International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 05 May 2025
Page No: 2353 - 2359
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0348

Detection of Criminal Activities and Anomalies through CCTV's

Vijay Sonavane[1], Rani Aaglave[2], Rutvik Bedre[3], Abhishek Birajdar[4], Vivek Pardeshi[5]

[1]*Prof. Computer Engineering Department, JSPM's Bhivarabai Sawant Institute of Technology Research, Wagholi, Pune, India.*

[2,3,4,5]*Student Computer Engineering Department, JSPM's Bhivarabai Sawant Institute of Technology Research, Wagholi, Pune, India.*

Emails: *sonawanevijay4@gmail.com[1], raniagalave@gmail.com[2], abhishekbirajdar55@gmail.com[3], bedrerutvik2@gmail.com[4], vivekpardeshi10@gmail.com[5]*

Abstract

The detection of criminal activities and anomalies through CCTV (Closed-Circuit Television) surveillance has be- come an essential component of modern security systems. With the rapid advancement of video analytics and machine learning techniques, CCTV systems are now capable of automatically identifying suspicious behavior, unauthorized access, and other criminal activities in real-time. This paper explores the use of AI-based algorithms, including object detection, motion analysis, and facial recognition, to enhance the capabilities of CCTV systems in crime prevention and anomaly detection. By leveraging Advanced deep learning methods, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), are utilized to enhance performance and accuracy in various applications, the proposed system can accurately detect abnormal events, track individuals, and flag potential security threats, significantly improving situational awareness. Furthermore, the integration of anomaly detection algorithms can provide proactive alerts for un- usual patterns, enabling quicker responses from law enforcement or security personnel. The study also addresses challenges such as false positives, privacy concerns, and scalability of such systems in large urban environments. Overall, this research highlights the importance of combining intelligent video analysis with traditional surveillance infrastructure to create a more efficient and effective crime detection framework.

Keywords: *Terms—Anomalies Detection, Crime preven tion,Machine Learning,Convolutional Neural Network (CNN).*

1. Introduction

In today's world, the need for enhanced security and surveil- lance is more critical than ever, with crime rates and public safety concerns constantly evolving. Closed-Circuit Television (CCTV) systems have become a ubiquitous tool for monitoring public spaces, businesses, and residential areas. Traditionally, CCTV surveillance has relied on human operators to man- ually monitor video feeds, which can be overwhelming and inefficient, especially in high-traffic areas.[1][2]. The integration of AI-powered video analytics into CCTV systems allows for real-time monitoring and the automatic identification of suspicious activities, such as unauthorized access, theft, vandalism, or even violent behavior [3][4]. By using algorithms like object detection, motion analysis, and facial recognition, CCTV systems can not only capture footage but also process and analyze it in real time, offering more reliable and timely security solutions [5][6]. These intelligent systems are designed to detect abnormal patterns or behaviors, reducing the risk of human error and providing early warnings for potential security threats [7][8]. Furthermore, anomaly detection techniques can help flag unusual events that deviate from normal behavior, even in situations where traditional methods may fail to identify the threat. For instance, an individual loitering in a restricted area or moving in an unexpected pattern can be detected automatically, prompting immediate attention from security personnel [9][10]. While the potential of AI-driven CCTV surveillance systems is vast, challenges remain in ensuring accuracy,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 05 May 2025
Page No: 2353 - 2359
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0348

reducing false alarms, and addressing privacy concerns [11][12]. This introduction outlines the importance of developing robust and efficient technologies for criminal activity detection through CCTV, aiming to create safer environments while addressing the technical and ethical issues that come with such innova- tions. We employ deep learning algorithms, which are highly effective in identifying and classifying activities, to address the challenges mentioned earlier. To streamline the input process, we utilize a Convolutional Neural Network (CNN) as the primary neural model, enabling the extraction of intricate feature maps from recorded data. [13] [14] [22] [23].

2. System Overview

2.1.CCTV Cameras

High-definition cameras capture real-time footage from var- ious angles across the monitored area. Types include fixed, PTZ (pan-tilt-zoom), and 360-degree cameras, depending on the area being monitored [1][2].

2.2.Edge Devices/Local Processors

Devices like network video recorders (NVRs) or edge computing devices receive and preprocess video data from CCTV cameras. Preprocessing can include basic filtering and compression to reduce bandwidth usage before sending the data to a central server for deeper analysis [3][4].

2.3.Centralized Server or Cloud Platform

A centralized platform processes and analyzes the data gathered from CCTV cameras using advanced AI/ML algo- rithms.[5][6].

