International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(15s) 2026 pp. 394-407
https://doi.org/10.70917/ijcisim-2026-4423
Article

An Intelligent Cloud-Based IoT Framework Integrating Artificial Intelligence, Machine Learning, Computer Vision, Big Data Analytics, and Cybersecurity for Smart Industrial Management Applications

Alok Kumar Bhargava[1]*, Eyed Mahdi Al Qarni[2], Sneha C A[3], Naresh Konduri[4], R.Z Inamul Hussain[5], Arpan[6]

[1*]TrayiVani Foundation, India; Developer, The Inner Engine Framework™ for Conscious Leadership Assessment; Author of TrayiVāṇī – Eternal Verses on Peace, Silence & Discernment and The Inner Engine of Leadership Trilogy; TrayiVani Foundation, Ghaziabad – 201016, Uttar Pradesh, India.
E-mail: founder@trayivani.in , Orcid Id: 0009-0009-1805-3075,
Google Scholar: https://scholar.google.com/citations?hl=en&user=XRzNh50AAAAJ
[2]Department of Security Affairs, Ministry of Interior, Saudi Arabia,
Specialization in Information Systems (Information Assurance and Cybersecurity Management)
E-mail Id:mr.ayed94@gmail.com, Orcid Id: 0009-0006-6255-8343
[3]Department of Electronics and Telecommunication, Rungta International Skills University, Bhilai, Chhattisgarh, Pincode-490023, E-mail: dimpi.ca@gmail.com ,Orcid Id: 0009-0009-4425-1534
[4]Department of CSE (IoT & CS including Block Chain Technology), Specialization in Computer Science and Engineering, Sasi Institute of Technology & Engineering (Autonomous), Tadepalligudem, Andhra Pradesh, India
Directorate of Research & Development, Jawaharlal Nehru Technological University Kakinada (JNTUK)
E-mail Id: naresh.konduri@gmail.com, Orcid Id: 0009-0000-1363-8773
[5]Department of Computer science and Engineering, C. Abdul Hakeem College of Engineering and Technology, Melvisharam, Tamil Nadu, Pincode: 632509, E-mail Id:inamulhasan.rz@gmail.com, Orcid Id:0009-0000-3574-8818
[6]Parul Institute of Engineering and Technology - Diploma Studies, Parul University
E-mail Id: arpan.singh40452@paruluniversity.ac.in, Orcid Id: 0009-0000-2860-6475

Abstract: Smart industrial management requires integrated systems that can monitor machine conditions, detect cyber threats, inspect product quality, and support operational decision-making. However, many existing Industrial IoT systems handle these functions separately, which limits coordinated industrial control and decision support. This study aimed to design and simulate a cloud-oriented Industrial IoT framework integrating machine learning, cybersecurity analytics, computer vision, big data-style preprocessing, and decision fusion for smart industrial management applications. The proposed framework used three data sources: a smart manufacturing dataset, an Industrial IoT network cybersecurity dataset, and a casting image dataset. Machine learning models were developed for machine condition prediction, cybersecurity models were used for binary intrusion detection and multi-class cyberattack classification, and a convolutional neural network was implemented for casting defect detection. The outputs of these modules were combined using a rule-based decision fusion engine to generate risk levels, alerts, decisions, and recommended actions. The results showed that Gradient Boosting achieved the best smart manufacturing performance with a weighted F1-score of 98.73%. The cybersecurity module achieved 99.71% weighted F1-score for binary intrusion detection and 90.62% weighted F1-score for multi-class cyberattack classification. The CNN model achieved 83.08% validation accuracy for casting defect detection. Overall, the proposed framework demonstrates the potential to support predictive maintenance, cyberattack detection, automated quality inspection, and simulated industrial decision support through an integrated Industrial IoT analytics workflow.
Keywords: Industrial IoT, Artificial Intelligence, Machine Learning, Cybersecurity, Computer Vision

1. Introduction

The rapid advancement of Industry 4.0 has transformed traditional industrial environments into intelligent, connected, and data-driven systems. The Internet of Things (IoT) devices, cloud computing, artificial intelligence (AI), machine learning (ML), computer vision, big data analytics, and cybersecurity mechanisms are becoming more vital to modern industries to enhance productivity, reliability, and operation safety. Cloud computing and IoT can be used to connect to the industrial data, which allows for the real-time monitoring of machines, production systems, and network activities, all of which can be stored on a massive scale and accessed remotely [1]. In the context of smart manufacturing, huge amounts of data are collected from industrial sensors, machines, controllers, cameras, communication networks, etc. The ability to use big data analytics to extract useful information from these complex datasets and to aid intelligent decision making is important [2].

This is why machine learning is becoming an important tool in the analysis of IoT data, as it can discover hidden patterns, predict the behavior of a system, and help with the automation of classification tasks [3]. Data analytics can be used to process high volume, high velocity and heterogeneous data from connected devices and production systems in Industrial IoT environments [4]. Moreover, predictive, classification, anomaly detection, and intelligent automation are the key areas where machine learning and data analytics are extensively adopted in IoT applications [5]. These techniques are especially beneficial for smart manufacturing applications like predictive maintenance, machine condition monitoring, production optimization, and quality inspection.

AI also offers significant assistance in smart manufacturing, with capabilities like automated reasoning, fault diagnosis, process control, and intelligent decision-making [6]. But the more industrial systems are interconnected, the more they are susceptible to cyberattacks. Denial of service, unauthorized access, data manipulation, ransomware and intrusion are some of the potential threats to IIoT networks. Hence, cybersecurity should be regarded as an integral part of the smart industrial management framework. In the context of smart manufacturing, using machine learning in conjunction with sophisticated security measures can enhance access control, threat detection, and system resilience in secured Industrial IoT architectures [7].

