International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

IDS based Trust Computation Algorithm in Industrial IoT using Machine Learning Techniques

Mr. Vaibhav Prakash Repe[1], Dr. Sarika Jadhav[2]

[1,2,]Computer engineering/ Padmabhooshan Vasantdada Patil Institute of Technology (Pvpit)/Savitribai Phule Pune University/India

Abstract

The rapid evolution of Industrial Internet of Things (IIoT) systems has added tremendous improvements to automation, process observables, and smart decision making in fields like medicine, manufacturing and smart infrastructure. With this increased automation, the IIoT systems become more vulnerable. Specially, maintaining trust and shielding IIoT systems from new, advanced, and growing cyber-attacks has proven to be a challenge. Typical Intrusion Detection Systems (IDS) detect intrusions to a network from attacks, but are insufficient to new advanced threats and attacks. Furthermore, such IDS fail to assess trust and dynamically adjust to a more sophisticated level in real time. This study outlines the details of such a challenge, and addresses these challenges with a hybrid trust-based intrusion detection framework that combines machine learning for efficient computation of trust in IIoT adaption environments. The model proposed in this study provides an assessment of validity of nodes in the network from an IIoT adaption framework, and such assessment is based on and integrated from several dimensions of control including communication, collaboration, and level of control exercised. Adaptive machine learning and control is based on a combination of both unsupervised and supervised control. More specifically, the supervision of control employs support vector machines (SVM), Naive Bayes (NB), and hybrid machine learning (HML) model based on random forest with AdaBoost. The evaluation methodology included both simulated datasets and datasets from real-world IoT applications. The results showed that Naïve Bayes scored 96.13% in accuracy, 96.4% in precision, 96.13% in recall, and 96.26% in F1 score; and SVM scored 93.2% in accuracy, 96.52% in precision, and 94.81% in F1 score. The results indicated that the proposed model, the HML, achieved a competing 98.2% in accuracy, 96.43% in precision, 98.2% in recall, and 97.31% in the F1 score, thus outperforming all other models in testing and demonstrating superior performance, robustness, and adaptability. In summary, combining the trust-based evaluation model and hybrid machine learning approaches provides a significant improvement in the detection and protection of IIoT systems; thus, it becomes applicable for real-time deployment in mission-critical systems.

Keywords: IIoT, Intrusion Detection System, Machine Learning, Trust Management, Support Vector Machine, Naïve Bayes.

I. Introduction

Real-time controlling of healthcare, manufacturing, and energy management, aided by smart real-time

decision-making, requires an integrated sensor, communication system, and smart analytics. With the ability to adjust relative to fast-changing environments. The Industrial Internet of Things (IIoT) is among the critical elements in the development of smart and intelligence systems.

IIoT systems must constantly adapt in order to remain operational and competitive in the fast-evolving and IoT systems heterogeneity. IIoT systems have significant advantages, but security remains a challenge. Attacks, such as malicious nodes, data alteration, denial of service (DoS), and insider threats pose significant issues and undermine the system's resiliency and trust [1, 4]. IIoT security systems have a disadvantage due to adapting to the static, pre-defined, and static structures of the network. The systems lack the ability to respond to behavioral changes due to the absence of a network in the IIoT system [6, 7].

The challenges associated with large, smart, and urban systems characterized by rapidly changing, diverse structures, sets the bar for the basic network model for flexibility and reallocation to maintain the systems. Integrated machine learning-enabled trust systems with Intrusion Detection Systems (IDS) serve as an example that enhances security through a positive fortification of the system [2, 8].

Network attacks include all intentional and wrongful operations by users at various network points with the purpose of disturbing the normal functioning of the network and/or destroying the integrity of its information. This paper analyzes a Trust-based Internal Security Framework Internal Security Framework that is meant to recognize and eliminate internal and external attacks by counteracting aggressive attacks. Malicious nodes intentionally degrade the quality of the system by stealing, modifying, or arbitrarily destroying data during transmission. They may employ advanced attacks compromising transmission integrity, such as the man-in-the-middle attack.

