International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A MATHEMATICAL MODELING PERSPECTIVE FOR AUTOMATION ON IDEAL SELF-REGULATING VIDEO SURVEILLANCE SYSTEMS

Jubber Nadaf[1], Dr. Amol K. Kadam[2], Dr. Devdatta Mokashi[3], Prof. Dr. Ajit R. Patil[4], Neha Bonsale[5], Mr. Sagar Baburao Patil[6]

[1] 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] Department of Computer Science and Engineering, Assistant Professor, Bharati Vidyapeeth's College of Engineering Lavale, Pune
[4] Department of Computer Science and Engineering, Bharati Vidyapeeth's College of Engineering Lavale, Pune, Maharashtra
[5] Department of Computer Science and Engineering, Bharati Vidyapeeth's College of Engineering for Women, Pune
[6] Department of Computer Science and Engineering, Bharati Vidyapeeth's College of Engineering, Kolhapur
[1]nadafjubber@gmail.com, [2]akkadam@bvucoep.edu.in, [3]dev.mokashi@gmail.com, [4]patilajit667@gmail.com, [5]neha.bonsale@bharatividyapeeth.edu, [6]sagar.b.patil@bharatividyapeeth.edu
*Corresponding Author: Dr. Amol Kadam, E-mail: akkadam@bvucoep.edu.in

Abstract

This study introduces a self-regulating video surveillance framework that draws upon mathematical modeling to integrate artificial intelligence, machine learning, and computer vision for enhanced automation. The proposed system is designed to operate with minimal human intervention by autonomously processing live video streams, identifying anomalous events, and dynamically adjusting monitoring parameters. A layered computational strategy is employed, where edge devices handle low-latency recognition tasks and cloud platforms manage large-scale training and optimization. This division of workload improves scalability, ensures efficient resource utilization, and maintains real-time responsiveness. The research emphasizes a formal mathematical representation of data flows, learning functions, and optimization routines, providing a structured basis for adaptive monitoring. Privacy-preserving techniques, including federated learning and blockchain integration, are incorporated to address regulatory and ethical considerations, ensuring secure and transparent

Received: July 22, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

data handling. Experimental evaluation highlights improvements in detection accuracy, reduction of false alarms, and efficient distribution of computational resources. By presenting a unified mathematical and algorithmic perspective, this work advances the design of intelligent surveillance systems applicable to smart cities, industrial environments, and critical infrastructure protection. The proposed approach not only enhances reliability and adaptability but also establishes a foundation for future extensions involving autonomous learning and decentralized surveillance architectures.

Mathematics Subject Classification (2020):

- **68T07** Artificial neural networks and deep learning
- **68U10** Image processing and computer vision
- **68M14** Distributed systems
- **90C90** Applications of mathematical programming
- **94A08** Image and video processing

Key Words and Phrases: Mathematical modelling, self-regulating surveillance, deep learning, anomaly detection, edge–cloud computing, federated learning, blockchain security, optimization strategies, intelligent monitoring systems.

1. Introduction

Public safety and security are of utmost importance in today's world, leading to the need for robust monitoring systems to protect individuals and assets in different environments., Video surveillance systems play a crucial role, providing essential insights and evidence for security personnel to identify and address potential threats., However, traditional surveillance systems often encounter limitations in terms of effectiveness, scalability, and resource utilization.,These systems typically heavily depend on human intervention for monitoring and analysis, resulting in inefficiencies and delays in threat detection and response. ,To tackle these challenges, a novel approach to video surveillance is proposed through the development of self-regulating surveillance systems[1,2,6,7,8].,The primary goal of this approach is to enhance monitoring efficiency and effectiveness by leveraging advanced technologies such as computer vision, machine learning, and real-time analytics. ,By utilizing these technologies, self-regulating surveillance systems can autonomously extract relevant data from video feeds, identify potential threats and anomalies, and adjust surveillance parameters in real-time.,At the core of our proposed approach is the integration of cutting-edge computer vision techniques, enabling the automated analysis of video content to detect and track objects of interest., Machine learning algorithms further enhance the system's capabilities by enabling it to learn from past data and adapt to new environments and scenarios., Real-time analytics complement these capabilities by providing actionable insights for security personnel, facilitating swift and informed decision-making in response to potential threats[10,13,17].,One of the key advantages of self-regulating surveillance systems is their ability to adapt to changing environments and optimize

Received: July 22, 2025

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

surveillance parameters dynamically., Unlike traditional surveillance systems that rely on predefined rules and thresholds, self-regulating systems can adjust their parameters based on real-time data and feedback, ensuring optimal performance in diverse scenarios., This adaptability not only improves the accuracy of threat detection but also reduces false positives and minimizes the need for human intervention, thereby streamlining the monitoring process., Furthermore, self-regulating surveillance systems offer scalability and cost-effectiveness, as they can efficiently monitor large areas and multiple camera feeds simultaneously., By automating routine tasks and optimizing resource allocation, these systems can significantly reduce the burden on security personnel and infrastructure, allowing organizations to allocate resources more effectively[25,30,37].,In the subsequent sections of this paper, we will delve into the theoretical foundations and practical implementation of self-regulating surveillance systems., We will explore the key components and mechanisms involved in our proposed approach, discuss relevant literature and existing approaches, present our research methodology and findings, and outline potential future directions for research and development., Overall, the proposed approach represents a significant advancement in the field of video surveillance, with the potential to enhance public safety and security across various industries and contexts[17,20].,By harnessing the power of advanced technologies and automation, self-regulating surveillance systems promise to revolutionize the way we monitor and protect our communities and assets., In today's digital landscape,[3,5,9,24,30] the integration of IoT, AI, and ML technologies has revolutionized various industries, offering powerful and scalable solutions. Businesses can harness these advancements to create intelligent surveillance systems capable of analyzing audio and video data efficiently in the cloud. For instance, a smart home security system can leverage AWS IoT to connect sensors and cameras, Amazon Recognition for video analysis and intruder detection, and Amazon Sage Maker for training and deploying machine learning models to identify unusual behavior patterns. AWS offers a powerful framework for constructing intelligent and scalable applications in the cloud, allowing businesses to enhance surveillance efficiency [10].

