International Journal of Electrical and Computer Engineering (IJECE)
Vol. 14, No. 6, December 2024, pp. 7169~7177
ISSN: 2088-8708, DOI: 10.11591/ijece.v14i6.pp7169-7177

Framework for detecting and resisting cyberattacks on cyber-physical systems in internet of things

Jyoti Metan[1], Mahantesh Mathapati[2], Prasad Adaguru Yogegowda[3], Kurilinga Sannalingappa Ananda Kumar[4]

[1]Department of Information Science and Engineering, Atria Institute of Technology, Bengaluru, India
[2]Department of Computer Science and Engineering, Amruta Institute of Engineering and Management Sciences, Bengaluru, India
[3]Department of Computer Science and Engineering, SJB Institute of Technology, Bengaluru, India
[4]Department of Information and Science Engineering, Atria Institute of Technology, Bengaluru, India

Article Info

Article history:

Received Apr 13, 2024
Revised Jul 29, 2024
Accepted Aug 6, 2024

Keywords:

Anomaly
Cyber attacks
Cyber-physical system
Internet of things
Machine learning

ABSTRACT

Cyber-physical system (CPS) is an integral part of an internet of things (IoT) with established wide spread applications. An increasing concern towards being highly vulnerable to various forms of dynamic cyber-attacks has been increasingly evolving. A review of existing research methodology showcases complex solutions that can offer sub-optimal security strength when exposed to dynamic cyber-attack forms while increasing the computational burden. Therefore, this manuscript presents a novel yet simplified computational framework capable of determining and resisting critical anomalies within internet-of-cyber physical systems (IoCPS). The presented scheme contributes towards preprocessing following a distinct oversampling method targeting balancing the data. An ensemble machine learning model using a discrete variant of AdaBoost and neural decision tree (NDT) has been implemented to optimize the learning process and improve the threat detection efficiency. The comparative outcome of the proposed study showcases that it offers approximately 7.2% increased threat detection accuracy and approximately 68% reduced response time compared to frequently adopted learning mechanisms towards threat detection over an IoT environment.

Corresponding Author:

Jyoti Metan
Department of Information Science and Engineering, Atria Institute of Technology
ASKB Campus, 1st Main Rd, AGS Colony, Anandnagar, Hebbal, Bengaluru-560024, Karnataka, India
Email: jyotimetan@gmail.com

1. INTRODUCTION

The rapid advancement of technologies year after year has introduced a new system of interrelated objects known as the internet of things (IoT). It aims to connect multiple electronic equipment and smart devices to the Internet to automate the system [1]. However, the large-scale connection of such electronics and smart devices requires massive storage space and computing power [2]. Therefore, the cyber-physical system (CPS) creates a huge storage space and high computing power through cloud computing technology [3]. CPS refers to an interconnected environment of communication with their interaction with the IoT and the cloud will lead to futuristic CPS, namely the internet of cyber-physical things (IoCPT), which refers to an advanced system of the seamless integration of computation empowered by cloud computing and physical components empowered by IoT [4]. This futuristic technology interests research communities and industries due to its potential benefits to society, the environment, and the economy [5], [6]. Anomalies in IoCPS data can occur for various reasons, including system malfunctions, cyber-attacks, or human error. Anomalies in a network refer to unusual or abnormal behavior that deviates from the expected pattern or behavior [7]. These anomalies can have serious consequences, such as decreased efficiency, increased downtime, and potential safety risks [8]. Attackers may target these systems to steal sensitive information, alter or disrupt normal operations, or gain unauthorized control. In some cases, an attacker may exploit a vulnerability in the system to cause a malfunction or failure [9]. Similarly, an industrial control system anomaly could result in a production line shutdown, leading to significant financial losses and operational disruptions [10]. Therefore, it is essential to detect anomalies in the data generated by intelligent sensors as quickly and accurately as possible. Anomaly detection identifies patterns or behaviors in data that deviate from standard patterns in real time. Various literature discusses approaches to detect intrusions and anomalies in these systems, including rule-based systems, signature-based systems [11] and machine learning-based systems [12]. Machine learning-based systems effectively detect new types of attacks and anomalies, but they can be complex and time-consuming to implement [13].

