IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BIG DATA ENABLED REAL-TIME CROWD SURVEILLANCE AND THREAT DETECTION USING ARTIFICIAL INTELLIGENCE AND DEEP LEARNING

[1] Samiksha Nanaso Bhagat, [2]Dinesh B. Hanchate, [3]Sachine S. Bere

1PG Student, Department of Computer Engineering, DGOI, FOE, Swami-Chincholi, Bhigwan,
2HOD Department of Computer Engineering, DGOI, FOE, Swami-Chincholi, Bhigwan,
3Associate Professor, DGOI, FOE, Swami-Chincholi, Bhigwan.

Abstract: This survey investigates the growing imperative for effective abnormal event detection in video monitoring applications, propelled by the ubiquitous deployment of surveillance cameras in both public and private spaces. Recognizing the challenges posed by labour-intensive human-based surveillance, the study focuses on the current landscape of state-of-theart methodologies in machine learning and deep learning for abnormal event detection. By expanding on prior research, the survey meticulously assesses the techniques' applications within the context of surveillance videos, scrutinizing datasets utilized and providing a nuanced analysis of their strengths and limitations. Through an exhaustive literature review, the paper aims to shed light on the principal challenges inherent in abnormal event detection, distilling key insights to guide future research endeavors in this critical domain. Moreover, the survey contributes to the discourse on bolstering security through intelligent video surveillance systems by synthesizing existing knowledge. In a parallel exploration, the review delves into the realm of crime prediction employing machine learning and deep learning techniques. Examining over 150 articles, the paper elucidates the diverse algorithms applied in predicting crime occurrences, offering insights into patterns and trends. Access to datasets used by researchers is provided, along with an analysis of prevalent approaches and factors influencing criminal activities. The paper identifies potential gaps and proposes future directions to enhance prediction accuracy. As a comprehensive reference for researchers, this overview serves to consolidate the multifaceted landscape of crime prediction using machine learning and deep learning approaches, facilitating advancements in this field.

Index Terms - Video Monitoring, Surveillance Cameras, Artificial Intelligence , Machine Learning, Deep Learning, Scrutinizing Datasets, Crime Prediction, Threat Detection, Crowd Surveillance.

I. INTRODUCTION:

The contemporary challenges associated with managing large-scale gatherings in urban environments have necessitated a departure from traditional crowd surveillance methods, prompting a shift towards innovative solutions. Despite the widespread use of Closed Circuit Television (CCTV) cameras, the sheer volume of data generated demands sophisticated technologies to extract meaningful insights. This research endeavors to address these limitations by leveraging the capabilities of Artificial Intelligence (AI), Deep Learning, and Big Data processing. The overarching objective is to redefine real-time crowd surveillance, introducing capabilities such as precise behavior analysis, facial recognition, and anomaly detection. The catalyst for this research is the inadequacy of conventional approaches, exemplified by events like the "Kumbh Mela, 2019," where the scale of participants underscored the critical need for advanced systems. The proposed system integrates cutting-edge findings into a comprehensive framework, employing sophisticated algorithms for crowd analysis, facial recognition, and anomaly detection. The anticipated benefits include heightened security, automated surveillance, and accurate crowd analysis, positioning the system as a scalable and adaptable solution for diverse environments. The pervasive issue of gun violence in the United States, as highlighted by the Gun Violence Archive, underscores the urgent need for innovative technological solutions to mitigate security threats and enhance public safety. With an alarming daily toll of around 100 deaths and 200 injuries from gunrelated incidents, coupled with over 350 mass shootings in 2019 alone, the social impact extends far beyond immediate casualties, creating a pressing demand for effective measures against such violence. Traditional surveillance methods, while omnipresent, face limitations such as human fatigue and information overload in real-time monitoring, necessitating the integration of Artificial Intelligence (AI), Machine Learning (ML), and Internet of Things (IoT) to enable intelligent, automated threat detection. This technological advancement presents the prospect of preventing mass shootings and terrorist attacks by deploying AI-powered security camera systems capable of real-time identification of weapons, masked faces, and suspicious objects. The application of AI, ML, and IoT in security technology introduces the potential for transformative advancements in surveillance systems.

