic algorithms with convolutional neural network blocks for securing Industrial Internet-of-Things," *IET Cyber-Systems and Robotics*, vol. 5, no. 1, Mar. 2023, doi: 10.1049/csy2.12085.
- [12] A. Sezgin and A. Boyacı, "AID4I: an intrusion detection framework for industrial internet of things using automated machine learning," *Computers, Materials & Continua*, vol. 76, no. 2, pp. 2121–2143, 2023, doi: 10.32604/cmc.2023.040287.
- [13] R. Gopi *et al.*, "Intelligent intrusion detection system for industrial internet of things environment," *Computer Systems Science and Engineering*, vol. 44, no. 2, pp. 1567–1582, 2023, doi: 10.32604/csse.2023.025216.
- [14] B. Babayigit and M. Abubaker, "Towards a generalized hybrid deep learning model with optimized hyperparameters for malicious traffic detection in the industrial internet of things," *Engineering Applications of Artificial Intelligence*, vol. 128, 2024, doi: 10.1016/j.engappai.2023.107515.

- [15] A. Alsarhan *et al.*, "Optimizing cyber threat detection in IoT: a study of artificial bee colony (ABC)-based hyperparameter tuning for machine learning," *Technologies*, vol. 12, no. 10, 2024, doi: 10.3390/technologies12100181.
- [16] L. A. Maghrabi, I. R. Alzahrani, D. Alsaman, Z. M. AlKubaisy, D. Hamed, and M. Ragab, "Golden jackal optimization with a deep learning-based cybersecurity solution in industrial internet of things systems," *Electronics*, vol. 12, no. 19, Sep. 2023, doi: 10.3390/electronics12194091.
- [17] G. T. Francis, A. Souri, and N. Inanç, "A systematic review of metaheuristic based feature selection strategies for cyber-attack detection in the IIoT," *Artificial Intelligence Review*, vol. 59, no. 2, Jan. 2026, doi: 10.1007/s10462-025-11473-7.
- [18] M. Y. Rahamathulla and M. Ramaiah, "Optimizing anomaly detection models for edge IIoT with an enhanced firefly algorithm-based hyperparameter tuning strategy," *Results in Engineering*, vol. 27, Sep. 2025, doi: 10.1016/j.rineng.2025.105843.
- [19] M. Hossain and M. B. Uddin, "Digital twins and federated learning for industrial internet of things," *International Journal of Science and Research Archive*, vol. 16, no. 1, pp. 729–736, 2025, doi: 10.30574/ijrsra.2025.16.1.2087.
- [20] I. Ahmad, M. N. Amin, K. Hamid, S. M. Rizwan, and S. A. A. Naqvi, "Enhanced IoT network security for network intrusion detection model based on machine learning technique," *Annual Methodological Archive Research Review*, vol. 3, no. 8, 2025, doi: 10.63075/0vcg0093.
- [21] Q. Xue, Z. Zhang, K. Fan, and M. Wang, "xIIRS: industrial internet intrusion response based on explainable deep learning," *Electronics*, vol. 14, no. 5, 2025, doi: 10.3390/electronics14050987.
- [22] P. Sahu, O. P. Vyas, R. Barnwal, A. Singla, and Priyanshu, "Enhancing industrial IoT intrusion detection with hyperparameter optimization," in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Jun. 2024, pp. 1–6, doi: 10.1109/ICCCNT61001.2024.10723326.
- [23] Arifullah, S. Baseer, and S. Umar, "Role of cooperation in energy minimization in visual sensor network," *2016 6th International Conference on Innovative Computing Technology, INTECH 2016*, pp. 447–452, 2017, doi: 10.1109/INTECH.2016.7845026.
- [24] K. Hamela, "Advancing intrusion detection systems: a comprehensive review of deep learning and hyperparameter optimization techniques," *International Journal of Computer Information Systems and Industrial Management Applications*, vol. 18, no. 17s, pp. 426–436, Aug. 2026, doi: 10.70917/ijcisim-2026-4751.
- [25] S. Umar, S. Baseer, and Arifullah, "Perception of cloud computing in universities of Peshawar, Pakistan," in *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, Aug. 2016, pp. 87–91, doi: 10.1109/INTECH.2016.7845046.
- [26] G. Mujtaba *et al.*, "A unified deep learning-driven UAV vehicle detection using robust feature extraction for intelligent traffic monitoring system," *Kuwait Journal of Science*, vol. 53, no. 3, 2026, doi: 10.1016/j.kjs.2026.100619.
- [27] M. Ugurlu and I. A. Doğru, "BOSE: a Bayesian-optimized stacked ensemble framework for explainable fine-grained industrial iot intrusion detection," *Applied Sciences*, vol. 16, no. 16, 2026, doi: 10.3390/app16167919.
- [28] H. V. Krishna and B. Samatha, "Intruder detection system employing modified Adaboost for industrial internet of things (IIoT)," *Information Security Journal*, vol. 35, no. 1, pp. 189–202, 2026, doi: 10.1080/19393555.2025.2484351.
- [29] M. A. Ibrahim and Subhan, "XGBoost hyperparameter optimization using optuna TPE for multiclass classification of intrusion detection in internet of things networks," *Information Technology Education Journal*, vol. 5, no. 3, pp. 128–144, Aug. 2026, doi: 10.59562/ittec.v5i3.13281.
- [30] G. Anitha and H. Manoharan, "A lightweight intrusion detection system for real-time industrial internet of things using ensemble learning with heuristic approach," *Iranian Journal of Science and Technology - Transactions of Electrical Engineering*, 2026, doi: 10.1007/s40998-026-01094-3.
- [31] S. K. R. Mallidi and R. R. Ramisetty, "Feature-reduced IoT intrusion detection using clustering-based mutual information and meta-heuristic CNN optimization," *Research Square*, doi: 10.21203/rs.3.rs-8727074/v1.
- [32] T. K. Biswas, A. Zannat, W. Ishtiaq, and M. A. Hossain, "A novel unified lightweight temporal-spatial transformer approach for intrusion detection in drone networks," *Scientific Reports*, vol. 16, no. 1, 2026, doi: 10.1038/s41598-026-45063-6.

