International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(14s), (2026), pp. 356-373

https://doi.org/10.70917/ijcisim-2026-4236
Article

Intelligent CCTV Surveillance Systems: Analysis of Recent Trends and Challenges

Sunil Kumar*
Department of Computer Science and Engineering
Guru Jambheshwar University of Science and Technology, Hisar, Haryana, India
skvermacse@gmail.com, ORCID=0000-0003-1758-5204

Abstract: There is a lot of video footage coming into the picture from many social media sources related to daily societal problems. These video footage or clips look sometime too horrible and pathetic to see the situation where no instant solutions reflect. These societal issues attract the attention of researchers and practitioners to think deeply about solutions. The recent surveillance system is presented as a transformative and effective solution to the limitations of conventional systems. The conventional surveillance system could not process the paramount videos in time to prevent accidents or any incidents. To address such issues, there is an urgent requirement to focus attention on digital-based advanced solutions. As technology advances, the demand for advanced surveillance systems also increases to alert users to abnormal situations before they occur. Sometimes, it is not applicable in a real-time environment due to privacy and security issues with CCTV surveillance systems that have default passwords and are easily accessible to someone with malicious intent. This research explores the burgeoning realm of intelligent surveillance systems with embedded modules and explainable AI for various applications. Explainable AI and advanced machine learning algorithms could also make the system more accurate, transparent and accountable for real time behaviours as proactive surveillance. This article critically analyses the challenges associated with intelligent surveillance systems, including algorithmic bias, ethical concerns, and privacy issues affecting individuals. Overall, the aim of this study is to propose a framework for a proactive surveillance system that emphasizes regulatory safeguards, accountability, and real time transparency. The paper concludes with future directions and highlights the need for continued research on current issues and to harness its full potential for the betterment of sustainable societal development.

Keywords: Pro-Surveillance, Explainable AI, Privacy protection, Actionable AI**,** CCTV Surveillance

1 INTRODUCTION

With the rise of digital technology, surveillance systems are playing a major role in controlling crowds and responding to recent incidents or accidents. These incidents are on the rise these days like heists, molestations, murders, domestic fires, etc. and accidents happen with elder people indoors or outdoors [1]. Surveillance systems have become an important backbone of the modern security infrastructure in the past decade. Historically, people used simple cameras like closed-circuit television (CCTV) to cover local areas surveillance [2]. With the time these systems have been found to be a time-consuming process for analyses and interpret recorded data manually. It mainly relies on a human operator monitoring the video either in real time or examining it later after the event of an incident [3]. This process is manual, time taking and error-prone sometimes due to the operator's tiredness. Another side urban area is also becoming more intricate day by day, where security is becoming a necessity in all sensitive areas and at street intersections. Traditional approaches are unable to process threat detection and prevention in a timely manner. The evolution of technology has led to the convergence of cutting-edge computing, networking and data processing to empower monitoring systems for improved safety across joint public or private venture [4].

This article mainly focuses on the application involving the surveillance of people, objects, etc. It also involves a wide range of methods belonging to the surveillance process, including various criteria. The installation of CCTV cameras in public areas is commonplace. But in personal or private areas, the remote person-specific recognition has become an important aspect of smart surveillance systems for public safety and policing. State-of-the-art surveillance systems employ deep learning technologies working under data driven computer vision approaches for person-specific identification in large and crowded spaces like airports, metro rail stations and public events [5]. Biometric databases include multimodal cues such as facial features, gait, body shape and behavioral cues.

These systems continually track and identify individuals against watchlists in real time [6]. Upon potential identification, real-time alerts are triggered to help law enforcement respond swiftly. While there have been considerable advances, issues such as occlusion, low quality images and privacy are still critical areas for research. In critical security sectors such as military installations, transportation infrastructure and government buildings, access control has evolved from traditional methods of identity verification to smart and automated surveillance systems. Current systems use multimodal biometric matching, such as facial, gait, iris and body features. The systems are connected to real-time video analytics and edge computing to gather and process information as people approach secure areas [7]. Matching these features against a database of pre-registered individuals can automatically grant or deny access. The latest developments also include contactless recognition and adaptive learning systems to improve performance and resilience to environmental changes.