The envisaged AIpowered security camera system, described above, exemplifies the possibilities of leveraging deep learning models to enhance object detection and semantic segmentation in live video streams. However, the deployment of such sophisticated MLenabled surveillance applications at the network edge poses computational challenges, necessitating careful consideration of the resource-intensive nature of these technologies. Despite these challenges, the integration of AI, ML, and IoT in surveillance stands as a promising avenue to revolutionize security measures, offering the potential to proactively prevent incidents rather than merely responding reactively. Moreover, the escalating challenges associated with large-scale gatherings in urban environments further compound the need for advanced surveillance solutions. Traditional crowd surveillance methods, illustrated by the shortcomings in events like the ”Kumbh Mela, 2019,” necessitate a paradigm shift towards innovative approaches. The proposed research, outlined in the third paragraph, aims to address these limitations by leveraging AI, Deep Learning, and Big Data processing. By redefining real-time crowd surveillance through precise behavior analysis, facial recognition, and anomaly detection, the research seeks to enhance security, automate surveillance, and provide accurate crowd analysis. The emphasis on interdisciplinary collaboration underscores the complex nature of real-time crowd surveillance, calling for a balance between security imperatives and ethical considerations to ensure responsible deployment and integration of these transformative technologies. One key innovation lies in the incorporation of a motion detection module based on the frame difference method, enhancing the system's responsiveness to dynamic scenarios. By calculating the absolute difference between adjacent frames in captured video, the module detects changes in the scene in real-time, triggering the capture of high-quality images for subsequent threat detection classification. The seamless integration of this module across both camera and cloud sides fortifies the system's capacity to identify moving objects promptly and adapt to evolving surveillance conditions. Furthermore, the development of a user-friendly web-based interface using the Python Flask Framework enhances the accessibility of the threat detection system. This interface enables users to upload or capture images directly from the camera, providing realtime feedback on weapon detection results. The contributions of this paper extend beyond the technical framework, emphasizing the practical utility of the system for security personnel. The proposed AI-powered system not only addresses the challenge of real-time weapon detection but also offers a generic solution applicable to diverse fields requiring realtime processing, such as transportation, thereby contributing to the broader landscape of intelligent surveillance and threat detection technologies.

A. Aims and objectives :

The underlying goal is getting a complex system which is based on big data analytics, artificial intelligence, and deep learning and does real-time crowd monitoring and threat detection. The key objectives include: • To integrate comprehensive monitoring by involving multiple data sources. • To employ deep learning algorithms in the computer vision domain to analyze video streaming and detect hazards. • To understand the capability of instantaneous critical intelligence and agile reaction to newly discovered potential threats. • To be able to manage crowds, resources for security purposes and increasing public safety. • To modify the system's accuracy and efficiency as the need arises through constant improvement.

II. RELATED WORK:

In the realm of video surveillance, current approaches predominantly rely on cloud-based analysis, introducing latency and increased communication overheads. This section provides an exhaustive review of existing works, shedding light on diverse applications such as human-weapon activity recognition, crime detection, traffic monitoring, indoor surveillance, object tracking, and face identification. Notably, Lim et al. [7] addressed human-weapon activity recognition through a dataset of gun images, utilizing a single-stage object detector with multi-level feature pyramids. However, the centralized server-based training and validation processes hinder real-time responsiveness. Similarly, crime detection systems, such as the one proposed by [9], deploy deep learning models on CCTV images but suffer from limited prediction accuracy due to constrained datasets and pre-trained models. These approaches often rely on cloud computing, impeding timely security actions. In the context of firearms detection, Grega et al. [8] developed an algorithm based on recorded CCTV image analysis, combining a CNN model with an MPEG7 classifier. Despite efforts, the model's performance was compromised by poor-quality and low-resolution datasets. The domain of traffic monitoring witnessed contributions from Zhang et al. [10], who proposed a vehicle detection algorithm based on fine-tuned CNN models, showcasing the capability to identify vehicles and extract properties from recorded traffic videos. The indoor surveillance method presented by Liu et al. [11] employed a pre-trained Mask R-CNN model, but its classification accuracy suffered from underfitting due to a small training dataset. Object tracking, a crucial component in video surveillance, was explored by Cui et al. [12], introducing a multiple granular cascaded model that demonstrated 61Distinctively, advancements in face recognition using surveillance videos were highlighted in] proposed a trunkbranch ensemble CNN platform, while utilized a pre-trained VGG face model fine-tuned with a web-scraped dataset for real-world face recognition. Nevertheless, most existing video surveillance approaches either operate on recorded videos or offload data to centralized servers in the cloud, limiting their applicability for real-time threat detection. Moreover, the computational constraints of security cameras hinder the deployment of these approaches, preventing the optimization of communication delays in mission-critical security tasks. To address these limitations, the paper introduces a novel AIpowered system that integrates on-site video analysis with both camera and cloud components, aiming to enhance real-time threat detection capabilities. The proposed system leverages edge computing resources, such as the Intel NCS 2 device and Raspberry Pi 3, to empower surveillance cameras for local processing and reduce dependence on cloud computing, thereby overcoming the drawbacks associated with existing video surveillance approaches.