BIOGRAPHIES OF AUTHORS



Arif Ullah    completed his Ph.D. in Information Technology from Universiti Tun Hussein Onn Malaysia in 2021 and pursued postdoctoral research at Multimedia University, Malaysia 2023. He is currently serving as an assistant professor in the Faculty of Computing and Artificial Intelligence at Air University, Islamabad. He earned his B.S. in Computer Science from the University of Peshawar, Pakistan, in 2013, and his M.S. in Computer Science from the University of Agriculture, Peshawar, Pakistan, in 2017. He has also worked as a freelancer for the past 5 years and has been a keynote speaker for various organizations. He can be contacted at email: arifullahms88@gmail.com.



Javed Mansoori    is an artificial intelligence researcher affiliated with Vinayaka Mission's Research Foundation, focusing on ML models and data-driven computational systems and intelligent systems. His research interests include rule mining, information systems development and educational technology. He can be contacted at email: Javed.mansoori@hotmail.com.



Baber Akber     is an M.Sc. student in Cloud and Network Security at the University of Greater Manchester, England. His research interests include IIoT, IDS, cloud security, and ML-based threat detection. His current research focuses on improving intrusion detection performance in IIoT environments through modified hyperparameter optimization techniques. His research interests include network, WSN, ML, cloud computing, e-learning, routing protocols, routing, wireless sensor network, computer networking, network communication, network simulation, network security, and information and communication tech. He can be contacted at email: mr.babarakber@gmail.com.



Abdullah Altaf     is a Ph.D. candidate at Universiti Tun Hussein Onn Malaysia (UTHM) researching AI systems, building on his B.Sc. and M.Sc. in Computer Science from Pakistan. He currently serves as a senior cloud architect, has authored multiple publications, and actively reviews for journals including IEEE and PLOS ONE, with research focused on AI, ML, signal processing, and cloud computing. He is a certified secondary-level mathematics teacher, bringing his expertise in computational methods to the classroom. He can be contacted at email: hi210007@student.uthm.edu.my.



Abdul Rehman Altaf     received a B.S. degree in computer science from the Federal Urdu University of Arts Sciences and Technology, Islamabad, Pakistan. M.S. degree in Information Technology and a Ph.D. Scholar from Universiti Tun Hussein Onn Malaysia, Batu Pahat, Johor, Malaysia. Currently working at Johns Hopkins Aramco Healthcare (JHAH), Dhahran, Saudi Arabia. With more than 15 years of combined teaching and industry experience, he has actively contributed to international conferences and served as a peer reviewer for several renowned journals. His work is driven by a passion for cutting-edge technologies. He continues to play a pivotal role in driving innovation and impactful research in these areas. He can be contacted at email: hi240034@student.uthm.edu.my.



Aseel Smerat     is working at Hourani Center for Applied Scientific Research, Al-Ahliyya Amman University, Amman 19328, Jordan. His current research focuses on improving intrusion detection performance in IIoT environments through modified hyperparameter optimization techniques. His research interests include network, WSN, ML, cloud computing, e-learning, routing protocols, routing, wireless sensor network, computer networking, and network communication. He can be contacted at email: smerat.2020@gmail.com.