Crowd flow analysis is commonly performed with surveillance systems. These systems employ sophisticated human detection and tracking algorithms to calculate crowd density, trajectories, and flow rates in places like shopping centers, railway stations and stadiums [5]. This information aids in effective crowd control, crowd density avoidance and safety measures. Real-time monitoring and predictive analytics powered by AI technologies help authorities to anticipate and proactively manage crowd congestion and potential threats. Intelligent surveillance systems perform anomaly detection, which involves detecting suspicious human and object activities. Using machine learning and behavior analysis, they can differentiate between normal and suspicious events such as loitering, intrusion, leaving objects or outbreaks in a crowded area. In places such as shopping malls, airports and other public spaces, these systems can identify theft or security breaches. Alarms or notifications to security staff can be automatically triggered. Research focuses on improving the effectiveness of these systems and reducing false alarms through context-sensitive and adaptive approaches.

Current surveillance systems employ multiple cameras that communicate with each other to support crowd-scale monitoring of people and objects. Multi-camera surveillance systems use data fusion, object re-identification and spatio-temporal analysis to keep track of objects across multiple camera views, even when they are out of sight [8]. This technology is extensively employed in smart environments to monitor people or objects across large-scale spaces such as campuses, public infrastructure and commercial properties. It also allows identification of object movement patterns and abnormal behaviours involving unattended and handed-over objects. The emergence of distributed and cloud computing has enhanced the power of such systems.

Therefore, there is a wide range of applications that motivates researchers worldwide. As IEEE has sponsored conferences in the field of surveillance systems, IEEE and other publisher have been instrumental in hosting many international conferences and workshops. One such event is the IEEE International Conference on Advanced Video and Signal-Based Surveillance, held annually. This event provides a platform for the dissemination of the latest research in video analytics, signal processing and smart surveillance systems, and facilitates knowledge exchange among leading researchers and practitioners in the field. This article contributes through the following sections. Section 2 describes the range of traditional and recent research on surveillance system under the heading of literature review. It explores multiple sub sections with different sub domains on existing research. Section 3, explore the research gaps and analysis of the literature study. Section 4, cover the future works for the advancement of the security and pro-surveillance system. The last section 5 concludes the complete research study of this paper.

2 BACKGROUND STUDY

The history of video surveillance systems is also indicative of an overarching trend of technological progress in image processing, network and smart data processing [9]. The initial attempts at surveillance systems emerged in the mid-20th century and were based on the concept of analog CCTV. CCTVs are mostly used to provide security in areas of great sensitivity like bank systems and government buildings. The drawbacks of these systems included the fact that they required constant monitoring by humans, low-resolution imaging and inability to store the data in a flexible way. The adoption of digital recording in place of analog in the late 1990s was an important milestone because it enabled higher image quality, compression methods like MPEG standards, and the incorporation of digital storage. This change also enabled remote access and scalability, forming the basis of current networked surveillance infrastructures [10].

2.1 Evolution of CCTV and Surveillance Technologies

The traditional CCTV system was designed as an analog-type surveillance system that required continuous human monitoring, videotape based recording, and coaxial cable. These systems are basically employed in public areas, banks, transportation hubs and commercial buildings for basic security reasons. The traditional CCTV systems had some drawbacks, however: low image quality, limited storage capacity, and lack of intelligent analysis capability of the captured video data. As digital imaging and communication technology has evolved over the years, so have High-Definition (HD) cameras, which have greatly enhanced the clarity of video imaging, zooming, and evidence collection. In crowded areas, the HD surveillance system improved the efficiency of monitoring by providing accurate facial recognition, object detection, and incident investigation [11]. The transition from analog to digital surveillance has been identified as a significant change in security infrastructure and the effectiveness of monitoring.

Smart cameras and networked systems contributed further to the evolution of surveillance technology. Smart surveillance solutions of today are powered by Artificial Intelligence (AI), Internet of Things (IoT), Cloud Computing and Edge Processing to facilitate automated monitoring and immediate decision making. Networked surveillance architectures provide the ability for multiple cameras to communicate and share data in a centralized system, supporting the ability to track objects, analyze behavior and re-identify people between different camera views. They are commonly used in smart cities, airports, shopping malls and critical infrastructure for large scale security management. The researchers [10], [12] have shown that intelligent video surveillance systems offer better situation awareness through automatic event detection and spatio-temporal analysis; they can diminish reliance on manual observation with better operational efficiency.

2.2 Technological Foundations of Modern Surveillance

The modern surveillance technologies are based on the concept of combining advanced imaging systems with artificial intelligence, machine learning, and networked communication infrastructures, allowing for real-time monitoring and automated decision-making. The video surveillance systems became more intelligent and decentralized with the advent of the Internet and internet protocol technologies. Traditional analog cameras were replaced with IP cameras, which can be used to stream live, monitor remotely and easily combine with other security systems. It was also during this stage that video analytics gained interaction with algorithms starting to be useful in motion detection, object tracking, and anomaly detection [11].

