

HYPOTHETICAL APPROACH FOR ADVANCING AI-ENABLED VIDEO PROCESSING IN CLOUD-BASED SURVEILLANCE SYSTEMS

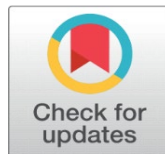
Jubber Nadaf¹, Dr. Amol K. Kadam², Sachin Wakurdekar³, T. B. Patil⁴

¹ Ph.D. Scholar Department of Computer Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India 411043

² Department of Computer Science and Business Systems, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India 411043

³ Assistant Professor, Department of Computer Engineering, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India 411043

⁴ Assistant Professor, Department of Information Technology, Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India



Corresponding Author

Dr. Amol K. Kadam,
akkadam@bvucop.edu.in

DOI

[10.29121/shodhkosh.v4.i1.2023.5799](https://doi.org/10.29121/shodhkosh.v4.i1.2023.5799)

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Copyright: © 2023 The Author(s). This work is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

With the license CC-BY, authors retain the copyright, allowing anyone to download, reuse, re-print, modify, distribute, and/or copy their contribution. The work must be properly attributed to its author.

ABSTRACT

This abstract presents an overview of the transformative potential of integrating IoT, AI, and ML technologies in cloud-based surveillance systems for audio/video processing. The convergence of these technologies has led to the development of intelligent surveillance solutions capable of enhancing security measures through real-time detection and response to threats. By employing advanced algorithms such as object detection, facial recognition, and anomaly detection, businesses can significantly improve the accuracy and efficiency of surveillance operations. Platforms like Amazon SageMaker and Google Cloud AI Platform offer the infrastructure and tools necessary for training and deploying these algorithms, enabling organizations to tailor surveillance systems to their specific requirements. Looking towards the future, the integration of edge computing technology with cloud-based surveillance systems holds promise for further innovation and efficiency gains. The research carried out explores automation in self-regulating video surveillance using cloud computing, microservices, and advanced data processing techniques. The primary focus is on optimizing traffic management and incident detection through AI and IoT integration. This paper introduces an efficient architectural framework and mathematical formulations for real-time data analysis, storage, and retrieval, ensuring improved performance and automation. The ultimate goal is to create a safer and more secure environment by leveraging AI-enabled video processing to mitigate security threats effectively. This abstract underscores the importance of ongoing research and collaboration in harnessing the full potential of AI-enabled video processing for audio/video surveillance in cloud-based systems.

Keywords: Intelligent Surveillance, AI, IOT Integration, Cloud Computing, Data Privacy, Future Trajectories, Societal Implications



1. INTRODUCTION

Traditional surveillance methodologies are transcended by the integration of state-of-the-art technologies, notably the convergence of Internet of Things (IoT), Artificial Intelligence (AI), and Machine Learning (ML). This synergy ushers in an era of intelligent surveillance systems capable of processing audio and video data with unparalleled efficiency, particularly in cloud-based environments. This hypothetical approach endeavors to explore the vast potential of AI-

enabled video processing within cloud-based surveillance systems, with a focal point on augmenting security measures through real-time threat detection and response mechanisms. By harnessing the prowess of AI and ML algorithms, businesses are poised to revolutionize surveillance operations, propelling them towards proactive threat mitigation and agile incident management.

The aim of this comprehensive investigation is to delve into the theoretical underpinnings, practical implementations, and future trajectories of AI-enabled video processing within cloud-based surveillance ecosystems. Commencing with an elucidation of the transformative impact of IoT, AI, and ML technologies on traditional surveillance paradigms, we shed light on the myriad benefits derived from their integration. Subsequently, an in-depth exploration of diverse AI and ML algorithms ensues, encompassing object detection, facial recognition, anomaly detection, and natural language processing, elucidating their pivotal roles in bolstering audio/video surveillance capabilities within the cloud.

Moreover, an examination of the technological infrastructure and platforms facilitating the training and deployment of AI models for video processing within cloud-based surveillance systems is imperative. Platforms such as Amazon SageMaker and Google Cloud AI Platform serve as indispensable conduits, furnishing organizations with the requisite tools and resources to develop bespoke AI models tailored to their unique surveillance imperatives[12,14]. Concurrently, the imperatives of data privacy and security loom large, mandating the adoption of ethical AI practices and privacy-preserving techniques to assuage potential risks and ensure regulatory compliance.