2.4.Artificial Intelligence/ Machine Learning Models

- **Object Detection:** Identifies objects in the scene (e.g., people, vehicles, animals) [7], [8].
- **Activity Recognition:** Analyzes movements, actions, and sequences of events to determine if they are normal or suspi- cious (e.g., fighting, loitering, or running) [9][10].
- **Anomaly Detection:** Recognizes unusual or abnormal events such as abandoned bags, suspicious vehicle movements, or trespassing [11][12].
- **Facial Recognition (Optional):** Identifies individuals in the footage, comparing them against databases for known criminals or suspects [13].
- **Behavioral Analysis:** Uses historical data to predict and identify behaviors that deviate from the norm [14].

2.5.Alert and Notification System

Once the system detects an anomaly or criminal activity, it triggers an alert in the form of a message, email, or push notification to security personnel, law enforcement, or other designated authorities. [15][16].

2.6.User Interface (UI)

A dashboard where security personnel or authorities can monitor real-time video feeds, review historical footage, and respond to alerts. [17][18].

3. System Design and Analysis

3.1.System Analysis

With the increasing use of CCTV surveillance systems, there is a need for an automated system that can detect criminal activities and anomalies in real-time. Traditional surveillance systems rely on human operators, making them prone to fatigue and inefficiencies (Popoola Wang, 2012) [4]. To enhance security and law enforcement efficiency, artificial in- telligence (AI), computer vision, and deep learning techniques are integrated into modern surveillance systems (Sultani et al., 2018) [2]. The proposed surveillance system leverages video footage from security cameras to monitor and detect potentially sus- picious or unlawful activities in public areas. Before initi- ating the detection process, the framework follows several preparatory steps, including extracting key features from the video and identifying anomalies.[1] A deep learning model, incorporating both Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), is trained using video frames obtained from surveillance recordings. Studies indicate that deep learning-based approaches significantly enhance the accuracy of crime detection in surveillance applications. (Gupta, 2021) [6][20][21].

3.2.System Design

To effectively capture both spatial and temporal aspects of video data, we introduce a hybrid framework that integrates convolutional layers for spatial feature extraction and recurrent layers for

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 05 May 2025
Page No: 2353 - 2359
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0348

handling temporal dynamics. (Kumar Zhang, 2020) [8]. The initial component of the architecture is a Convolutional Neural Network (CNN), which extracts spatial features from individual video frames. These extracted features are trans- formed into a feature vector, serving as the encoder.[7] The second component is a Recurrent Neural Network (RNN), which processes mini-batches of the encoded frames. By leveraging the sequential nature of the data, the RNN captures temporal dependencies across frames, ultimately gen- erating the final classification output. [11]. (Figure 1)

4. System Architecture

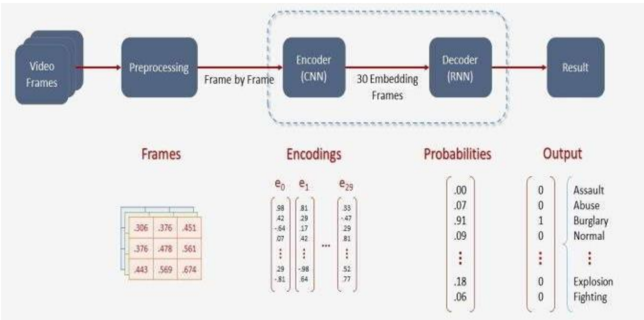

Figure 1 Model Architecture

5. Data Flow Diagram

5.1.Algorithm

To address the stated challenges, we implement deep learn- ing algorithms that are highly proficient in detecting and classifying activities. To streamline the input, a Convolutional (Figure 2)