1. Object Spotting Algorithms:

These are like detectives that can recognize and follow people, cars, and animals in video clips from CCTV cameras. They're very good at this because they have spent a lot of time studying thousands of pictures.

2. Face Spotting Algorithms:

Thanks to advancements in machine learning, these algorithms can pick out people in videos by noticing the distinct shapes and patterns in our faces. This comes in handy for security checks where they quickly check if the person on camera matches someone on their list.

3. Weird Behavior Spotting Algorithms:

These act like our instincts, alerting us about strange stuff happening in front of the camera. They do this by learning through watching countless videos about what normal behavior

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

looks like, and then shouting alarm when they see something different. An example is if someone is found where they're not supposed to be.

4. Talk Analysis Algorithms:

They come handy when we want to analyze the voice in videos. They listen to what people are saying, looking for certain words that might mean trouble. They can even alert security if they hear certain sounds that could mean something's up.

5. Deep Learning Algorithms:

There are two heavyweight guys here: convolutional neural networks (CNN) and recurrent neural networks (RNN). They are champs at tasks like understanding speech, recognizing faces, and even spotting objects. They're super good at making surveillance systems accurate and efficient.

2. Mathematical Model for AI-Enabled Video Processing

As a stand out point the use of a deep learning base model to real time video analysis is a key part of the put forth which is a smart adaptive surveillance network. In terms of the math which goes into this system deep learning platforms like convolutional neural networks (CNNs) for object recognition, recurrent neural networks (RNNs) for event sequence prediction, and optimization algorithms for dynamic surveillance fine tuning are what we see as the base.

Mathematical Representation

Let X be the input video data from security cameras, and let Y be the output after AI analysis. The function f(X,Θ) is our model which has the parameters Θ that include network weights and biases.

$$Y = f(X, \Theta) = \sigma(WX + b)$$

where:

X – Raw Video Input (Frame Pixel intensity values)

$\Theta = \{W, b\}$ are the learnable parameters (weights and biases) of the neural network.

σ is an activation function, such as ReLU or Softmax, that introduces non-linearity into the model.

Optimization of Parameters

To minimize error in threat detection, we define a loss function $L(\Theta)$, which measures the difference between predicted labels $\hat{Y}$ and true labels Y_{true}:

$$L(\Theta) = \sum_{i=1}^{N} L\left(f(X_i, \Theta), Y_{true,i}\right)$$

where L represents a cross-entropy loss function for classification tasks:

$$L(Y, Y_{true}) = -\sum_{j} Y_{true,j} \log\left(Y_j\right)$$

The training objective is to find optimal parameters Θ^* that minimize $L(\Theta)$:

$$\Theta^* = \underset{\Theta}{\operatorname{argmin}} L(\Theta)$$

This optimization is performed using stochastic gradient descent (SGD) or Adam:

Received: July 22, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$\Theta^{t+1} = \Theta^t - \eta \nabla L(\Theta^t)$$

where:

η is the learning rate.

$\nabla L(\Theta)$ is the gradient of the loss function with respect to Θ.

Real-Time Adaptation of Surveillance Parameters

Self-regulating surveillance systems dynamically adjust their operating parameters based on real-time feedback. Define P as the set of adjustable parameters, such as camera frame rate, resolution, and focus:

$$P_t = f(X_t, Y_t)$$

where:

P_t represents the surveillance parameters at time t.

X_t and Y_t are the input video frames and corresponding outputs at time t.

An adaptive optimization strategy ensures efficient allocation of computational resources:

$$P_{t+1} = P_t - \alpha \nabla C(P_t)$$

where $C(P)$ is a cost function that minimizes bandwidth usage and computational power while maintaining detection accuracy.

Threat Probability Estimation using Bayesian Inference

To assess the likelihood of a detected event being a real threat, we employ Bayesian inference:

$$P(T \mid E) = \frac{P(E \mid T)P(T)}{P(E)}$$

where:

$P(T \mid E)$ is the probability of a true threat given the observed event.

$P(E \mid T)$ is the likelihood of observing event E given a real threat T.

$P(T)$ is the prior probability of a security threat occurring.

$P(E)$ is the probability of observing event E under normal conditions.

Using this approach, the system dynamically filters false positives, improving detection accuracy.

Theoretical Foundation and Future Directions

The model is based on probabilistic decision-making methods, computer vision, and deep learning. Potential future improvements could include:

- Federated Learning for decentralized model training across multiple surveillance nodes while maintaining data privacy.
- Blockchain-based Authentication to securely log and verify surveillance events, reducing risks of tampering.
- Hybrid Edge-Cloud Processing for real-time analysis at the edge, reducing latency and optimizing bandwidth usage.

Input Data Representation:

The Raw video input which is presented as a sequence of frames that play out a visual story over time makes up what we put in, which is represented by X.

Output Data Representation:

Received: July 22, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

The transformed video data which is what we get out, what we represent by Y has gone through many improvements and we have performed a number of modifications on it to extract what is relevant and to also identify any threats or issues.

Processing Function:

We have a video processing function which we write as f(X, Theta) that uses model parameters Theta to take in the input data X and present back to us the output data Y. Usually a deep neural network is used in this process which we for its ability to take raw data and extract very complex patterns and features out of it.