Even with these advances, there are still many industrial systems that perform machine monitoring, detect cyberattacks, conduct visual inspection and make decisions on the same machine as distinct tasks. This results in an uncoordinated industrial management and the impossibility of making a coherent decision from an operational point of view. To fill this void, the present study introduces a cloud-based Industrial IoT framework for smart industrial management applications, which consists of machine learning, cybersecurity analytics, computer vision, big data style pre-processing and decision fusion.

The goals of this study are: to design a cloud-based Industrial IoT framework for smart industrial monitoring and management; to develop modules based on machine learning and cyber security for machine condition prediction, intrusion detection and classification of cyber-attacks; to implement a module for casting defect detection by computer vision for industrial quality inspection; and to fuse the results of the machine learning, cyber security and computer vision modules by a rule based decision fusion engine for supporting industrial decision making under simulated conditions.

2. Literature Review

Industrial Internet of Things (IIoT) is one of the most important pillars of smart manufacturing, as it brings industrial machines, sensors, controllers, production systems and cloud platforms together into a single digital space. With this connectivity, industries are able to track the production process, gather operational data, and enhance automation. In the field of smart industrial automation, machine learning-powered IoT systems have been extensively used for connected manufacturing environments, such as intelligent prediction, process monitoring, fault detection, and decision making [8].

The use of artificial intelligence in manufacturing is on the rise to enhance production reliability and manufacturing quality. AI-powered quality inspection systems can identify defects, minimizing human inspection mistakes, and ensuring product uniformity. These systems can be applied in smart manufacturing for automated visual inspection, surface defect detection and production quality control [9]. There are also recent reviews of machine learning and IoT based industrial applications that demonstrate that ML models can be applied in predictive maintenance, process optimization, machine monitoring, anomaly detection and industrial automation. There are still issues of data quality, deployment, generalization of models and integration with the existing industrial infrastructure [10].

Artificial Intelligence of Things (AIoT) has paved the way for AI systems in the industrial setting. The Industrial AIoT is the integration of IoT connectivity with AI-based analytics, which enables the smart sensing, autonomous control, predictive maintenance and intelligent production planning. But industrial AIoT has its scalability, interoperability, latency, data privacy, cybersecurity and computational resource management issues [11]. In cloud-based and edge-driven industrial systems, where vast amounts of operational and security data need to be efficiently processed, these challenges are particularly relevant.

Industrial IoT poses a challenge for cybersecurity because connected machines and networked control systems are subject to attacks like DoS, DDoS, ransomware, injection, password attacks, scanning and man-in-the-middle attacks. While integrating with edge computing can enhance responsiveness and decrease latency, it can also create new security concerns. Thus, cybersecurity solutions for IIoT-edge environments must be able to detect threats, protect communication, control access, and be designed to be resilient [12].

Another crucial aspect of smart industrial management is computer vision. The visual defect detection methods are widely used in industrial inspection, which can detect the defect of the surface, casting error, structural irregularity, and defect of the product quality, more consistently than the manual inspection [13]. Furthermore, machine vision systems can be used to enhance the understanding of manufacturing events, if combined with other industrial data sources, enabling the visual inspection results to be used to inform other production decisions [14]. Overall, the previous studies indicate that there is good progress in the areas of IoT based automation, AI based quality inspection, industrial AIoT, cyber security and computer vision. But most of the studies are related to specific tasks instead of an integrated workflow of industrial management. Hence, there is a need for an industrial IoT system that is cloud-based, incorporates machine learning, cyber security analytics, computer vision, preprocessing, and rule-based decision fusion for smart industrial management.

3. Methodology

The study employed an experimental method to design and simulate a cloud-based Industrial IoT framework for smart industrial management using Python programming language. The framework combines the use of sensor analytics, machine learning, cyber security detection, computer vision, preprocessing and decision fusion. While the implementation was local, the workflow was designed to simulate the process of acquiring data from the Internet of Things, storing it in the cloud, preprocessing it, performing intelligent analysis, fusing decisions and monitoring the results in a dashboard.

3.1 Framework Design

The proposed framework was based on a layering approach of Industrial IoT. The first layer was IoT data sources like machine sensors, network sensors and computer vision cameras. These were the sources of smart manufacturing data, network traffic data and casting image data. The second layer was cloud based storage of raw data, processed data, trained models and dashboard outputs. The third layer preprocessed and engineered features. The fourth layer consisted of layers of machine learning, cybersecurity and computer vision. The last layer utilized decision fusion to produce maintenance, cyber security, quality inspection, and production suggestions.

3.2 Dataset Selection and Loading

Three sets of data were employed. Machine condition prediction and production status classification were performed using the smart manufacturing data set [15]. Two binary intrusion detection and multi-class attack classification tasks on the network cybersecurity dataset were performed [16]. Defective and non-defective casting image classification was done using the casting image data set [17]. The datasets were loaded in Python from local and runtime path. Data shape, column names, missing values, duplicate rows, sample data, class distribution and some basic visualizations were included in the initial analysis.

3.3 Data Preprocessing

Structured datasets were processed using a reusable pipeline. Numerical features were imputed with median and scaled to a standard scale. Most frequent imputation and one hot encoding were used for categorical features. The steps were merged together with a ColumnTransformer. The experiment was made more realistic by adding "controlled" noise. To emulate variations in the sensors and networks, Gaussian noise was added to the numerical features. Noise was only introduced in training labels, but not in test labels, so as to make an unbiased evaluation.