The related work in this direction follows: Jin *et al.* [14] presented a multilayer learning model to detect anomalies in power systems using a convolution neural network (CNN) to learn the typical data patterns and detect anomalies in real time. The result suggests that this scheme performs better than conventional methods, such as Kalman filtering and support vector machine (SVM). Chen *et al.* [15] used a deep learning-based approach to detect anomalies in smart grid data. This scheme adopted a recurrent neural network (RNN) model to capture the temporal relationships between data points and detect real-time anomalies. The outcome demonstrates that the presented approach is practical over conventional methods, such as Bayesian networks and decision trees. Gu *et al.* [16] presented a rule-based system for intrusion detection in CPS. The system was based on a set of predefined rules and policies that were used to detect potential intrusions. The authors evaluated the system using real-world CPS data and found it effectively detected intrusions with high accuracy. However, this system is limited in countering new attacks and anomalies. Bao *et al.* [17] suggested a system based on predefined patterns to detect intrusions and anomalies in IoT data. Real-world IoT data is used in the evaluation, and results indicate that it effectively detected only known intrusions and anomalies. Ingre *et al.* [18] a decision tree-based system was proposed, effectively detecting intrusions and anomalies in CPS data. The simulation outcome shows that this method outperformed other traditional learning algorithms regarding accuracy and speed. Liu *et al.* [19] employed a random forest for intrusion detection in IoT systems. The result shows that the system effectively detects intrusions and anomalies in IoT data and outperforms other traditional machine learning algorithms regarding accuracy and speed. Li *et al.* [20] have described the effectiveness of deep learning-based intrusion detection CPS. Aouedi *et al.* [21] designed a deep belief network, and Derhab *et al.* [22] developed a multilayer deep neural network (DNN) to detect anomalies in IoT network data and evaluate the model's performance using real-world IoT network data. Althobaiti *et al.* [23] adopted DNN to identify intrusion patterns in CPS data. Awotunde *et al.* [24] have developed protocol-independent independent IDS using deep learning to detect dynamic attacks such as blackhole, distributed denial of service (DDoS), opportunistic service, Sinkhole, and Wormhole attacks. Tushkanova *et al.* [25] explored existing approaches, suggested developing threat detection based on the behavior analyses, and adopted an unsupervised learning approach. Tang *et al.* [26] presented a threat detection based on a diffusion model for industrial CPS. A diffusion model is adopted to balance the dataset, and then bi-directional long-short-term-memory (BiLSTM) is adopted to classify the anomaly. Kandhro *et al.* [27] adopted a joint approach of unsupervised learning and generative adversarial network to detect potential cyber-attacks in IoT-driven cyber infrastructure. The result shows the effectiveness of the presented scheme in that it outperforms another similar model in terms of accuracy, reliability, and detection efficiency.

The core research problems identified from a literature review are: i) degraded scalability, ii) higher false positive outcome and iii) data imbalance factor associated with the network dataset. IoT and CPS systems often involve many connected devices, and it can be challenging to apply complex and specifically designed deep learning techniques in a scalable manner to detect anomalies in high volumes of streaming network data. Apart from this these systems often experience imbalanced data distributions, with a small number of anomalies or intrusions among a large amount of standard data. This can make it difficult for deep learning models to identify anomalies accurately. Therefore, the research work reported in this paper suggests an optimal security system by combining the strengths of multiple optimized classifiers followed by an effective data modelling scheme to achieve high accuracy, faster response time and robustness in detecting dynamic security threats.

In response to the studies mentioned above, this manuscript's contribution is an effective security solution based on an ensemble learning technique integrated with optimal data sampling operation. The prime aim of the proposed system is to perform the detection of anomalies and classification of intrusions on a real-time basis. The value-added novelties of this work are as follows: i) A novel and simplified architecture of network concentrating edge computing concept that enables efficient execution of the proposed learning-driven security system, ii) a practical data modelling approach is presented followed by suitable preprocessing operation and data sampling approach to balance data, overcome biased predictive outcome, and empower anomaly detection, iii) An ensemble learning as joint approach of M-Ada Boost and neural decision tree (NDT) has been presented to perform predictive modelling for anomaly and intrusion detection in IoCPS. The following section discusses about adopted research methodology.

2. METHOD

The proposed research methodology aims to construct a novel computational model capable of determining the lethal threats associated with anomalies in IoCPS. The proposed study has introduced a novel integrated framework to counter security threats in a modern network of IoCPS. Figure 1 illustrates the conceptual architecture of the proposed system based on the edge networking concept, statistical methods for network data modelling, and ensembled learning mechanism. The core notion of this architecture is to empower predictive analytics on the streaming network traffic for real-time anomaly detection.

