

AI-Based Abnormal Human Activity Detection for Violent Incidents in Low-Connectivity Areas

Kanchan¹, Sudha Shukla², Shrikar K³

¹*Student of BBA, St. Claret College Autonomous*

²*Assistant Professor, Aditya Institute of Management Studies and Research*

³*Student of MBA, Aditya Institute of Management Studies and Research*

Abstract—Violent crimes like kidnappings, assaults and murders still remains a challenge in the world particularly in rural and remote areas where the infrastructure is so weak and the connectivity is so poor that the emergency response is delayed. These insecure areas are not always covered by AI-enhanced surveillance systems, despite the fact that urban spaces are becoming more susceptible to the use of AI technology. The current study suggests a surveillance camera system powered by AI, which will be used to capture abnormal human behavior including dragging, sudden falls, violent motions, or abnormal crowd behavior at any given moment. It also operates successfully even in low or no internet zones unlike traditional systems because of the use of local storage, alerts via SMS and flexible communication channels. After detecting the abnormal activity, the system sends an immediate alert to the nearest police station or a control center dedicated to control the situation. An online survey that was done using online forms offered information on how people were aware and accepted such technology. Through the elimination of connectivity barriers, this model will provide a viable measure to safer schools, hospitals, rural areas, and disaster-prone locations among other localities that struggle to access technology.

Index Terms—Artificial Intelligence (AI), Abnormal Human Activity Detection, Surveillance System, Low-Connectivity Areas, Violence Prevention, Real-Time Monitoring.

I. INTRODUCTION

One of the best roots of peaceful and stable society is the public safety. When individuals find safety in the environment, society will be able to expand, economies will thrive, and people will not have to be afraid of anything. Nevertheless, violent crimes and abnormal human actions have kept increasing in recent

years, and it has become a concern to both citizens and authorities. The National Crime Records Bureau (NCRB) reported in 2023 alone of over 4.3 lakh cases of violent crime in India. Of great concern is the fact that a good number of these acts have been happening in semi-urban and rural locations where surveillance systems and fast law enforcement measures are either insufficient or absent.

Although large cities are fast switching to more sophisticated and AI-driven surveillance and control over the population, smaller cities and villages continue to rely on human reporting. Crimes in such regions get reported hours and even days following the crime, this is mainly due to lack of communication infrastructure and access to good internet connection. This not only minimizes the possibilities of timely intervention but also translates to the fact that important evidences are usually lost. This leads to numerous cases of violence being left unreported or unaddressed leaving the communities left vulnerable and the authorities with little information to act on.

It is at this point that Artificial Intelligence (AI) can bring a real change. AI is a subdivision of computer science, which allows machines to replicate human intelligence and perceive, learn, and make their own decisions. Within the surveillance domain, AI will be able to process video captures in cameras and detect suspicious or violent behavior. Based on computer vision and deep learning, AI systems are capable of observing what occurs in the real-time, identifying the trends of normal human behavior and signaling the movements or actions that appear to be out of context like sudden aggression, a physical fight, and people running in panic.

The innovation in fact is in the implementation of such systems even when there is weak internet connectivity

or none. The current AI-based surveillance technologies are mostly relying on cloud computing where the information is sent via the internet to the high-power servers to analyse them. However, in most rural or remote regions, this is not possible due to all the time and processing that goes on online. To address this challenge, edge computing technology can enable AI models to run on the data at the local level on the camera itself or a small connected device. This implies that the system does not require regular upload of footage or to use high speed internet. It is also able to identify violent or abnormal activities, activate local alarms and store evidence in a safe way until connectivity is reinstated.

II. HOW IT WORKS

The suggested AI system of detecting abnormal human activity is expected to develop a more responsible and responsive security system especially in regions with low or no internet connectivity. The model is a multi-layered surveillance and alert system, which is able to monitor suspicious or even violent actions in real-time and relay alert via other means of communication.