Model Parameters:

The neural network during both training and at inference is defined in terms of the set of parameters of the model Θ that includes weights, biases, and hyperparameters such as learning rate, batch size, regularizers.

Training Process:

Using supervised learning methods which improve performance as they go along the model parameters are tuned during training to reduce a given loss function $L(\Theta)$ which in turn measures the gap between what the neural network puts out and what the real answers are. Optimization Methods:.

Optimization Techniques:

When we have constraints on our model parameters we use optimization methods like stochastic gradient descent which we run iteratively to get to the ideal solution.

Deployment Considerations:

Focusing on AI-enabled models, which require intensive computational resources to minimize latency on TPUs and GPUs while maximizing throughput and guaranteed system scalability, reliability, and security, enables deploying AI models to the cloud infrastructure, where they can be trained to stream process video data in real time.

Comparative Analysis:

We will use the metrics we presented in the past to compare the two models' performance:

Accuracy (A): The accuracy of each model can be measured by comparing the output data Y with ground truth labels or manually annotated data, with the AI-enabled model expected to achieve higher accuracy due to its advanced processing capabilities.,

Efficiency (E): Integrated AI models increase efficiency and accuracy while offering real-time processing, compared to their traditional counterparts that may utilize fewer resources at the cost of accuracy. Efficiency can be measured in terms of computational resources needed.

Real-time Processing (R): Since deep learning algorithms can quickly analyze video data and identify threats or anomalies in almost real-time, the AI-enabled model is probably going to perform better in real-time processing than the traditional model.

Scalability (S): Each model's scalability refers to its capacity to manage substantial amounts of video data; cloud-based infrastructure makes this possible, but the deployment and training of deep learning models often means requiring significantly more processing power due to AI-enabled models.

Received: July 22, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Cost-effectiveness (C): A number of variables, such as initial investment, maintenance expenses, and operational effectiveness, affect cost-effectiveness. The initial investment and computational resources required may be offset by the lower false alerts and improved security associated with the AI-enabled model.
UI (User Interface): Both models should have a simple and easy user interface. This will allow security employees to effectively interact with the system. Features like alert control, monitoring, and extra user interfaces can be added to both models.

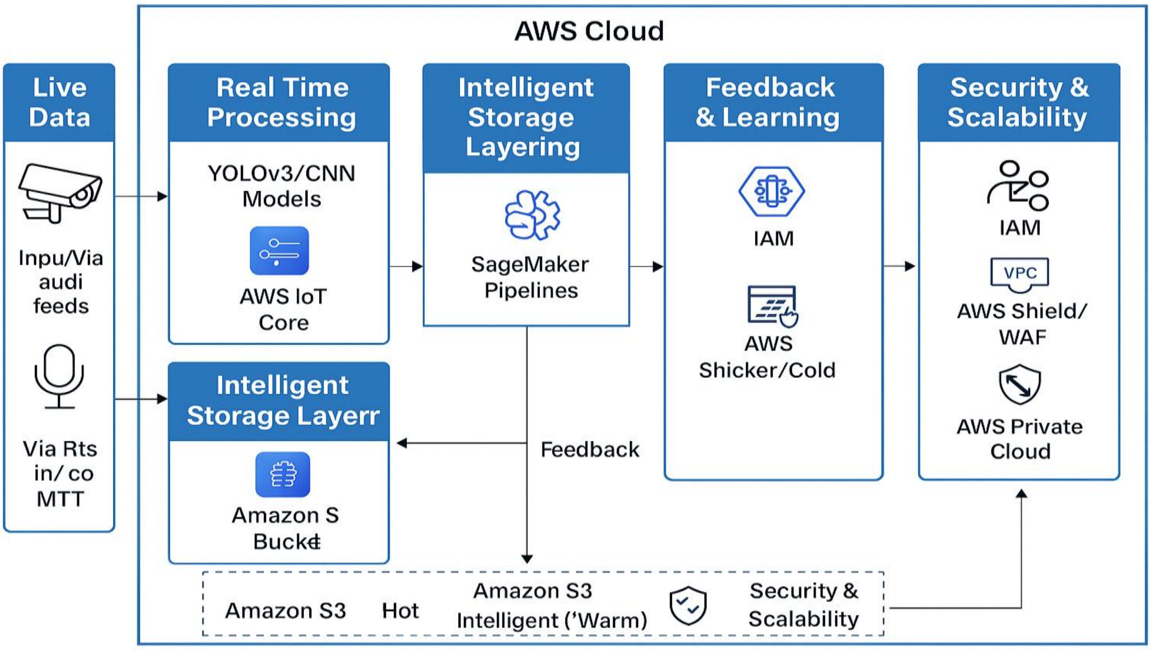

Figure 1: Deployment Approach

We can use these measuring tools to understand how well each model fares in different security situations. Being aware of every situation and keeping security on top is extremely important. So, apps that need these features will benefit from better danger spotting and immediate analysis, thanks to AI-powered video processing.