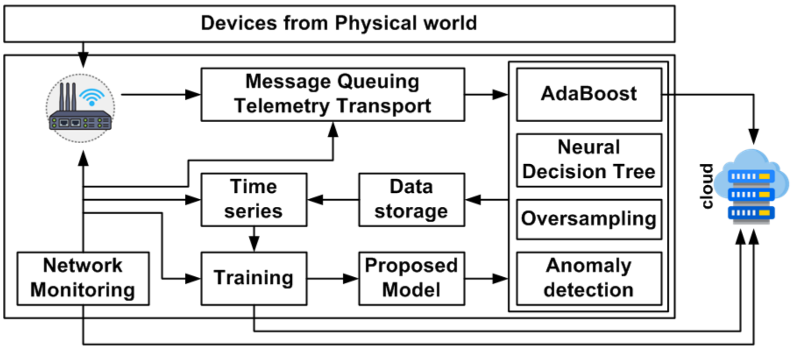


Figure 1. Schematic architecture of the proposed integrated framework

As depicted in Figure 1, the system design comprises three essential modules: IoCPS, edge computing infrastructure, and the cloud system. The IoCPS module is a cutting-edge system that integrates cyber systems enabled by cloud computing and physical components empowered by IoT. This innovative technology attracts significant attention from research communities and industries for its potential benefits to society, the environment, and the economy. The IoCPS module encompasses physical components such as intelligent electronic devices, sensor nodes, and cyber components responsible for computation, storage, and network management tasks, all leveraging cloud technology. The edge computing infrastructure encompasses networking methods for data routing and the proposed predictive system for anomaly detection. It features an IoT gateway for routing streaming network data (time series). The IoT gateway collects data from various devices and sends it to the messaging layer, powered by the message queuing telemetry transport (MQTT) protocol. The data store and processing components extract the data from the messaging layer, process it in a queue, and pass it through the trained anomaly detection model. The proposed anomaly detection algorithm retrieves data from the designated queues, performs anomaly detection, and sends the results to the cloud for centralized alerting and reporting. Additionally, the model stores the data in a database for potential future updates and improvements to the model through additional observational data. The system also incorporates an offline training scheduling mechanism that periodically retrieves bulk data from the database, compresses it, and sends it to the cloud for future use, such as a training model with new observations.

The integration of the edge computing concept is motivated by the growing amount of data produced by IoT devices in the IoCPS system, leading to increased demands on network bandwidth, storage, and compute resources. As a result, relying solely on centralized data processing, including in the cloud, has become increasingly costly and can result in prolonged delays in data processing. Edge computing offers a more effective means of utilizing ML-based anomaly detection by bringing data processing closer to the data source. This approach reduces the burden on the cloud, ensures immediate data processing, improves response times, and decreases network demand and cloud costs, resulting in a more cost-efficient and effective solution. The proposed scheme uses a preprocessing mechanism with a unique oversampling approach adopted for data modelling and to handle the heavily imbalanced nature of the IoT data [28]. The study implementation uses an ensemble model based on M-AdaBoost and NDT algorithm for anomaly detection. An exploratory analysis is carried out for the dataset while an oversampling approach is applied to obtain a balanced dataset suitable for subjecting it to a machine learning approach. The proposed scheme uses ensemble learning, which associates multiple learning models to improve the accuracy and robustness of predictions. The basic idea behind ensemble learning is to use multiple models to make predictions and then combine their predictions to make a final prediction. This approach can lead to better performance than using a single model, as the errors made by individual models can be averaged out. This paper presents a novel system developed based on the assembling of M-AdaBoost and NDT models to perform anomaly detection.

M-AdaBoost is an improved version of the adaptive boosting algorithm, widely adopted for binary classification problems. M-AdaBoost is designed to handle multi-class classification problems, which involve classifying instances into multiple categories rather than just two. In this model, the basic idea is to train multiple binary classifiers, one for each class against all the others, and then combine their predictions to make the final multi-class prediction. The binary classifiers are trained in a sequential manner, where each classifier focuses on correcting the misclassifications made by the previous classifier. The final prediction is made by taking a weighted sum of the predictions of all binary classifiers, where the weights reflect the classifier's accuracy.

On the other hand, NDT optimized learning classifier combines the strengths of decision trees and neural networks. It uses the tree-like structure of decision trees to make predictions and the representation learning capabilities of neural networks to learn more complex data representations. In this model, each internal node of the tree is represented by a neural network, which is trained to learn a more complex representation of the data, which allows for efficient capture of the nonlinear relationships between the features and the target, thereby improving accuracy, higher interpretability, and robustness of the algorithm in the predictive task. The proposed ensembled learning model can be mathematically represented as a weighted sum of the class probabilities predicted by each classifier. Given two classifiers, f_1 (M-AdaBoost) and f_2 (NDT), the final ensemble classifier can be defined as (1):

$$f(x) = w_1 x f_1(x) \ + w_2 x f_2(x) \tag{1}$$

According to expression (1), the variable x represents the input sample, and w_1 and w_2 are the weights assigned to each classifier. The weights w_1 and w_2 determine the relative importance of each classifier in the ensemble, followed by the voting mechanism. The voting mechanism combines the predictions of models $f_1(x)$ and $f_2(x)$. In the proposed ensemble learning model, a soft voting mechanism is used to consider the weighted average of the class probabilities to predict the class. Therefore, the weights w_1 and w_2 are set proportional to the accuracy of each classifier. If classifier $f_1(x)$ has a higher accuracy, it will have a higher weight in the ensemble, and vice versa. The final ensemble prediction y is obtained by taking the class with the highest weighted sum of class probabilities, numerically given as (2):

$$y = arg_{max}(ci)\ (w_1 xP1c \ + \ w_2 xP2c) \tag{2}$$

According to expression (2), the variable c is the class index, and $P1c$ and $P2c$ are the class probabilities predicted by classifiers $f_1(x)$ and $f_2(x)$ for class c_i. Therefore, it can be noted that the proposed scheme has introduced a progressive and sequential process of confirming the presence of anomalies and performing classification. The prime novelty of this implementation strategy is associated with its detection capability of most complex anomalies or any form of dynamic threats present within the IoCPS environment. The classification optimizes the learning process, considering the potential of neural networks and decision trees. Hence, the proposed system has noted an optimal balance between computational effort and resistivity features. The following section presents a discussion of the accomplished outcome of the study.

