



Artificial Intelligence in Cyber-Physical Security and Intelligent Surveillance: A Comprehensive Survey

Reshma Abhang Pramod Jadhav*, Sonal Jamdade, Amol Kadam, Aradhana Thorat, Ajit R. Patil

Abstract: Modern times require smart solutions for crime detection to enhance public security levels because crime detection remains a fundamental challenge. Traditional surveillance relies on human monitoring but has weaknesses due to time consumption and human error. The automated crime detection system runs on machine learning and deep learning platforms using Convolutional Neural Networks and Recurrent Neural Networks, along with YOLO, Faster R-CNN, and the Azure Face API. The AI models perform two functions: detecting suspicious activities and identifying weapons and faces, and recognising patterns of criminal behaviour. The combination of local servers and cloud platforms powered by AI detects crimes precisely in real time through enhanced monitoring, improves accuracy, and prevents false alarms, while also enabling broader crime-prevention capabilities.

Keywords: Crime Detection, Cyber-Physical Systems, Machine Learning, Deep Learning, Smart Surveillance, Object Detection.

Nomenclature:

YOLO: You Only Look Once
R-CNN: Region-based Convolutional Neural Network
API: Application Programming Interface
CCTV: Closed-Circuit Television
SSD: Single Shot MultiBox Detector
HDL: Hybrid Deep Learning
VGGNet: Visual Geometry Group Network
CPS Cyber-Physical Systems
AE: Autoencoders
CAE: Convolutional Autoencoder

Manuscript received on 01 September 2026 | Revised Manuscript received on 06 September 2026 | Manuscript Accepted on 15 September 2026 | Manuscript published on 30 September 2026.

Reshma Abhang, Department of Computer Science and Business Systems, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: rdabhang@bvucop.edu.in ORCID ID: [0009-0004-2012-2731](https://orcid.org/0009-0004-2012-2731)

Dr. Pramod Jadhav*, Department of Computer Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: pajadhav@bvucop.edu.in ORCID ID: [0000-0003-1069-0853](https://orcid.org/0000-0003-1069-0853)

Sonal Jamdade, Department of Computer Science and Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: srjamdade@bvucop.edu.in ORCID ID: [0009-0005-6674-3901](https://orcid.org/0009-0005-6674-3901)

Dr. Amol Kadam, Department of Computer Science and Business Systems, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: akkadam@bvucop.edu.in ORCID ID: [0000-0002-2350-4397](https://orcid.org/0000-0002-2350-4397)

Aradhana Thorat, Department of Computer Science and Business Systems, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune (Maharashtra), India. Email ID: asthorat@bvucop.edu.in ORCID ID: [0009-0001-2564-1010](https://orcid.org/0009-0001-2564-1010)

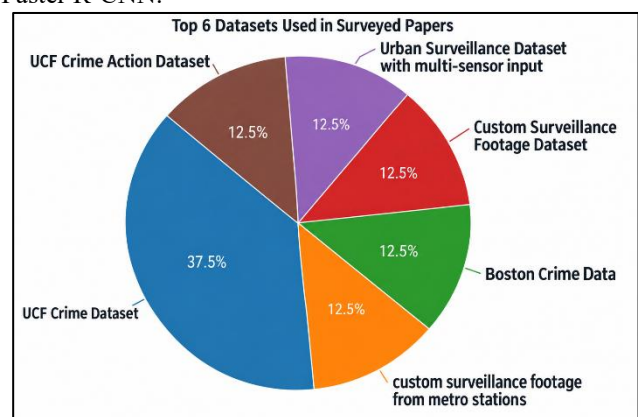
Dr. Ajit R. Patil, Department of Computer Engineering, Bharati Vidyapeeth College of Engineering, Lavale, Pune, Maharashtra, India. Email ID: patilajit667@gmail.com, ORCID ID: [0000-0002-2076-9963](https://orcid.org/0000-0002-2076-9963)

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

VAE: Variational Autoencoder
GANs: Generative Adversarial Networks
CNNs: Convolutional Neural Networks
LSTM: Long Short-Term Memory
EMI-LSTM — Early-exit Multiple-Instance Long Short-Term Memory