Anticipating the trajectory forward, we envision a paradigmatic shift in the domain of audio/video surveillance, propelled by ongoing innovations in AI, ML, and cloud computing realms[16,17]. The synergistic integration of edge computing with cloud-based surveillance infrastructures holds immense promise for further optimization and efficiency enhancements, engendering real-time data processing and analysis at the network periphery. Moreover, advancements in explainable AI and federated learning methodologies are poised to elevate the interpretability and transparency of AI models, fostering trust and confidence among stakeholders within surveillance ecosystems[26]. In essence, the hypothetical approach delineated herein underscores the transformative potential of AI-enabled video processing within cloud-based surveillance systems. By leveraging the symbiosis of IoT, AI, and ML technologies, organizations stand poised to fortify security measures, mitigate risks, and orchestrate agile responses to emergent security threats in real-time. As societies traverse towards an increasingly interconnected and digitized epoch, the adoption of AI-enabled surveillance systems emerges as a linchpin in fortifying safety, security, and resilience across diverse domains and organizational landscapes[12,13].

2. TECHNOLOGICAL LANDSCAPE AND ADVANCEMENTS

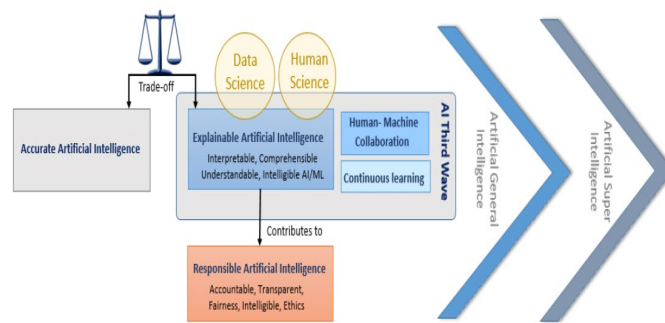
The technological landscape of modern surveillance systems is shaped by the integration of IoT, AI, and ML technologies, each playing a pivotal role in augmenting the capabilities of traditional surveillance methodologies[8,15]. IoT devices such as sensors, cameras, and actuators serve as the foundational components, facilitating the collection and transmission of vast amounts of audio and video data to centralized cloud-based platforms. These platforms act as the nerve center of surveillance operations, leveraging AI and ML algorithms to process and analyze incoming data streams in real-time[7,9].

At the forefront of this technological revolution are AI and ML algorithms, which enable surveillance systems to perform sophisticated tasks such as object detection, facial recognition, anomaly detection, and natural language processing[10]. Object detection algorithms, powered by deep learning techniques, enable surveillance systems to identify and track objects of interest in video streams, including people, vehicles, and other entities. Facial recognition algorithms leverage convolutional neural networks (CNNs) to extract unique facial features and match them against a database of known individuals, enabling accurate identification and authentication processes[5,6].

Anomaly detection algorithms play a critical role in identifying deviations from normal behavior patterns in surveillance data, alerting security personnel to potential security threats or unusual activities[3,4]. These algorithms utilize statistical techniques and machine learning models to detect outliers and anomalies in audio and video data, enabling proactive threat mitigation and incident response. Additionally, natural language processing (NLP) algorithms enable surveillance systems to analyze and interpret spoken language or text data, facilitating the detection of keywords or phrases indicative of suspicious behavior[29,20].

3. TECHNOLOGICAL INFRASTRUCTURE AND PLATFORMS

The development and deployment of AI-enabled surveillance systems rely on robust technological infrastructure and platforms capable of supporting complex data processing and analysis tasks. Cloud computing platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) provide the necessary infrastructure and tools for building and deploying surveillance applications at scale[28]. Platforms like Amazon SageMaker and Google Cloud AI Platform offer a comprehensive suite of tools and services for training and deploying AI and ML models for video processing. These platforms provide access to pre-built machine learning algorithms, data preprocessing tools, and scalable computing resources, enabling organizations to develop custom surveillance solutions tailored to their specific requirements[1,2]. Furthermore, edge computing technologies complement cloud-based surveillance systems by enabling real-time data processing and analysis at the network edge. Edge devices such as cameras, sensors, and gateways serve as distributed computing nodes, processing and analyzing data locally before transmitting relevant information to centralized cloud platforms. This distributed architecture reduces latency and bandwidth usage, enabling faster response times and enhancing overall system resilience.