A malicious node is any node that, within the network, executes harmful or unauthorized actions. Such nodes aggravate the challenges of the stability, efficiency, and security of the IIoT systems. This makes it imperative to detect and purge such nodes to guarantee stable and secure operation of the network.

II. LITERATURE SURVEY

Alzaylaee et al. (2026) [1] an AI-based threat detection software which integrates computer vision and machine learning to identify threats as they happen. Their method utilizes visual and network data to identify sophisticated attacks and demonstrates an increase in detection accuracy and response speed in comparison to older methods. The study emphasizes an AI-based technique merger to address the ever-growing need for advanced cybersecurity.

Sinha et al. (2026) [2] a machine learning-based framework in the scope of industrial cyber-physical systems and system behavior anomaly detection and cyber threat prevention and detection. The results of their study show a marked improvement in detection and response and a reduction in false positives in industrial systems and environments. Their framework is highly effective in monitoring and preventing cyber threats in real time.

Ang et al. (2026) [3] a multi-layer cybersecurity framework for the banking industry utilizing next-generation firewalls in combination with intruder detection and prevention systems. Their architecture is the combination of a multitude of defense layers for maximal working protection. The study points to a combination of attacking and defending mechanisms as a tool to ensure improving security systems for important infrastructure.

Alsubai et al. (2026) [4] the use of quantum mechanical concepts to improve the transfer learning of edge machine learning in cross-domain cybersecurity threat detection and classification. Their research

is the integration of advanced quantum strategies in the field of cybersecurity. The overall findings of the study indicate major potential in the area of advanced machine learning techniques applied to cybersecurity.

In [5] the year 2026, Olasehinde and his colleagues study the power system's cyber and physical vulnerabilities and threats and append the study with possible control mechanisms to lessen the threats. The study also comprehensively overviews several attack vectors and their effects on the stability of the system. The study states that in the critical system designs, lack of secure design, and the lack of active monitoring, remain the main contributors to the challenges.

In [6] the year 2025, Arora's study shows the impact of artificial intelligence on the field of cybersecurity. The study shows that machine learning models improve response mechanisms, and add automation to the processes. Some of the challenges that the study brings to light include data quality and how much control the user has over the model. The study claims that the impact of AI on most of the processes of cybersecurity is undeniable.

In [7] the 2025 study by Sathyabama and Katiravan, the study proposes that in the 2025 model of cybersecurity, the data sharing will be improved by means of the use of DDN and be secure with the use of DDN & Blockchain. The network will be trustworthy, and transparent due to the blockchain technology. The anomalous data detection and sharing will improved by the DDN's capability. The experiments conducted showed an improvement in the system security and in the detection capability.

In [8] the year 2025, Kandasamy and Roseline develop a model of a hybrid deep learning system that will be able to mitigate attacks that are man-in-the-middle. The model is one that is geared towards enabling a variety of neural architectures so that they can accurately detect attacks. In relation to other attacks, the system is one that has the potential to prove that network attacks can be controlled and that this can be done in a seamless and an efficient manner.

In [9] Rai et al. (2025), researchers examine AI-based intrusion detection systems and their possible applications in securing systems. The authors implement state-of-the-art machine learning models for the identification of anomalous behavior and patterns within network traffic. As a result, the system within the study achieves a higher rate of correct identification of anomalous traffic with a reduction in the number of false positives, demonstrating the value of AI-based intrusion detection systems (IDS) within contemporary network security.

In Malik et al. (2025) [10] an AI-based cybersecurity system utilizing machine learning for sophisticated threat identification and defense. The authors of this paper propose a new paradigm integrated with several algorithms to optimize imprecision in classification and latency in response. The new proposed system is aimed to be proactive against high order and adaptive vulnerabilities. The authors describe a notable improvement of the proposed system even in comparison to the existing state-of-the-art security systems.