3.4 Machine Learning and Cybersecurity Modules

For smart manufacturing, Target_Class was used as the target variable. Data was stratified to get 80% training and 20% testing. Logistic Regression, Random Forest and Gradient Boosting were trained and compared. Weighted F1-score was used for the selection of the best model. Permutation importance was also used to analyse feature importance. In the case of cybersecurity, the label column was used to classify the binary normal/attack and the type column was used for multi-class attack classification. For both tasks a Random Forest (RF) classifier with balanced class weight was trained. Unsupervised anomaly detection was also performed by using the Isolation Forest.

3.5 Computer Vision Module

The image dataset was extracted from the casting and the image files were recursively identified from the extracted folders. This complete extracted data set comprised 8648 images of two classes: defective casting images (def_front) and non-defective casting images (ok_front). The experiment was performed with the subset of discovered images (1,300 images) which had organized class folders for def_front and ok_front for CNN training. A CNN model was developed using TensorFlow/Keras to classify casting defect into two categories: good and bad. The images were resized to 128 × 128 pixels, and split into training and validation sets with 80:20 ratio, which gives 1,040 training images and 260 validation images. To enhance the efficiency of training and generalization of the model, data augmentation, caching, shuffling and prefetching were implemented. CNN consisted of convolutional layers, max-pooling layers, flattening layer, dense layers, dropout regularization layers and softmax output layer for class prediction.

3.6 Model Evaluation and Decision Fusion

The accuracy, weighted precision, weighted recall, weighted F1-score, classification report and confusion matrix were used to evaluate structured models. The training and validation accuracy and loss curves were used to assess the CNN. The decision fusion engine merged the results of the machine learning, cybersecurity and computer vision modules. The most critical threats were cybersecurity, critical machine failure and casting defects. The system provided risk levels, alerts, decisions and recommended actions for industrial management.

3.7 Ethical Considerations

The framework considered data privacy, access control, anonymization, transparency, and human review of critical decisions. Human-in-the-loop validation was included to improve accountability and safety in industrial operations.

4. Results

This section introduces the experimental results from the proposed Industrial IoT framework. The results are presented in six sections: smart manufacturing prediction, cybersecurity classification, anomaly detection, computer vision defect detection, decision fusion, and dashboard simulation.

4.1 Smart Manufacturing Prediction Results

The smart manufacturing data set had 14 columns and 10,000 rows. Target_Class was used as the target variable. The dataset was imbalanced, with Quality_Degraded having the maximum number of records, and Energy_Inefficient having the minimum number of records. The distribution of the target classes is shown in Table 1.

Table 1. Target class distribution of the smart manufacturing dataset

Target class	**Number of records**
Quality_Degraded	3,599
High_Downtime	2,650
Optimal_Operation	2,414
Critical_Failure	1,317
Energy_Inefficient	20
Total	**10,000**

The data set was split into 80% training data and 20% test data in an 80:20 ratio, with a stratified split. In order to simulate realistic industrial conditions, the feature values were corrupted by numerical sensor noise and 240 training labels were corrupted, resulting in a 3% label noise rate. Three models were trained and compared: Logistic Regression, Random Forest and Gradient Boosting. They are presented in Table 2.

Table 2. Performance comparison of smart manufacturing models

Model	Accuracy	Precision	Recall	F1-score
Logistic Regression	0.7935	0.9106	0.7935	0.8456
Random Forest	0.9865	0.9846	0.9865	0.9855
Gradient Boosting	0.9865	0.9887	0.9865	0.9873

The model with the best weighted F1-score was Gradient Boosting, which was chosen as the optimal smart manufacturing model. Random Forest also had a good performance and Logistic Regression had a lower accuracy and recall. This means that ensemble models performed better than the linear baseline model in the machine condition prediction. Figure 1 displays the classification performance of the Gradient Boosting model selected.

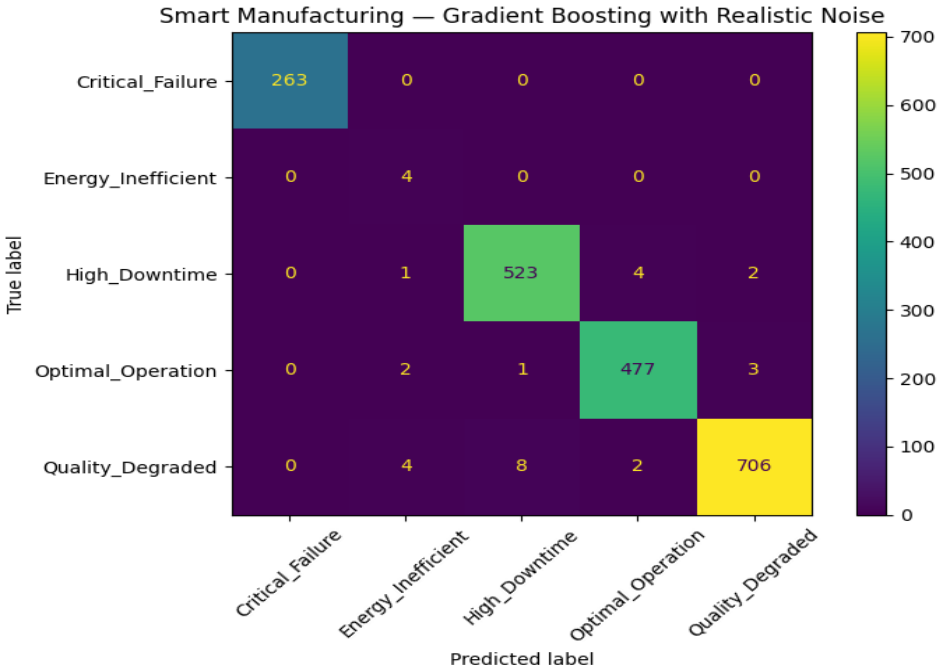

Figure 1. Smart Manufacturing — Gradient Boosting with Realistic Noise.