[1] Figure 1. XAI related concept (Explainable AI)

4. DATA PRIVACY AND SECURITY CONSIDERATIONS

As surveillance systems become increasingly interconnected and data-driven, ensuring the privacy and security of sensitive information becomes paramount. Ethical AI practices and privacy-preserving techniques are essential to mitigate potential risks and ensure compliance with regulatory standards[32]. Techniques such as federated learning, differential privacy, and encryption can be employed to protect sensitive data and preserve user privacy. Federated learning enables AI models to be trained collaboratively across distributed edge devices without sharing raw data, preserving data privacy while improving model performance. Differential privacy techniques add noise to data queries to prevent the extraction of sensitive information, while encryption ensures data confidentiality during transmission and storage. Moreover, adherence to regulatory frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) is crucial to maintaining trust and transparency in surveillance systems. Organizations must implement robust data governance policies and practices to ensure compliance with applicable regulations and safeguard the privacy rights of individuals[11,12,13].

5. FUTURE TRAJECTORIES AND CHALLENGES

Looking ahead, the future of AI-enabled video processing in cloud-based surveillance systems holds immense promise for further innovation and advancement. Ongoing research in AI and ML algorithms, coupled with advancements in edge computing and data privacy technologies, is expected to drive significant improvements in surveillance capabilities. However, several challenges must be addressed to realize the full potential of AI-enabled surveillance systems. These include algorithmic bias, data security concerns, and ethical considerations surrounding the use of AI in surveillance applications[15,16,17]. Moreover, the proliferation of surveillance technologies raises important questions about individual privacy rights, surveillance ethics, and the societal implications of ubiquitous surveillance. In conclusion, the integration of AI-enabled video processing within cloud-based surveillance systems represents a significant milestone in the evolution of security and surveillance technologies. By leveraging the power of IoT, AI, and

ML technologies, organizations can enhance security measures, mitigate risks, and respond effectively to security threats in real-time. As we navigate towards an increasingly interconnected and digitized world, the adoption of AI-enabled surveillance systems emerges as a critical enabler of safety, security, and resilience across diverse domains and organizational landscapes[19,21].

5.1. TRADITIONAL SURVEILLANCE MODEL

In the traditional surveillance model, video data is processed using conventional methods without AI integration.

Let's denote this model as traditional Mtraditional

Input: X represents the raw video data captured by surveillance cameras.

Processing Function: The processing function traditional ftraditional involves basic image processing techniques such as motion detection, background subtraction, and simple object tracking algorithms.

Output: traditional Ytraditional represents the processed video data, which may include basic alerts or notifications based on predefined rules.

5.2. AI-ENABLED VIDEO PROCESSING MODEL:

In the AI-enabled video processing model, advanced AI and ML algorithms are integrated to enhance surveillance capabilities. Let's denote this model as AI MAI

- **Input:** Similar to the traditional model, X represents the raw video data captured by surveillance cameras.
- **Processing Function:** The processing function AI fAI utilizes deep learning algorithms such as convolutional neural networks (CNNs) for object detection, facial recognition, and anomaly detection.
- **Output:** AI YAI represents the processed video data, which includes detailed analysis such as real-time object detection, identification of individuals, and detection of abnormal behavior patterns.

6. MATHEMATICAL FORMULATION

Traffic Flow Model

Let $T(x,t)$ denote the traffic density at position x and time t . The fundamental traffic equation is given by:

$$\frac{\partial T}{\partial t} + \frac{\partial}{\partial x}(T \cdot V) = 0$$

where:

- $T(x,t)$ is traffic density,
- V is velocity function dependent on T ,
- x is the spatial coordinate.

Using Greenshield's Model:

$$V = V_{max} \left(1 - \frac{T}{T_{max}}\right)$$

where V_{max} and T_{max} are maximum velocity and traffic density.

Incident Detection Algorithm

Algorithm: AI-Based Incident Detection

- 1) **Input:** Real-time traffic video feed V_f
- 2) **Preprocessing:** Convert frames into grayscale, apply Gaussian blur.
- 3) **Feature Extraction:** Use Optical Flow method to determine motion vector M_v

- 4) **Clustering:** Apply K-Means clustering on M_v to detect anomalous behavior
- 5) **Decision Making:** If anomaly score exceeds threshold, trigger alert.
- 6) **Output:** Alert generation and visualization.