III. METHODOLOGY

The proposed architecture depicts an entire machine learning workflow, starting with the collection of a dataset, which then goes through to the initial stage of data preprocessing to remove noise, fill in gaps, and reformat the data into an appropriate form for analysis. After this, the data is split into training and testing sets, where the training portion is used for model construction and learning and the testing portion is reserved for evaluating model performance. The model is then subjected to testing and validation, with feedback used to guide refinements of the model in order to enhance accuracy and build

robustness. A model is deemed the proposed model when it can sustain a satisfactory level of performance. The proposed model is then utilized for prediction or classification in real-time applications. The system analyzes data as it is received or streamed and renders the results as clear, trusted, or untrusted decisions to enable reliable decision making in operational contexts.

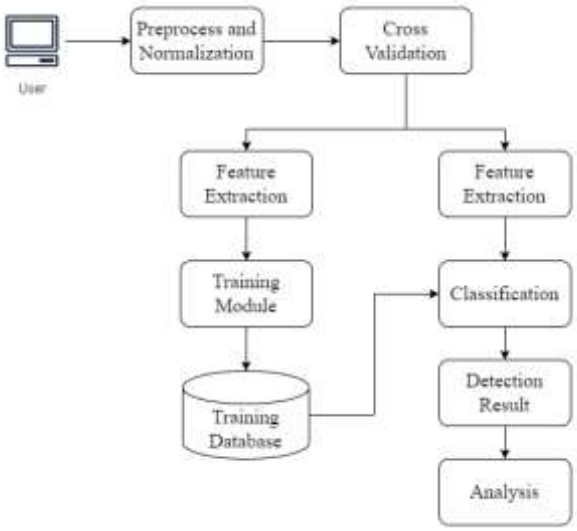

Figure 1: System Architecture

The proposed system outlines a systematic machine learning approach to identifying malicious nodes and assessing trust within the IIoT domain. The approach is described in the following stages:

Dataset: The starting point for any machine learning project is the data collection step. The primary sources of data can include network traffic, sensor data, system logs, or communication logs. These datasets include multiple samples of the nodes' activities within the network. However, model performance can be impacted by the presence of noisy data, redundancy in samples, and missing values; therefore, the data should be carefully examined.

Data Pre-Processing: The primary goal of data preprocessing is to improve the quality and consistency of the data, which is ultimately done by cleaning the raw data and structuring it to match anticipated formats. The specific data preprocessing steps can include:

- Removal of noise and duplicate records
- Addressing missing (or null) values
- Normalization or rescaling of features
- Data labeling to enable supervised learning

Data Splitting (for Training and Testing the Model): The data set is split into two primary categories: training data and testing data. The training data subset is what the machine learning model is fit to. The testing data subset is how model performance is assessed. This separation helps reduce chances of overfitting the model and ensures the model's generalization is evaluated without bias.

Model Training and Testing: During this phase of the procedure, machine learning models are trained on the data, and evaluated on how well they learn patterns and relationships. The system uses classifiers such as Support Vector Machine (SVM), Naive Bayes (NB), and a Hybrid Machine Learning (HML) model based on the combination of Random Forest and AdaBoost. The system predicts and tests on 'unseen' data, i.e. data that has not been previously encountered by the model and is therefore used to

assess the system's predictive capabilities.
Optimization and evaluation allow the selection of the best optimized model as the final model. In the context of this research, the hybrid model has proved most successful, therefore, it is the most fit model for implementation in IIoT ecosystems

Prediction / Classification
The model that has been trained is now ready to process. It is capable of real-time analysis and. By virtue of learned patterns, network nodes are classified as normal or malicious. The end result provides system administrators or automated systems with a classified diagnosis. The classifications are rendered as:

- Trusted Label
- Untrusted Label

Model Evaluation: In evaluating model performance, accuracy, precision, recall and F1-score are used. These indicators allow the effectiveness and dependability of the model to identify malicious activities to be established.