As shown in Figure 1, the Gradient Boosting model successfully classified most of the machine operating conditions. The model was good for Critical_Failure, High_Downtime, Optimal_Operation and Quality_Degraded. The Energy_Inefficient class, however, only had 20 records, which meant that the class-level evaluation was limited. The most influential smart manufacturing features are shown in Figure 2.

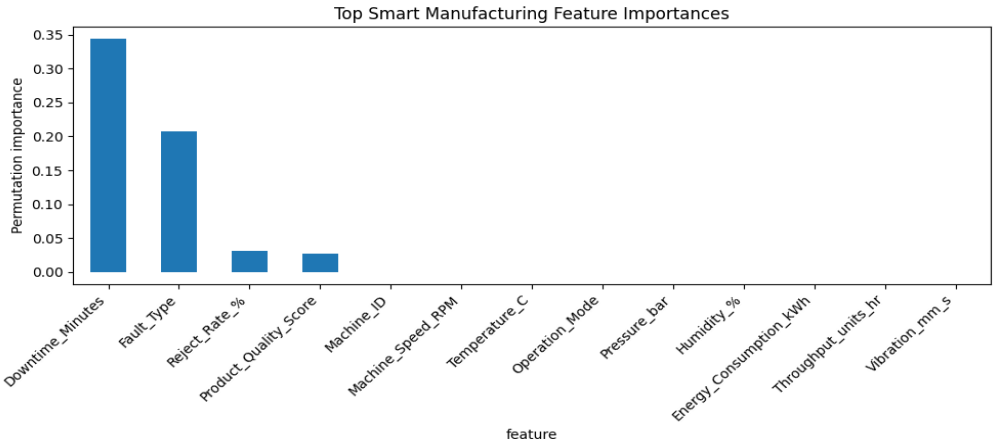

Figure 2. Top Smart Manufacturing Feature Importances.

As illustrated in Figure 2, variables like the downtime, fault type, reject rate, and product quality indicators were significant factors in machine condition classification. The results are in line with the use of the smart manufacturing module for predictive maintenance and production monitoring.

4.2 Industrial IoT Cybersecurity Classification Results

The Industrial IoT cybersecurity dataset had 211,043 records and 44 columns. It contained network-level attributes like source and destination IP information, ports, protocol, service, packet statistics, DNS attributes, HTTP attributes, SSL attributes, and cybersecurity labels. There were also 20,569 duplicate rows in the data set. For efficient execution, a representative sample of 60,000 records was used for model training and testing. The label column was used to train the Random Forest classifer for the binary intrusion detection problem. The model categorised the flow of network traffic into normal or attack. The results are shown in Table 3.

Table 3. Binary intrusion detection performance

Task	**Accuracy**	**Precisio n**	**Recall**	**F1-score**
Binary intrusion detection	0.9971	0.9971	0.9971	0.9971

The binary intrusion detection model got 99.71% accuracy and 99.71% weighted F1 score. This indicates that the model performed very well in differentiating between normal traffic and attack traffic. The binary intrusion detection confusion matrix is presented in Figure 3.

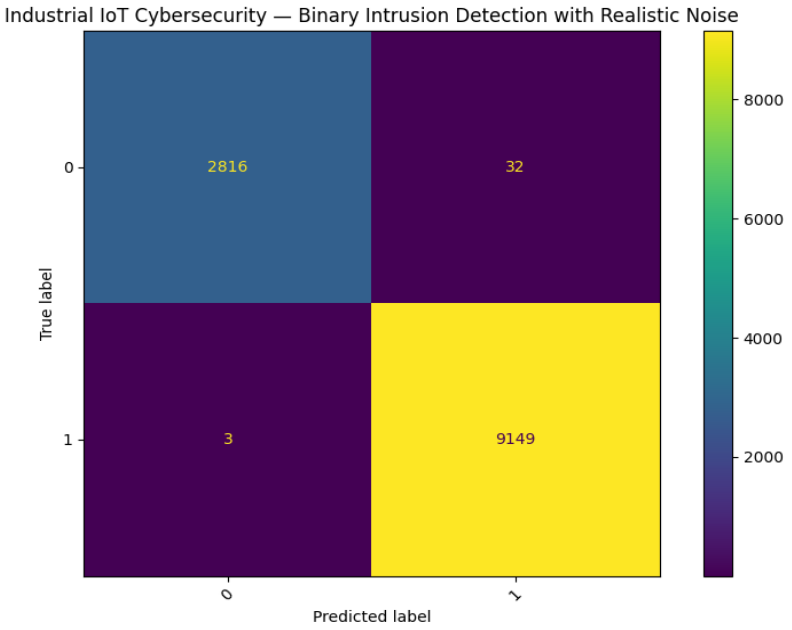

Figure 3. Industrial IoT Cybersecurity — Binary Intrusion Detection with Realistic Noise.

The binary model also resulted in very few misclassifications between normal and attack traffic, as is confirmed by Figure 3. This finding is in line with the appropriateness of the cybersecurity module for intrusion detection. Multi-class attack classification was also performed using the same cybersecurity dataset. Normal traffic and various attack categories such as backdoor, DDoS, DoS, injection, man-in-the-middle, password attack, ransomware, scanning, and XSS were classified using the type column. The overall performance is shown in Table 4.