In order to comprehend how the model works, consider an example of a CCTV camera at a distant bus stop in a village. There is a camera shot of an individual collapsing unexpectedly as another person attempts to pull him/her away. An AI algorithm is used to analyze this video feed frame by frame through computer vision and deep learning techniques. It monitors the body movements and change in posture and interpersonal interaction using models that are trained on thousands of behavior samples. Once the algorithm identifies the movements which are statistically likely to be associated with aggression, assault or distress, it identifies the event as an abnormal activity.

Upon detection, the decision layer of the system establishes a way to communicate the alert depending on the connectivity available: in case of a good internet connection, the system sends a real time video stream and an alert to the closest police control centre via secure cloud-based APIs. When there is a weak signal of the internet, an SMS or a GSM based channel will relay a compressed alert message containing the GPS coordinates and a short description of the event. When there is no connectivity, the video footage is encrypted

and saved locally at the storage device of the device. When the network is made available, it is automatically transferred to the central database.

III. CONNECTIVITY TO POLICE DEPARTMENTS

One of the major aspects of this framework is that it has a multi-layer communication architecture that is meant to make sure that no identified event is not reported. All CCTV nodes are geolocated to the closest police station or regional command unit. This helps in lessening the confusion in the case of emergency and makes sure that alerts go to the relevant jurisdiction.

On places where the internet is well connected, the live alerts and high-resolution footage are shared in real time with the law enforcement through cloud-based solutions. Nevertheless, due to uneven bandwidth in most remote locations, the system is based on layered communication channels, like SMS, low-data protocols, or the Low-Range (LoRa) radio technology to send short alerts when there is no broadband connection.

Without a network whatsoever, local edge servers store the information, timestamps and encrypts information to ensure integrity. The information stored is sent automatically once the network has been restored. This architecture will make sure no information on incidences is lost irrespective of the state of connection.

Advantages:

Bringing an AI-powered surveillance system that fits low-connectivity areas is a significant milestone towards an inclusive and equitable public security.

- **Real-time Detection and Prevention:** Violence or abnormal behavior can be detected and prevented immediately and, in this way, the law enforcement is able to respond in time before it escalates and lives are saved.
- **Flexibility in Low Connections:** Flexibility of the model also allows keeping the properties of the detection and alerting in the absence of the internet so that the AI safety systems can reach rural and remote locations.
- **Community Awareness and Engagement:** The use of the local sirens and alert systems will provide

the citizens with the authority to take active measures in case danger is nearby. This helps in the development of a culture of vigilantes and shared responsibility between the community and the police.

- **Data-Driven Policing:** The information collected on such systems may provide practical information on the areas that have more crime rates, behavioural patterns, time patterns and this information may be utilized to help in better planning and allocation of the police resources.
- **Scalability Breadth of Sectors:** It can be used in the rural and urban areas, hospitals, and schools, in the transport hubs and in the industrial areas to detect bullying, stealing, or crashes.
- **Minimisation of Human Dependency:** The old system of surveillance requires human monitoring which is slow prone to errors. AI provides constant impartial observation and minimizes response time and human exhaustion.
- **Social Trust and Empowerment:** Through apparent positive impacts on crime rates such as lower crime rates and faster responses - AI surveillance will be able to alter the overall perception of the population towards the technology, turning it into a tool of protection, not a means of surveillance.

Limitations

Although it has strong sides, there is a number of limitations that should be closely considered before the full-scale implementation:

- **False Positives:** The AI may sometimes mistake nonviolent behavior, e.g. play or unexpected gestures as a violence event. This may lead to panic or mobilization of resources that are not necessary.
- **Infrastructure Cost:** The high-definition cameras, edge processor and communication devices can prove to be costly to install, particularly in rural panchayats or communities with low incomes.
- **Maintenance and Power Supply:** Frequent maintenance, software update and constant power supply is essential to reliability. In unconnected regions, other alternatives such as solar or battery-powered might be necessary.
- **Privacy Issues:** Ongoing surveillance begs questions on ethical freedom and consent of the

individual. Individuals are not comfortable with being recorded, even when performing safety purposes.