3. RESULTS

This section presents and assesses the outcome of the simulation executed to validate the scope of the proposed ensembled model for anomaly detection in the IoCPS. The design and development of the proposed system is developed with a Python environment executed on Anaconda distribution. The analysis concerns various performance indicators, and their results are compared in multiple scenarios. The results are discussed from the perspective of the implementation environment, data modelling, and accomplished results.

3.1. Implementation environment

The dataset used to model the proposed system is DS2OS IoT, obtained from the Kaggle platform [28]. This dataset is collected from an IoT network and contains many features related to network behavior and system performance. The dataset provides a unique opportunity to study anomalies in IoT networks and develop machine-learning algorithms to detect these anomalies effectively. The dataset is imbalanced, with only a small percentage of the data being anomalous, making it challenging for machine learning models to accurately predict the type of anomalies.

3.2. Data modelling

As a pre-request step, the proposed work performs an exploratory analysis of the dataset; the insight shows that the dataset consists of large samples, i.e., 357,951 in a row and 12 features in the column. Further analysis is carried out towards analyzing the missing values in the dataset, which shows that the dataset has 148 missing values about column "accessed node type" and 2,050 missing instances subjected to column name "value". The missing values are removed under essential preprocessing operation. Also, the dataset consists of both numerical and categorical values. The categorical values are transformed and encoded using one hot encoding mechanism. In the subsequent process, the dataset's values are normalized under the min-max scaling scheme and made suitable for further tasks. It has been observed that the adopted dataset consists of eight classes, including one regular and seven attacks, which is related to a multi-class prediction task problem. Further analysis reveals that the dataset has a significant class imbalance problem. The distribution of data concerning each class is shown in Figure 2.

Figure 2 shows that the dataset is imbalanced; most samples belong to intrusion class 7, where the average class is encoded with 0, and the rest are different intrusion classes 1 to 7. Implementing deep learning or machine learning will always get biased towards predicting the majority class. Therefore, the study adopts over sampling of the minority classes towards data preparation and unbiased supervised learning. The oversampling approach works by synthesizing new samples for the minority class by interpolating between existing samples. To do this, the proposed oversampling approach first selects a minority class sample at random and then selects its nearest neighbors. The algorithm then synthesizes a new sample by randomly interpolating between the selected sample and one of its neighbors. This process is repeated until the minority class is oversampled to balance the data. The implementation process involves splitting the dataset into training and testing sets using the $train\_test\_split$ function from scikit-learn. Next, proposed oversampling is used to oversample the minority class. Finally, the dataset is oversampled, as shown in Figure 3. As shown in Figure 3, the dataset is oversampled and balanced with even distribution, i.e., each class with 243,513 samples. The next step is to perform predictive analytics using the proposed ensembled mechanism.