I. INTRODUCTION

Growing concerns about security in cities and public areas have made crime detection and prevention critical. On-device crime detection combines Early Stopping–Multiple Instance Learning with sub-Nyquist video sampling to reduce inference time and computational resources on edge devices while addressing latency and privacy concerns [1]. Human-operated surveillance systems perform poorly because operators become tired and make errors. Rising crime statistics have encouraged law enforcement agencies to use modern technology to enhance monitoring, accelerate response, and improve surveillance. The paper [2] presents findings on the problems with manual crime detection while introducing AI-powered cloud solutions. The system achieves higher face-recognition precision by integrating Microsoft Azure Cognitive Services and the Face API for identifying criminals and missing individuals in CCTV data. The research paper [3] evaluates real-time crime detection of weapons and suspicious objects through deep learning-based object detection frameworks, including YOLO, SSD, and Faster R-CNN.



[Fig.1: Top Six Datasets Used in the Surveyed Papers]

The study [4] examines the development and future of automated video surveillance, focusing on the shift from traditional detection models to transformer-based machine learning models and anomaly anticipation. The research highlights the advantage of transformer architectures for modelling intricate spatio-temporal relationships, which



Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

are more effective than previous CNN and RNN models at detecting irregularities in smart cities and industrial environments. The research uses statistical models and queueing systems to improve observation efficiency in security-sensitive areas. The research introduces an AI security bot that uses YOLO-based weapon detection and RNN-based text analysis to generate time-sensitive criminal alerts. According to Chackravathy S. et al. [5], intelligent surveillance systems stem from smart city projects. The HDL model described in this research uses CNN and RNN together to boost the detection accuracy of criminal activities in densely populated urban areas. The research paper by Naval Gund, U. V., & K. P. [6] uses VGGNet-19 along with other deep learning models to detect weapons to trigger automatic law enforcement alerts. Together, these studies show how cutting-edge AI surveillance transforms crime detection by combining automated face recognition with anomaly detection, behavioural analysis, and object detection. These strategies make both processes more efficient and accurate, yet shortcomings such as biased information, incorrect detections, privacy violations, and high computational needs remain. Progress in crime detection relies on improving AI models, implementing them with edge computing technologies for instant information processing, and maintaining ethical standards during implementation. The study by Raza, A. et al. [17] notes that Cyber-Physical Systems (CPS) are complex critical infrastructures, such as Industrial Control Systems (ICS), a Smart Grid and the Industrial Internet of Things (IIoT), that add to the vulnerability to advanced threats, including Denial of Service (DoS), zero-day exploits, and Advanced Persistent Threats (APTs), due to the pervasive nature of information and communications technology (ICT) and the significance of interconnected physical components. Modern research increasingly adopts data-driven Machine Learning (ML) frameworks because traditional security solutions (such as firewalls, signature-based intrusion detection systems (IDS), and fixed physical-model detectors) struggle with high-order system dynamics and unmodelled environmental noise, which often generate many false alarms.

II. LITERATURE SURVEY

A. AI and ML

Smart surveillance combines AI technology with ML functions to produce accurate crime alerts quickly. Earlier surveillance methods relied on human observers, which made the work inefficient because they took too long to respond and missed many events. Researchers developed AI-based methods to improve security operations by building systems that detect objects in real time, analyse human behaviour, and perform automatic face recognition. The document focused on a system for criminal detection and recognition on CCTV Data Using Cloud and Machine Learning [2], explaining how Microsoft Azure Cognitive Services with Face API enables cloud-based facial recognition for automatic identification of faces in CCTV videos while minimising human involvement. The system speeds up identification but still struggles with inadequate lighting and distorted images. Implementing cloud computing in surveillance improves security because it

lets scalable AI models run in the cloud without expensive local hardware. The main obstacles to using these systems stem from privacy issues and the need for a dependable internet connection.

B. Deep Learning

The article by Mohammed Boukabous and Mostafa Azizi [3] shows how deep learning and object detection methods play a crucial role in crime detection. Choudhry et al. [4] broadly categorise deep learning solutions for surveillance video anomaly detection into three paradigms: data supervision, model mechanics, and operational trade-off learning.

i. Supervised Learning (Full Supervision):

Core Models: Support Vector Machines (SVM), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) networks.