Table 4. Multi-class cyberattack classification performance

Task	**Accuracy**	**Precision**	**Recall**	**F1-score**
Multi-class cyberattack classification	0.9058	0.9211	0.9058	0.9062

The multi-class model obtained an accuracy of 90.58% and an F1 score of 90.62% (weighted). Several classes, such as normal traffic, backdoor, ransomware, scanning, XSS, DDoS, and DoS, achieved good results. Injection, password attack and man-in-the-middle classes were found to have lower performance. The multi-class cyberattack classification confusion matrix is displayed in Figure 4.

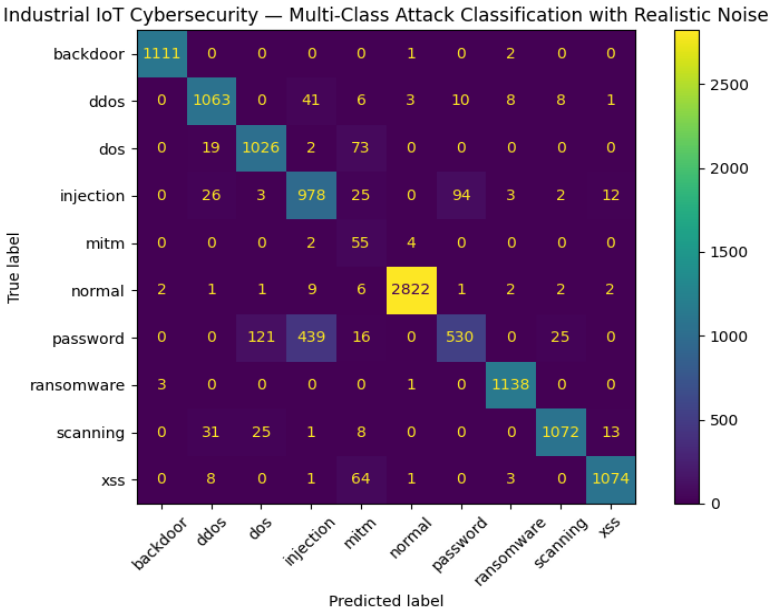

Figure 4. Industrial IoT Cybersecurity — Multi-Class Attack Classification with Realistic Noise.

Figure 4 shows that most attack categories were correctly classified, although some confusion occurred among more difficult attack classes. This means that the model is able to classify attacks, but there are still improvements to be made for each class.

4.3 Unsupervised Network Anomaly Detection Results

Isolation Forest was added as an extra unsupervised cybersecurity layer. Numerical network features were used in the model and the contamination rate was set to 5%. The anomaly detection output is given in Table 5.

Table 5. Isolation Forest anomaly detection results

Anomaly category	**Count**
Normal-like	57,000
Anomaly	3,000
Total	**60,000**

The Isolation Forest model has detected 3,000 abnormal records and 57,000 normal-like records. As the contamination rate was set as 5%, the number of anomalies was also 5% of the sampled data set. Hence this result should be treated as an extra layer of monitoring, not as a complete attack detection result.

4.4 Computer Vision-Based Casting Defect Detection Results

The computer vision data was employed in casting defect detection. It had two image classes: defective casting images and non-defective casting images. Table 6 displays the class of students.

Table 6. Casting image class distribution

Image class	**Count**
Defective casting image (def_front)	4,992
Non-defective casting image (ok_front)	3,656
Total	**8,648**

The entire image set was 8,648 images, but the CNN experiment was limited to the subset of 1,300 images that were organized into folders of def_front and ok_front. To train the model, representative casting images of the def_front class were displayed prior to the training, as illustrated in Figure 5.

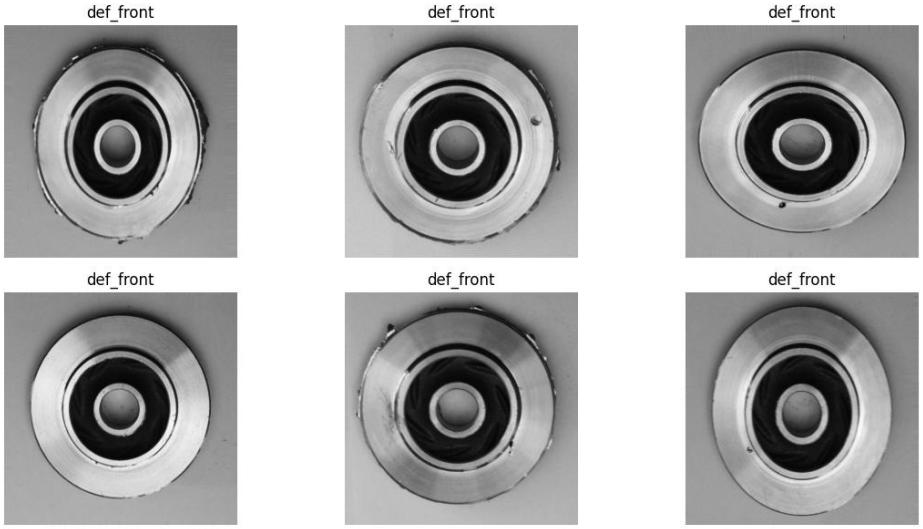

Figure 5. Sample Casting Images.

Sample defective casting images used for the purpose of demonstrating the visual inspection problem addressed by the computer vision module are shown in figure 5. The CNN model was supposed to learn the surface level casting defects shown in these samples. The 1300 images were split into 1040 training images and 260 validation images in an 80:20 ratio. The CNN model had 3,304,898 trainable parameters and was trained for 8 epochs. Table 7 displays the last CNN performance.