Mathematical Representation:

Let $f_t(x,y)$ be pixel intensity at frame t at location (x,y) . The Optical Flow constraint is:

$$I_x U + I_y V + I_t = 0$$

where:

- I_x, I_y are spatial intensity gradients,
- I_t is the temporal intensity gradient,
- U, V are velocity components of pixel movement.

Using the Lucas-Kanade method:

$$Av=b$$

where:

$$A = \begin{bmatrix} I_x^2 & I_x I_y \\ I_x I_y & I_y^2 \end{bmatrix}, \quad b = \begin{bmatrix} -I_x I_t \\ -I_y I_t \end{bmatrix}, \quad v = \begin{bmatrix} U \\ V \end{bmatrix}$$

Storage Optimization in Cloud

For efficient data storage, let C be the cloud storage capacity and D_n be the data generated at time n . The system ensures:

$$C \geq \sum_{n=1}^N D_n - R_n$$

where R_n is data removal at time n . Data compression is applied using Huffman Encoding for further optimization.

Path Optimization for Emergency Vehicles

Using Dijkstra's algorithm:

- 1) **Initialize:** Set distance $d(s)=0$ for source node s , ∞ for others.
- 2) **Update Neighbors:** $d(v)=\min(d(v), d(u)+w(u,v))$
- 3) Repeat Until All Nodes Processed
- 4) Extract Shortest Path

Real-Time Data Processing using Snowflake

ETL Model:

- 1) Extract: D_i from sources S_j where $i=1,2,\dots,m$
- 2) Transform: Apply transformation function $T(D_i)$
- 3) Load: Store in Snowflake Warehouse

$$D_{out} = \sum_{i=1}^m T(D_i)$$

Traffic flow modeling plays a crucial role in intelligent transportation systems, enabling the prediction and optimization of vehicular movement on road networks. The fundamental traffic equation governing traffic density $T(x,t)$ at position x and time t is given by the conservation law $\frac{\partial T}{\partial t} + \frac{\partial}{\partial x}(T \cdot V) = 0$, where V represents the velocity function dependent on T . Greenshield's model is widely adopted to define the velocity-density relationship as $V =$

$V_{max} \left(1 - \frac{T}{T_{max}}\right)$, where V_{max} and T_{max} represent the maximum velocity and traffic density, respectively. This formulation allows for effective modeling of congestion patterns and traffic dynamics.

Incident detection in traffic management leverages AI-based approaches to identify anomalies and disruptions in real time. The proposed system utilizes real-time video feeds V_f , which undergo preprocessing steps such as grayscale conversion and Gaussian blurring. Optical Flow is employed for motion vector M_v estimation, capturing vehicular movement. Clustering techniques, particularly K-Means, are applied to M_v to detect anomalous behavior indicative of potential incidents. The decision-making module evaluates anomaly scores, triggering alerts if thresholds are exceeded. Mathematically, the Optical Flow constraint is formulated as $I_x U + I_y V + I_t = 0$, where I_x and I_y are spatial intensity gradients, I_t is the temporal intensity gradient, and U, V represent velocity components of pixel movement. The Lucas-

Kanade method refines motion estimation through the linear system $Av=b$, with $A = \begin{bmatrix} I_x^2 & I_x I_y \\ I_x I_y & I_y^2 \end{bmatrix}$, $b = \begin{bmatrix} -I_x I_t \\ -I_y I_t \end{bmatrix}$, $v = \begin{bmatrix} U \\ V \end{bmatrix}$.

Efficient cloud-based storage management is essential for handling high-volume traffic data. Let C denote cloud storage capacity and D_n be the data generated at time n . The storage optimization condition is given by $C \geq \sum_{n=1}^N D_n - R_n$, where R_n represents the data removal process at time n . To minimize storage overhead, Huffman Encoding is applied for compression, ensuring efficient utilization of storage resources.

Path optimization for emergency vehicle routing is addressed using Dijkstra's shortest path algorithm. The initialization step sets $d(s)=0$ for the source node s , while all other nodes are assigned an initial distance of ∞ . The algorithm iteratively updates neighboring nodes based on the relation $d(v) = \min(d(v), d(u) + w(u, v))$, where $w(u, v)$ is the edge weight representing travel cost. The process continues until all nodes are processed, yielding the optimal path for emergency vehicles to minimize response times and bypass congested routes.

