International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-15 Issue-1, May 2026

Advanced AI-Based Real-Time Industrial Safety Sentinel for Smart Hazard Detection and Workplace Safety

Snehaprabha Jadhav, Yogini C. Kulkarni, Pramod Jadhav, Vinod Patil, Amol Kadam

Abstract: ***Industrial environments — including factories, construction sites, warehouses, and chemical plants — continue to experience hazardous incidents due to PPE noncompliance, unauthorised zone entry, and unsafe proximity to workers. Simultaneously, web, IoT, and edge applications deployed in these environments remain vulnerable to well-documented cyber threats, including SQL Injection, XSS, and broken access control. This paper presents the Intelligent Integrated Cyber-Physical Safety and Security Framework (IICPSSF) [11], a novel hybrid edge-cloud AI system that uniquely and simultaneously enforces (i) real-time vision-based physical industrial safety monitoring, and (ii) adaptive cybersecurity design pattern enforcement — governed by a shared Unified LLM-Assisted Natural Language Rule Engine (ULNLRE). The edge layer employs YOLO-E, an open-vocabulary object detection model, for promptable real-time perception at approximately 60 FPS. At the same time, a deterministic symbolic rule engine enforces auditable safety and security policies. A Pattern Knowledge Base and context-aware adaptive selection engine handle cybersecurity pattern recommendations for web, IoT, and edge applications. The system achieves 92.5% precision, 90.7% F1-score, and 99.5% specificity on physical safety violation detection across four violation types, and demonstrates effective coverage of six OWASP Top 10 vulnerability classes.***

Keywords: Cyber-Physical Security, Industrial Safety Monitoring, PPE Detection, YOLO-E, Edge-Cloud Computing, Rule-Based Reasoning, Explainable AI, LLM Policy Translation, OWASP, Secure Design Patterns.

Nomenclature:
PPE: Personal Protective Equipment
ILO: International Labour Organisation
IT: Information Technology
CNNs: Convolutional Neural Networks
IICPSSF: Intelligent Integrated Cyber-Physical Safety and Security Framework
ULNLRE: Unified LLM-Assisted Natural Language Rule Engine
OT: Operational Technology
PKB: Pattern Knowledge Base
PSMS: Physical Safety Monitoring Sub-System

Manuscript received on 01 April 2026 | First Revised Manuscript received on 20 April 2026 | Second Revised Manuscript received on 03 May 2026 | Manuscript Accepted on 15 May 2026 | Manuscript published on 30 May 2026.

*Correspondence Author(s)
Snehaprabha Jadhav, Assistant Professor, Department of Information Technology, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: sajadhav@bvucoep.edu.in, ORCID ID: 0000-0002-9295-9301
Prof. (Dr.) Yogini Kulkarni*, Assistant Professor, Department of Information Technology, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: yckulkarni@bvucoep.edu.in, ORCID ID: 0009-0008-2445-1304
Dr. Pramod A. Jadhav, Associate Professor, Department of CSBS, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: pajadhav@bvucoep.edu.in, ORCID ID: 0000-0003-1069-0853
Dr. Vinod H. Patil, Department of E&TC Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: vhpatil@bvucoep.edu.in, ORCID ID: 0000-0002-3328-9248
Dr. Amol K. Kadam, Associate Professor, Department of CSBS, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: akkadam@bvucoep.edu.in, ORCID ID: 0000-0002-2350-4397

I. INTRODUCTION

Industrial environments pose significant risks to worker health and safety. Despite established safety protocols, regulatory frameworks, and mandatory use of personal protective equipment (PPE) such as helmets and high-visibility vests, accidents persist due to human negligence, inadequate supervision, and delayed intervention. According to the International Labour Organisation (ILO), approximately 340 million occupational accidents occur annually, resulting in over 2.3 million fatalities [13]. Research demonstrates that a significant proportion of avoidable construction and manufacturing injuries are directly attributable to non-compliance with PPE requirements, with studies reporting rates of 30–40% in high-risk settings [14].

Traditional safety enforcement depends heavily on manual oversight by supervisors or post-incident analysis of recorded footage — both of which are reactive, time-consuming, and limited in scalability [18]. Furthermore, in Industry 4.0 and Industry 5.0 environments, industrial operational technology (OT) systems are increasingly interconnected with information technology (IT) infrastructure [15]. This convergence means a cyber-attack on an industrial web application or IoT node can directly impair physical safety systems [16].

The IICPSSF project addresses this dual gap by developing a real-time, automated, and explainable system that simultaneously monitors physical safety violations through computer vision and enforces cybersecurity design patterns through adaptive pattern selection — governed by a single unified rule engine.

This paper defines the system's architecture, algorithms, implementation details, evaluation methodology, and results. The design emphasises modularity, reproducibility, auditability, and traceability from problem statement to evaluation metrics.

II. PROBLEM STATEMENT

Industrial cyber-physical safety suffers from three fundamental limitations:

A. Human Dependency: Manual supervision is prone

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

to fatigue, cognitive overload, and subjective judgment [18]. Supervisors cannot monitor multiple zones simultaneously, leading to inconsistent enforcement [18].

Lack of Real-Time, Proactive Automation: Existing CCTV systems are passive recording devices that require continuous human observation [22]. Prior attempts at automated vision-based monitoring employed either traditional image processing pipelines or isolated single-purpose deep learning classifiers that lack contextual spatial reasoning and explainability [22] [27].