Algorithm 1: Trust-Based Hybrid ML-Based IDS for IoT
Input: Raw dataset D (network traffic / sensor data / logs)
Output: Classification label (Trusted / Untrusted / Malicious)
Step 1: Data Collection:
Acquire raw dataset D from IIoT environment

Step 2: Data Preprocessing:
For each record r in D do
If r is duplicate OR noisy then
Remove r
End If
If r has missing values then
Replace missing values using mean/mode/forward fill
End If
End For
Normalize feature values in D
Encode labels (Normal = 0, Attack = 1)
D_clean ← processed dataset

Step 3: Dataset Splitting:
Split D_clean into:
Training set D_train (80%)
Testing set D_test (20%)

Step 4: Trust Computation:
For each node n in network do
Compute:

CommunicationScore(n)
CollaborationScore(n)
ControlScore(n)

Trust(n) = w1 * CommunicationScore
+ w2 * CollaborationScore
+ w3 * ControlScore

If Trust(n) < Trust_threshold then
Mark n as Untrusted
Else
Mark n as Trusted
End If
End For

Step 5: Model Training:
Train the following models using D_train:
M1 ← Support Vector Machine (SVM)
M2 ← Naïve Bayes (NB)
M3 ← Hybrid Model (Random Forest + AdaBoost)

Step 6: Testing and Prediction:
For each sample x in D_test do

If Trust(x.node) < Trust_threshold then
Label(x) ← "Malicious"
Continue to next sample
End If

y1 ← M1.predict(x)
y2 ← M2.predict(x)
y3 ← M3.predict(x)

Final_Prediction(x) ← MajorityVote(y1, y2, y3)

If Final_Prediction(x) == Attack then
Label(x) ← "Untrusted"
Else
Label(x) ← "Trusted"
End If

End For

Step 7:. Model Evaluation:
Compute:
Accuracy
Precision
Recall
F1-Score

End.

IV. RESULTS

The Trust-Based Hybrid Machine Learning model for Anomaly Detection for Industrial Internet of Things (IIoT) was tested against simulated datasets and actual traffic data within IoT networks. The evaluation of system performance was done using standard classification metrics of Accuracy, Precision, Recall, and F1-score. The research involved the comparison of three machine learning techniques—Support Vector Machine (SVM), Naïve Bayes (NB), and the developed hybrid model of machine learning (HML), which is based on Random Forest and AdaBoost.

Table 1: Performance Comparison of Models.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Naïve Bayes	96.13	96.40	96.13	96.26
SVM	93.20	96.52	94.81	95.00
HML (Proposed)	98.20	96.43	98.20	97.31

Table 1 the Naïve Bayes model achieved 96.13% accuracy with 96.40% precision, 96.13% recall, and 96.26% F1-score. This demonstrates consistent performance in probabilistic classification. The Support Vector Machine (SVM) model achieved 93.20% accuracy with 96.52% precision, 94.81% recall, and an F1-score just below 95%. This reflects strong classification ability, although it has slightly lower accuracy than Naïve Bayes. The proposed Hybrid Machine Learning (HML) model, in comparison, demonstrates marked improvement over all other models. HML model achieved 98.20% accuracy with 98.20% recall and 97.31% F1-score with 96.43% precision. This notable improvement in performance validates the combination of ensemble learning (Random Forest and AdaBoost) and trust-based decision mechanism as an effective strategy for improving the accuracy of intrusion detection.