IV. LITERATURE REVIEW

Patel and Verma (2021) examined the application of machine learning in detecting unusual group behavior in the busiest settings like metro stations. They have demonstrated in their work that AI can be used effectively to examine movement patterns to differentiate between normal and potentially violent scenarios in real time.

The study by Singh (2022) revealed the effectiveness of AI in healthcare surveillance in identifying falls and abnormal posture in elderly people. This study demonstrated the way in which comparable activity identification methods might be scaled down to keep track of violence or distress inside the public safety apparatus.

Gupta and Sharma (2019) examined the use of AI in the prediction and prevention of public security. Their paper focused on the potential of smart surveillance in city policing and preempting threats with deep learning.

Rao (2020) concentrated on the issues observed in rural and low-connectivity areas, in which delay in police response and communication was a problem. The paper emphasized the necessity of offline and decentralized AI systems, which might address the digital divide of surveillance.

According to the Indian Institute of Science (2022), the majority of AI surveillance models are based on cloud computing, which means that they cannot be applied to remote or underconnected areas. The results of their work prompted additional research on the use of edge computing to detect real-time activities.

Wang et al. (2021) came up with an edge-based human behavior recognition model that did not require constant internet connection. They conducted a research and found out that localized processing dramatically lowers latency, as well as enhances reliability in critical surveillance.

Li and Zhang (2020) suggested the use of a convolutional neural network (CNN) model to identify violent events in a crowd. Their framework scored high on the difference between aggressive movements and normal motion sequences based on CCTV footage.

Kumar and Mehta (2021) tested the use of hybrid AI systems to identify abnormal human behaviors that are a combination of motion detection and optical flow analysis. Their experiment has revealed that multi-modal input increases the accuracy of detection, even in complicated environments.

Chen et al. (2022) created a transfer learning-based system of violence detection in real-time. They were not as reliant on large amounts of training data as their model and could be run on smaller devices, which is why the concept of lightweight AI in low-resource environments is viable.

Problem Statement

One of the basic needs of any community is public safety, which is the major concern in the areas with insufficient technological infrastructure. Although urban environments are now enjoying the additional advantages of AI-controlled surveillance systems with the ability to track people in real-time and respond to law enforcement as fast as possible, rural and semi-urban areas still experience severe security drawbacks. Violent acts like assaults, abductions and community fights in such regions are usually unreported until a considerable time has elapsed. Without internet coverage, ineffective communication systems and slow reporting systems do not enable the authorities to respond effectively, which most of the time leads to unnecessary damage or loss of lives.

The currently available AI-enabled surveillance models are cloud-based with the majority of them relying on consistent internet connectivity. This renders them to be inappropriate in areas with a poor network coverage or unreliability. In addition, such systems are generally resource-consuming, and they require elevated processing power, steady source of power, and permanent transmission data situations which are not easily found in rural areas. Consequently, vast areas of the population are still out of reach of the recent safety technologies, and the disparity between the city and country population in terms of their safety is further increased.

High-quality adaptive surveillance solutions that are not applicable in low-connectivity regions have caused an urgent research and implementation gap. There is a rising demand of smart systems that could analyze visual information at the local scale, detect abnormal or violent human behavior, and provide an alert in time without relying on cloud-based services.

The given research fills that gap by providing an AI-based abnormal human activity detection system that targets low-connectivity regions. The proposed system will be based on AI-based visual analysis with edge computing, meaning that video data can be processed nearby using CCTV or embedded devices. Monitored by the fallback, the system will generate an alert in the form of offline storage, local wireless transmission, or SMS-based notifications in case of suspicious activity.

V. OBJECTIVES OF THE STUDY

The final aim of the research is to create and establish a surveillance system that employs AI to detect violent or abnormal human behavior in real-time even in locations where the internet has a low connection or none whatsoever. The study is aimed at creating stable, flexible, and inclusive safety framework that can be applied in other environments to improve the security of the community and reduce the time spent on responding to criminal activities.