Operational Role: Models are explicitly trained on annotated normal and abnormal video sequences to capture temporal dependencies, recognise high-dimensional actions, and characterise high-dimensional behaviour.

Key Bottleneck: It requires dense, expensive frame-level annotations, has high computational overhead, suffers from vanishing gradients over long sequences, and is sensitive to environmental noise.

ii. Semi-Supervised Learning (Coarse & Normal Supervision):

Core Models: Multiple Instance Learning (MIL), One-Class Classification (OCC), and Transfer Learning (TL) are Core Models

Operational Role: Overcomes the problem of fine-grained anomaly labels either by computing ranking losses on video “bags” (MIL), or by learning boundary enclosures around a large set of normal data (OCC), or by fine-tuning pre-trained vision backbones (TL).

Key Bottleneck: Likely to be subject to instance vs. bag label ambiguity, domain discrepancy, and degradation in performance due to unexpected noise and out-of-distribution behaviours.

iii. Unsupervised Learning (Zero-Label Supervision):

Core Models – Autoencoders (AE, CAE, VAE), Generative Adversarial Networks (GANs), Convolutional Neural Networks (CNNs / 3D-CNNs).

Operational Role: Unsupervised discovery of intrinsic visual patterns based on flagging high reconstruction errors (AEs), game-theoretic generator/discriminator scoring (GANs), or direct spatiotemporal feature maps (3D-CNNs).

Common pitfalls include Blurry frame reconstruction, Training instability (e.g., GAN mode collapse), high false-alarm rates in dynamic environments, and model interpretability.

The study investigates three deep learning models, namely You Only Look Once [8], [9], Single Shot Multi-Box Detector and Faster R-CNN, for detecting criminal objects such as firearms and knives. YOLOv5 best meets real-time crime-detection requirements because it

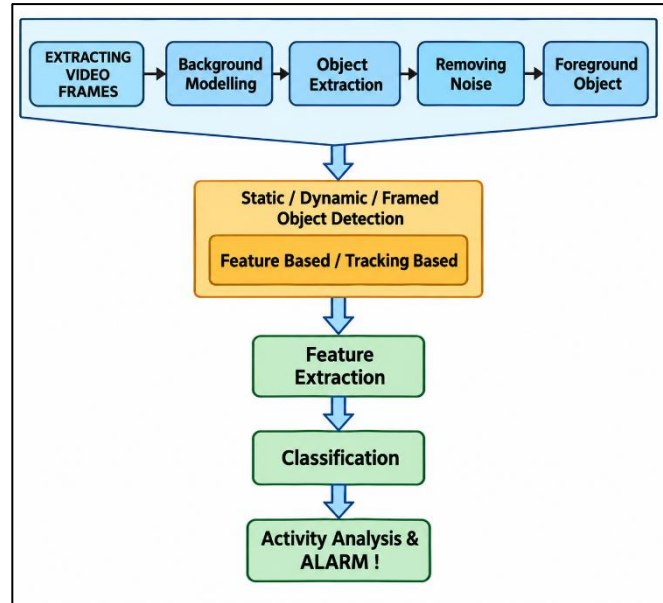


offers both high accuracy and fast performance. Identifying small objects is challenging in crowded areas under low-light conditions. The researchers developed an AI-based reporting system [9] that combines YOLO weapon detection with RNN-based text analysis for automated law enforcement alerts. NLP models in this system have limited ability to process unclear emergency communications, which can lead to incorrect alerts.

C. Challenges

According to a survey, huge challenges exist in real-world anomaly data, such as its lack of labelled real-world anomaly footage, poor performance under dynamic lighting and camera view changes, high computational latency for real-time deployment, and the "black-box" nature of deep neural networks, which are difficult to explain [4]. According to the research paper [5], deep learning applications in smart city surveillance are investigated through an HDL system that integrates CNNs for object recognition with RNNs to analyse behaviours. The detection system monitors suspicious actions such as loitering, sudden crowd formation, and aggressive conduct. However, high processing requirements and biases in the training dataset limit its performance. The research article [6] recommends implementing VGGNet-19 deep convolutional neural networks to analyse weapons and aggressive body postures detected by security cameras. The system provides real-time alerts using a live notification feature, but it requires substantial training data to identify changing criminal activities. Research on crime detection through Edge AI uses Multiple Instance Learning with Early Stopping, allowing models to run in real time on Raspberry Pi devices. Edge AI models' processing restrictions limit their ability to handle complex security applications, even though they can operate offline with privacy-preserving monitoring. The research paper "Survey Paper on Automatic Alert Generation in Surveillance Systems for Smart City