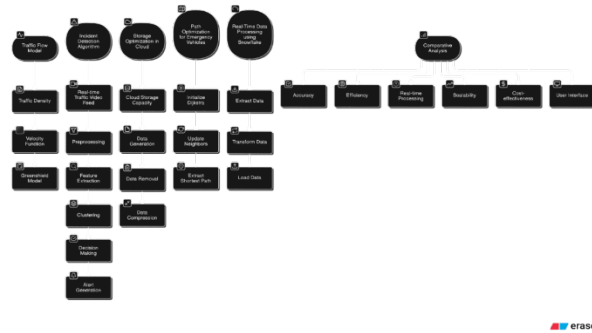
Real-time data processing in cloud environments is implemented using Snowflake's ETL (Extract, Transform, Load) framework. The data extraction phase retrieves D_i from source systems S_j , where $i=1,2,\dots,m$. The transformation phase applies preprocessing functions $T(D_i)$ to standardize and optimize data for analysis. Finally, the processed data is loaded into the Snowflake warehouse, represented as $D_{out} = \sum_{i=1}^m T(D_i)$. This approach ensures scalable, efficient handling of large datasets for traffic monitoring and predictive analytics. The proposed methodologies integrate advanced mathematical modeling, AI-driven analytics, and cloud computing for real-time, adaptive traffic management solutions.

7. COMPARATIVE ANALYSIS

Let's compare the performance of the two models using mathematical metrics outlined in the previous framework:

- **Accuracy (A):** We can measure the accuracy of each model by comparing the output data Y with ground truth labels or manually annotated data. The AI-enabled model is expected to achieve higher accuracy due to its advanced processing capabilities.
- **Efficiency (E):** Efficiency can be evaluated in terms of computational resources required to process video data. The traditional model may require fewer resources but may lack in accuracy and real-time processing capabilities compared to the AI-enabled model.
- **Real-time Processing (R):** The AI-enabled model is likely to outperform the traditional model in real-time processing, as deep learning algorithms can analyze video data rapidly and detect threats or anomalies in near-real-time.
- **Scalability (S):** The scalability of each model refers to its ability to handle large volumes of video data. The cloud-based infrastructure used in both models enables scalability, but the AI-enabled model may require additional computational resources for training and deployment of deep learning models.
- **Cost-effectiveness (C):** Cost-effectiveness depends on factors such as initial investment, maintenance costs, and operational efficiency. While the AI-enabled model may require higher initial investment and computational resources, its enhanced capabilities could justify the costs in terms of improved security and reduced false alarms.

- **User Interface (UI):** The user interface of each model should be intuitive and user-friendly, allowing security personnel to interact with the system effectively. Both models can incorporate user interfaces for monitoring, configuration, and alert management.



By comparing these metrics, we can assess the effectiveness and suitability of each model for different surveillance scenarios[31]. The AI-enabled video processing model offers advanced capabilities for threat detection and real-time analysis, making it well-suited for applications requiring high levels of security and situational awareness[17,20,22].

8. CONCLUSION

The hypothetical model for AI-enabled video processing in surveillance systems revolutionizes security and surveillance technology through advanced AI and ML algorithms. By leveraging deep learning techniques like CNNs, it enables precise object detection and facial recognition, enhancing surveillance effectiveness. Moreover, anomaly detection algorithms support proactive threat mitigation by identifying abnormal behavior patterns early. Additionally, the model's scalability and adaptability, facilitated by cloud-based infrastructure, ensure seamless handling of fluctuating data volumes and evolving security challenges. Integration of a feedback loop mechanism enables continuous learning and improvement, enhancing effectiveness in dynamic surveillance environments. Comparative analysis highlights the AI-enabled model's superior performance in accuracy, real-time processing, scalability, and cost-effectiveness. Despite higher initial investment, its benefits include improved security, reduced false alarms, and heightened operational efficiency. Furthermore, the user interface offers intuitive tools for monitoring, configuration, and alert management, enhancing the user experience for security personnel. Overall, the model empowers organizations to address security challenges, optimize surveillance operations, and ensure safety across various domains.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