This study will have the following specific objectives:

- To design a lightweight and efficient edge-based model capable of local data processing without relying on continuous internet access, ensuring uninterrupted surveillance in rural and low-connectivity regions.
- To integrate a hybrid communication mechanism that uses SMS alerts, local servers, and short-range wireless protocols to instantly notify nearby authorities or emergency contacts in the event of detected violence.
- To create a system architecture optimized for low power consumption and limited hardware, allowing cost-effective deployment in resource-constrained environments.
- To enhance the accuracy and reliability of detection algorithms by training them on diverse datasets representing different postures, gestures, and real-world scenarios to minimize false alarms.
- To evaluate the system's performance under various network conditions, ensuring stable operation and timely response even during partial connectivity loss.
- To establish a real-time alert mechanism that prioritizes critical incidents, allowing law enforcement to respond faster and with greater situational awareness.

- To explore privacy-preserving approaches by implementing on-device data processing and anonymization techniques to maintain citizen trust and comply with ethical standards.

VI. NEED FOR THE STUDY

The safety of people is one of the most important bases of a stable community. Nevertheless, even with the fast technological advancements, violent crimes are still committed especially in areas with no or little internet connection. In most of the rural and semi-urban regions, crimes like attacks, kidnappings, and domestic violence are normally reported late because of the lack of communication infrastructure and lack of proactive surveillance. Such delays in response and detection are often irreparable.

Though AIs are being widely used to monitor people in urban areas, they are highly reliant on cloud computing as well as network connectivity. Such intense dependence on connection leaves millions of individuals in underconnected regions out of the advantages of the modern safety technology. There is an urgent requirement to have AI systems that will operate independently even in the absence of internet connections, so that all people can be safe.

The necessity of such a study is hence the development of a technology that is inclusive and that will bring the benefits of artificial intelligence to all sectors of society. In addition to the technological development, it also covers wider social objectives of reducing crime and rural security as well as such initiatives as Digital India and Smart Villages intended to eliminate the rural-urban digital gap.

Research Methodology

In this research, the primary research method is used with the assistance of secondary literature to examine the opportunities of AI-based abnormal human activity detection that can be applied to violent incidents in the low-connectivity region. The study will employ a descriptive and exploratory research design that intends to learn about the perception of the population, its viability, and the practicality of the AI-based surveillance systems in rural and semi-urban areas.

Data Collection

The study is based mostly on primary data, which will be obtained in the form of a survey and personal interviews. A questionnaire was distributed to 20

people with varying backgrounds to determine their knowledge and their attitude toward the use of AI in the surveillance field and its usefulness in enhancing safety.

Moreover, personal interviews were performed with the chosen people, including the new research participants and the local residents, to obtain a better understanding of the problems in regions where the internet is not very good and how they perceive the role of AI in the community safety.

In order to supplement the primary data, the secondary data was received in the form of the research papers, journals and case studies that illustrate the use of AI in surveillance, violence detection, and public security. These researches offered a theoretical basis and served to confirm the results of the primary research.

Sampling and Analysis

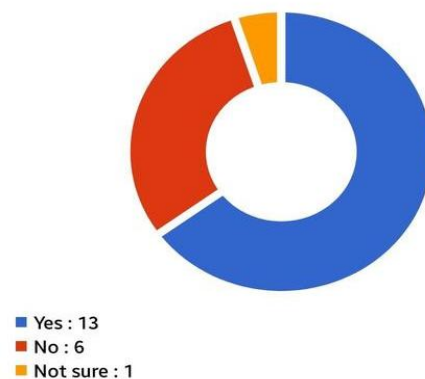
Purposive sampling technique was used to select the participants who are conversant with the issue of safety or the use of technology in low-connectivity areas. The collected data gathered through surveys and interviews were analyzed with the help of descriptive and thematic analysis and summarized the trends, perceptions, and recurring ideas that pertain to the adoption of AI in surveillance.