Environment Using Deep Learning" [10] investigates CNN-based surveillance models for anomaly detection, noting that high training epochs combined with low learning rates help prevent false positives. In the paper by Kim and Park (2021) [16], key future priorities include the establishment of real-time detection deadlines before physical system states move beyond irreparable bounds; construction of resilient architecture recovery strategies, including software-defined networking re-routing and simplex redundancy; and the use of generative adversarial networks (GANs) to generate malicious training data and address the significant real-world lack of anomalous CPS datasets.



[Fig. 2: Flowchart from the Paper "Suspicious Action Detection in Intelligent Surveillance System Using Action Attribute Modelling" (2020) [11]]

Table I: Research Methodologies Analysis

Reference	Algorithm Evaluation Results				
	Year	Pros	Limitations	Method	Accuracy
[1]	2020	The system runs on low-power edge devices, reducing privacy threats.	Computer speed limitations create obstacles when deploying computers on a large scale for operational purposes.	EMI-LSTM	91.30%
[10]	2020	The CNN-based system shows great success in anomaly detection and generates few false alarms in its operations.	The deployment of several operational locations results in scalability problems	CNN	100% (PEL dataset)
[5]	2018	The system implements hybrid artificial intelligence technology for monitoring suspicious activities that occur in public spaces.	Real-time processing demands excessive computational resources because of its cognitive model.	Hybrid Deep Learning	92.40%
[6]	2018	The platform identifies weapons and aggressive actions simultaneously using its instant detection system.	The system needs a wide range of training data to generalise successfully.	VGGNet-19	100% (training dataset)
[3]	2023	Detects crime-related objects, such as weapons, in real time.	It becomes challenging for the device to identify small objects due to numerous distractions within its operational environment.	YOLOv5	56.92% (mAP@.5)

III. ALGORITHMS USED

Artificial intelligence uses machine learning and deep learning algorithms to enable automated crime detection by identifying threats, analysing behaviours, and recognising objects during surveillance activities. The three essential components of smart crime analysis are Convolutional Neural Networks, which extract features from images; You Only Look Once for real-time object detection; and Long Short-Term Memory for processing sequential crime data. These algorithms improve results and increase operational efficiency when detecting security risks and abnormal behaviour.

A. CNN in Crime Detection

Crime detection relies heavily on CNNs for their ability to extract features and classify images. The research presents a CNN-RNN system that combines them to analyse city surveillance videos for criminal activity detection. CNNs extract spatial features, while RNNs track temporal patterns to detect abnormal crowd behaviour, aggressive movements, and loitering. The research "Survey Paper on Automatic Alert Generation in Surveillance Systems for Smart City Environment Using Deep Learning" [10] demonstrates the use of CNN-based models to identify violent behavioural patterns within video frames. A system named "Crime Intention Detection System Using Deep Learning"[6] employs VGGNet-19 as its deep CNN architecture design to detect weapons and aggressive human postures. Implementing CNNs faces two main obstacles: costly computation and the need for extensive labelled data.

Table II: Accuracy of CNN Models Over the Papers

Reference	CNN	
	Year Published	Accuracy (%)
[3]	2023	56.92
[1]	2020	91.3

B. YOLO for Object Detection

The crime detection field has widely adopted YOLO for weapon and suspicious-object identification tasks. The paper "Image and Video-Based Crime Prediction Using Object Detection and Deep Learning" [3] shows how YOLOv5 successfully finds firearms and knives in CCTV records. YOLO delivers real-time efficiency because it evaluates complete images through a single forward pass. YOLOv5 struggles to identify small or partially obscured objects in crowded areas, producing false negatives. This research combines YOLO-based weapon detection with RNN-based text analysis to create an automatic crime alert system in "A Smart Crime Reporting Bot Using YOLO-Based Weapon Detection and RNN-Based Text Analysis" [9]. YOLO performs well, but it needs further development in complex environments and dim lighting.