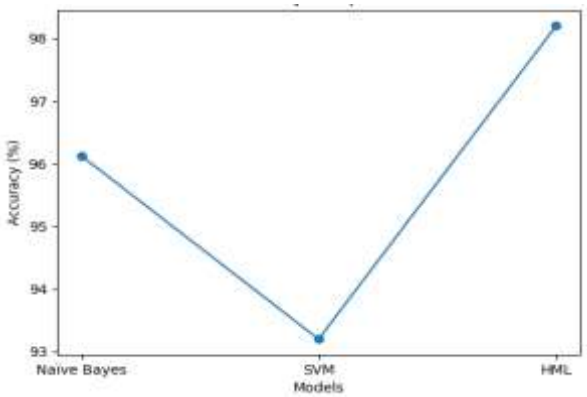

Figure 2: Accuracy Comparison of Models

Figure 2 shows accuracy results for the three classification models Naïve Bayes, Support Vector Machine (SVM) and the proposed Hybrid Machine Learning (HML) model. The HML model achieved an accuracy of 98.20%, which is an improvement over Naïve Bayes (96.13%) and SVM (93.20%). This suggests that the hybrid method, as a result of combining different learning approaches, improves the accuracy of classification and, consequently, the predictive power.

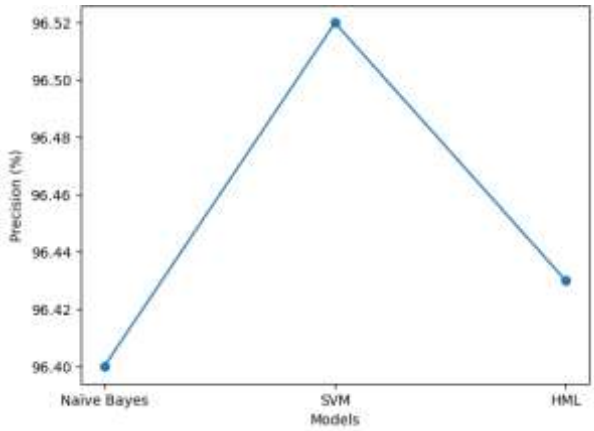

Figure 3: Precision Comparison of Models

Figure 3 shows the precision statistics for the models. SVM attained the highest precision (96.52%) and is closely followed by the HML model (96.43%) and Naïve Bayes (96.40%). While there seems to be little difference in the results, it is clear that all models have high precision and, thus, a low rate of false positives. The HML model shows that precision is competitive and that all other performance metrics are improvements.

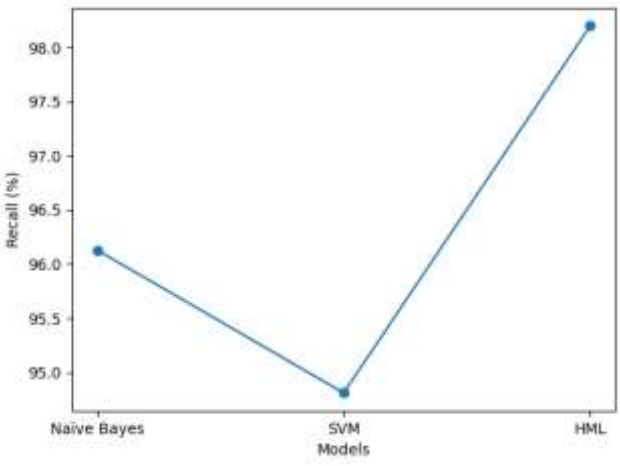

Figure 4: Recall Comparison of Models

Figure 4 provides a comparison of recall metrics across different models. It can be seen that the proposed HML model outperforms all other models with a recall of 98.20%, a significant improvement when compared to the recall of Naïve Bayes (96.13%) and SVM (94.81%). It can be concluded that the HML model is particularly adept at identifying positive instances in the data and minimizing false negatives—a critical requirement in the intrusion detection domain.

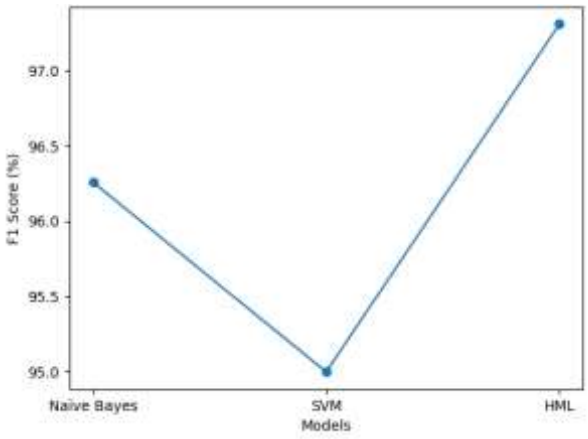

Figure 5: F1-Score Comparison of Models

Figure 5 presents a comparison of F1-score, which is a function of precision and recall. The model HML obtained the highest F1-score of 97.31%, beyond Naïve Bayes (96.26%) and SVM (about 95%). This shows HML provides the best balance between precision and recall and attests to the model's strength and trustworthiness in classification tasks.