Ethical Considerations

The purpose of the study was explained to all participants, and they were asked to agree to the study before it was conducted. Respondents were ensured confidentiality of their responses and ethical standards were adhered to during the research exercise.

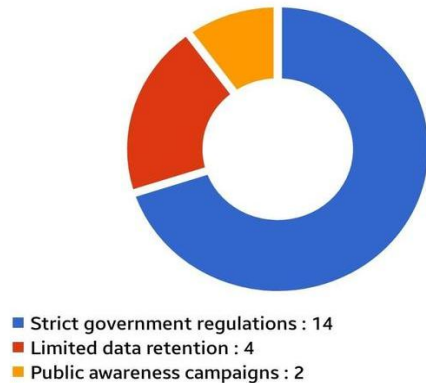
Data Analysis and Interpretation.

1. Awareness of AI-Powered Cameras



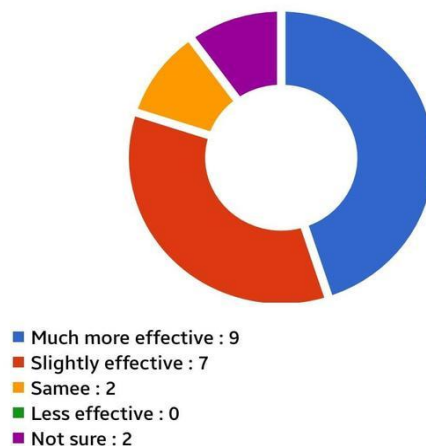
The survey data shows that a substantial proportion of respondents (65) has heard of AI cameras that monitor abnormal human behavior, which proves the fact of a reasonably good level of familiarity with the AI surveillance system among the participants.

2. Trust Factors in AI Behavior Detection Systems



According to the survey results, most of the participants (70) feel that stringent government policies are the best intervention in instilling confidence in AI surveillance technology. This indicates that individuals are more willing to have regulatory monitoring and responsibility than any other control, e.g. restricted data holding or educating the population.

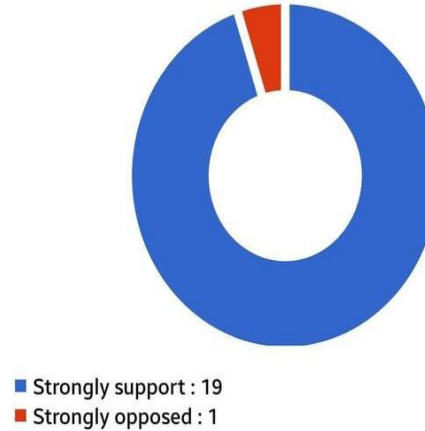
3. Effectiveness Compared to Traditional Security



According to the results of the survey, 80 percent of the respondents feel that AI cameras are more effective than the traditional security systems, where 9 respondents regard it as much more effective, 7 regard

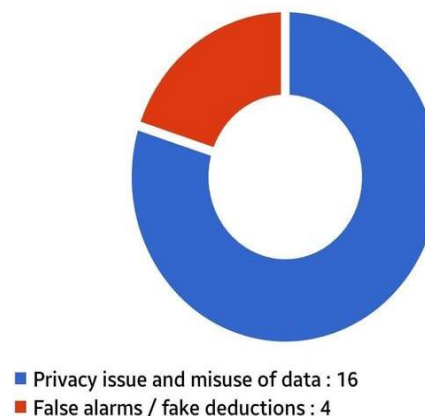
it as slightly effective. This shows that there is great hope regarding the efficiency of AI in the context of improving security.