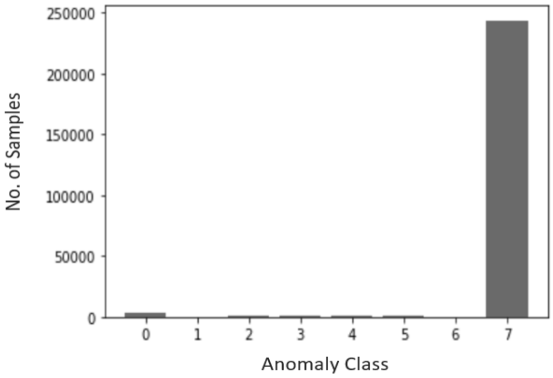


Figure 2. Statistics of data distribution number of samples vs anomaly classes

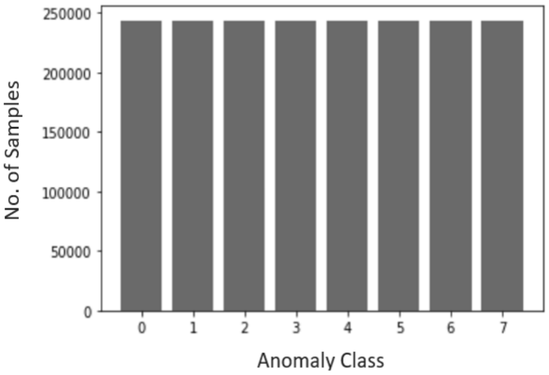
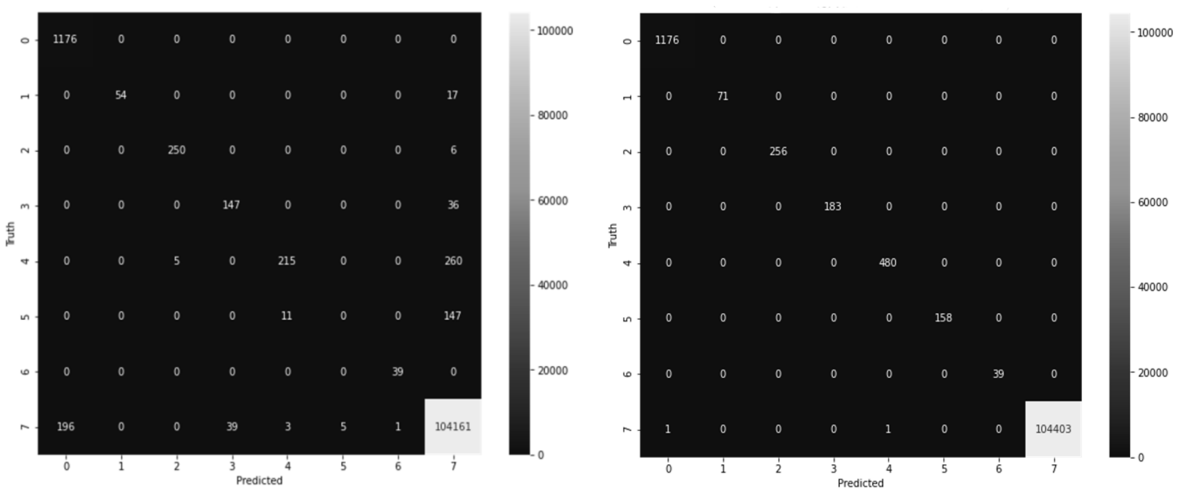


Figure 3. Statistics of data distribution after oversampling number of samples vs anomaly classes

The first part of the result analysis is carried out without an oversampling approach. The proposed ensembled learning model is trained over the imbalanced dataset. To perform a comparative analysis, the study evaluates M-AdaBoost and NDT. The confusion plot for the proposed model without the oversampling method is shown in Figure 4(a), while the proposed model's analysis with oversampling is shown in Figure 4(b).

Figure 4(b) shows that the proposed model provides a better detection rate with 100% precision, recall and F1-score results. The reason behind this is that this approach combines the oversampling and the ensemble of NDT and M-Ada Boost algorithm to handle the heavy imbalanced nature of the IoCPS data and provide an effective solution for anomaly detection. The results indicate that the proposed approach provides good performance for anomaly detection and can potentially improve the security of IoCPS by identifying potential threats in real-time.



(a) (b)

Figure 4. Confusion plot for the proposed system (a) model without the oversampling method and (b) model's analysis with oversampling

The next part of the analysis is about comparing the outcome of the proposed study Prop with existing learning-based methods. For this purpose, the existing learning methods considered are i) supervised learning techniques, e.g., support vector machine (SVM), random forest (RF), and decision tree (DT), ii) unsupervised learning techniques, e.g., k-means clustering (kMC), Density-based spatial clustering of applications with noise (BDSCAN), and isolation forest (IF), and iii) deep learning scheme e.g., recurrent neural network (RNN), long short-term memory (LSTM), and autoencoder (AE). The assessment of comparative analysis is carried out concerning threat detection accuracy and response time. The numerical outcome is exhibited in Table 1, which shows that the proposed scheme offers approximately 7.2% improved threat detection accuracy and 68% reduced response time compared to all the existing learning schemes.

Table 1. Numerical outcome of comparative analysis

Approaches	Threat detection accuracy (%)	Response time (s)
Prop	98.4	0.399
SVM	92.83	0.937
RF	89.55	1.99
DT	90.11	0.997
kMC	85.11	1.37
BDSCAN	90.37	0.983
IF	90.99	0.952
RNN	92.11	0.898
LSTM	94.25	0.791
AE	94.92	0.803

The graphical outcome of the numerical evaluation is shown in Figures 5 and 6 for simplifying the inference of the outcome. A significant trade-off is observed for existing learning approaches where there is much fluctuation between threat detection accuracy and response time. The cumulative outcome reflects the proposed scheme to excel in a better balance between both performance metrics.