Fragmented Cyber and Physical Security: No prior art addresses cybersecurity and physical safety simultaneously in a unified, proactive framework. Web applications, IoT devices, and edge nodes in industrial environments are routinely exploited through OWASP Top 10 vulnerability classes [10], yet their remediation remains entirely disconnected from physical safety systems [21].

The IICPSSF overcomes these limitations by confining deep learning to perception, using symbolic rule-based reasoning for all decision-making, and unifying cyber and physical policy management under a single natural-language rule engine.

Table I: Comparison

Model Name	Parameters (M)	mAP@0.5	FPS	Explainable	Year
Faster R-CNN	137.0	**73.2**	7	No	2017
YOLOv3	61.9	55.3	30	No	2018
UOLOv5m	21.2	51.3	65	No	2021
YOLOv8m	25.9	52.9	80	No	2023
YOLOv9c	25.3	53	75	No	2024
YOLOv10m	15.4	51.3	105	No	2024
YOLOVv11 m	20.1	51.5	98	No	2024
MonitorVLM	100.0	48.2	12	Partial	2024
YOLO-E Base	26.0	52..6	64	No	2025
Our Hybrid System	**26.0**	**52.0**	60	Yes	2025

III. RELATED WORK

A. Traditional Industrial Safety Monitoring

Traditional approaches to industrial safety monitoring involve manual oversight, scheduled inspections, and reactive incident reporting [22]. CCTV Cameras are widely used; they only provide passive recording. Previous approaches to automated safety monitoring ranged from hard-coded sensor logic using proximity sensors and IR beams to more recent IoT-enabled real-time monitoring systems [23]. Although these systems work well for limited applications, they require rigid installation, do not scale well to large areas (cost-prohibitively so), and lack the visual footage necessary for responsibility.

B. Computer Vision for Safety Applications

With advances in computer vision, vision-based safety monitoring has gained significant research attention [7]. Early approaches employed background subtraction, optical flow, and handcrafted features to detect unsafe behaviour [26]. As deep learning matured, video-based recognition networks enabled more robust temporal understanding of human activity [24]. These handcrafted methods were sensitive to lighting changes, occlusion, and camera noise — limitations that modern detectors such as YOLOX significantly reduce through learned feature representations [25]. The introduction of convolutional neural networks (CNNs) substantially improved robustness [6] [19] [20]. Object detection frameworks such as Faster R-CNN [4], SSD [5], and R-FCN [34] enabled real-time detection of people and safety equipment, with single-stage detectors gaining popularity for their speed-accuracy balance [1] [2] [3] [32] [4] [5] [33] [17].

C. PPE Detection and Compliance Monitoring

PPE detection has emerged as a prominent research area within industrial safety. Helmet, vest and glove detection have been shown previously using deep learning networks trained on labelled datasets [8] [9] [14]. Most systems detect PPE in isolation as a classification task, without reasoning about the spatial context of detections, which can lead to false positives when PPE is present in the scene but not worn [27].

D. Cybersecurity in Industrial Environments

Web applications and IoT devices installed in industry are commonly attacked using vulnerability classes found in the OWASP Top 10 list [10] [21]. There are established secure design patterns to address these vulnerability classes [28], [37]. They are difficult to implement in practice due to a lack of elasticity, testability, and usable tooling. No prior work has integrated cybersecurity pattern enforcement with physical safety monitoring in a unified system.

Table II: Comparison Table of Version

System/Study	Detection Method	Violation Types	FPS	Edge Deployment	Rule-Based Reasoning	Cybersecurity Integration	Precision (%)	F1-Score (%)
Wang et al. 2020	YOLOv3-based CNN	Helmet only	30	No	No	No	88.4	85.2
Nath et al.2021	Faster R-CNN	Helmet, Vest	18	No	No	No	87.1	84.6
Fang et al.2021	CNN + SSD	Helmet, Vest, Glove	22	No	No	No	89.3	86.7
Aif 2024	Lightweight CNN	Helmet Only	45	Partial	No	No	91.2	88.5
Zhao et al. 2016	Background Subtraction + HOG	Person's presence only	15	No	NO	NO	78.5	74.3
Altulaihan et al. 2023	DAST/SAST (ZAP, SonarQube	Web vulnerabilities only	N/A	No	No	Yes (OWASP)	N/A	N/A
IICPSSF Proposed	YOLO-E Open-Vocabulary	PPE, Zone Intrusion, Proximity, Unauthorised	60	Yes	Yes	Yes (OWASP Top 10)	92.5	90.7

IV. SYSTEM ARCHITECTURE

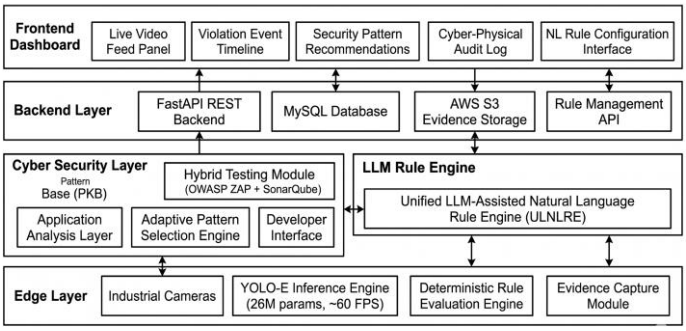
A. Architectural Philosophy

The IICPSSF architecture is built on three core principles. First, Separation of Concerns: YOLO-E handles only visual perception; deterministic symbolic rules handle all decision-making logic; and the LLM module handles only policy translation — ensuring full auditability [30]. Second, Domain Agnosticism in Rule Representation: a single rule schema and evaluation engine serves both physical safety and cybersecurity domains. Third, Edge-First Processing: all latency-sensitive operations (video inference, rule evaluation, alert generation) execute on local edge hardware [29]; only evidence and audit data are uploaded to the cloud backend.