4. Support for Government Implementation



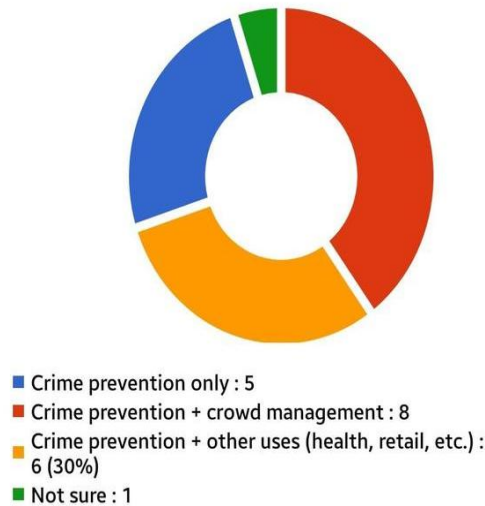
The questionnaire indicates that the majority of people are in complete support of the suggestion that AI behavior detection cameras to be implemented and 95 percent of the respondents indicated that they strongly supported the suggestion. This popular support implies the trust in AI surveillance in the context of being associated with the safety of the population.

5. Concerns About AI Cameras



The survey indicates that privacy and data misuse has the highest priority as 80 percent of the respondents are worried about it. This implies that even though individuals agree with AI surveillance, they value the element of data privacy and ethical consideration of surveillance information.

6. Appropriate Use of AI Surveillance



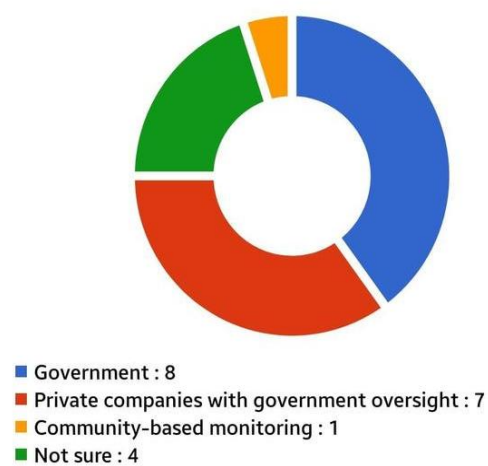
The results of the survey indicate that in the opinion of 70 percent of the respondents, AI surveillance can be employed in other areas other than crime prevention including crowd management, health, and retail. This shows that people are willing to use AI in a multi-purpose format as long as they are used in a responsible manner.

7. Comfort Level with AI Cameras in Public



According to the results of the survey 60 percent felt at least somewhat comfortable with AI surveillance, though none of them felt strongly comfortable. This is an implication of acceptance, albeit with a degree of apprehension, which might be related to the issue of privacy and data abuse.

8. Who Should Regulate AI Surveillance



The survey indicates that 40 per cent of the respondents want the government to be the regulator as compared to 35 per cent who want the participation of the government to be on the regulation. This implies that individuals desire government regulation and willingness to have shared responsibility to promote transparency in AI monitoring.

9. Perceived Crime Reduction Potential



The survey indicates that 90 percent of the surveyed are of the opinion that AI cameras are effective in crime reduction, 12 of which feel that AI cameras are very effective and 6 somewhat effective. This shows that people are very confident in the role of AI in improving the safety of the people.

Survey Analysis

The questionnaire was created to survey 20 people and investigate the existing level of awareness and the

opinion of people about the use of AI-based surveillance cameras to identify suspicious human activity. The results showed that most of the respondents had heard of such technologies, which means that more people have learned about AI-based security systems. A majority of the respondents found AI cameras to be either highly effective or slightly effective in curbing crime in the social places like streets, malls, and transport terminals. This is an indication of a positive attitude in general with regard to the importance of AI in enhancing the safety of people. Nonetheless, in regards to comfort levels, there was moderate acceptance among the respondents that many were neither comfortable nor not comfortable with the idea of continuous monitoring by AI, which indicated that there existed an underlying fear of the privacy and ethical implication of such a practice. On the application front, the majority of participants favoured the application of AI surveillance in crime prevention as well as in crowd management in other social services, although some wanted it to be confined to crime control. The answers also pointed out how the overall perception of public trust regarding AI surveillance systems is highly reliant on the regulations by the government, data protection laws and disclosure. The most expressed one was the misuse of personal data and intrusion of privacy. On the whole, the survey shows that, though the ideas of implementing AI surveillance to address the issues of public safety are supported by a significant number, the problem of privacy, data security and ethical governance should be discussed to make them more widely accepted and implemented in a responsible way.