The integration of machine learning technologies greatly increased the ability of these systems to work with massive amounts of video data independently. Consequently, surveillance became not only a passive process but also a proactive threat detection. It enhanced the efficiency of surveillance in the context of the use of such applications as urban security, traffic control and security of critical infrastructure [13]. Today's surveillance systems utilize computer vision, deep learning algorithms, and sensor fusion for anomaly detection, behavioral analysis, object and facial recognition in large-scale environments. Cloud computing, IoT, and edge-based analytics have greatly improved the scale, effectiveness and real-time capabilities of intelligent surveillance systems in smart cities and security critical applications.

In cutting-edge technology, machine learning and deep learning with AI have transformed the scenario of operational capabilities for surveillance systems [4]. AI-based CCTV systems can supervise and report any suspicious activities autonomously. Recently face based recognition approaches have helped people and classify abnormal events in real-time [14], [15], [16], [17]. It might save the life of someone and help in advance before executing anything irrelevant. Therefore, such types of transforming and monitoring mechanisms are evolving the recent system from a reactive to proactive paradigm [17]. Preventive measures can be taken well in advance, before any incident is likely to occur. This system can be used for crowd analysis and behaviour of any suspected situation to predict the risk of stampedes. It can also be applied to other objects, such as suspicious bags placed in public places, and the aggressiveness of any individual at public gatherings. This has revolutionized the requirements of the security agencies. How they are approaching auto surveillance, law enforcement, private organizations, or any open area event [18][19][20]

2.3 Role of Artificial Intelligence and Machine Learning

Surveillance technology has been in high demand with the advancement of digital systems and network infrastructures. Current monitoring system are not limited to simple video recording but now adopted intelligent techniques capable of detecting unusual activities automatically [21], [22]. These intelligent surveillance systems use a combination of computer vision, artificial intelligence, machine learning, and image processing techniques for video data analysis and to interpret the occurrence of events in a controlled environment. As a result, this type of surveillance system becomes more effective in security, reducing the reliance on manual monitoring and improving the capability to identify threats in real time [4], [23].

With this advancement, security has also turned out to be a major concern for governments, organizations, police departments, private offices, and individuals at home. The increase in the number of crimes, theft and safety concerns have created a demand for effective surveillance [20], [24]. Due to the rise in crime, there is a high demand for better monitoring systems to protect people and assets before incidents occur. AI based surveillance systems are widely and very helpful in maintaining civic safety since they allow real-time monitoring of deployed places and provide crucial evidence when something goes wrong. These systems might help authorities easily understand the problem, detect issues early, and respond swiftly in emergencies. It improves safety in various types of areas like residential areas, workplaces, healthcare facilities, public spaces, stockyards, and sensitive workplaces. Overall, details have introduced that AI based surveillance opens doors for new possibilities by enabling automated analysis of large volumes of visual data [25].

The driving forces of the evolution in the recent years have been artificial intelligence, cloud computing, and edge processing [6]. The latest surveillance systems are based on the deep learning models of facial recognition, behavioral control, and predictive analytics, increasing the level of performance and ethical concerns [26]. The real-time processing and scaling of systems is supported by cloud-based storage and edge computing architectures that are less latent and bandwidth-intensive [24]. Also, introduction of IoT devices has introduced new surveillance opportunities to smart cities and connected spaces [27]. Nonetheless, these innovations have brought up the issues of privacy, data security and regulatory compliance, and the current research on responsible AI implementation and privacy-preserving surveillance methods [28]

Figure 1 provides a comprehensive overview of intelligent surveillance systems, showcasing the various stages of data collection, analysis, decision-making and future advancements in the field. The architecture starts with the data acquisition layer for collecting data from sources like CCTV cameras, IP cameras, drones, IoT sensors and edge nodes. The data processing and analytics step involves advanced technologies, such as computer vision, deep learning, AI analytics, object detection, tracking, facial recognition, gait analysis, behavior analysis and re-identification. The processed information can be used for multiple surveillance applications, including access control, crowd flow analysis, anomaly detection and person recognition. These applications are further supported by a multi-camera surveillance network, which allows data fusion, object re-identification, cloud computing, spatio-temporal analysis, distributed monitoring and law enforcement support. The information produced is fed into the decision and response layer, which offers real-time alerts, security monitoring, access decisions, threat prevention and law enforcement responses. The framework also mentions important research challenges such as occlusion, low resolution imagery, privacy issues, scalability, false alarms and environment variation. It identifies future research directions, with a particular focus on explainable AI, privacy-preserving surveillance, edge intelligence, federated learning, smart city integration and adaptive surveillance systems to enhance the effectiveness, transparency and scalability of future surveillance solutions.