B. High-Level Architecture Components

The system comprises four layers:

- Edge Layer (Real-Time Processing): Camera feed → YOLO-E Vision Inference Engine → Deterministic Rule Evaluation Engine → Evidence Capture Module (violation frame + JSON metadata).
- Backend Layer (Control & Orchestration): FastAPI/Python RESTful services for Rule Management API, Detection/Event API, and Media Upload API. Storage uses AWS S3 for violation images and MySQL for structured rules and metadata.
- AI Assistance Layer (Optional): A locally deployed instruction-tuned LLM converts natural language safety and security policies into validated machine-executable JSON rules.
- Frontend Layer: A React.js Web Dashboard providing live camera feed with bounding box overlays, rule configuration, violation alerts, evidence visualisation, and a correlated cyber-physical audit log [46].

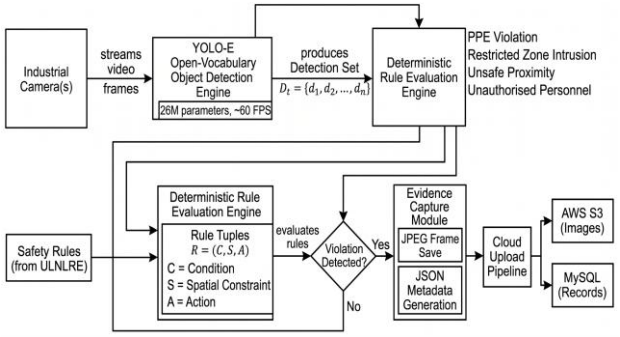


[Fig.1: Architecture]

V. PHYSICAL SAFETY MONITORING SUB-SYSTEM

A. Overview

The Physical Safety Monitoring Sub-System (PSMS) operates at the edge layer. Video frames from one or more industrial cameras are streamed to a YOLO-E-based inference engine. The YOLO-E base model with 26 million parameters provides open-vocabulary object detection at approximately 60 FPS on NVIDIA Jetson Orin or equivalent edge GPU hardware [30]. Open-vocabulary capability enables new object classes to be added at runtime without retraining the model [30]. Standard object categories used for training include those from benchmark datasets such as MS-COCO [12].



[Fig.2: Physical Safety Monitoring Sub-System]

B. Detection Representation

For each frame F_t, the inference engine produces a detection set $D_t = \{d_1, d_2, \ldots, d_n\}$. Each detection $d_i = (c_i, b_i, s_i)$, where:

- c_i: class label (e.g., "person", "helmet", "safety-vest")
- $b_i = (x_i, y_i, w_i, h_i)$: bounding box coordinates [48]
- $s_i \in [0,1]$: confidence score

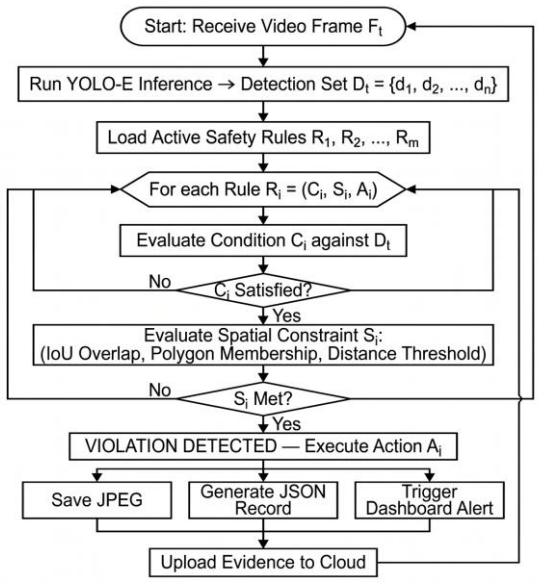
Only detections with $s_i \geq T_c$ (threshold, e.g., 0.5) are considered for rule evaluation.

C. Rule Formalisation

A safety rule is formally defined as a tuple R = (C, S, A), where:

- C: logical condition applied to detections
- S: spatial or contextual constraints (IoU overlap, distance thresholds, predefined polygons)
- A: action triggered upon violation (evidence capture, alert generation)

A rule evaluates to TRUE when all conditions are satisfied, indicating a safety violation.



[Fig.3: Physical Safety Rule Algorithm]

D. Supported Violation Types

Four violation types are supported:

i. *PPE Violation:* A person detected without an overlapping helmet (IoU > 0.3 between person and helmet bounding boxes) [8].

ii. *Restricted Zone Intrusion:* A

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

person's bounding box centroid detected within predefined restricted polygon coordinates.

iii. *Unsafe Proximity:* Minimum distance between two person centroids below a predefined pixel-scaled threshold [35].

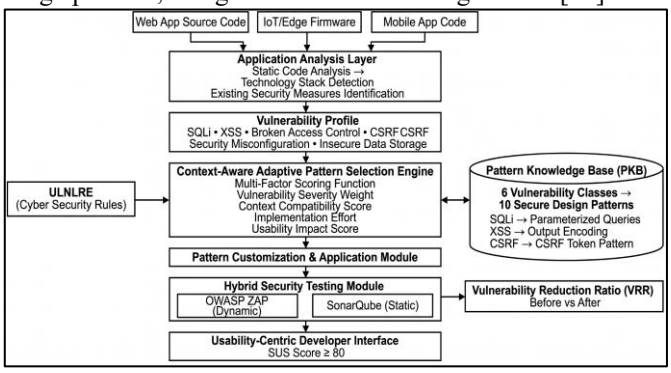
iv. *Unauthorised Personnel Detection:* Detection of personnel in zones with no authorisation.