III. PROPOSED METHODOLOGY :

In the realm of anomaly detection, the challenge arises from the diverse interpretations of actions that can be considered abnormal. This stems from the underlying assumption in anomaly detection techniques that deviations from established patterns are indicative of abnormal events. Research studies, categorize anomalies into three distinct types to provide a nuanced understanding. Point anomalies, the most fundamental form, manifest when the behaviour of an individual entity deviates irregularly from the overall dataset. An example of a point anomaly could be a car positioned unexpectedly in the middle of a road. Contextual

anomalies, on the other hand, occur when a data value behaves irregularly within a specific context, taking into account the observer's subjectivity and overall perception of the situation. An instance of a contextual anomaly could be the act of parking a passenger car in a designated busonly parking area. Lastly, collective anomalies manifest when a collection of data samples collectively deviates from the norm. For instance, a group of people congregating at the exit of a door could be considered a collective anomaly. The literature on anomaly detection has witnessed various approaches tailored to both crowded and uncrowded environments. A particular study explored the intricate relationship between the number of moving objects within a video clip and the complexity of the methods employed for anomaly detection. The study delineated environmental categories, ranging from slightly crowded environments at a 10 square feet/per person to moderately crowded environments at a 4.5 square feet/per person and crowded environments at a 2.5 square feet/per person.

This categorization emphasizes the significance of environmental factors in determining the efficacy of anomaly detection methods, offering valuable insights for researchers and practitioners alike. Anomaly detection, with its multiple facets and environmental considerations, has spurred extensive research efforts to devise effective methodologies. The existing body of work serves as a foundation for understanding and addressing the intricacies associated with different anomaly types and environmental contexts, facilitating the development of robust anomaly detection systems applicable across diverse scenarios. A. Algorithm Implementation In the pursuit of advancing real-time crowd surveillance and threat detection, the project places a central emphasis on leveraging machine learning algorithms. These algorithms, rooted in the analysis of extensive datasets, enable the system to discern and assimilate patterns, fostering adaptability to dynamic crowd behaviors. Notably, Convolutional Neural Networks (CNNs) are integral to the project's facial recognition tasks within crowded scenes, utilizing deep learning models to automatically extract hierarchical features from facial images. This approach enhances the accuracy of individual identification in large crowds, augmenting the overall efficacy of the surveillance system. The temporal dimension of crowd behavior is addressed through the employment of recurrent neural networks (RNNs), specifically Long Short-Term Memory (LSTM) networks, which capture temporal dependencies crucial for predicting and responding to real-time crowd dynamics. Spatial understanding within crowds is facilitated by density-based clustering algorithms, with DBSCAN being a notable example.

These algorithms contribute significantly to discerning the spatial distribution of individuals, identifying clusters and aiding in anomaly detection. The machine learning toolkit, encompassing various clustering and classification algorithms, proves instrumental in interpreting complex crowd interactions and deviations from normal patterns. Anomaly detection, a critical component of the project, involves the application of machine learning models such as Isolation Forests and One-Class SVM, excelling in identifying deviations from normal behavior patterns within large datasets. This augmentation enhances the system's capability to detect potential threats in real-time crowd surveillance scenarios, contributing to the development of a sophisticated and adaptive surveillance system. The project's alignment with the machine learning domain signifies a significant contribution to the discourse on practical applications of these technologies in enhancing public safety. By integrating machine learning principles, the project not only achieves more accurate and efficient crowd surveillance but also fosters broader advancements in the field of artificial intelligence. This endeavor opens avenues for innovative solutions to address complex real-world challenges in urban environments, demonstrating the transformative potential of machine learning in the realm of public safety and security.