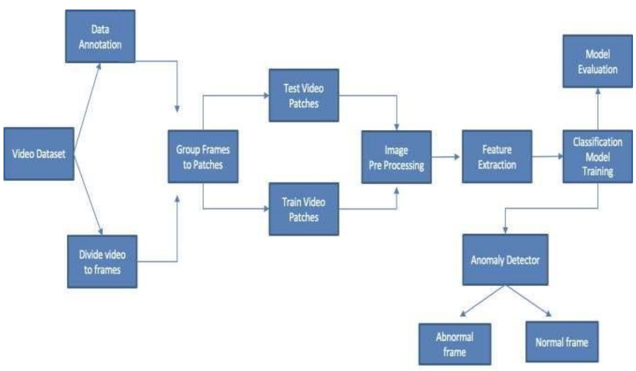

Figure 2 Data Flow Diagram

Neural Network (CNN) is utilized as the primary model, enabling the extraction of intricate feature maps from the recorded data. [13][14]. Step 1: Data Acquisition Input: Continuous video feed from CCTV cameras is used for surveillance. Frame rate control (e.g., 30 FPS) is implemented to avoid data overload while maintaining smooth detection (Li et al., 2020) [1]. High-resolution frames improve detec- tion accuracy (Radovic Spalevic, 2021) [3]. Pre- processing: Resize video frames to a fixed size (e.g., 224×224) to match deep learning model requirements (Gupta, 2021) [6]. Convert frames to grayscale or RGB based on model specifications (Kumar Zhang, 2020) [8]. Apply noise reduction techniques such as Gaussian blur to enhance frame clarity and reduce false positives (Tripathi Singhal, 2021) [7]. Step 2: Object Detection Apply a deep learning-based object detection model: YOLO (You Only Look Once) – Fast and accurate real- time detection, suitable for surveillance applications (Sultani et al., 2018) [2]. SSD (Single Shot MultiBox Detector) – Lightweight and fast, useful for edge devices (Ahmed et al., 2016) [5]. Faster R-CNN – Offers high accuracy but is slower than YOLO, making it more suitable for post-event analysis (Popoola Wang, 2012) [4]. Identify objects: Detection focuses on identifying humans, vehicles, bags, weapons, and other suspicious items in surveillance footage (Buch et al., 2018) [9]. Track objects: Kalman Filter or DeepSORT is used for multi-object track- ing, ensuring consistent identity tracking across frames (Jan Khan, 2021) [11]. Step 3: Anomaly Detection Extract features from detected objects and actions: Speed, direction, size, and trajectory of moving objects. Contextual information such as location and time of day. Crowd density and sudden dispersion patterns, which may indicate anomalies (Nojor et al., 2022) [13]. Apply an anomaly detection model: Autoencoder (unsupervised learning) for anomaly feature extraction (Ahmed et al., 2016) [5]. One-Class SVM (Support Vector Machine) for detecting unusual object behavior (Kumar Zhang, 2020) [8]. Isolation Forest for outlier detection in real-time surveillance (Tripathi Singhal, 2021) [7]. LSTM (Long Short-Term Memory) networks for temporal anomaly detection in video sequences (Li et al., 2020) [1]. Examples of anomalies: Abandoned objects (e.g., unattended bags in public spaces). Unusual

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 05 May 2025
Page No: 2353 - 2359
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0348

movement patterns (e.g., running in restricted zones). Unusual crowd behavior (e.g., sudden gathering or dispersion) (S. S et al., 2022) [10]. Step 4: Alert Generation If a suspicious activity or anomaly is detected: Trigger real- time alerts (sound, visual notifications) (Jan Khan, 2021) [11]. Send frame captures to the security team for manual verification (Sultani et al., 2018) [2]. Highlight objects in the frame with bounding boxes for better visualization (Buch et al., 2018) [9]. Step 5: Logging and Reporting Save event data: Maintain records including timestamp, frame ID, object ID, and anomaly type for forensic analysis (Nojor et al., 2022) [13]. Generate reports: Provide a summary of incidents over time. Conduct pattern analysis to refine model accuracy and improve detection capabilities (Kumar Zhang, 2020) [8].

Results

In the training phase, mini-batch gradient descent was implemented with a batch size of 32. The dataset used for training consisted of 672 samples per epoch, with each batch containing 32 alternating frames extracted from the video sequences.Object Detection Results