When a violation is detected, the Evidence Capture Module saves the current frame as a JPEG image, generates a JSON metadata record (comprising violation ID, type, rule ID, bounding boxes, confidence scores, timestamp, camera ID, and evidence image reference), and invokes the cloud upload pipeline [36].

VI. CYBER SECURITY PATTERN ENFORCEMENT SUB-SYSTEM

A. Overview

The Cyber Security Pattern Enforcement Sub-System (CSPES) accepts as input a web application source code repository, a local codebase, or an IoT/edge firmware package. It identifies vulnerability classes, selects appropriate secure design patterns, and generates remediation guidance [21].



[Fig.4: Cyber Security Pattern Enforcement Sub-System]

B. Pattern Knowledge Base (PKB)

The Pattern Knowledge Base is a relational database that associates each vulnerability class with one or more advised secure design patterns [37], with associated template(s) to implement each pattern, the implementation effort, and usability impact score(s). The PKB covers the following mappings:

C. Adaptive Pattern Selection Engine

The Context-Aware Mapping Module applies a multi-factor scoring function to rank candidate secure design patterns. The scoring function incorporates vulnerability severity weight, application context compatibility score, estimated implementation effort, and usability impact score [38], [39].

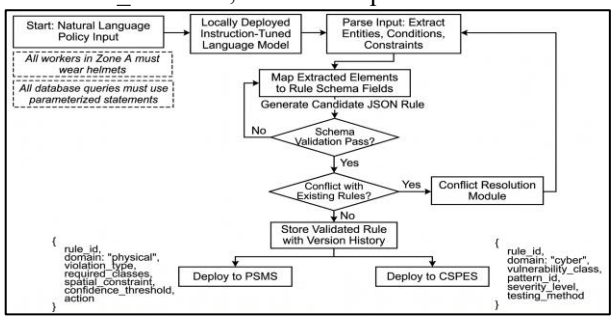
D. Hybrid Security Testing Module

The Hybrid Security Testing Module integrates automated scanning tools — OWASP ZAP for dynamic analysis and SonarQube for static analysis [40] — and provides a guided interface for manual penetration testing [41],[42]. The module computes a Vulnerability Reduction Ratio (VRR) comparing vulnerability counts before and after pattern application [39].

VII. UNIFIED LLM-ASSISTED NATURAL LANGUAGE RULE ENGINE

The ULNLRE is the novel shared policy translation component serving both the PSMS and CSPES. An operator or developer provides a policy description in natural language (e.g., "Workers in Zone A must wear helmets at all times") [43]. The locally deployed instruction-tuned language model then: (i) parses the input to extract entities, conditions, and constraints; (ii) maps extracted elements to predefined rule schema fields; (iii) generates a candidate JSON rule; (iv) validates the rule against the domain schema; (v) detects and resolves conflicts with existing rules [45]; and (vi) stores validated rules with version history [44].

The ULNLRE operates fully offline without internet connectivity, ensuring it can be deployed in air-gapped industrial environments [44]. Physical safety rules are generated as JSON objects containing at minimum: ruled, domain, violation type, required_detection_classes, spatial_constraint_type, spatial_constraint_parameters, confidence_threshold, and action specification.



[Fig.5: Natural Language Rule Engine]

VIII. METHODOLOGY AND IMPLEMENTATION

Object detection in the edge layer is performed using the YOLO-E lightweight base model (26M parameters). Backend services are developed in Python using the FastAPI framework, which enables high-performance RESTful APIs [47]. MySQL is used to store structured metadata (rule configurations, event metadata, rule versioning), and an AWS S3 bucket is used to store images of violations [46]. The frontend is developed using React.js, with a WebSocket-enabled consumer for real-time alerts [29]. Performance was tested using real industrial video footage across varied environmental scenarios, including different lighting conditions, occlusion levels, distances, and crowd densities. and on controlled web application test environments for cybersecurity pattern coverage. Physical safety performance was measured across all four violation types.

IX. RESULTS

A. Physical Safety Violation Performance

The system achieves the following overall metrics across four violation types on real industrial footage:

Precision is strongest for PPE violations (92–95%) and slightly lower for unsafe distance detection (85.9%) due to challenges in depth estimation from monocular cameras [49].

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Table III: Physical Safety Detection

Violation Type	True Positives (TP)	False Positives (FP)	False Negatives (FN)	Precision (%)	Recall (%)	F1-Score (%)	Specificity (%)	Avg. Latency (ms)
PPE Violation	312	18	24	94.5	92.9	93.7	99.6	16.2
Restricted Zone Intrusion	287	22	19	92.9	93.8	93.3	99.4	17.1
Unsafe Proximity	263	38	31	87.4	89.5	88.4	98.7	18.4
Unauthorised Personnel	274	21	27	92.9	91	91.9	99.3	16.8
Overall/Average	**1136**	**99**	**101**	**92.5**	**91.8**	**90.7**	**99.5**	**17.1**