Table III: Accuracy of YOLO Models Over the Papers

Reference	YOLO	
	Year Published	Accuracy (%)
[3]	2023	56.92% (mAP@.5)
[9]	2025	85-90%

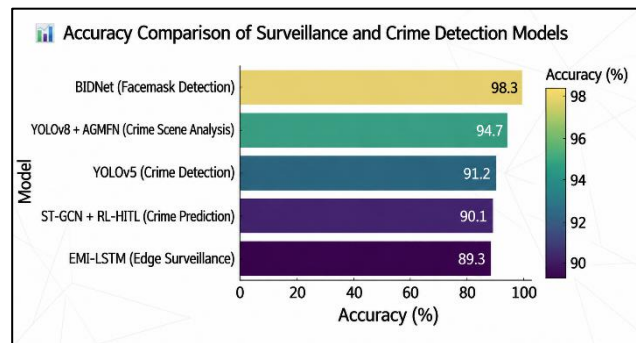
C. LSTM for Sequential Crime Analysis

LSTM operates as a time-dependent crime analysis tool within the Recurrent Neural Networks (RNNs) family. An EMI-LSTM model serves as the core mechanism in "Real-

Time Surveillance-Based Crime Detection for Edge Devices" [1] to identify crimes on limited-resource edge devices. The Early Stopping (EMI) method improves computational speed by automatically stopping operations when decisions become obvious, enabling real-time processing. The model processes video frames sequentially to provide uninterrupted crime surveillance without relying on powerful computing systems. Implementing LSTM-based systems requires substantial training data to reduce detection errors and bias. The research paper "A Smart Crime Reporting Bot Using YOLO-Based Weapon Detection and RNN-Based Text Analysis" [9] applies LSTM to emergency message processing, analysing text to distinguish real threats from false reports. LSTM's effectiveness is limited because it requires substantial computational resources, which restricts its use on low-power systems.

Table IV: Accuracy of LSTM Models Over the Papers

Reference	LSTM	
	Year Published	Accuracy (%)
[1]	2020	91.3% (EMI- LSTM)
[9]	2025	87% (LSTM)



[Fig.3: Accuracy Comparison of Various Algorithms Through a Bar Chart [12], [15], [8], [7], [1]]

IV. CONCLUSION

The full implementation of AI-driven crime detection faces several obstacles that prevent widespread use. The main obstacle is their reliance on high-quality datasets. The successful operation of CNN [12], YOLO [8], and LSTM [1], [9] frameworks depend on large, well-defined datasets, but real-life crime environments tend to evolve continuously and remain complex. Three key factors, such as lighting conditions, camera perspectives, and visual blockages, negatively influence the ability of detection systems to identify objects and analyse behavioural patterns. Unreliable surveillance results stem from two major limitations: harmless activities are misidentified as suspicious, while genuine threats go undetected. The main constraint behind computational efficiency is the need for improved performance. CNN-based architectures, along with LSTMs and other deep learning models, require substantial processing power, making real-time deployment on resource-limited devices impractical. Cloud computing solutions [2] address these issues but introduce additional challenges by requiring internet access and raising data privacy concerns. Using facial recognition [12] along with behaviour tracking





creates major ethical challenges because it seriously violates privacy rights. Improper implementation of these innovations through mass surveillance systems, alongside discriminatory law enforcement, creates moral issues that require clear rules and regulatory mechanisms. Crime detection and smart surveillance [13] have advanced through AI technology, despite the challenges encountered. Intelligent surveillance system performance [14] increased dramatically after combining YOLO with LSTM for sequential data processing and CNN for image analysis. These models support instant identification of weapons, suspicious conduct, and anomalies, allowing police to respond quickly to security risks. Upcoming developments in this technology should prioritise model optimisation to reduce false alarms, edge-computing speed-ups, and privacy-protecting artificial intelligence technologies. AI surveillance technology continues to advance toward becoming a preventive crime intervention tool that respects ethical and legal regulations.