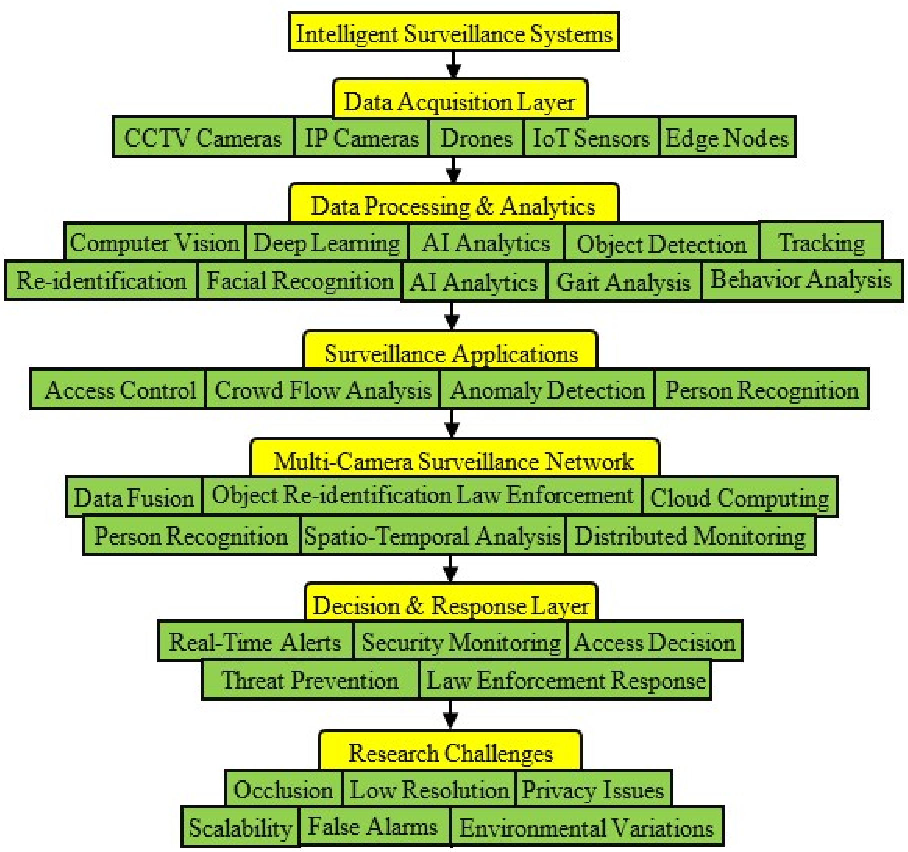

Figure 1 Overview of the processing of intelligent surveillance systems.

2.4 Challenges in AI-Driven Surveillance

AI driven systems have been found to work with a smooth flow and amplify existing societal biases available in their training data. There is a higher false rate observation in facial recognition systems during prediction of individual's faces, different skin tones and improper training model [29], [30]. These issues may result in biases with suspicion, discriminatory profiling, and unnecessary detention. These types of challenges together highlight the persistent importance of XAI in surveillance systems.

There are a number of challenges, along with the countless benefits, of recent technology; ethical and legal issues belong to AI-based surveillance systems. All these issues are directly/ indirectly interconnected with one ground reality that the majority of deep learning models are working as a black box [31]. Even though the deployed models might be intelligent to deliver a state-of-the-art result in anomaly detection or object detection and person recognition [32]. Even though, majority of users would never get to know what truly happened that influence a particular decision. Therefore, the non-interpretability of any deep learning models may open the back door to a number of threats. The ethical concern is also a major problem as well as foremost issue in surveillance system. As people are having two interpretation ether privacy or safety [33]. AI models have been found to perpetuate and exaggerate the social biases based on parameters of its training datasets. For example, error rates of facial recognition algorithms for women and people with dark skin are higher. These prejudices can be the part of wrong procedure, suspicious decision, unwarranted arrest or someone's discrimination [34].

All these above discussed problems highlight the urgency to implement XAI in surveillance. One of the important issues is legal responsibility in jurisdictions where surveillance system evidence can be presented in court [35]. Nevertheless, the system may lack in credibility as the legal authority sometimes cannot deliver clear and reasonable explanations of the system generated video [35], [36]. Therefore, they might raise questions on the admissibility of the evidence. Another side, there is a critical aspect about public trust as they never willing to have AI-based surveillance as it is not transparent. So, there are risks in operation, like lack of transparency and failure of the system operator to detect errors and adjust the model according to the environment and threats. These interconnected problems suggest designing open and explainable AI systems that are legally sound. This type of model may increase confidence in the population and minimize the risk of violations during surveillance.