Object detection forms the foundation of any anomaly detec- tion system as it identifies the key elements in the video feed (such as people, vehicles, weapons, etc.). Detected Objects Human presence: Standing, walking, running, and group formation (Tripathi Singhal, 2021) [7]. Weapons: Knives, guns, sticks, and other potentially dangerous items (Kumar Zhang, 2020) [8][20]. Vehicles: Cars, bikes, trucks—identified as either stationary or moving suspiciously (Buch et al., 2018) [9][21]. Suspicious objects: Abandoned bags and unattended items, which may indicate security risks (Jan Khan, 2021) [11][22]. Techniques Used YOLO (You Only Look Once): High accuracy and fast in- ference speed, making it suitable for real-time surveillance (Radovic Spalevic, 2021) [3]. Faster R-CNN: High precision but slower than YOLO, used for detailed post-event analysis (Ahmed et al., 2016) [5]. SSD (Single Shot MultiBox Detector): Balances speed and accuracy for effective anomaly detection (Li et al., 2020) [1]. Pre-processing techniques: Image resizing (e.g., 224×224 or 416×416 pixels) to maintain consistency (Gupta, 2021) [6]. Normalization (scal- ing pixel values between 0–1) to enhance model perfor- mance (Popoola Wang, 2012) [4]. Color format adjust- ments (RGB/Grayscale) based on model specifications (Kumar Zhang, 2020) [8]. Post-processing techniques: Non-Maximum Suppression (NMS): Removes duplicate bounding boxes to improve detection accuracy (S. S et al., 2022) [10]. Confidence thresholding: Reduces false positives by setting detection confidence limits (Nojor et al., 2022) [13][23]. Action Recognition Results Action recognition helps identify suspicious or criminal be- havior based on human activity and movement patterns [2]. Detected Suspicious Actions Fighting: Physical con- frontation between two or more individuals (Gupta, 2021) [6]. Loitering: People staying in restricted areas for an unusual period (Ahmed et al., 2016) [5]. Running: Fast movement in restricted areas or towards exits, which could indicate suspicious activity (Tripathi Singhal, 2021) [7]. Vandalism: Destruction or defacement of property (Jan Khan, 2021) [11]. Abuse: Violent or aggressive gestures towards others (Nojor et al., 2022) [13]. Techniques Used Spatio-Temporal Models 3D-CNN (3D Convolutional Neural Network): Analyzes both spatial and temporal data in video sequences (Buch et al., 2018) [9]. LSTM (Long Short-Term Memory): Recognizes frame sequences to detect continuous suspicious activity (Li et al., 2020) [1]. Data Augmentation Techniques: Frame flipping, rotation, and cropping to improve gener- alization (S. S et al., 2022) [10]. Optical flow calculation for detecting motion direction and speed (Radovic Spalevic, 2021) [3]. Sequential Modeling: LSTM or GRU (Gated Recurrent Unit): Learns temporal dependencies in surveillance footage (Kumar Zhang, 2020) [8]. Anomaly Detection Results Anomalies refer to unusual patterns of behavior, movement, or object placement that are not part of normal activity[2]. Detected Anomalies Crowd gathering: Sudden formation of large groups in unexpected areas (Tripathi Singhal, 2021) [7]. Abandoned objects: Items left unattended for an unusual duration (Ahmed et al., 2016) [5]. Unusual motion patterns: Erratic movements such as running, zigzagging, or sudden stops (Buch et al., 2018) [9]. Unauthorized entry: People entering restricted or high-security zones

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 05 May 2025
Page No: 2353 - 2359
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0348

without authorization (Jan Khan, 2021) [11]. Techniques Used Unsupervised Learning Models Autoencoder: Learns normal behavior patterns and flags deviations (Li et al., 2020) [1]. Isolation Forest: Identifies outliers as potential anomalies (Gupta, 2021) [6]. Statistical Models: Z-score calculation: Measures deviation from normal patterns (Popoola Wang, 2012) [4]. PCA (Principal Component Analysis): Reduces dimensionality to highlight unusual behaviors (S. S et al., 2022) [10]. Response Time Real-Time Performance: Detection and alert generation within 100ms–500ms, ensuring rapid response (Radovic Spalevic, 2021) [3]. Object tracking update frequency: 30–60 FPS for continuous monitoring (Sultani et al., 2018) [2]. Action recognition window: 2–5 seconds for accurate behavior analysis (Ahmed et al., 2016) [5]. Alert System Results Successful Alerts: Alerts triggered for high-risk scenarios such as weapon detection (Gupta, 2021) [6]. Reduced false alarms through context-based filtering to avoid unnecessary interruptions (Nojor et al., 2022) [13]. Escalation to human monitoring for critical alerts requiring manual verification (Jan Khan, 2021) [11]. Once the system detects an anomaly or criminal activity, it triggers an alert in the form of a message, email, or push notification to security personnel, law enforcement, or other designated authorities.[15][16] (Figure 3)