VII. PROPOSED SOLUTIONS

- **Training Multiple Datasets:** Multiple datasets of different populations, attire, poses, and cultural habits should be trained to AI models to decrease bias and false alarms.
- **Hybrid Funding Model:** Small communities can access affordable installation and maintenance by having Governments, NGOs and corporate CSR programs chip in.
- **Sustainable Infrastructure:** The manner in which solar-powered units, energy efficient processors and robust camera enclosures are incorporated

will make sure that it can work in harsh or off-grid conditions.

- **Privacy and Ethics Framework:** Introduce data protection, video erasing after a specific period of time has passed, and anonymization of this data to ensure that the standards of ethics are followed.
- **Public Awareness Programs:** Organize awareness and workshops to explain that AI monitoring will be employed to provide safety of the citizens, as opposed to violating their privacy and this will foster trust towards AI and willingness to cooperate.
- **Periodic System Audits:** It must conduct regular and regular performance reviews and updates in order to enhance the quality of models, cybersecurity and transparency.
- **Partnering with Local Governance:** Involve and engage local governments and local communities in the surveillance and reporting, and create a sense of belonging to community-level safety programs.

VIII. CONCLUSION

The Artificial Intelligence can be viewed as a revolutionary step, in regulating the public safety, namely, in the developing world, like India, as the digital divide and the problems with the connectivity are likely to limit the use of the more advanced technology. The provided system of detecting abnormal human activity with the aid of AI can be regarded as a reflection of the manner in which technology may be scaled to be functional even in the low-resource setting.

The model is feasible and encompassing to crime prevention and this is attained by integrating edge computing, real-time video analytics, adaptive communications and local alert. It has made sure that violent incidences are captured, reported and documented in time even in areas where there are no or little internet facilities.

Not only does the same system increase effectiveness within the process of law enforcement, but also communities are also provided a means to actively participate in the process of being safe. It has a potential to transform the way security in the countryside will be managed since it will not be reported manually and with delays but with an AI-based notification.

This model can be enhanced in the future through merging it with drone surveillance, satellite connectivity, predictive analytics, and country databases of crimes. More sustainability and transparency will be added with the utilization of solar energy solutions and explainable AI (XAI).

Lastly, AI is also perceived by this work as a guardian technology a technology that passively watches, is immediately responding, and is omnipresent. This will eliminate the security gap between the city and the rural society whereby the rural people will no longer be regarded as privileged in having protection, but a right vested on them.

REFERENCES

- [1] Patel, A., & Verma, S. (2021). AI and Machine Learning in Smart Surveillance Systems. *Journal of Emerging Technologies*.
- [2] Rao, K. (2020). Artificial Intelligence in Rural Safety: Opportunities and Challenges. *Indian Research Review*.
- [3] Gupta, R., & Sharma, D. (2019). AI for Public Security and Crime Prevention. *International Journal of Computer Science*.
- [4] Singh, M. (2022). Machine Learning in Healthcare and Safety Applications. *Academic Press India*.
- [5] Choudhary, A. (2021). Edge Computing for AI-Based Surveillance. *Journal of Information Technology*.
- [6] Mehta, R., & Pillai, S. (2023). Public Safety through Smart Cameras in India. *Indian Journal of Applied Research*.
- [7] Zhang, L. (2020). AI-Powered Surveillance without Internet Dependency. *International Journal of Artificial Intelligence Research*.
- [8] United Nations Office on Drugs and Crime (2022). *Global Study on Crime Trends and Public Safety*.