Table 7. CNN casting defect detection results

Metric	Value
Training images	1,040
Validation images	260
Trainable parameters	3,304,898
Epochs	8
Final training accuracy	0.7865
Final training loss	0.4296
Final validation accuracy	0.8308
Final validation loss	0.3796

The CNN model accuracy across training epochs is shown in Figure 6.

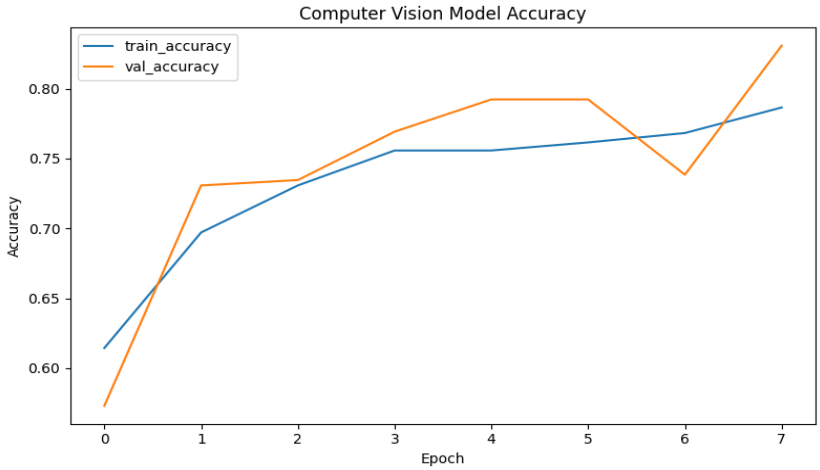

Figure 6. Computer Vision Model Accuracy.

The accuracy of the validation set increased with the training and finally reached 83.08% accuracy in the last epoch (see figure 6). This means that CNN was able to learn useful image features for distinction of casting images with defects and without defects. The CNN loss curve is shown in Figure 7.

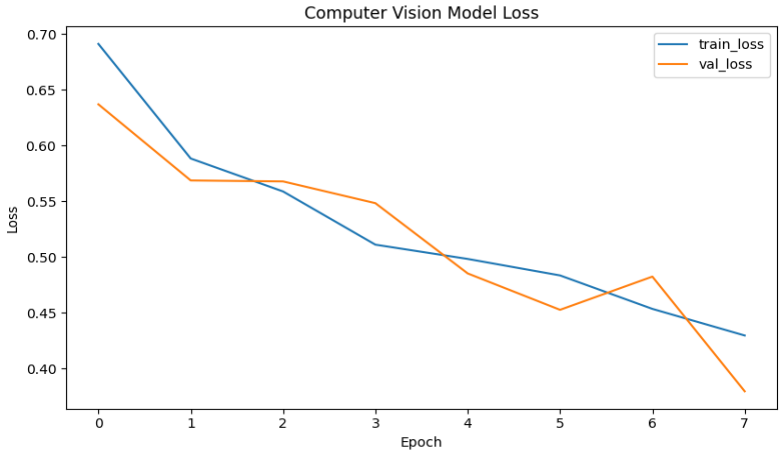

Figure 7. Computer Vision Model Loss.

The loss values for training and validation are plotted against the epochs in Figure 7. The final validation loss was 0.3796 and the final training loss was 0.4296. The results demonstrate reasonable learning behavior, but the model might be improved with the use of the entire image dataset, transfer learning and more hyperparameter tuning.

4.5 Decision Fusion Results

The decision fusion engine combined the outputs of the smart manufacturing, cybersecurity, and computer vision modules. The most critical threats to cybersecurity, critical machine failure, and visual defects were ranked first, second, and third, respectively. This prioritization allowed cyberattacks to be considered as critical risks as they could break the whole Industrial IoT system. There are example cases of decisions that are fused in the table 8.

Table 8. Decision fusion example cases

Machine prediction	**Cyber prediction**	**Vision prediction**	**Risk level**	**Alert type**
Optimal_Operation	normal	ok_front	Low	Normal Operation

Quality_Degraded	normal	def_front	High	Quality Inspection Alert
High_Downtime	normal	ok_front	Medium	Maintenance Alert
Critical_Failure	normal	ok_front	Critical	Machine Failure Alert
Optimal_Operation	ddos	ok_front	Critical	Cybersecurity Warning
Critical_Failure	ransomware	def_front	Critical	Cybersecurity Warning

The combinations of module outputs, and the resulting risk levels and alert types are presented in Table 8. Even if the machine and vision conditions were not the primary cause, Cybersecurity attacks like ddos and ransomware generated Critical risk levels. One machine sensor record, one network record and one image prediction were then used in a single integrated event simulation. The results obtained are presented in Table 9.

Table 9. Final integrated decision for one simulated Industrial IoT event

Input/output	**Result**
Machine prediction	High_Downtime
Cybersecurity prediction	dos
Vision prediction	ok_front
Final risk level	Critical
Alert type	Cybersecurity Warning
Decision	Investigate IoT network traffic and isolate suspicious devices
Recommended action	Trigger security incident response, block malicious traffic, and verify device integrity

The smart manufacturing model predicted High_Downtime, the cybersecurity model predicted dos and vision module predicted ok_front as shown in Table 9. The final risk level was determined to be Critical, as a DoS attack was detected. This validates the fusion engine's emphasis on cybersecurity risk and its ability to produce a common industrial management decision.