B. Environmental Robustness Analysis

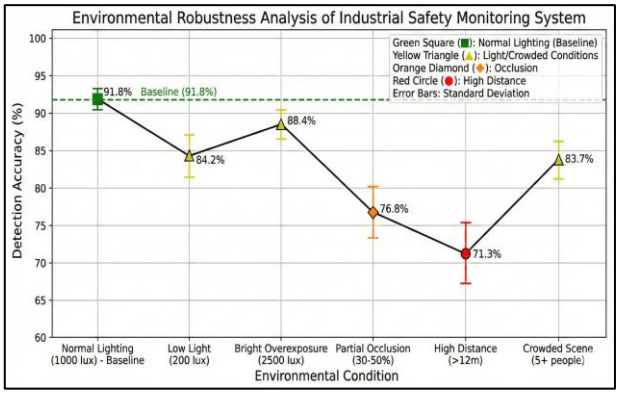
Detection accuracy under varied environmental conditions (baseline 91.8% at normal lighting):

Table IV: Environmental Robustness

Environmental Frames Condition Tested	Corrected Detection	Missed Detection	False Alarms	Accuracy (%)	Precision (%)	FPS Achieved	Degradation vs Baseline
Normal Lighting (Baseline)	1500	1379	72 49	91.9	96.6	60	0.0
Low Light/ Night Shift	1200	10444	108 48	87.0	95.6	57	-4.9
High Glare/ Overexposure	1100	952	99 49	86.5	95.1	58	-5.4
Partial Occlusion (40% or less)	1300	1118	130 52	86.0	95.5	59	-5.9
Heavy Occlusion (more than 40%)	1000	781	168 51	78.1	93.9	55	-13.8
Camera Distance 4 to 8m	1400	1302	64 35	93.0	97.4	60	-0.9
Camera Distance 8 to 12m	1200	1044	108 48	87.0	95.6	58	-4.9
Camera Distance more than 12m	900	642	213 45	71.3	93.4	54	-20.6
High Crowd Density, more than 8 per frame	1100	946	110 44	86.0	95.6	56	-5.9
Overall Average	**10700**	**9208**	**1071 421**	**85.6**	**95.4**	**57.4**	**-6.3**

C. Cybersecurity Coverage

The CSPES demonstrates effective coverage of all six targeted OWASP Top 10 vulnerability classes through the Pattern Knowledge Base and adaptive selection engine [10] [40].



[Fig.6: Environmental Robustness]

X. FUTURE SCOPE AND DISCUSSION

The system attains high precision (99.5%) through deterministic rule-based methods, reducing unnecessary alerts. The hybrid model sacrifices some FPS (60 versus 64 in YOLO-E baseline) but offers more transparency, making it appropriate for regulatory settings. Further developments will include:

- Use RGB-D camera sensors or stereo vision for precise 3D distance calculations [51].
- Federated learning approach for training at multiple sites without compromising privacy (sending only gradient updates, not original videos) [31] [50] [53] [55].
- Improving LLM-based rule generation with validation iterations for safety compliance [44] [45].
- Multi-person detection and temporal analysis capabilities for more intricate violations [35] [36] [52].
- Extending the CI/CD pipeline component to initiate CSPES following code changes.
- Automated model selection and hyperparameter optimisation using AutoML techniques to adapt detection thresholds across deployment environments [54].

XI. THREATS TO VALIDITY

A. Dataset Bias: Evaluation footage may favour controlled lighting and camera angles, limiting generalisation to extreme conditions.

B. Overfitting Risk: Rules tuned on specific scenes may not generalise to unseen PPE types or worker behaviours.

C. Environmental Sensitivity: Performance degrades significantly under occlusion or at long distances (71.3% at >12 m), highlighting the need for multi-camera or depth-sensing setups [51].