A simplified form of hyperparameter tuning is carried out in proposed scheme. The scheme configures the rate of training at 0.01 while in order to resist any possibility of overfitting, the scheme further configures the regularization parameter as 0.0001 while 125 batch size is maintained. The experimentation has initially considered total number of estimators as 50,100,150,200,250 while best estimator has been found to be 250. The rate of learning is initialized to 0.1,0.2,0.3,0.4,0.5,0.6,0.7,0.8,0.9,1 while the best learning rate was observed at 0.5. The strategies to mitigate overfitting is as follows: -AdaBoost trains the neural decision trees sequentially. After each iteration, it adjusts the weights of misclassified instances to prioritize them in the subsequent iteration. This iterative training process helps in gradually improving the model's accuracy on difficult examples without overfitting to the entire dataset in one go. The boosting technique employed by M-AdaBoost places more emphasis on instances that are harder to classify correctly.

By iteratively focusing on these instances, the model learns to generalize better rather than memorizing the training data, which reduces the risk of overfitting.

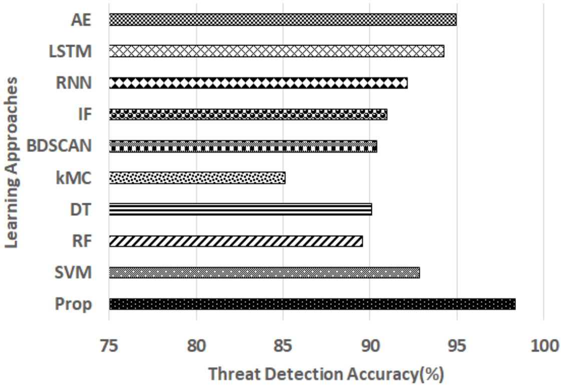


Figure 5. Comparative analysis of threat detection accuracy

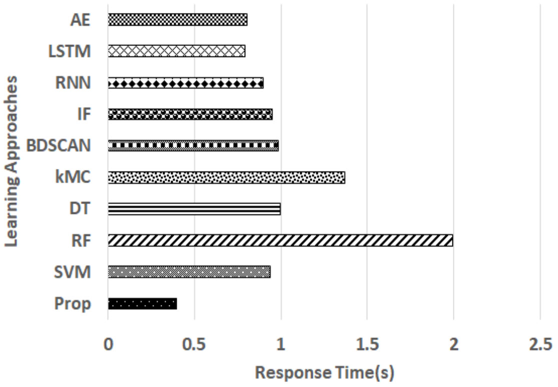


Figure 6. Comparative analysis of response time

The better performance of proposed system in contrast to existing machine learning approaches can be attributed from multiple perspective. The primary rationale is its reduced set of iteration with more contextual data related to traffic information leading to reduced computational effort and higher accuracy. M-AdaBoost is a variant of AdaBoost that combines multiple classifiers (in this case, NDT) to improve overall accuracy. By aggregating the predictions of multiple models, it tends to reduce variance and improve generalization, thus increasing accuracy. Neural decision trees, which are essentially decision trees where each node is a neural network, can capture complex, non-linear relationships in the data. This flexibility allows them to model intricate patterns that traditional decision trees might miss, thereby improving accuracy.

The comparative outcome of proposed scheme shows better numerical scores with accomplishment of 7.2% of increased accuracy and 68% of minimized response time. Hence, the prime strength of the proposed model is associated with improving classification by sequentially applying weak learners to focus on instances that are harder to classify correctly. This iterative approach helps in gradually improving accuracy. While NDT can potentially overfit, but by combining them with AdaBoost, which penalizes misclassifications and emphasizes difficult examples, the overall model tends to generalize better, leading to higher accuracy on unseen data.

The prime purpose of the study is towards strengthening system strength in presence of anomalies. The importance of the study is towards a novel and cost-effective anomaly detection scheme. The model not only offers effective network monitoring but also facilitates practical world scenarios by considering time-series approach towards data storage. Adoption of this model is beneficial for all future potential applications that demands massive number of interconnected machines working on public networks for offering cost-effective data security.

4. CONCLUSION

Anomaly detection is a critical challenge in modern networks like IoT and CPS, as it can indicate abnormal behavior that potentially compromises the system's integrity. The proposed work has presented a novel and significant work-based data balancing and ensemble learning mechanism. The proposed approach consists of two phases. The first phase is data preprocessing, where the IoCPS data is processed and cleaned to remove irrelevant information. The data is then split into training and testing sets. The second phase is the modelling phase, where the oversampling approach is implemented to balance data and train the model. This model consists of two major components: M-AdaBoost and NDT algorithm, which are combined based on the weighted voting to make the final prediction and adjust the weights based on the accuracy of each classifier. The experiment shows promising precision, recall, and F1-score results. The concluding outcome of the comparative analysis showcases that the proposed scheme offers a significantly improved threat detection accuracy and faster response time compared to supervised, unsupervised, and deep learning schemes frequently adopted to secure IoT environments.