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:** Based on my understanding, this article has no conflicts of interest.
- **Funding/Grants/Financial Support:** This article has not been sponsored or funded by any organisation or agency.
- **Ethical Approval and Consent to Participate:** The data provided in this article are exempt from ethical approval or participant consent requirements.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contribution:** Each author has individually contributed to the article. **Reshma Abhang:** Conceptualisation, writing a draft, Data curation; **Dr Pramod A. Jadhav:** methodology identification, manuscript review; **Sonal R. Jamdade:** data analysis; **Dr Amol K. Kadam:** Formal Analysis; **Aradhana Thorat:** Visualization; **Dr Ajit R. Patil:** supervision, review, editing

REFERENCES

1. Venkatesh, S., Anand, A., Gokul S., Ramakrishnan, A., & Vineeth Vijayaraghavan. (2020). Real-time Surveillance-Based Crime Detection for Edge Devices. Proceedings of the 17th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications, 801–809.
DOI: [10.5220/0008990108010809](https://doi.org/10.5220/0008990108010809)
2. Shirsat, S., Naik, A., Tamse, D., Yadav, J., Shetgaonkar, P., & Aswale, S. (2019, March 1). Proposed System for Criminal Detection and Recognition on CCTV Data Using Cloud and Machine Learning. IEEE Xplore. DOI: [10.1109/ViTECoN.2019.8899441](https://doi.org/10.1109/ViTECoN.2019.8899441)
3. Boukabous, M., & Azizi, M. (2023). Image and video-based crime prediction using object detection and deep learning. Bulletin of Electrical Engineering and Informatics, 12(3), 1630–1638.
DOI: [10.11591/eei.v12i3.5157](https://doi.org/10.11591/eei.v12i3.5157)
4. Choudhry, N., Abawajy, J., Huda, S., & Rao, I. (2023). A Comprehensive Survey of Machine Learning Methods for Surveillance Video Anomaly Detection. IEEE Access, 11, 114680–114713.
DOI: [10.1109/ACCESS.2023.3321800](https://doi.org/10.1109/ACCESS.2023.3321800)
<https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10271300>
5. Chackravathy, S., Schmitt, S., & Yang, L. (2018, October 1). Intelligent Crime Anomaly Detection in Smart Cities Using Deep Learning. IEEE Xplore. DOI: [10.1109/CIC.2018.00060](https://doi.org/10.1109/CIC.2018.00060)
6. Naval Gund, U. V., & K., P. (2018). Crime Intention Detection System Using Deep Learning. 2018 International Conference on Circuits and

Systems in Digital Enterprise Technology (ICCSDET).

DOI: [10.1109/iccsdet.2018.8821168](https://doi.org/10.1109/iccsdet.2018.8821168)