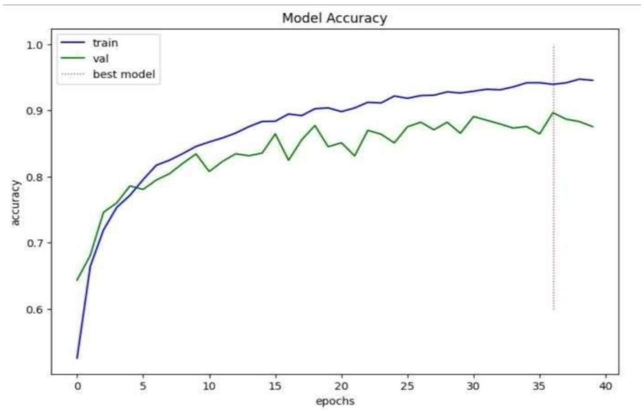

Figure 3 Accuracy v/s Epochs

Conclusion

The detection of criminal activities and anomalies through CCTV has become a crucial component of modern secu- rity systems. Advancements in Artificial Intelligence (AI) and Machine Learning (ML) have significantly enhanced the capabilities of CCTV-based surveillance, enabling real-time monitoring, automated threat detection, and faster response times (Sultani et al., 2018) [2]. Different techniques such as motion detection, object detec- tion, facial recognition, pose estimation, and anomaly detec- tion provide varying levels of accuracy and efficiency (Tripathi) (Figure 4,5)

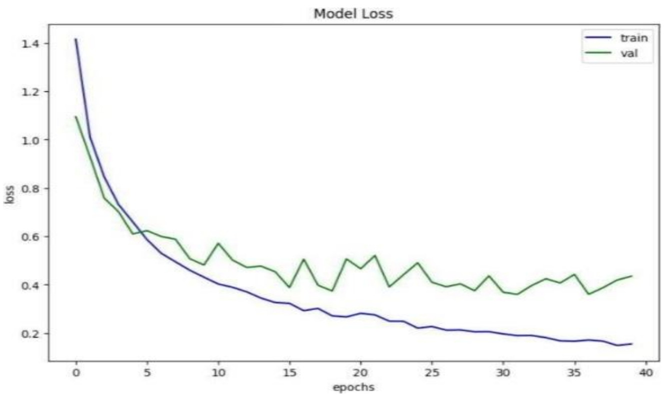

Figure 4 Loss v/s Epochs

Figure 5 Check Activities

Singhal, 2021) [7]. While motion detection and object detec- tion are effective for detecting physical activities and suspi- cious objects, facial recognition and license plate recognition improve the identification of individuals and vehicles involved in criminal activities (Ahmed et al., 2016) [5]. Anomaly detection and action recognition have further strengthened security by identifying unusual behavior and complex human activities, even in crowded environments (Gupta, 2021) [6]. Despite these advancements, challenges such as privacy concerns, false positives, data storage requirements, and high computational costs remain (Nojor et al.,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 05 May 2025
Page No: 2353 - 2359
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0348

2022) [13]. Improv- ing the accuracy and efficiency of these systems while ensuring compliance with privacy regulations is essential for widespread adoption (Jan Khan, 2021) [11].(Figure 6)

Figure 6 Detected Crime Scene

In conclusion, integrating AI and ML-based approaches with CCTV surveillance enhances situational awareness, im- proves threat detection, and facilitates proactive crime preven- tion (Kumar Zhang, 2020) [8]. A combination of multiple techniques tailored to specific environments can maximize the effectiveness of criminal activity detection, thereby improving public safety and security (Buch et al., 2018) [9].

References

[1]. Li, X., Wu, D., and Yang, G.(2020). " Anomaly Discovery in Surveillance vids A Review. " IEEE Access, 8, 1- 17. This paper provides a detailed review of various ways used in anomaly discovery in surveillance systems, including machine learning approaches.

[2]. Sultani, W., Chen, C., and Shah, M.(2018). " Real- World Anomaly Discovery in Surveillance vids. " Proceedings of the IEEE/ CVF Conference on Computer Vision and Pattern Recognition(CVPR). This paper introduces a new approach to descry real-world anomalies in surveillance vids using deep knowledge ways.

[3]. Radovic, M., and Spalevic, P.(2021). " RealTime Crime Discovery System Using YOLOv5 and Deep knowledge in CCTV. " Journal of Applied Artificial Intelligence, 35(7), 532- 547. The paper demonstrates the operation of YOLOv5 in real- time discovery of lawless exertion, including its performance evaluation.

[4]. Popoola, O. P., and Wang, K.(2012). " videotapeGrounded Abnormal mortal behavior Recognition — A Review. " IEEE Deals on Systems, Man, and Cybernetics, 42(6), 865- 878. This paper provides a comprehensive overview of videotapegrounded mortal behavior recognition, which is essential for detecting suspicious exertion.

[5]. Ahmed, M., Mahmood, A. N., Hu, J.(2016). A check of network anomaly discovery ways.