It should be noted that proposed study targets towards anomaly detection using novel machine leaning approach; however, they are not meant to secure the AI-based cyberthreats. Such form of cyberthreats is formed when attacker itself adopts AI to introduce the threats and this is one limitation of proposed model. This limitation can be overcome in future work where a novel detection algorithm can be designed using AI that can identify the anomalies associated with AI-based processor itself or the device/ component that runs the security algorithm. Blockchain approach along with bioinspired algorithm can be integrated towards accomplishing this target in future to resist AI-powered cyber threats. Further work can be carried out towards investigating the model on other publicly available dataset.

REFERENCES

[1] İ. Kahraman, A. Köse, M. Koca, and E. Anarim, "Age of information in internet of things: a survey," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 9896–9914, Mar. 2024, doi: 10.1109/JIOT.2023.3324879.

[2] P. M. Chanal and M. S. Kakkasageri, "Security and privacy in IoT: a survey," *Wireless Personal Communications*, vol. 115, no. 2, pp. 1667–1693, Nov. 2020, doi: 10.1007/s11277-020-07649-9.

[3] Y. Jiang, S. Wu, R. Ma, M. Liu, H. Luo, and O. Kaynak, "Monitoring and defense of industrial cyber-physical systems under typical attacks: from a systems and control perspective," *IEEE Transactions on Industrial Cyber-Physical Systems*, vol. 1, pp. 192–207, 2023, doi: 10.1109/TICPS.2023.3317237.

[4] E. H. Hafshejani *et al.*, "Self-aware data processing for power saving in resource-constrained IoT cyber-physical systems," *IEEE Sensors Journal*, vol. 22, no. 4, pp. 3648–3659, Feb. 2022, doi: 10.1109/JSEN.2021.3133405.

[5] I. Graja, S. Kallel, N. Guermouche, S. Cheikhrouhou, and A. Hadj Kacem, "A comprehensive survey on modeling of cyber-physical systems," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 15, Aug. 2020, doi: 10.1002/cpe.4850.

[6] D. Hastbacka *et al.*, "Dynamic edge and cloud service integration for industrial IoT and production monitoring applications of industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 1, pp. 498–508, Jan. 2022, doi: 10.1109/TII.2021.3071509.

[7] Y. Gao, J. Chen, H. Miao, B. Song, Y. Lu, and W. Pan, "Self-learning spatial distribution-based intrusion detection for industrial cyber-physical systems," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 6, pp. 1693–1702, Dec. 2022, doi: 10.1109/TCSS.2021.3135586.

[8] A. A. AlZubi, M. Al-Maitah, and A. Alarifi, "Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques," *Soft Computing*, vol. 25, no. 18, pp. 12319–12332, Sep. 2021, doi: 10.1007/s00500-021-05926-8.

[9] Bharathi. V and C. N. S. V. Kumar, "A real time health care cyber attack detection using ensemble classifier," *Computers and Electrical Engineering*, vol. 101, Jul. 2022, doi: 10.1016/j.compeleceng.2022.108043.

[10] A. Bhardwaj, F. Al-Turjman, M. Kumar, T. Stephan, and L. Mostarda, "Capturing-the-invisible (CTI): Behavior-based attacks recognition in IoT-oriented industrial control systems," *IEEE Access*, vol. 8, pp. 104956–104966, 2020, doi: 10.1109/ACCESS.2020.2998983.

[11] J. Tang *et al.*, "Anomaly detection in social-aware IoT networks," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 3162–3176, Sep. 2023, doi: 10.1109/TNSM.2023.3242320.

[12] K. Atefi, S. Yahya, A. Rezaei, and S. H. Binti Mohd Hashim, "Anomaly detection based on profile signature in network using machine learning technique," in *2016 IEEE Region 10 Symposium (TENSYMP)*, May 2016, pp. 71–76, doi: 10.1109/TENCONSpring.2016.7519380.

[13] X. Yan, Y. Xu, X. Xing, B. Cui, Z. Guo, and T. Guo, "Trustworthy network anomaly detection based on an adaptive learning rate and momentum in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6182–6192, Sep. 2020, doi: 10.1109/TII.2020.2975227.

[14] W. Jin, S. Zhang, B. Sun, P. Jin, and Z. Li, "An analytical investigation of anomaly detection methods based on sequence to sequence model in satellite power subsystem," *Sensors*, vol. 22, no. 5, Feb. 2022, doi: 10.3390/s22051819.

[15] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, "Evaluation of reinforcement learning-based false data injection attack to automatic voltage control," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2158–2169, Mar. 2019, doi: 10.1109/TSG.2018.2790704.

[16] Z. Gu, X. Zhou, T. Zhang, F. Yang, and M. Shen, "Event-triggered filter design for nonlinear cyber–physical systems subject to deception attacks," *ISA Transactions*, vol. 104, pp. 130–137, Sep. 2020, doi: 10.1016/j.isatra.2019.02.036.

[17] Z. Bao, D. He, M. K. Khan, M. Luo, and Q. Xie, "PBidm: Privacy-preserving blockchain-based identity management system for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1524–1534, Feb. 2023, doi: 10.1109/TII.2022.3206798.