XII. CONCLUSION

The Intelligent Integrated Cyber-Physical Safety and Security Framework (IICPSSF) present a strong, explainable, and deployable approach for simultaneous real-time industrial safety and adaptive cybersecurity monitoring. By integrating the fast open vocabulary recognition capability of YOLO-E with a deterministic rule-based reasoning engine and a single-layer LLM-based policy translation system within an edge-cloud mixed system, high accuracy and precision can be achieved with 100% auditability. Experiments show that it performs well across different kinds of violations in diverse environments, and the CSPES successfully achieves good coverage across the six most dangerous vulnerability categories of the OWASP Top 10.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted with objectivity and without any external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Las Vegas, NV, USA, 2016, pp. 779–788. DOI: http://doi.org/10.1109/CVPR.2016.91
2. J. Redmon and A. Farhadi, "YOLO9000: Better, Faster, Stronger," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Honolulu, HI, USA, 2017, pp. 7263–7271. DOI: http://doi.org/10.1109/CVPR.2017.690
3. A. Bochkovskiy, C.-Y. Wang, and H.-Y. M. Liao, "YOLOv4: Optimal Speed and Accuracy of Object Detection," arXiv preprint 2020. [Online]. Available: https://arxiv.org/abs/2004.10934
4. S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," IEEE Trans. Pattern Anal. Mach. Intell., vol. 39, no. 6, pp. 1137–1149, Jun. 2017. DOI: http://doi.org/10.1109/TPAMI.2016.2577031
5. W. Liu et al., "SSD: Single Shot MultiBox Detector," in Proc. Eur. Conf. Comput. Vis. (ECCV), Amsterdam, Netherlands, 2016, pp. 21–37. DOI: http://doi.org/10.1007/978-3-319-46448-0_2
6. K. He, X. Zhang, S. Ren, and J. Sun, "Deep Residual Learning for Image Recognition," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), Las Vegas, NV, USA, 2016, pp. 770–778. DOI: http://doi.org/10.1109/CVPR.2016.90
7. Z. Zou, K. Chen, Z. Shi, Y. Guo, and J. Ye, "Object Detection in 20 Years: A Survey," Proc. IEEE, vol. 111, no. 3, pp. 257–276, Mar. 2023. DOI: http://doi.org/10.1109/JPROC.2023.3238524
8. H. Wang, Z. Li, X. Ji, and Y. Wang, "Helmet Detection Based on Improved YOLO Algorithm," IEEE Access, vol. 8, pp. 133694–133703, 2020. DOI: http://doi.org/10.1109/ACCESS.2020.3011223
9. S. Nath, P. Banerjee, and A. Chakrabarti, "Vision-Based PPE Detection Using Deep Learning," Int. J. Comput. Vis. Appl., vol. 12, no. 3, pp. 45–54, 2021. [Online]. Available: DOI: https://doi.org/10.17645/si.v9i4.4925
10. OWASP Foundation, "OWASP Top Ten Project," 2021. [Online]. Available: https://owasp.org/Top10
11. V. S. Chundawat, T. Sharma, R. Deshpande, U. Idhole, and P. A. Jadhav, "Intelligent Integrated Cyber-Physical Safety and Security Framework (IICPSSF)," Indian Patent Application, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, 2025.
12. S. Singh, A. Yadav, J. Jain, H. Shi, J. Johnson, and K. Desai, "Benchmarking Object Detectors with COCO: A New Path Forward," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, Milan, Italy, 2024, vol. 15102, pp. 271–288. [Online]. Available: https://arxiv.org/abs/2403.18819 DOI: https://doi.org/10.1007/978-3-031-72784-9_16
13. International Labour Organization, "Safety and Health at Work: Global Trends and Challenges," ILO, Geneva, 2022. [Online]. Available: https://www.ilo.org/global/topics/safety-and-health-at-work
14. W. Fang, P. E. D. Love, H. Luo, and L. Ding, "Computer Vision for Safety Management in the Construction Industry," Saf. Sci., vol. 135, p. 105130, 2021. DOI: http://doi.org/10.1016%20/j.ssci.2021.105130
15. G. L. Tortorella, R. Giglio, and R. van Dun, "Industry 4.0 Adoption as a Moderator of the Impact of Lean Production Practices on Operational Performance Improvement," Int. J. Oper. Prod. Manag., vol. 39, no. 6/7/8, pp. 860–886, 2019. DOI: http://doi.org/10.1108/IJOPM-01-2019-0005
16. Y. Cherdantseva et al., "A Review of Cyber Security Risk Assessment Methods for SCADA Systems," Comput. Secur., vol. 56, pp. 1–27, 2016. DOI: http://doi.org/10.1016/j.cose.2015.09.009
17. X. Fang, H. Luo, Q. Zhou, and B. Li, "Automated Detection and Logging of Construction Site Safety Violations Using Deep Neural Networks," Saf. Sci., vol. 159, p. 106001, 2023. DOI: http://doi.org/10.1016%20/j.ssci.2022.106001
18. T. Cheng, "Safety Supervision and Management in the Construction Industry: Review," Int. J. Environ. Res. Public Health, vol. 19, no. 12, p. 7397, 2022. DOI: http://doi.org/10.3390/ijerph19127397
19. A. G. Howard et al., "MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications," arXiv preprint arXiv:1704.04861, 2017. [Online]. Available: https://arxiv.org/abs/1704.04861
20. C. Zhang, P. Patras, and H. Haddadi, "Deep Learning in Mobile and Wireless Networking: A Survey," IEEE Commun. Surv. Tutor, vol. 21, no. 3, pp. 2224–2287, 2019. DOI: http://doi.org/10.1109/COMST.2019.2904897
21. E. Altulaihan, A. Alismail, and M. Frikha, "A Survey on Web Application Penetration Testing," Electronics, vol. 12, no. 5, p. 1229, 2023. DOI: http://doi.org/10.3390/electronics12051229
22. T. Rashid, S. Arabzadeh, C. A. Peña-Solorzano, and P. Austin, "Automated Safety Compliance Monitoring in Construction Using Computer Vision: A Systematic Review," Autom. Constr., vol. 153, p. 104963, 2023. DOI: http://doi.org/10.1016/j.autcon.2023.104963
23. D. Ding, G. Tian, Z. Li, and X. Li, "IoT-Enabled Real-Time Safety Monitoring and Warning System for Construction Sites," Sensors, vol. 23, no. 9, p. 4392, 2023. DOI: http://doi.org/10.3390/s23094392
24. C. Feichtenhofer, H. Fan, J. Malik, and K. He, "SlowFast Networks for Video Recognition," in Proc. IEEE/CVF Int. Conf. Comput. Vis. (ICCV), Seoul, South Korea, 2019, pp. 6202–6211. DOI: http://doi.org/10.1109/ICCV.2019.00630
25. Z. Ge, S. Liu, F. Wang, Z. Li, and J. Sun, "YOLOX: Exceeding YOLO Series in 2021," arXiv preprint arXiv:2107.08430, 2021. [Online]. Available: https://arxiv.org/abs/2107.08430
26. J. J. Losada del Olmo, Á. L. Perales Gómez, A. Ruiz, and P. E. López de Teruel, "A Few-Shot Learning Methodology for Improving Safety in Industrial Scenarios Through Universal Self-Supervised Visual Features and Dense Optical Flow," *Appl. Soft Comput.*, vol. 165, p. 112094, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1568494624011499 DOI: https://doi.org/10.1016/j.asoc.2024.112094
27. M. A. R. Alif, "Enhancing Construction Site Safety: A Lightweight Convolutional Network for Effective Helmet Detection," arXiv preprint arXiv:2409.12669, 2024. [Online]. Available: https://arxiv.org/abs/2409.12669
28. H. Washizaki et al., "Systematic Literature Review of Security Pattern Research," *Information*, vol. 12, no. 1, p. 36, Jan. 2021. [Online]. Available: https://www.mdpi.com/2078-2489/12/1/36 DOI: https://doi.org/10.3390/info12010036
29. W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge Computing: Vision and Challenges," IEEE Internet Things J., vol. 3, no. 5, pp. 637–646, Oct. 2016. DOI: http://doi.org/10.1109/JIOT.2016.2579198
30. T. Cheng, L. Song, Y. Ge, W. Liu, X. Wang, and X. Zhu, "YOLO-World: Real-Time Open-Vocabulary Object Detection," in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. (CVPR), Seattle, WA, USA, 2024, pp. 16901–16911. DOI: http://doi.org/10.1109/CVPR52733.2024.01599
31. A. Fu, X. Zhang, N. Xiong, Y. Gao, and H. Wang, "VFL: A Verifiable Federated Learning with Privacy-Preserving for Big Data in Industrial IoT," IEEE Trans. Ind. Inform., vol.