IV. PROPOSED SYSTEM WORKING:

The proposed cutting-edge system represents a transformative approach to urban security, utilizing advanced technologies such as Artificial Intelligence (AI), Deep Learning, and Big Data processing to establish real-time crowd surveillance and threat detection capabilities. At the heart of the system is a sophisticated integration of machine learning algorithms dedicated to crowd behavior analysis, facial recognition, and anomaly detection. This amalgamation, supported by adaptive deep learning models, ensures a proactive and adaptive stance against security challenges in densely populated areas. The system leverages efficient data processing mechanisms to handle large datasets swiftly, facilitating accurate monitoring of crowded environments with unparalleled accuracy and efficiency

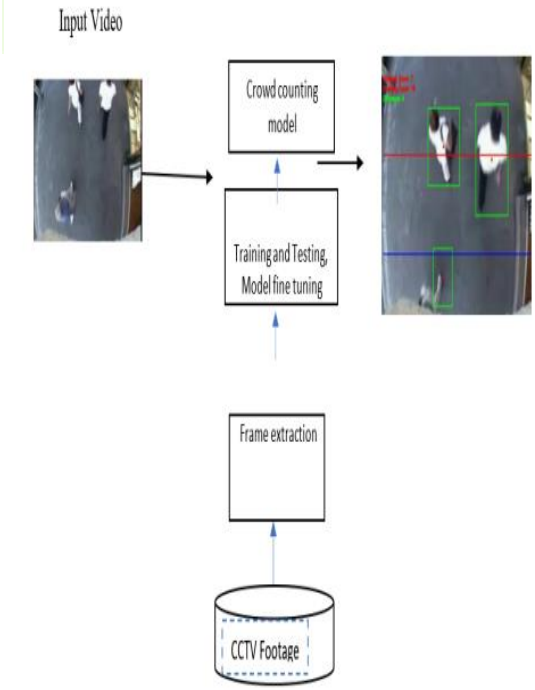

Fig 1: System Architecture

The operational framework of the system revolves around a user-friendly web-based interface, incorporating privacy features and equipped with threat identification and reporting capabilities. This interface not only enhances the accessibility of the system but also contributes to the ethical considerations surrounding privacy in urban surveillance. The system's comprehensive approach is designed to redefine urban security, offering scalability and integration with existing surveillance infrastructure. By providing a holistic solution that aligns with the dynamic nature of urban security, the proposed system addresses the intricate complexities of modern crowd monitoring, setting the stage for an advanced and adaptive paradigm in safeguarding public spaces. At its core, the system prioritizes real-time insights, empowering operators with a dashboard overview, video feeds, and facial recognition panels. This enables operators to make immediate threat responses, significantly reducing response time in critical situations. The scalability of the system is a key design consideration, ensuring seamless integration with diverse surveillance infrastructures prevalent in urban environments. This scalability not only accommodates current needs but also anticipates future expansions, underscoring the system's adaptability and relevance in the evolving landscape of urban security.

A. Scope of project :

This project covers the building of a complete system that combines data from different sources, namely the CCTV cameras' video feeds, social media data streams, and inputs coming from sensors and IoT devices placed in the vicinity of the crowd [5]. It will use big data technologies to receive, store, and work with the huge data collections in real-time. Sophisticated deep learning models will be developed and trained for the video data processing. This will include the use of technologies like object detection, crowd behavioral analysis, and crowd density estimation. Social media data will be filtered via natural language processing for useful details. In the future, multimodal fusion approaches will use data from all the sources of information to detect suspicious activity or any signs of threats. The system will give immediate alerts and visualization for security personnel, subsequently reaction will become faster. Privacy measures, like anonymization, and ethical AI principles will be applied to avoid any misuse of data. The MLOps pipelines will be used by the team for continuous model updates and system enhancements [15]. The long-term goal is an AI-powered surveillance solution that is cost-effective, accurate, as well as responsible.