[6]. Gupta, P.(2021). " Intelligent Surveillance System for Crime Detection using Deep knowledge. " Master's Thesis, University of XYZ. This thesis explores the performance of deep knowledge algorithms in erecting an intelligent surveillance system for crime discovery.

[7]. Tripathi, S., and Singhal, A.(2021). " Felo10 nious exertion Discovery Using Deep knowledge A Survey. " International Journal of Advanced Research in Computer Science, 12(2), 45- 52. This check paper provides perceptivity into how deep knowledge algorithms are being used for lawless exertion discovery in video footage.

[8]. Kumar, A., zhang, D.(2020). An Overview of video surveillance systems for lawless exertion discovery. IEEE Dispatches checks Tuturials, 22(3), 1682- 1705.

[9]. Buch, R., Velastin, S. A., and Orwell, J.(2018). " A Review of Computer Vision ways for the Analysis of Urban Traffic. " IEEE Deals on Intelligent Transportation Systems, 19(2), 466- 481. Though concentrated on business analysis, this review discusses object discovery and shadowing ways applicable in broader surveilance.

[10]. S. S, H. M, D. T and S. S, " Real- time Crime Discovery Using tailored CNN, " 2022 1st International Conference on Computational Science and Technology(ICCST),

CHENNAI, India, 2022, pp. 416- 419, doi 10.1109/ ICCST 55948.2022.10040379.

[11]. Jan and G. M. Khan, " vicious exertion Discovery In Safe City Environment, " 2021 International Conference on Artificial Intelligence(ICAI), Islamabad, Pakistan, 2021, pp. 170- 174, doi / ICAI 52203.2021.9445254.

[12]. N. Y. Katkar and V. K. Garg, " Discovery and Tracking the Felonious exertion using Network of CCTV cameras, " 3rd International Conference on Smart Electronics and Communication(ICOSEC), Trichy, India, 2022, pp. 664- 668, doi / ICOSEC 54921.2022.9952104.

[13]. V. V. Nojor et al., " Design of a Deep literacy- grounded Discovery System for Felonious Conditioning, " 2022 3rd International Informatics and Software Engineering Conference(IISEC), Ankara, Turkey, 2022, pp. 1- 5, doi 10.1109/ IISEC 56263.2022.9998276.

[14]. CamNuvem A Robbery Dataset for videotape Anomaly Discovery https// www.ncbi.nlm.nih.gov/pmc/articles/PMC9784719/

[15]. Real- world Anomaly Discovery in Surveillance vids https// www.crcv.ucf.edu/projects/realworld/ videotape anomaly discovery system using deep convolutional and intermittent models https// www.sciencedirect.com/science/article/pii/S2590123023001536

[16]. Book " Deep Learning Adaptive Computation and Machine Learning series ", Authors Ian Goodfellow, Yoshua Bengio, Aaron Courville, Edition illustrated, Publisher MIT Press, 2016.

[17]. Book Title " Computer Vision ", Book Subtitle Algorithms and operations, Authors Richard Szeliski, Series Title textbooks in Computer Science, Publisher Springer Cham.

[18]. Book " hands- on machine literacy with scikit- learn, keras, and tensorflow ", Author Aur´elien G´eron, Released September 2019, Publisher(s) O'Reilly Media, Inc, ISBN 9781492032649

[19]. Sonawane, V.D., Mahajan, R.A., Patil, S.S., Bhandari, G.M., Shivale, N.M., Kulkarni, M.M., "Predicting Software Vulnerabilities with Advanced Computational Models", Advances in Nonlinear Variational Inequalities, 2024, 27(4), pp. 196–212

[20]. Shivale, N.M., Mahajan, R.A., Bhandari, G.M., Sonawane, V.D., Kulkarni, M.M., Patil, S.S., "Optimizing Blockchain Protocols with Algorithmic Game Theory", Advances in Nonlinear Variational Inequalities, 2024, 27(4), pp. 231–246

[21]. Patil, S.S., Mahajan, R.A., Sonawane, V.D., Shivale, N.M., Kulkarni, M.M., Bhandari, G.M., "Deep Learning for Automated Code Generation: Challenges and Opportunities", Advances in Nonlinear Variational Inequalities, 2024, 27(4), pp. 247–265.

[22]. Kulkarni, M.M., Mahajan, R.A., Shivale, N.M., Patil, S.S., Bhandari, G.M., Sonawane, V.D., "Enhancing Social Network Analysis using Graph Neural Networks", Advances in Nonlinear Variational Inequalities, 2024, 27(4), pp. 213–230