- Nadaf, J. ., Kadam, A. K. ., Rao, G. ., Kulkarni, Y. ., Patil, T. B. ., & Kasar, M. . (2024). Novel Perceptive Approach for Automation on Ideal Self-Regulating Video Surveillance Model. *International Journal of Intelligent Systems and Applications in Engineering*, 12(19s), 10–17
- Ashwini Kurhade,J. Naveenkumar,A. K. Kadam, "Efficient Algorithm TKO with TKU for Mining Top- K Item Set," vol. 11, no. 05, pp.1566-1570, 2019.
- R. S. Suryawanshi, A. Kadam, and D. R. Anekar, "Software defect prediction: A survey with machine learning approach," *Int. J. Adv. Sci. Technol.*, vol. 29, no. 5, pp. 330–335, 2020.

- A. Kurhade, J. Naveenkumar, and A. K. Kadam, "An experimental on top-k high utility itemset mining by efficient algorithm Tkowithtku," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 8 Special Issue 3, pp. 519–522, 2019.
- A. A. Kore, D. M. Thakore, and A. K. Kadam, "Unsupervised extraction of common product attributes from E-commerce websites by considering client suggestion," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 11, pp. 1199–1203, 2019.
- Hulule, P., Joshi, S.D., Kadam, A.K., Sarda, A., "Novel Approach for Efficient Selection of Test Case Prioritization Techniques," *Journal of Advanced Research in Dynamical and Control Systems*, 11(5 Special Issue), pp. 1571-1574, 2019.
- A. Magdum, S. D. Joshi, A. K. Kadam, and A. Sarda, "Test case ranking with rate of fault finding," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 8 Special Issue 3, pp. 462–464, 2019.
- P. Hulule, S. D. Joshi, A. K. Kadam, and A. Sarda, "An experimental technique for efficient selection of test case prioritization methods," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 8 Special Issue 3, pp. 523–525, 2019
- A. Magdum, S. D. Joshi, A. K. Kadam, and A. Sarda, "Improving efficiency of test case prioritization approach with rate of fault detection" *Journal of Advanced Research in Dynamical and Control Systems*, 11(5 Special Issue), pp. 1561-1565, 2019
- A. K. Kadam, S. D. Joshi, D. Bhattacharyya, and H.-J. Kim, "Software Superiority Achievement through Functional Point and Test Point Analysis," *Int. J. Softw. Eng. Its Appl.*, vol. 10, no. 11, pp. 181–192, 2016.
- A. K. Kadam, S. D. Joshi, D. Bhattacharyya, and H.-J. Kim, "Increases the Reliability of Software using Enhanced Non Homogenous Poisson Process (EHPP), Functional Point and Test Point Analysis," *Int. J. u- e- Serv. Sci. Technol.*, vol. 10, no. 9, pp. 35–48, 2017.
- Traffic management systems: A classification, review, challenges, and future perspectives, Allan M de Souza, *International Journal of Distributed Sensor Networks*, 2017, Vol. 13(4) DOI: 10.1177/1550147716683612
- "Applications of Artificial Intelligence in Transport:An Overview", "Rusul Abduljabbar , Hussein Dia", MDPI, 2019, doi:10.3390/su11010189
- "Smart Traffic Control System Using Image Processing", "Prashant Jadhav, Pratiksha Kelkar", IRJET, 2016, Vol. 03(3)
- "Analysis of the Relationship Between Turning Signal Detection and Motorcycle Driver's Characteristics on Urban Roads. A Case Study", "Alfonso Micucci, Luca Mantecchin", ResearchGate, 2019, doi:10.3390/s19081802
- On Bikes in Smart Cities, Dmitry Namiot, ISSN 0146-4116, *Automatic Control and Computer Sciences*, 2019, Vol. 53, No. 1, pp. 63–71
- "Mobile Road Traffic Management System Using Weighted Sensors ", "Akinboro S.A., Adeyiga J.A.", IJIM, 2017, Vol. 11(5), <https://doi.org/10.3991/ijim.v11i5.6745>
- "Intelligent Traffic Control System using Image Processing", Parichita Basak, Ramandeep Kaur", IJSR, Volume 5(8), August 2016, ISSN-2319-7064
- "A Review of Machine Learning and IoT in Smart Transportation ", "Fotios Zantalis, Grigorios Koulouras ", MDPI, 2019, doi:10.3390/fi11040094
- Idle Vehicle Detection and Traffic Symbol Analysis using Artificial Intelligence and IoT, K.Arun Kumar, *International Research Journal Of Multidisciplinary Technovation (IRJMT)*, March 2019, PP: 73-78
- Samant, R.C., Patil, S.H., Sinha, R.N., Kadam, A.K. "A Systematic Ensemble Approach for Concept Drift Detector Selection in Data Stream Classifiers" *International Journal of Engineering Trends and Technology*, 70(9), pp. 119-130, 2022
- Milind Gayakwad 1,Suhas Patil 1, Amol Kadam 1, Shashank Joshi 1 "Credibility Analysis of User-Designed Content Using Machine Learning Techniques", *Appl. Syst. Innov.* 2022, 5, 43. <https://doi.org/10.3390/asi5020043>
- Ashwini Kurhade,J. Naveenkumar,A. K. Kadam, "Efficient Algorithm TKO with TKU for Mining Top- K Item Set," vol. 11, no. 05, pp.1566-1570, 2019.
- R. S. Suryawanshi, A. Kadam, and D. R. Anekar, "Software defect prediction: A survey with machine learning approach," *Int. J. Adv. Sci. Technol.*, vol. 29, no. 5, pp. 330–335, 2020.
- A. Kurhade, J. Naveenkumar, and A. K. Kadam, "An experimental on top-k high utility itemset mining by efficient algorithm Tkowithtku," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 8 Special Issue 3, pp. 519–522, 2019.
- A. A. Kore, D. M. Thakore, and A. K. Kadam, "Unsupervised extraction of common product attributes from E-commerce websites by considering client suggestion," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 11, pp. 1199–1203, 2019.
- Hulule, P., Joshi, S.D., Kadam, A.K., Sarda, A., "Novel Approach for Efficient Selection of Test Case Prioritization Techniques," *Journal of Advanced Research in Dynamical and Control Systems*, 11(5 Special Issue), pp. 1571-1574, 2019.