B. CONCLUSION:

In conclusion, the Big Data Enabled Real-Time Crowd Surveillance and Threat Detection System, leveraging Artificial Intelligence and Deep Learning, signifies a substantial advancement in addressing contemporary challenges in ensuring public safety within crowded environments. This comprehensive system amalgamates AI, deep learning, and big data analytics to provide accurate crowd behavior analysis and threat detection. Its advantages span enhanced security, automated surveillance, efficient data processing, and adaptability to dynamic settings, underscoring its scalability and potential for technological evolution in the field of crowd surveillance. Nonetheless, the system grapples with inherent limitations, including privacy concerns, potential biases in AI algorithms, and the necessity for high-quality surveillance infrastructure. Achieving a delicate equilibrium between security imperatives and ethical considerations is crucial for garnering public trust. Ongoing collaboration among technology experts, legal professionals, ethicists, and the wider community is essential for addressing these challenges. The responsible deployment of this technology entails continuous refinement based on realworld feedback, compliance with privacy laws, and transparent communication. Ultimately, the proposed system holds the promise of reshaping the crowd surveillance landscape, contributing not only to public safety but also advancing technological capabilities. Navigating the complexities demands a thoughtful and multidisciplinary approach, ensuring benefits are realized while upholding individual rights and societal values in the ongoing pursuit of effective, ethical, and responsible crowd surveillance.

REFERENCES

1. A.A. A. Member, "Jhawk-eyean ai-powered threat detector for intelligent surveillance cameras.," IEEE and MATHIAS ECHI1, 2021.
2. M. B. J. M. L. K. W. J. Lim, M. I. Al Jobayer and J. See, "Gun detection in surveillance videos using deep neural networks," in Proceedings of the IEEE Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, ser. APSIPA ASC '19, p. 1998–2002, 2019.
3. Rajendran, L. and Shankaran, R.S., 2021, January. Bigdata enabled realtime crowd surveillance using artificial intelligence and deep learning. In 2021 IEEE International Conference on Big Data and Smart Computing (BigComp) (pp. 129-132). IEEE.
4. G. F. Shidik, E. Noersasongko, A. Nugraha, P. N. Andono, J. Jumanto, and E. J. Kusuma, "A systematic review of intelligence video surveillance: Trends, techniques, frameworks, and datasets," IEEE Access, vol. 7, no. 1, pp. 457–473, 2019.
5. J. Chen, K. Li, Q. Deng, K. Li, and P. S. Yu, "Distributed deep learning model for intelligent video surveillance systems with edge computing," IEEE Transactions on Industrial Informatics, vol. 1, no. 1, pp. 1–8, 2019.
6. K. He, G. Gkioxari, P. Dollar, and R. Girshick, "Mask R-CNN," in ´ Proceedings of the IEEE International Conference on Computer Vision, ser. ICCV '17, 2017, pp. 2980–2988.
7. S. Huang, "An advanced motion detection algorithm with video quality analysis for video surveillance systems," IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 1, pp. 1–14, 2011.
8. "Flask framework: A web-based framework written in python," accessed April 15, 2021. [Online]. Available: https://flask.palletsprojects.com/en/ 1.1.x/
9. J. Lim, M. I. Al Jobayer, V. M. Baskaran, J. M. Lim, K. Wong, and J. See, "Gun detection in surveillance videos using deep neural networks," in Proceedings of the IEEE Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, ser. APSIPA ASC '19, 2019, pp. 1998–2002.
10. M. Grega, S. Łach, and R. Sieradzki, "Automated recognition of firearms in surveillance video," in Proceedings of the IEEE International MultiDisciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, ser. CogSIMA '13, 2013, pp. 45–50.

11. U. Navalgund and K. Priyadharshini, "Crime intention detection system using deep learning," in Proceedings of the IEEE International Conference on Circuits and Systems in Digital Enterprise Technology, ser. ICCSDET '18, 2018, pp. 1–6.
12. S. M. Grega and R. S. 2013, "Automated recognition of firearms in surveillance video," IEEE International Multi Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, ser. CogSIMA '13, p. 45–50, 2013. L. S. R. Y. Zhou, L. Liu and M. Mellor, "Fast automatic vehicle annotation for urban traffic surveillance," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 6, p. 1973–1984, 2018.
13. S. P. J. Y. Liu, Y. Yang and L. Haowei, "Intelligent monitoring of indoor surveillance video based on deep learning," IEEE International Conference on Advanced Communication Technologu, ser. ICACT'19, p. 648–653, 2019.
14. P. Z. Cui, Z. Wei and D. Zhang, "A multiple granular cascaded model of object tracking under surveillance videos," ACM International Conference on Algorithms, Computing and Artificial Intelligence, ser. ACAI 18, 2018.