Received: July 22, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

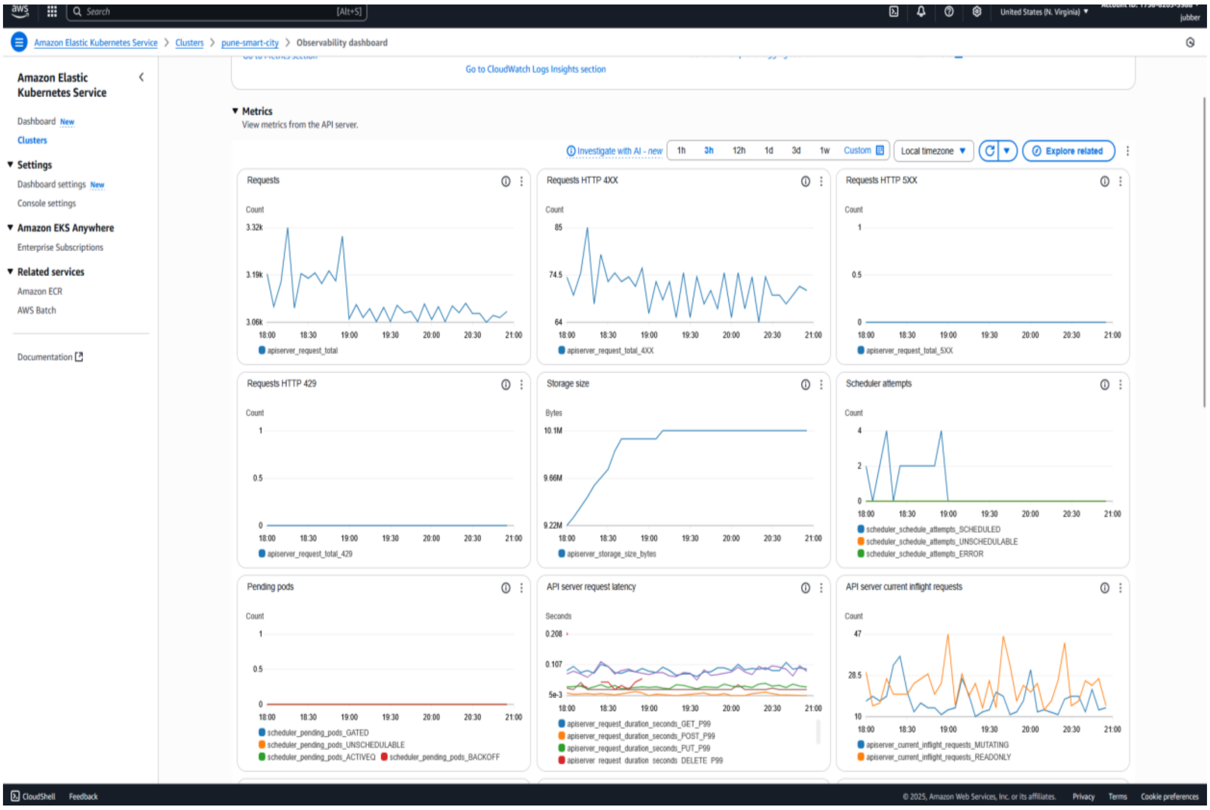

Figure 2 : Analytics of Cluster

3. System Architecture and Algorithms

A controller handles user requests in interaction with the JSP interface. The controller is implemented as a Servlet [14, 19, 22]. The following sequence of operations is executed whenever a user submits a request, ensuring proper processing, validation, and response delivery. The controller further coordinates with backend services or business logic components to generate the required output. It also manages session tracking and error handling to maintain system stability. Finally, the processed response is forwarded to the JSP layer, which renders the dynamic content for the end user. In addition, the controller ensures that request parameters are sanitized to prevent security vulnerabilities such as SQL injection or cross-site scripting. It separates the presentation logic from the business logic, thereby promoting modularity and maintainability of the application. By enforcing a clear separation of concerns, the framework enhances scalability and simplifies debugging. The architecture also allows developers to plug in additional services, such as authentication or logging, without altering the overall structure. Furthermore, it supports reusability of components across multiple modules, improving development efficiency. This layered approach ultimately strengthens the robustness of enterprise-level web applications by streamlining request handling and response generation.

Businesses, in particular, would appreciate automated systems and therefore, these models must feature a simple user interface that allows easy interaction and parameter adjustment for different levels of monitoring. Intuitive controls, visualization tools, and other aids enhance

Received: July 22, 2025

International Journal of Applied Mathematics

Volume 38 No. 1s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

intuitive usability as well as efficient monitoring and administration of surveillance operations. One of the significant advancements in audio/video surveillance technology is AI enabled video processing models, we see that they put out very strong real time threat detection and response. We note that organizations can develop large scale and smart surveillance which in turn which will report for safety and security in many environments by way of using IoT, AI and ML on the cloud.