The concept of AI-driven surveillance is a marvelous option from research point of view. However, it also introduces a mess of technical, ethical and legal issues. Even after, the majority of the deep learning models are black boxes, as they strip off some superheroic achievements in seeing things, trailing individuals, marking suspicious activity [37]. Virtually nobody knows how they arrive at their judgment. That is not only annoying, but it is dangerous. AI is more likely to identify and even amplify the biases present in the data it is trained on. It can result in false claims and judgments.

2.5 Anomaly Detection and Behavioral Analysis

In the current literature, AI-driven CCTV cameras have focused on developments in anomaly detection, face recognition and behavioral analysis [30], [32], [43]. Nevertheless, the transparency of the deep learning models deployed in such applications is a major problem. The existing literature on XAI has shown it to be useful in improving the interpretability of AI, with the help of feature engineering techniques and rule-based explanations [46], [47]. This section examines the weaknesses associated with the traditional surveillance AI models and the increasing demand for transparency in the decision-making of the traditional surveillance AI models.

Conventional AI-based surveillance systems are typically a black-box type of implementation [31], [36]. This implies that the executive processes in these models are not easy to understand by human beings. In practical terms, these systems can make significantly precise predictions or determinations. However, it remains unexplained as to why such decisions were taken. This secrecy poses severe issues, particularly in important uses such as face recognition and automatic alert creation, where it is vital to be aware of the rationale behind a choice in order to uphold accountability and justice [48]. The lack of transparency in these models not only makes it harder to build user trust but also makes it harder to identify and correct errors or biases made by AI systems.

AI models lack explainability due to traditional, highly questionable ethics. When it comes to the aspect of face recognition, e.g., there have also been reports of AI systems being biased against a particular demographic, thus resulting in false positives or false negatives [42]. These prejudices may be severe, including wrongful convictions. Likewise, the automated creation of alerts without explanations might lead to unjustified surveillance or false threat assessments. All these ethical issues emphasize the importance of AI systems that are both correct and understandable, so that their actions can be audited and their results interpreted by human beings. The following are some of the most interesting review papers that explore AI-driven CCTV surveillance, including explainable AI, privacy implications, and ethics [49], [50], [51]. All these research articles help to illuminate what AI means to the surveillance systems today, with the key point being that explainable models are the most important, ethical considerations and a well-established privacy protection are required to make AI-powered security responsible and trustworthy.

Surveillance is becoming increasingly dependent on XAI to make its anomaly detection systems more transparent and interpretable. These systems find use in the security field where they have the responsibility of detecting abnormal or suspicious activities in the surveillance videos, including unauthorized access or uncontrolled movements [73]. The complexity of machine learning models usually causes the system to be closed and thus hard to the security personnel to comprehend the reasoning behind the raised alerts. With the incorporation of XAI methods, such systems can offer clear descriptions of the exact patterns or behaviours that resulted in the discovery of an anomaly and therefore foster trust and enhance the usability of such systems in their practical implementation [1], [32].

Rule-based explanations are among the most effective methods for enhancing transparency in anomaly detection. In this approach, the system will furnish a set of rules or conditions that spell out the particular factors that lead to the identification of unusual activity [74]. For example, a security system can indicate that a person is visiting a restricted area outside normal working hours. The rule-based explanation may elaborate that the observation was provoked by an abnormality in movement, such as a person walking where he is not supposed to be in the first place. Such an explanation allows security personnel to more easily verify the system's decision and respond accordingly, i.e., whether the action is truly suspicious or part of an authorized event.

2.6 XAI integration in anomaly detection

XAI integration in anomaly detection is useful for increasing the system's trustworthiness and for managing a higher level of threats. Security teams would be well informed in the case of an alert to determine the severity of the situation and react accordingly when they have the opportunity to know the reasoning behind the alert [1]. Explanations based on rules can enhance the system's continuous improvement, as security personnel can provide feedback to refine detection rules and minimize false positives. By doing so, XAI facilitates a dynamic feedback mechanism that allows human knowledge to improve machine learning algorithms, ultimately resulting in better, more reliable anomaly detection in surveillance systems.

Surveillance EBA systems are changing how security personnel interpret the behaviors of individuals when detected and the response to them. These systems are intended to study the tendency of human activity and define the actions that can possibly denote potential threats or suspicious behaviour [75]. The behavioural analysis algorithms and models are often complex, and therefore the outputs are not transparent and human operators may not be able to see how certain conclusions have been arrived at [36]. XAI is essential to help fill this gap as it offers an explanation of some of the behavior and actions that culminated in the observation of a potential threat.