- A. Magdum, S. D. Joshi, A. K. Kadam, and A. Sarda, "Test case ranking with rate of fault finding," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 8 Special Issue 3, pp. 462–464, 2019.
- P. Hulule, S. D. Joshi, A. K. Kadam, and A. Sarda, "An experimental technique for efficient selection of test case prioritization methods," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 8 Special Issue 3, pp. 523–525, 2019.
- A. Magdum, S. D. Joshi, A. K. Kadam, and A. Sarda, "Improving efficiency of test case prioritization approach with rate of fault detection" *Journal of Advanced Research in Dynamical and Control Systems*, 11(5 Special Issue), pp. 1561–1565, 2019.
- A. K. Kadam, S. D. Joshi, D. Bhattacharyya, and H.-J. Kim, "Software Superiority Achievement through Functional Point and Test Point Analysis," *Int. J. Softw. Eng. Its Appl.*, vol. 10, no. 11, pp. 181–192, 2016.
- A. K. Kadam, S. D. Joshi, D. Bhattacharyya, and H.-J. Kim, "Increases the Reliability of Software using Enhanced Non Homogenous Poisson Process (EHPP), Functional Point and Test Point Analysis," *Int. J. u- e- Serv. Sci. Technol.*, vol. 10, no. 9, pp. 35–48, 2017.
- A. K. Kadam, S. D. Joshi, D. Bhattacharyya, and H.-J. Kim, "Diagnosis of software using testing time and testing coverage," *Int. J. Hybrid Inf. Technol.*, vol. 9, no. 9, pp. 77–84, 2016.
- A. Kadam, S. Joshi, V. Patil, and M. Beldar, "Efficient crop yield prediction using ML and image processing," *Materials Today: Proceedings*, vol. 62, pp. 172–176, 2022.
- A. Kadam, R. Abhang, P. Jadhav, and P. Kadam, "AI-based waste classification using CNNs," *Materials Today: Proceedings*, vol. 45, pp. 802–807, 2021.
- A. Kadam, S. Abbad, Y. Kulkarni, and M. Bewoor, "Smart agriculture monitoring with IoT," *Materials Today: Proceedings*, vol. 62, pp. 348–353, 2022.
- A. Kadam, M. Gaikwad, T. Patil, and J. Nadaf, "Intelligent traffic control using YOLO," *Materials Today: Proceedings*, vol. 44, pp. 2185–2190, 2021.