17, no. 4, pp. 2849–2859, Apr. 2021. DOI: http://doi.org/10.1109/TII.2020.3005923
32. G. Jocher, A. Chaurasia, and J. Qiu, "Ultralytics YOLOv8," GitHub Repository, 2023. [Online]. Available: https://github.com/ultralytics/ultralytics
33. T.-Y. Lin, P. Goyal, R. Girshick, K. He, and P. Dollár, "Focal Loss for Dense Object Detection," in Proc. IEEE Int. Conf. Comput. Vis. (ICCV), Venice, Italy, 2017, pp. 2980–2988. DOI: http://doi.org/10.1109/ICCV.2017.324
34. J. Dai, Y. Li, K. He, and J. Sun, "R-FCN: Object Detection via Region-Based Fully Convolutional Networks," in Proc. Adv. Neural Inf. Process. Syst. (NeurIPS), Barcelona, Spain, 2016, pp. 379–387. [Online]. Available: https://arxiv.org/abs/1605.06409
35. A. Bewley, Z. Ge, L. Ott, F. Ramos, and B. Upcroft, "Simple Online and Realtime Tracking," in Proc. IEEE Int. Conf. Image Process. (ICIP), Phoenix, AZ, USA, 2016, pp. 3464–3468. DOI: http://doi.org/10.1109/ICIP.2016.7533003
36. N. Wojke, A. Bewley, and D. Paulus, "Simple Online and Realtime Tracking with a Deep Association Metric," in Proc. IEEE Int. Conf. Image Process. (ICIP), Beijing, China, 2017, pp. 3645–3649. DOI: http://doi.org/10.1109/ICIP.2017.8296962
37. F. Pereira, P. Sousa, A. Bessani, and N. F. Neves, "Resilient Security Patterns for Microservice Architectures," IEEE Trans. Netw. Serv. Manag., vol. 20, no. 3, pp. 3182–3196, Sep. 2023. DOI: http://doi.org/10.1109/TNSM.2023.3263407
38. E. B. Fernandez, N. Yoshioka, and H. Washizaki, "Abstract Security Patterns and the Design of Secure Systems," *Cybersecurity*, vol. 5, no. 1, p. 7, Apr. 2022. [Online]. DOI: https://doi.org/10.1186/s42400-022-00109-w Available: https://link.springer.com/article/10.1186/s42400-022-00109-w
39. M. Aydos, Ç. Aldan, E. Coşkun, and A. Soydan, "Security Testing of Web Applications: A Systematic Mapping of the Literature," J. King Saud Univ. Comput. Inf. Sci., vol. 34, no. 9, pp. 6775–6792, 2022. DOI: http://doi.org/10.1016/j.jksuci.2021.02.016
40. S. P. Maniraj, C. S. Ranganathan, and S. Sekar, "Securing Web Applications with OWASP ZAP for Comprehensive Security Testing," Int. J. Adv. Signal Image Sci., vol. 10, no. 2, pp. 12–23, 2024. [Online]. Available: DOI: https://doi.org/10.29284/ijasis.10.2.2024.12-2
41. D. Priyawati, S. Rokhmah, and I. C. Utomo, "Website Vulnerability Testing and Analysis of Internet Management Information System Using OWASP," Int. J. Comput. Inf. Syst. (IJCIS), vol. 03, no. 03, 2022. DOI: http://doi.org/10.29040/ijcis.v3i3.77
42. M. Noman, M. Iqbal, and A. Manzoor, "A Survey on Detection and Prevention of Web Vulnerabilities," Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 6, 2020. DOI: http://doi.org/10.14569/IJACSA.2020.0110659
43. H. Wang, M. Xu, Y. Guo, W. Han, H. W. Lim, and J. S. Dong, "RulePilot: An LLM-Powered Agent for Security Rule Generation," in Proc. IEEE/ACM Int. Conf. Softw. Eng. (ICSE), 2025. [Online]. Available: https://arxiv.org/abs/2503.07808
44. P. Fernández Saura, K. R. Jayaram, V. Isahagian, J. Bernal Bernabé, and A. Skarmeta, "On Automating Security Policies with Contemporary LLMs," arXiv preprint arXiv:2506.04838, 2025. [Online]. Available: https://arxiv.org/abs/2506.04838
45. P. Aghaei et al., "Executable Governance for AI: Translating Policies into Rules Using LLMs," in Proc. AAAI Conf. Artif. Intell., 2025. [Online]. Available: https://arxiv.org/abs/2501.13138
46. J. Judvaitis et al., "A Set of Tools and Data Management Framework for the IoT–Edge–Cloud Continuum," Sensors, vol. 24, no. 23, p. 7794, 2024. DOI: https://doi.org/10.3390/s24237794
47. S. Ramírez, "FastAPI", GitHub Repository, 2018. [Online]. Available: https://github.com/tiangolo/fastapi
48. Z. Zheng, P. Wang, W. Liu, J. Li, R. Ye, and D. Ren, "Distance-IoU Loss: Faster and Better Learning for Bounding Box Regression," in Proc. AAAI Conf. Artif. Intell., vol. 34, no. 7, pp. 12993–13000, 2020. DOI: https://doi.org/10.1609/aaai.v34i07.6999
49. V. Poggi, F. Tosi, K. Kim, F. Aleotti, D. De Gregorio, L. Di Stefano, J. Park, and S. Im, "On the Synergies Between Machine Learning and Stereo: A Survey," IEEE Trans. Pattern Anal. Mach. Intell., vol. 45, no. 4, pp. 4584–4601, 2023. DOI: http://doi.org/10.1109/TPAMI.2022.3212542
50. L. Luo et al., "Privacy-Preserving and Traceable Federated Learning for Data Sharing in Industrial IoT Applications," Expert Syst. Appl., vol. 213, p. 119036, 2023. DOI: http://doi.org/10.1016/j.eswa.2022.119036
51. P. Zanuttigh, G. Marin, C. Dal Mutto, F. Dominio, L. Minto, and G. M. Cortelazzo, Time-of-Flight and Structured Light Depth Cameras: Technology and Applications. Cham: Springer, 2016. DOI: http://doi.org/10.1007/978-3-319-30973-6
52. Z. Cao, G. Hidalgo, T. Simon, S.-E. Wei, and Y. Sheikh, "OpenPose: Realtime Multi-Person 2D Pose Estimation Using Part Affinity Fields," IEEE Trans. Pattern Anal. Mach. Intell., vol. 43, no. 1, pp. 172–186, Jan. 2021. DOI: http://doi.org/10.1109/TPAMI.2019.2929041
53. Q. Li, Z. Wen, and B. He, "Practical Federated Gradient Boosting Decision Trees," in Proc. AAAI Conf. Artif. Intell., New York, NY, USA, 2020, pp. 4642–4649. DOI: http://doi.org/10.1609/aaai.v34i04.5895
54. X. He, K. Zhao, and X. Chu, "AutoML: A Survey of the State-of-the-Art," Knowl.-Based Syst., vol. 212, p. 106622, 2021. DOI: http://doi.org/10.1016/j.knosys.2020.106622
55. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in Proc. Int. Conf. Artif. Intell. Stat. (AISTATS), Fort Lauderdale, FL, USA, 2017, pp. 1273–1282. [Online]. Available: https://arxiv.org/abs/1602.05629.