7. Mandalapu, V., Elluri, L., Vyas, P., & Roy, N. (2023). Crime Prediction Using Machine Learning and Deep Learning: A Systematic Review and Future Directions. IEEE Access, 11(60154), 60153–60170.
DOI: [10.1109/access.2023.3286344](https://doi.org/10.1109/access.2023.3286344)
8. Oghenevovwero Zion Apene, Nachamada Vachaku Blamah, Imuetinyan, G., & Morufu Olalere. (2024). Development of a Mathematical Model for Crime Detection Based on YOLO Network Architecture. International Journal of Computer Applications, 186(20), 17–24. DOI: [10.5120/ijca2024923621](https://doi.org/10.5120/ijca2024923621)
9. Choi, S. (2025). A Smart Crime Reporting Bot Using YOLO-Based Weapon Detection and RNN-Based Text Analysis. IJournals: International Journal of Software & Hardware Research in Engineering, 13(1).
<https://ijournals.in/wp-content/uploads/2025/01/3.IJSHRE-131301-Choi.pdf>
10. Janakiramaiah, B., Kalyani, G., & Jayalakshmi, A. (2020). Automatic alert generation in a surveillance system for smart city environment using deep learning algorithm. Evolutionary Intelligence. DOI: [10.1007/s12065-020-00353-4](https://doi.org/10.1007/s12065-020-00353-4)
11. Mudgal, M., Punj, D., & Pillai, A. (2021). Suspicious Action Detection in Intelligent Surveillance System Using Action Attribute Modelling. Journal of Web Engineering. DOI: [10.13052/jwe1540-9589.2017](https://doi.org/10.13052/jwe1540-9589.2017)
12. Ul Haque, I., Alam Bhuiyan, M., Sayed Al Banna, S. M. A., Haq Bhuiyan, M., Alam, K., & Monir, M. F. (2024). A Smart Surveillance System for Facemask Detection Using Custom CNN—BiDNet. IEEE Access, 12, 122769–122784. DOI: [10.1109/access.2024.3407534](https://doi.org/10.1109/access.2024.3407534)
13. Shah, M., Agre, M., Chawdhary, A., & Deone, J. (2022). Smart Surveillance System. SSRN Electronic Journal. DOI: [10.2139/ssrn.4108852](https://doi.org/10.2139/ssrn.4108852)
14. Xu, J. (2020). A deep learning approach to building an intelligent video surveillance system. Multimedia Tools and Applications. DOI: [10.1007/s11042-020-09964-6](https://doi.org/10.1007/s11042-020-09964-6)
15. Veeram, S. B., & Satish, A. R. (2025). Design of an Integrated Model for Video Summarisation Using Multimodal Fusion and YOLO for Crime Scene Analysis. IEEE Access, 13(25008), 25008–25025.
DOI: [10.1109/access.2025.3538282](https://doi.org/10.1109/access.2025.3538282)
16. Kim, S., & Park, K. J. (2021). A survey on machine-learning-based security design for cyber-physical systems. In Applied Sciences (Switzerland) (Vol. 11, Issue 12). MDPI AG. DOI: [10.3390/app11125458](https://doi.org/10.3390/app11125458)
17. Raza, A., Memon, S., Nizamani, M. A., & Hussain Shah, M. (2022). Machine Learning-Based Security Solutions for Critical Cyber-Physical Systems. 2022 10th International Symposium on Digital Forensics and Security (ISDFS), 1–6.
DOI: [10.1109/ISDFS55398.2022.9800811](https://doi.org/10.1109/ISDFS55398.2022.9800811)

AUTHOR'S PROFILE



Mrs Reshma Abhang received B.E. and M.E. degrees in Computer Engineering and is currently pursuing a PhD. She is an Assistant Professor in the Department of Computer Science & Business Systems at Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India. Her research interests focus on Artificial Intelligence, Cyber Threat Intelligence, and LLM applications for threat detection. She holds patents in IoT cybersecurity and AI systems and has published several papers in peer-reviewed journals and international conferences.



Dr. Pramod A. Jadhav is a Professor in the Department of Computer Engineering 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, IoT, and emerging technologies. Dr Jadhav has contributed to various research publications in reputed journals and conferences. He is actively involved in curriculum development, student mentoring, and outcome-based education practices.





Sonal R. Jamdade is an Assistant Professor in the Department of Computer Science and Engineering at Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune. She has over 14 years of academic experience in teaching and research; her core areas of specialisation include Data Mining, Cloud Computing, Design Thinking, and Software Engineering. She has published multiple research papers in international journals and conferences focusing on secure semantic search, real-time tracking systems, and AI applications.



Dr Amol K. Kadam is the Head and a 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.



Aradhana Thorat is an Assistant Professor in Computer Science and Business Systems at Bharati Vidyapeeth (Deemed University) College of Engineering, Pune, India. She holds an M. Tech from Shivaji University, Kolhapur, and is currently pursuing her PhD in Engineering. Her research interests include deep learning, computer vision, natural language processing, medical AI, and data analytics. She has published in Scopus, Web of Science, and IEEE-indexed venues and holds a published patent. Prior to academia, she worked as a Software Engineer developing IoT-based data systems.



Dr Ajit R. Patil is an Associate Professor in the Department of Computer Engineering at Bharati Vidyapeeth's College of Engineering, Lavale, Pune, with more than two decades of teaching and academic experience. He holds a PhD in Computer Engineering with specialisation in Artificial Intelligence. He has taught Computer Engineering and Artificial Intelligence. He has guided numerous UG projects and actively contributed to research through 17 publications and 2 granted patents. Dr Ajit Patil has organised several national conferences, FDPs, workshops, and industrial training programs.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Publisher /Journal and/or the editor(s). The Publisher /Journal and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.