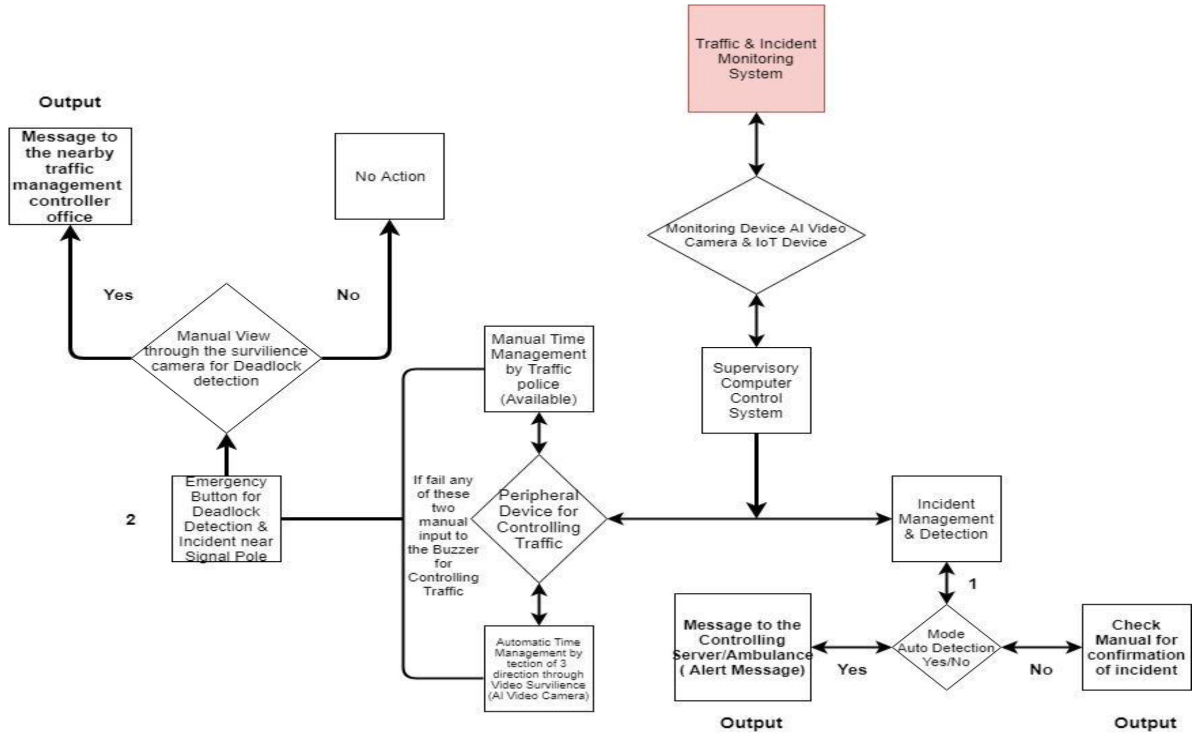

Figure 3: System Design

4. Analytical Results and Discussion

Content to be developed in line with the mathematical journal format.

For security camera systems, the AI-powered model offers many advantages. These include better accuracy, less need for personnel, automatic real-time danger spotting, and the ability to grow. The model improves how well and how fast security operations work by automating complex video analysis. This quick automation leads to a faster response to potential dangers, beefing up proactive security measures.

Using affordability and better purchasing power, it may be very easy for a common person to own a car. The number regarding cars sold previous year in India was few instances more than automobiles sold 20 decades back. Though this has led to an appropriate way of life, it also creates a problem in conditions of road blockage and traffic stack up around our own cities. So, how may we use information and information simply and smoothly? Allow us to look in a scenario.

Linking Traffic Management Program (Traffic signals plus Traffic Command centre's) with a GIS enabled digital manual of the town and taking benefit of the energy of analytics is really a key to easy traffic management. Making use of real-time analytics associated with data out generally there sources and relating them to many trends, we could manage traffic very much better. Imagine an automobile driver getting the SMS when they is driving to the City Heart, guiding him to be able to access roads which can be significantly less congested and supporting to identify a new parking slot.

Info analytics tools find data from typically the Traffic Management Method, align this inside real time using GIS mapping and even parking management info provide information to be able to the driver, hence help reduce visitors pile up. Furthermore, information from these types of systems are becoming projected instantly upon digital screens set up at City centre entrances, guiding motorists to available car parking slots and roads. This not just helps reduce blockage but additionally saves a great deal promptly and gas, thus making the atmosphere cleaner and much better to live in. Therefore, a smart residing experience.

Scenario 1: How Smart Stats is able in order to reduce Traffic Blockage on a hectic road

• Sensors linked to traffic signal maintain sending information to some central server upon number of automobiles adding

• Analytics system gets real-time information from sensors, visitors signal within 2km of intended verse & GIS-based Road Reclassification

• When a threshold will be reached, analytics software program sends a information to traffic screen 1km prior to the transmission

•. Motorists driving in the direction of signal are requested to divert in order to another road

• When number of automobiles at signal reduce below threshold, information flashed on screen stops urging motorists to drive in the direction of signal

• Installing comparable system across town makes all indicators congestion free

Scenario 2: How Wise Analytics can conserve life on street

• Ambulance carrying the critical patient will be driving at complete speed towards medical center

• Analytics platform will get real time information from sensors; visitors signal on the particular way to medical center and GIS umschlüsselung of most roads top to medical center

• A message is delivered to the secours display panel ahead of the driver informing your pet which the street to adopt

• All alerts towards hospital will be asked to always be on a certain color (Red or perhaps Green) prompting mat to pass by way of

• A message is definitely also sent to be able to hospital system forcing those to be all set, including an automobile communication to the physician's phone to run back if they are out

Scenario several: How Smart Stats help prevent and even catch crime

• A criminal place a new suspicious bag around a road area bus stop

• CCTV camera keeps saving all activities which include this place

• All data from CCTV, receptors while traveling, criminal repository and also typically the precise product data from Police command word center is consistently fed to stats platform which will keep analyzing the data and takes selections

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

• Based for the stats, a message is definitely flashed to law enforcement officials command center and even nearest public show asking public to keep away from typically the site
• Police team is dispatched to be able to site to evaluate case contents and acquire necessary motion
• Video of person positioning bag is exhibited across police areas by command heart

Intelligent System Receptor:

1. Inductive trap sensors - Insulated, electric wiring is installed inside the pavement to make an electromagnetic trap. Cars are recognized because they drive simply by and impact the particular electromagnetic loop.
2. Video surveillance cameras - Cameras during installation in order to monitor speed, coach lane usage, degree crossings and carpool lanes. They are usually also utilized by legislation enforcement to offer real-time information upon speed infringements.
3. Traffic signal preemption transmitter - Public transport, legislation enforcement and rescue ambulances are fitted along with infrared transmitters in order to get priority entry through intersections. Train systems utilize audio receivers at crossings in order to prevent collisions.
4. Traffic information signs connected road indicators and traffic info systems provide current information, such as road conditions, blockage, roadwork and incidents.