4.6 Dashboard Simulation Results

A dashboard-style output was generated for ten simulated Industrial IoT events. For each event, machine prediction, cybersecurity prediction, vision prediction, risk level, alert type, decision and recommended action were given. The complete dashboard output included detailed event level predictions, and Table 10 provides a summary of the final risk-level distribution.

Table 10. Dashboard simulation risk-level distribution

Risk level	**Number of events**
Critical	8
Medium	1
Low	1
Total	10

Table 10 indicates that the eight out of ten simulated events were identified as Critical and one event was identified as Medium and one event was identified as Low. The majority of Critical events were related to cybersecurity predictions like DoS, password attack, injection, scanning and DDoS. This validates the decision fusion engine's highest prioritization of cybersecurity threats. The Medium-risk event was correlated with high machine downtime with normal machine conditions, whereas the Low-risk event was correlated with the normal machine conditions, normal network traffic, and no visual defect. The overall dashboard simulation illustrates the feasibility of the proposed framework to translate individual machine learning, cybersecurity and computer vision predictions into actionable alerts, decisions and recommended actions for smart industrial management.

5. Discussion

Results of this study show that the proposed cloud-based framework for Industrial IoT can support the integration of machine learning, cybersecurity analytics, computer vision, big data-style preprocessing, and decision fusion for smart industrial management. The framework was able to integrate three data sources and translate outputs of the models into actual industrial decisions. This enables the adoption of AI-powered workflows that enable predictive maintenance, cyber attack detection, quality inspection, and operational decision making.

The classification performance was high in the smart manufacturing module with the best weighted F1 score being obtained by Gradient Boosting. This suggests that ensemble learning methods were more effective than Logistic Regression in the capture of the nonlinear relationships between machine conditions, sensor readings, production indicators and fault-related variables. The same is true of AI-powered industrial intelligence in Industry 4.0, which is employed to assist predictive maintenance, process optimization, and analytics, as well as digital twins and intelligent automation [18]. The number of samples in that class, however, was very low (Energy_Inefficient) so that a reliable class-level evaluation was not possible.

The preprocessing strategy also helped to improve model stability. Heterogeneous industrial data were prepared for machine learning using numerical imputation, scaling, categorical encoding, and controlled noise simulation. Data pre-processing is useful in enhancing the robustness of the system under realistic operating conditions, because all the data generated by Industrial IoT systems come from machines, sensors, cameras and network devices. AI and big data analytics has been recognized as one of the key enablers for Industry 4.0 applications, particularly for automation and data-driven decision making [19]. In this study, however, the preprocessing was done locally and should be taken as big data style preprocessing and not as a full distributed big data deployment.

The cybersecurity module exhibited extremely high performance in binary intrusion detection and high performance in multi-class cyberattack classification. The results show the promise of machine learning based intrusion detection for protecting connected industrial systems. Some attack categories were more challenging to categorize, however, including injection, password attack and man-in-the-middle. Furthermore, the cybersecurity dataset had duplicate rows, which can impact the evaluation of the model if there are any duplicates in the training and testing sets. Thus, future work should involve duplicate removal, better class balancing and validation of the cyber security for cloud-fog-edge [20].

The computer vision module demonstrated good performance in the casting defect detection. The CNN was validated with 83.08% accuracy, demonstrating the potential of deep learning in automated visual quality inspection. The CNN experiment used a subset of 1,300 images, however, the full extracted image dataset was 8,648 images. Thus, the outcome is to be considered as a subset experiment. Future improvements can be made by using the full image set, transfer learning, more epochs for training, and optimizing the CNN architecture. The improvements are significant because deep learning deployment to the cloud needs to take into account model efficiency, scalability and computational cost [21].

The outputs of the smart manufacturing, cybersecurity and computer vision modules were joined together in a single industrial decision process in the decision fusion engine. The priority logic based on the rules was practical since it gave the highest priority to cybersecurity threats, then machine failure and quality defects. The system was able to produce the risk levels, alerts, decisions and recommended actions for industrial management. At the enterprise level, this helps to link the shop-floor data with the higher-level decision making process, which is essential for the enterprise management systems based on IoT [22].

The framework was implemented locally, but designed as a cloud-based Industrial IoT architecture. Edge and cloud computing may help to minimize communication delays, enhance responsiveness, and enable real-time analytics near machines and sensors in real industrial settings [23]. This is particularly true for time-critical applications like

visual inspection, production monitoring, cyberattack response, and machine failure detection. Future work should take place on actual cloud deployment, latency testing, streaming data ingestion and real-time dashboard implementation[24].

The overall results validate the proposed smart industrial management framework. The study demonstrates that machine learning, cybersecurity analytics, computer vision, and decision fusion can be combined into one integrated workflow. The framework needs further testing through actual cloud deployment, duplicate-cleaned cybersecurity data, a complete casting image dataset, and real-time industrial data streams before it can be deemed suitable for real-world industrial use.

6. Conclusion

The study proposed and modelled a cloud-based framework for Industrial IoT for smart industrial management with the aid of machine learning, cybersecurity analytics, computer vision, preprocessing and rule-based decision-fusion. The framework integrated three datasets to solve machine condition prediction, network intrusion detection, classification of cyberattacks and casting defect detection in a single coordinated workflow. For the smart manufacturing module, Gradient Boosting was the best performing algorithm with a weighted F1-score of 98.73%, making it an appropriate classification algorithm for machine operating conditions with controlled noise. The module's weighted F1-scores in the binary intrusion detection and multi-class attack classification tasks were 99.71% and 90.62%, respectively, showing its capability to detect and classify attacks on the Industrial IoT network. The computer vision module using CNN achieved 83.08% accuracy for validating casting defect, demonstrating the potential of the deep learning approach in automated quality inspection. The decision fusion engine was able to convert the individual model outputs into risk levels, alerts, decisions and recommended actions, which enabled the integration of industrial monitoring. In general, it is found that the proposed framework can be used for predictive maintenance, detection of cyber-attacks, visual inspection, and decision level industrial management. The study was conducted locally rather than in a real cloud environment, however, full deployment in a real cloud environment, duplication cleaned cyber security data, full use of the image data set, real-time data streaming and testing in real industrial environments should be included in future work.