V. CONCLUSION

The study is of Trust-Based Hybrid Machine Learning Intrusion Detection Systems (IDS) aiming to protect cyber threats upon the Industrial Internet of Things (IIoT) environments. The framework design integrates trust evaluation and Machine Learning (ML) mechanisms to improve detection and classification of dynamic heterogeneous IIoT networks. The proposed system differs from traditional IDS systems that utilize static signatures and rule-based detection systems as it provides adaptive intelligence via hybrid ML of Support Vector Machine (SVM), Naïve Bayes (NB), and Random Forest and AdaBoost. The use of a trust computation models of Communication, Collaboration and Control (C3) Trust Framework, highlighted the gap of removing trusted nodes of users, thus, it filtered out null/unreliable nodes, preceding classification. The system's dual-layer approach improves detection accuracy and strengthens system reliability within a real-time operational environment. The experimental results showed the proposed system achieved 8.2% higher accuracy as compared to other methods. Additionally, precision, recall, and F1 score computations performed consistently, reflecting the capability of trusted adaptive, analytical systems improving intrusion detection. The system improves the security of IIoT structures and is adaptive and scalable. It is, best, suited for environments with real-time detection, trusted analytical systems, as the systems are secure and rapidly respond to threats. Systems may, also, be applied to Smart Manufacturing, Industrial Automation, and Advanced Healthcare Systems IIoT environments. Future design may consider the deployment of anti-viruses to safeguard systems and real-time deployed system security.

REFERENCES

1. Alzaylaee, Mohammed K., et al. "Advancing Cybersecurity: AI-Driven Computer Vision and Machine Learning Models for Real-Time Threat Detection and Prevention." Journal of Engineering Research (2026).
2. Sinha, Anurag, et al. "A Machine Learning Framework for Detecting and Preventing Cyber-Attacks in Industrial Cyber-Physical Systems." Engineering Reports 8.1 (2026): e70520.

3. Ang, Sokroeurn, et al. "A Multi-Layered Adaptive Cybersecurity Framework for the Banking Sector Integrating Next-Gen Firewalls with AI-Driven IDPS." STAP Journal of Security Risk Management 2026.1 (2026): 67-76.
4. Alsubai, Shtwai, et al. "Quantum transfer learning for cross-domain cybersecurity threat detection and categorization." Scientific Reports (2026).
5. Olasehinde, Daniel O., et al. "Cybersecurity in cyber-physical power systems: analyzing vulnerabilities, threats, and control structures." Cluster Computing 29.3 (2026): 133.
6. Arora, Anuj. "Transforming cybersecurity threat detection and prevention systems using artificial intelligence." Available at SSRN 5268166 (2025).
7. AR, Sathyabama, and Jeevaa Katiravan. "Enhancing anomaly detection and prevention in Internet of Things (IoT) using deep neural networks and blockchain based cyber security." Scientific Reports 15.1 (2025): 22369.
8. Kandasamy, V., and A. Ameelia Roseline. "Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks." Scientific Reports 15.1 (2025): 1697.
9. Rai, Hari Mohan, et al. "Advanced AI-powered intrusion detection systems in cybersecurity protocols for network protection." Procedia Computer Science 259 (2025): 140-149.
10. Malik, Anum, et al. "Artificial intelligence-driven cybersecurity framework using machine learning for advanced threat detection and prevention." Sch. J. Eng. Tech 6 (2025): 401-423.