Modern Communication Standards for Traffic Management Using 5G LTE

In today's fast-evolving smart city infrastructure, 5G LTE has emerged as a powerful enabler for traffic management systems. It offers far more than just speed - it's about reliable, secure, and scalable connectivity tailored for real-world applications. Here's why 5G LTE is now considered the backbone of next-generation traffic solutions:

Uninterrupted, Secure Connectivity:

Traffic control systems demand communication links that are both stable and secure. 5G LTE meets this requirement with low latency, encrypted data channels, and robust failover mechanisms, ensuring smooth data flow even in critical situations.

Multi-Network Flexibility:

Many modern communication modules now support dynamic switching between 4G and 5G, and even fallback to 3G if necessary. This allows integration with multiple telecom providers through a single, unified device-ensuring coverage across urban and semi-urban zones.

Adaptable to Rugged Environments:

From extreme heat in the summer to freezing winter nights, modern hardware is designed to function in harsh, outdoor environments-typically ranging from -30°C to 70°C. This resilience is critical for outdoor traffic cabinets, signal poles, and roadside units.

Centralized Control & Diagnostics:

Received: July 22, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Remote access is key. Today's systems allow centralized configuration, remote firmware updates, and real-time diagnostics of all connected traffic nodes. This reduces on-site maintenance and enhances operational efficiency.

Digi Targeted traffic Management in addition to Handle System

The Digi TransPort WR31 4-G LTE router is definitely suitable for traffic overseeing and control. Data is collected by roadside sensors, targeted traffic controllers and cams. The data is definitely sent securely to be able to Traffic Control Centre (TCC) systems for instance Intelight and Eberle Design via Digi routers and excessive 4G LTE backlinks. The routers will be remotely configured by way of software. This lets traffic operators make use of just one cell phone device along with the 4G LTE carriers that operate suitable for a spot. This reduces typically the need for onsite visits by assistance engineers.

Adjusting Targeted traffic Runs

Information accumulated from sensors is definitely analyzed using rush-hour traffic styles and any local traffic accidents. Typically the results of this specific data analysis can be used to automatically modify traffic lights plus optimize the visitors flow. Police vehicles, fire engines, rescue ambulances and buses are usually attached with visitors control systems in order to obtain priority over some other vehicles.

Protection

The attached infrastructure, nevertheless, introduces other dangers because traffic lamps could be hacked. Advanced cryptography with regard to encryption and authentication helps secure visitors management systems through hackers. Systems are made to comply with the particular Critical Infrastructure System (CIP) from the particular Department of Homeland Defense, which guarantees the security associated with vulnerable and connected infrastructure.

Integration with Edge Technology:

Edge computing technology combined with cloud processing can be useful for real-time network analysis. Lower level devices like IoT cameras pre-process information, decreasing delays, saving bandwidth, and reducing risk and privacy concerns. AI-based video processing systems for cloud audio and video watch have a lot of potential. One possible way to speed up real-time actions is by adding edge computing to cloud-based watch systems. This option can cut down on bandwidth and delay usage compared to other choices. By blending the quickness and effectiveness of edge computing with the cloud's expandability and processing power, we can create watch systems that are more dependable and strong. AI and ML improvements are set to make video processing tasks more exact and efficient. Methods like transfer learning, federated learning and self-teaching learning could improve surveillance models' ability to adjust and generalize. This means they can work well in different changing environments. Research in explainable AI, privacy-guarding techniques, and ethical AI will help make surveillance systems safer, more clear and socially responsible. The future of AI-enabled video processing for audio/video surveillance on the cloud is characterized by

Received: July 22, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

continued innovation, collaboration, and responsible deployment, with the ultimate goal of ensuring safety and security in an increasingly interconnected world. [27,29,31].