References

1. Botta A, De Donato W, Persico V, Pescapé A. Integration of cloud computing and internet of things: a survey. Future Generation Computer Systems. 2016;56:684-700.
2. Moyne J, Iskandar J. Big data analytics for smart manufacturing: case studies in semiconductor manufacturing. Processes. 2017;5(3):39.
3. Mahdavinejad MS, Rezvan M, Barekatain M, Adibi P, Barnaghi P, Sheth AP. Machine learning for Internet of Things data analysis: a survey. Digital Communications and Networks. 2018;4(3):161-175.
4. ur Rehman MH, Yaqoob I, Salah K, Imran M, Jayaraman PP, Perera C. The role of big data analytics in industrial Internet of Things. Future Generation Computer Systems. 2019;99:247-259.
5. Adi E, Anwar A, Baig Z, Zeadally S. Machine learning and data analytics for the IoT. Neural Computing and Applications. 2020;32(20):16205-16233.
6. Tran KP. Artificial intelligence for smart manufacturing: methods and applications. Sensors. 2021;21(16):5584.
7. Mrabet H, Alhomoud A, Jemai A, Trentesaux D. A secured industrial internet-of-things architecture based on blockchain technology and machine learning for sensor access control systems in smart manufacturing. Applied Sciences. 2022;12(9):4641.
8. Al Shahrani AM, Alomar MA, Alqahtani KN, Basingab MS, Sharma B, Rizwan A. Machine learning-enabled smart industrial automation systems using internet of things. Sensors. 2022;23(1):324.
9. Sundaram S, Zeid A. Artificial intelligence-based smart quality inspection for manufacturing. Micromachines. 2023;14(3):570.
10. Visconti P, Rausa G, Del-Valle-Soto C, Velázquez R, Cafagna D, De Fazio R. Machine learning and IoT-based solutions in industrial applications for smart manufacturing: a critical review. Future Internet. 2024;16(11):394.
11. Awaisi KS, Ye Q, Sampalli S. A survey of industrial AIoT: opportunities, challenges, and directions. IEEE Access. 2024;12:96946-96996.
12. Zhukabayeva T, Zholshiyeva L, Karabayev N, Khan S, Alnazzawi N. Cybersecurity solutions for industrial internet of things-edge computing integration: challenges, threats, and future directions. Sensors. 2025;25(1):213.
13. Czimmermann T, Ciuti G, Milazzo M, Chiurazzi M, Roccella S, Oddo CM, et al. Visual-based defect detection and classification approaches for industrial applications: a survey. Sensors. 2020;20(5):1459.
14. Xia K, Saidy C, Kirkpatrick M, Anumbe N, Sheth A, Harik R. Towards semantic integration of machine vision systems to aid manufacturing event understanding. Sensors. 2021;21(13):4276.
15. colabsss. Smart Manufacturing Process Dataset [dataset on the Internet]. Kaggle; Available from: https://www.kaggle.com/datasets/colabsss/smart-manufacturing-process-dataset

16. Abbas S. Train Test Network CSV [dataset on the Internet]. Kaggle; Available from: https://www.kaggle.com/datasets/shahidabbas76/train-test-network-csv
17. Ravirajsinh45. Real-life industrial dataset of casting product [dataset on the Internet]. Kaggle; Available from: https://www.kaggle.com/datasets/ravirajsinh45/real-life-industrial-dataset-of-casting-product
18. Huang Z, Shen Y, Li J, Fey M, Brecher C. A survey on AI-driven digital twins in industry 4.0: smart manufacturing and advanced robotics. Sensors. 2021;21(19):6340.
19. Jagatheesaperumal SK, Rahouti M, Ahmad K, Al-Fuqaha A, Guizani M. The duo of artificial intelligence and big data for industry 4.0: applications, techniques, challenges, and future research directions. IEEE Internet of Things Journal. 2021;9(15):12861-12885.
20. Kubiak K, Dec G, Stadnicka D. Possible applications of edge computing in the manufacturing industry: systematic literature review. Sensors. 2022;22(7):2445.
21. Tavana M, Hajipour V, Oveisi S. IoT-based enterprise resource planning: challenges, open issues, applications, architecture, and future research directions. Internet of Things. 2020;11:100262.
22. Jauro F, Chiroma H, Gital AY, Almutairi M, Abdulhamid SIM, Abawajy JH. Deep learning architectures in emerging cloud computing architectures: recent development, challenges and next research trend. Applied Soft Computing. 2020;96:106582.
23. Hernandez-Jaimes ML, Martinez-Cruz A, Ramírez-Gutiérrez KA, Feregrino-Uribe C. Artificial intelligence for IoMT security: a review of intrusion detection systems, attacks, datasets and Cloud-Fog-Edge architectures. Internet of Things. 2023;23:100887.
24. Park H, Kim N, Lee GH, Choi JK. MultiCNN-FilterLSTM: resource-efficient sensor-based human activity recognition in IoT applications. Future Generation Computer Systems. 2023;139:196-209.