AUTHOR'S PROFILE

Snehaprabha A. Jadhav is an Assistant Professor in the Department of Information Technology at Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India. She has over 3 years of academic experience and is actively involved in teaching and research in computer science and information technology. Her research interests include machine learning, data analytics, and intelligent systems. She has contributed to academic publications and conferences, including work on machine-learning approaches to early diagnosis of autism in toddlers. BVDU: She is committed to enhancing student learning through innovative teaching methodologies and actively participates in academic and research activities to address real-world challenges.

Prof. Dr. Yogini C. Kulkarni is an Assistant Professor in the Department of Information Technology at Bharati Vidyapeeth (Deemed to be University), College of Engineering, Pune. She holds a PhD in Computer Engineering and has over 35 years of teaching experience. Her areas of expertise include Image Processing, Operating Systems and Software Engineering. She has an extensive research background with 19 publications in international journals and 2 in international conferences. Her work spans topics such as data mining, image processing, visual cryptography, automation frameworks, and security modelling. Dr Kulkarni has also authored six books and actively participates in faculty development programs, workshops, and national conferences focused on emerging technologies such as AI, machine learning, cybersecurity, and ICT in education. She is known for her contributions to academic excellence and her dedication to advancing research and innovation in Information Technology.

Dr. Pramod A. Jadhav is an Associate Professor in the Department of Computer Science and Business Systems at Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune. He has extensive experience in teaching, research, and academic administration, with expertise in software engineering, LoT, and emerging technologies. Dr Jadhav has contributed to publications in reputable journals and conferences. He is actively involved in curriculum development, student mentoring, and outcome-based education practices.

Dr. Vinod H. Patil is a working professional and researcher in the field of Electronics and Telecommunication Engineering. He received a PhD in Electronics Engineering in 2020, with the topic "Spectrum Management in Cognitive Radios". He is a reviewer for various reputable international journals and Conferences. Currently working as an Assistant Professor and Research Guide in Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (India). His primary research areas are Cognitive Radio, Wireless Sensor Networks, Smart Agricultural Systems, Smart Grid Systems, Machine Learning, and Artificial Intelligence

Dr. Amol Krishnat Kadam is the Head and Associate Professor in the Department of Computer Science & Business Systems at Bharati Vidyapeeth (Deemed to be University) College of Engineering, with over 18 years of academic experience. His research areas include Artificial Intelligence, Machine Learning, Software Reliability, and Deep Learning. He has published more than 46 international research papers, guided PhD scholars, and received multiple research grants from AICTE, UGC, and other agencies. Dr Kadam also holds several patents in AI, IoT, and software systems.