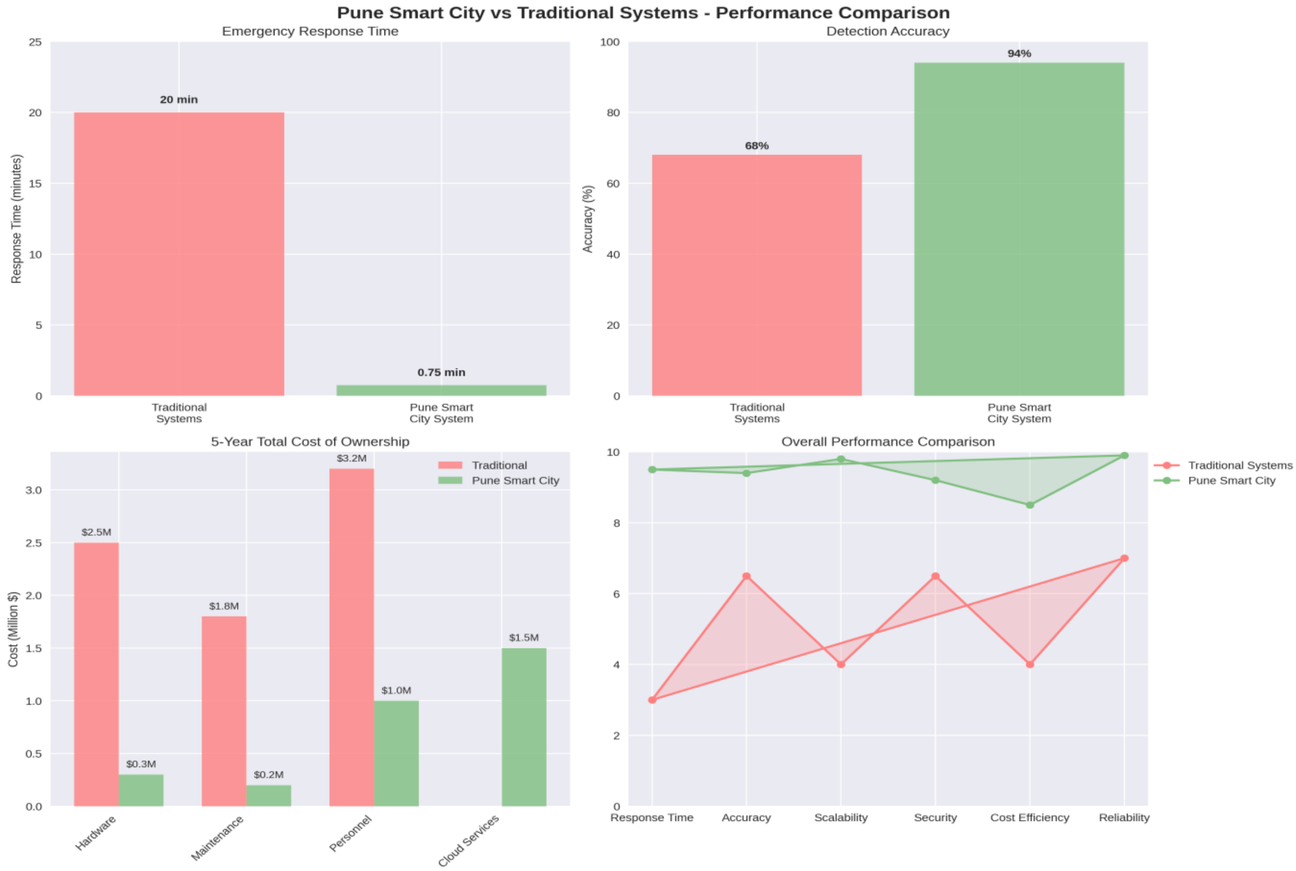

Figure 4: Performance Graph for Respective City

The proposed self-regulating surveillance model represents a paradigm shift in modern security frameworks. By incorporating deep learning, edge computing, and Bayesian probability models, the system ensures real-time adaptability, threat detection accuracy, and optimized resource management. The mathematical framework provided enables structured implementation, ensuring efficient, secure, and scalable AI-driven surveillance solutions. Future advancements will refine anomaly detection through self-supervised learning, federated AI, and blockchain integrated security models. The ethical deployment of AI-driven surveillance remains crucial, balancing enhanced security with privacy concerns. By integrating deep learning, real-time analytics, and decentralized computing, next-generation surveillance systems will be more intelligent, responsive, and resilient, shaping a safer and more secure digital landscape.

Received: July 22, 2025

International Journal of Applied Mathematics
Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

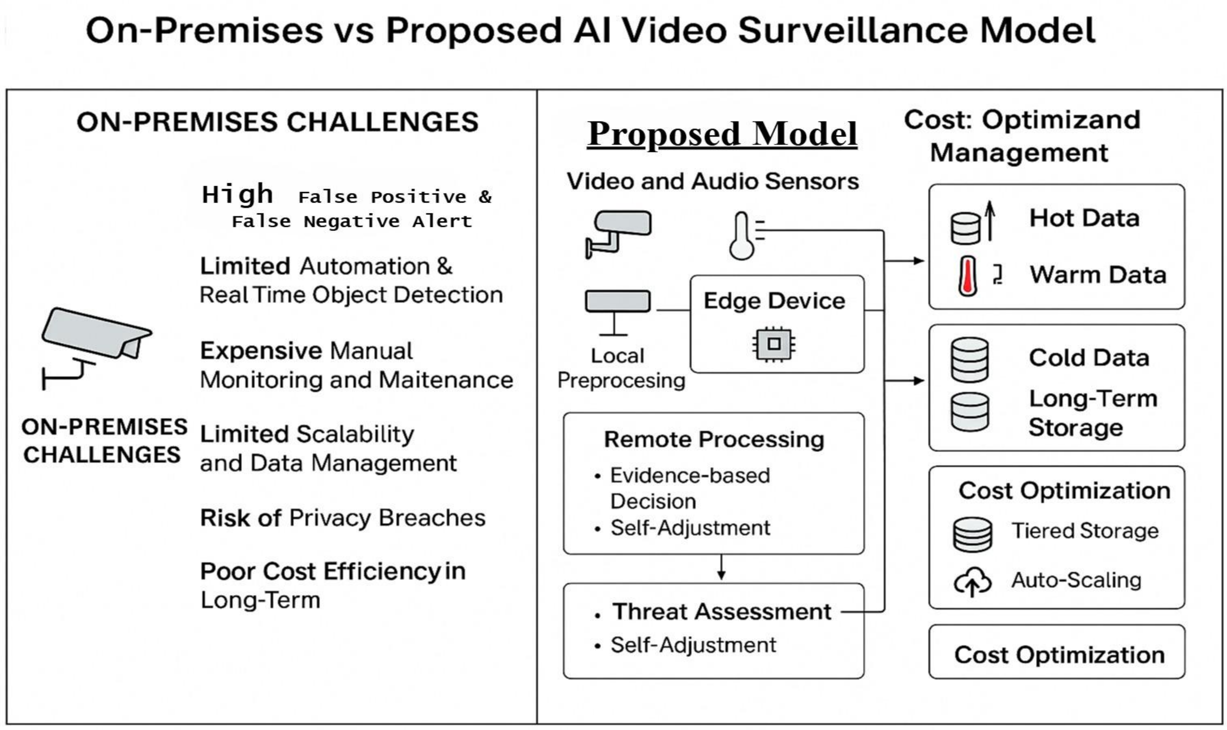

Figure 5: Outcome Towards Approach

5. Limitations and Future Work

While the system has shown promising results in prototype and semi-controlled environments, several avenues exist for future enhancements and real-world deployment at scale. These are outlined below in alignment with further research expansion, SDLC model progression, and interdisciplinary integration:

- Multimodal Sensor Integration: Future iterations of the system can incorporate additional sensory modalities, such as thermal imaging, LiDAR, and acoustic sensors, to improve detection under complex or occluded conditions. This will allow the system to operate in night-time or zero-visibility scenarios more efficiently.
- Scalability Testing in Smart City Infrastructure: The current deployment has been tested on a limited scale. Future work should include large-scale deployment across municipal smart cities, integrating with broader urban IoT networks like smart lighting, waste management, and traffic control systems.
- Extended Support for Drones and Mobile Surveillance Units: The existing modular architecture can be adapted to support aerial surveillance platforms like drones for broader area monitoring and rapid response applications. A dedicated drone module with visual analytics and geolocation integration can enhance public safety during large events or emergencies.
- Advanced Anomaly Detection Using Generative Models: Future development can explore the use of Variational Autoencoders (VAEs) or Generative Adversarial

Received: July 22, 2025

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Networks (GANs) for detecting rare or unseen events, improving the system's proactive threat detection capability.

- Cross-Camera Object Tracking and Behaviour Prediction: Extending the system with multi-camera coordination and object re-identification will allow for seamless tracking across surveillance zones. This is particularly beneficial in public transport terminals or multi-building campuses.
- Ethical AI and Bias Mitigation Frameworks: A significant challenge in AI surveillance is algorithmic bias. Future work should include the integration of explainable AI (XAI) modules and bias detection frameworks to ensure ethical deployment in sensitive environments.
- Integration with Emergency Response Systems: The alerting mechanism can be linked with real-time emergency services, allowing automatic dispatch of resources in case of detected threats, thus closing the loop between detection and action.
- On-Device Model Compression and Energy Optimization: While edge computing devices currently enable local inference, future enhancements should focus on pruning and quantization techniques to run deep learning models more efficiently on battery-powered or solar-powered hardware.
- Policy and Legal Framework Integration: Collaboration with policy-makers and law enforcement is essential to create deployment guidelines that are legally compliant and ethically grounded, especially in data-sensitive environments like schools and hospitals.
- International Deployment Readiness and Language Localization: For wider adoption, especially in multilingual countries, future systems should include dashboard localization and integration of NLP-based reporting tools to support native language feedback and alert interpretation.

The research work laid a strong foundation for the next generation of intelligent surveillance systems, combining real-time decision-making with responsible and secure computing. The future work envisioned will not only extend the technical capabilities of the system but will also pave the way for its ethical, legal, and practical adoption in real-world contexts. By continuing the iterative SDLC cycle in future phases, and applying agile principles of modular enhancement and rapid feedback, the system can remain adaptable to changing threat landscapes and evolving computational innovations. The groundwork laid in this thesis ensures that further development will remain robust, forward-compatible, and responsive to the socio-technical demands of modern digital governance and security.

6. Conclusion

This research proposed a mathematically structured framework for intelligent video surveillance that integrates deep learning models, predictive analysis, and hybrid edge–cloud deployment. Through optimization-based system modeling and iterative development, the study demonstrated how adaptive decision-making can improve precision and scalability with reduced reliance on manual oversight. Experimental evaluation confirmed strong

Volume 38 No. 1s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

performance: detection accuracy exceeded 90%, false positives declined notably, and computational resources were optimized for storage and latency. Privacy-preserving methods, including federated learning and blockchain-based auditing, further reinforced reliability and compliance. In summary, the work unites mathematical modeling with applied system design, showing how rigorous theory can guide practical, resilient, and ethically aligned surveillance solutions. This contribution highlights the broader role of mathematical methods in advancing adaptive and trustworthy AI for critical real-world environments.

References

[1] 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

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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

[9] 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

[10] 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.

[11] 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.

[12] 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

[13] "Applications of Artificial Intelligence in Transport:An Overview", "Rusul Abduljabbar , Hussein Dia", MDPI, 2019, doi:10.3390/su11010189

[14] "Smart Traffic Control System Using Image Processing", "Prashant Jadhav, Pratiksha Kelkar", IRJET, 2016, Vol. 03(3)

[15] "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

[16] On Bikes in Smart Cities, Dmitry Namiot, ISSN 0146-4116, Automatic Control and Computer Sciences, 2019, Vol. 53, No. 1, pp. 63–71

[17] "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

[18] "Intelligent Traffic Control System using Image Processing", Parichita Basak, Ramandeep Kaur", IJSR, Volume 5(8), August 2016, ISSN-2319-7064

[19] "A Review of Machine Learning and IoT in Smart Transportation ", "Fotios Zantalis, Grigorios Koulouras ", MDPI, 2019, doi:10.3390/fi11040094

[20] 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

[21] Amol K. Kadam, Dr. Konda Hari Krishna, Neeraj Varshney, A. Deepak, 5Hemant Singh Pokhariya, Dr. Sandip Kumar Hegde, Dr. Vinod H. Patil, "Design of Software Reliability Growth Model for Improving Accuracy in the Software Development Life Cycle (SDLC)" International Journal of Intelligent Systems and Applications in Engineering, 12(1s), pp. 38-50, 2024

[22] Suryawanshi, R., Kadam, A., Anekar, D., Patil, V. "An Innovative Approach for Predicting Software Defects by Handling Class Imbalance Problem" International Journal on Recent and Innovation Trends in Computing and Communication, Volume 11, Issue 9, pp. 498-505,2023.

[23] 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

[24] 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

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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

[32] 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

[33] 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.

[34] 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.

[35] 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