With XAI techniques, behavioral analysis systems are able to deconstruct and explain the pattern of activity that resulted in a conclusion, like a person making erratic movements or coming near a restricted zone [76]. These descriptions can be concentrated on certain behaviors, including lingering in a particular place unusually long or having suspicious body language. Explanations are also useful in assisting security teams in ensuring that the system has been assessed, as well as increasing accountability, as the process behind the decisions can be traced, and providing information on any potential weaknesses in the model predictions. Such transparency is especially important when behavior analysis is involved in forecasting threats or giving warnings in high-stakes situations such as airports, governmental buildings, or critical infrastructure sites.

XAI is also useful in enhancing the functionality of the behavioral analysis systems in the area of threat detection [24]. Provided that the security personnel is capable of understanding the rationale behind flagged behavior, the security personnel is in a better position to analyze the seriousness of the circumstance and react accordingly. XAI enables continuous system enhancement by allowing security teams to provide feedback on false positives or missed detections. This feedback mechanism ensures that the models are fine-tuned to minimize errors as well as it is the mechanism that shows that the system is receptive to new and emerging patterns. That being the case, it is accurate, reliable, and responsive to explainable behavioral analysis systems, which are crucial instruments in current security operations.

XAI has an active role in increasing the interpretability and transparency of AI-driven decisions on different surveillance applications [41]. In video analytics, XAI may help to explain the exact visuals and patterns that trigger the identification of possible security breaches, so that the personnel could confirm that it is accurate before taking any action. Likewise, in access control, XAI can provide information on why people are allowed into or denied access, including the facial recognition match score or predictive behavior, and trust the system will increase as a result. XAI based smart surveillance cameras can provide real-time clarifications to activities detected, and point out the characteristics or behaviors that indicated such a person was suspicious. XAI is also useful in threat detection systems elucidating patterns and anomalies underlying alert systems to provide informed and timely response to the possible threats.

XAI enhances monitoring of the crowd to immediate detection in that, it explains the behavioral patterns that result in abnormal crowd activity alerts, which will be helpful in managing the crowd [5]. XAI is also used in predictive analytics in surveillance to describe the risk forecasts by determining what factors contributed to it, enabling proactive actions to be taken to avoid incidences. All of these applications demonstrate the ways XAI can enhance transparency, accountability, and trust in AI-driven surveillance systems [77]. XAI enables human operators to trust and act upon the outputs of the system by making AI decisions transparent and verifiable, exploring system outputs, and doubting or confirming them, leading to better security management.

2.7 Explainable AI for CCTV Surveillance System

Explainable AI is an important solution to the gap between the abilities of AI and transparency that are necessary [41]. The goals of XAI are to interpret the decisions made by AI as the real-life processes and to obtain the information about the inner processes within the AI models. XAI techniques like feature attribution techniques and rule-based explanations enable users to understand what inputs contributed to a specific decision and in what way. XAI can support the trustworthiness and responsibility of AI systems by making them more understandable by explaining how they make decisions. The use of XAI in CCTV surveillance may be vital in ensuring that AI generated alerts and detections are clear and understandable [52].

Effective surveillance systems rely on trust, and the incorporation of XAI goes a long way in ensuring the establishment of such trust [53]. Users, including security personnel and the general public, will be more willing to trust these systems when they understand how the AI systems arrive at their decisions. This is the trust that will enable the widespread adoption and use of AI technologies in public security. In addition to that, explainable systems allow users to certify and confirm AI decisions, making sure that these decisions are dependable and have sound principles and regulatory criteria. Basically, XAI is used to hold the AI systems answerable to its actions.

The other most important issue covered by XAI is regulatory compliance. As AI is becoming more frequently used in surveillance, governments around the world are attaching higher demands of AI transparency and accountability [54]. XAI in CCTV surveillance also presents new opportunities to interaction and feedback in use. Explainable systems enable users to give informed feedback of AI decisions which could be utilized to tune and enhance AI models that suit the needs and expectations of users better. This article explores how XAI can be utilized in an attempt to enhance the role of CCTV surveillance in order to make AI-based security solutions effective and ethical. Explainable face recognition is a fast evolving area that sets out to increase the transparency and interpretability of face recognition systems using XAI techniques [70]. XAI methods, such as SHAP and LIME, can be used to resolve these issues since they offer a clear picture of how particular features of a face affect the system in making its decisions [71].