[18] B. Ingre, A. Yadav, and A. K. Soni, "Decision tree based intrusion detection system for NSL-KDD dataset," in *Information and Communication Technology for Intelligent Systems (ICTIS 2017)-Volume 2 2*, 2018, pp. 207–218.

[19] C. Liu, Z. Gu, and J. Wang, "A hybrid intrusion detection system based on scalable K-means+ random forest and deep learning," *IEEE Access*, vol. 9, pp. 75729–75740, 2021, doi: 10.1109/ACCESS.2021.3082147.

[20] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: federated deep learning for intrusion detection in industrial cyber–physical systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5615–5624, Aug. 2021, doi: 10.1109/TII.2020.3023430.

[21] O. Aouedi, K. Piamrat, G. Muller, and K. Singh, "Federated semisupervised learning for attack detection in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 286–295, Jan. 2023, doi: 10.1109/TII.2022.3156642.

[22] A. Derhab, A. Aldweesh, A. Z. Emam, and F. A. Khan, "Intrusion detection system for internet of things based on temporal convolution neural network and efficient feature engineering," *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1–16, Dec. 2020, doi: 10.1155/2020/6689134.

[23] M. M. Althobaiti, K. P. M. Kumar, D. Gupta, S. Kumar, and R. F. Mansour, "An intelligent cognitive computing based intrusion detection for industrial cyber-physical systems," *Measurement*, vol. 186, Dec. 2021, doi: 10.1016/j.measurement.2021.110145.

[24] J. B. Awotunde, C. Chakraborty, and A. E. Adeniyi, "Intrusion detection in industrial internet of things network-based on deep learning model with rule-based feature selection," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, Jan. 2021, doi: 10.1155/2021/7154587.

[25] O. Tushkanova, D. Levshun, A. Branitskiy, E. Fedorchenko, E. Novikova, and I. Kotenko, “Detection of cyberattacks and anomalies in cyber-physical systems: approaches, data sources, evaluation,” *Algorithms*, vol. 16, no. 2, Feb. 2023, doi: 10.3390/a16020085.

[26] B. Tang, Y. Lu, Q. Li, Y. Bai, J. Yu, and X. Yu, “A diffusion model based on network intrusion detection method for industrial cyber-physical systems,” *Sensors*, vol. 23, no. 3, Jan. 2023, doi: 10.3390/s23031141.

[27] I. A. Kandhro *et al.*, “Detection of real-time malicious intrusions and attacks in IoT empowered cybersecurity infrastructures,” *IEEE Access*, vol. 11, pp. 9136–9148, 2023, doi: 10.1109/ACCESS.2023.3238664.

[28] J. H. Joloudari, A. Marefat, M. A. Nematollahi, S. S. Oyelere, and S. Hussain, “Effective class-imbalance learning based on SMOTE and convolutional neural networks,” *Applied Sciences*, vol. 13, no. 6, Mar. 2023, doi: 10.3390/app13064006.

BIOGRAPHIES OF AUTHORS

Jyoti Metan currently working as an associate professor in the Information Science and Engineering Department, Atria Institute of Technology, Bangalore, India. She has received her PhD from VTU University, India in 2020. Her research area includes cryptography, wireless sensor networks, security and machine learning. She has more than 17 years of teaching experience. She can be contacted at email: jyotimetan@gmail.com.

Mahantesh Mathapati is currently working as an associate professor in the Department of Computer Science and Engineering, Amruta Institute of Engineering and Management Science, Bengaluru, affiliated with Visvesvaraya Technological University, Belagavi. He has 20 years of teaching experience. His research interests are wireless sensor networks, internet of things, deep learning and machine learning. He can be contacted at email: manteshkrishna@gmail.com.

Prasad Adaguru Yogegowda working as associate professor, computer science and engineering at SJB Institute of Technology, Bangalore, Karnataka, India. He pursued a Ph.D degree in computer science engineering, 2020, M.Tech. in CSE-2011, B.E.in CSE-2009, all degrees awarded from Visvesvaraya Technological University, Belagavi. Karnataka, India. He published a total of 32 International Journals and Conference papers. He published 5 Indian patents. He is a life member of professional societies like IAENG, LMISTE, SDIWC, IMAP and AICTSD. His research areas of interest are wireless sensor networks, data mining, AI, and blockchain technology. He can be contacted at email: ayprasad26@gmail.com.

Kurilinga Sannalingappa Ananda Kumar received PhD from Visvesvaraya Technological University, Belagavi, Karnataka, India. Having 12 years of teaching experience. Currently, he is working as an associate professor in the Department of Information Science and Engineering at Atria Institute of Technology, Bangalore, India. His research area interests are WSN, data mining, machine learning, and cloud computing. He can be contacted at email: anandgdk@gmail.com.