Table 1 presents a comprehensive study relevant to this paper, extracted from the literature, summarizing the contribution, strengths, and findings of each mentioned research article. The capability of feature attribution techniques to identify the face features, including the mouth shape, nose, or eyes, to be most useful in producing the recognition result. Such techniques operate by isolating and measuring the effect of individual components of the face to provide human operators with the capability of verifying and learning the reason behind a particular decision being made [64]. As an illustration, the XAI techniques can help determine whether the error was made by the face recognition system recognizing the wrong person, or the error was caused by a defect in face features, including light, age, and facial expression. These contributing factors can be isolated, and the system refined and retrained, leading to better accuracy and fairness.

Given the high stakes in the application of face recognition systems, transparency is particularly important for addressing issues of bias and inaccuracy. As an example, it has been established that face recognition systems tend to be discriminatory against racial and gender backgrounds with certain populations being wrongly identified more than others [72]. These biases may be computed and addressed using XAI methods, providing deeper insight into the relationship between facial features and recognition errors. Moreover, this degree of exposure enables easier questioning and verification of face recognition systems, which helps to make sure that it is efficient and effective. Lastly, explainable face recognition can make user and stakeholder trust in these technologies by simplifying their decision-making processes for access and understand.

To address these challenges, XAI methods have been proposed to make AI decisions more transparent and understandable. SHAP and LIME are feature attribution techniques that are under researched recently [75]. The methods are used to determine the most important characteristics to a model decision, thus increasing the responsibility of AI surveillance systems. Also, rule-based methods, such as decision trees and logic-based models, offer human-readable explanations by projecting AI predictions to explicit and structured rules.

Despite the potential of XAI, it has yet to become part of AI-driven surveillance systems, and its application remains a research issue. The trade-off between model complexity and explainability is one of them. The most common objective of deep learning models is to maximize

Table 1 Detailed strengths and findings of the research paper.

Ref.	**Models**	**Contributions**	**Strengths**	**Findings**
[57]	Advanced Computer Vision	Examines how visual AI techniques are shaping modern surveillance	Provides cross-domain perspective	Highlights growing reliance on AI with associated ethical concerns
[58]	AI + Policy Integration	Discusses both technical and regulatory aspects of surveillance systems	Connects policy with system design	Emphasizes need for responsible AI deployment
[40]	CNN, RNN Architectures	Reviews application of deep learning in video-based monitoring	Broad coverage of algorithms	Indicates high performance but dependency on large datasets
[59]	AI + IoT Frameworks	Focuses on surveillance deployment in smart city environments	Real-world implementation insights	Identifies scalability and infrastructure challenges
[5]	Deep Neural Networks	Proposes techniques for identifying individuals across cameras	Improves multi-camera tracking	Performance affected by environmental variations
[35]	Conceptual Ethical Models	Investigates ethical risks of AI surveillance	Strong critical perspective	Raises concerns about privacy and misuse
[34]	Deep Learning Models	Develops methods to detect unusual patterns in video streams	Handles complex event recognition	Rare event detection remains challenging
[60]	Adversarial Learning Models	Analyzes weaknesses in AI-based surveillance systems	Highlights system vulnerabilities	Shows susceptibility to manipulation attacks
[61]	CNN-based Detection Models	Introduces datasets and evaluation methods for detection tasks	Supports real-world testing	Enhances detection reliability in practical scenarios
[62]	Reinforcement Learning	Applies AI for coordinated surveillance using drones	Enables automated monitoring	Effective for large-scale environments
[40]	Deep Learning Models	Reviews limitations in tracking individuals across views	Comprehensive problem analysis	Identifies unresolved accuracy issues
[27]	AI + IoT Systems	Explores current developments and future directions	Forward-looking approach	Suggests need for adaptive systems
[63]	YOLO, Faster R-CNN	Presents high-speed object detection techniques	Suitable for live monitoring	Trade-off between speed and precision
[3]	Video Analytics Models	Surveys methods for extracting insights from video data	Covers multiple techniques	Improves automated decision-making
[41]	IoT + AI Integration	Studies interconnected surveillance devices	Enhances system connectivity	Introduces additional security risks
[63]	YOLO Model	Proposes fast detection mechanism for objects	High processing speed	Effective in time-sensitive applications
[25]	CNN (VGG)	Introduces deep architectures for feature learning	High accuracy in classification	Computational cost is significant
[64]	Neural Networks	Provides theoretical basis for AI systems	Strong conceptual framework	Enables development of modern models
[65]	CNN (AlexNet)	Demonstrates deep learning for image tasks	Breakthrough performance	Basis for later advancements
[1]	Deep Learning Models	Uses real-world datasets for anomaly detection	Practical evaluation	Improves detection benchmarking
[66]	Autoencoders	Detects anomalies without labeled data	Reduces need for annotation	Limited adaptability to new scenarios
[67]	Fast R-CNN	Improves speed of object detection	Faster processing	Suitable for real-time systems
[68]	HOG Features	Uses feature-based human detection	Simple implementation	Less effective than deep learning
[69]	Regulatory Models	Defines privacy protection standards	Legal enforcement strength	Influences surveillance policies

the model accuracy, but simplifying them to enhance interpretability can lead to poorer performance. There are several different models that are accuracy-maintaining with transparency and have been suggested by researchers, a blend of a deep learning approach and an explainable approach based on rules. The purpose of these hybrid structures is to keep AI in its predictive ability, but ensure its decision-making can be easier to interpret by the security personnel and the regulatory body [53].

Although AI-based CCTV surveillance can achieve considerable progress in security, the lack of transparency in deep learning models is one of the key challenges. This literature highlights the relevance of XAI techniques to enhancing the transparency of models, fairness and privacy compliance. Future studies are to shift to creating scalable, interpretable, and unbiased AI models to increase the level of trust and accountability in security applications. These issues will be essential to make AI-based surveillance systems effective and ethically accountable.

2.8 Ethical Concerns for Explainable AI

All AI based surveillance systems need to be embedded with Explainable AI. It is not an additional feature of surveillance, as it is a necessity of time. Accountability in the law is also a large affair. The results of these systems are present in court evidence in many locations [38]. However, when the AI cannot justify how it made a call, judges and lawyers will not trust it, and the evidence may be dismissed. The question of public trust is also important. Unless all the things occur in front of a curtain, people will not be willing to back up AI watching them. When people develop a feeling that something looks murky, they oppose it, even to the point of court.

Another side operation headache may arise, and without a transparent system, the operators will be unable to determine what went wrong and how to update the model when the threats evolve. All of these problems are intertwined and lead to the one solution for the creation of AI systems that are clear, can be trusted in court and are also trusted by people [39]. This type of solution may allow the operators to perform their duties in reality. Otherwise, there is only a continued accumulation of the risks.

Many new regulations and requirements of AI involve explainability as a significant requirement, as well as a matter of fairness [42]. It is a question of privacy, human control and ensuring that people are in control. The general population is getting aware of the functionality of such surveillance systems and why certain decisions are made, the more trust increases. When individuals understand what exactly is going on in the background, they will not be willing to resist surveillance. It is the right of every person to inquire and contest a judgement taken by automated systems according to GDPR of the European Union. XAI offers the right tools to fulfil these regulatory needs by ensuring the transparency and explainability of AI decisions. By taking steps to adhere to such regulations, XAI can not only reduce legal risks but also ensure AI systems align with the values and norms of society at large.

There is a bright prospect of this through the use of XAI in CCTV based pro-surveillance alerts to achieve a tradeoff between security and the protection of privacy [55]. On the one hand, AI-driven alerts make the security process more effective by enabling timely responses to potential threats. Conversely, explainability makes sure that such alerts are founded on clear and defensible principles and protects the privacy rights of individual people. Such two-fold approach toward security and privacy plays a vital role in ensuring the general acceptance and approval of surveillance efforts. XAI can also alleviate the worries surrounding unnecessary surveillance and violations of privacy by giving explanations on how AI-driven decisions are made [56].

Partials in AI models can be detected and minimized using XAI techniques. The AIs can be biased because of multiple causes such as biased training data and incorrect algorithmic [5]. XAI enables stakeholders to identify and address these biases in advance by making the decision-making process transparent. This is especially true when used in surveillance, where preferences may result in unfair targeting of certain groups. XAI will help ensure that AI is used ethically in the security of the population by enhancing fairness and equity.

The global adoption of the use of the CCTV surveillance systems has radically changed the aspect of security in the public [35]. These systems have now been developed to take advantage of advanced technologies of artificial intelligence as earlier used to only offer passive observation. This advancement has made it possible to monitor surveillance in real-time and accomplish automated threat detection. This makes the system highly effective in ensuring that the security agencies can detect and respond in time to the threats. The introduction of AI to CCTV surveillance has also presented the ability to perform anomaly detection, face recognition and behavioral analysis features, which have never existed before [43]. Nevertheless, such developments are associated with other issues such as the issue of transparency and interpretability of AI-driven models.

The application of AI in CCTV surveillance has been an area of recent interest, transforming the world of security through surveillance and threat detection [3], [4]. Traditional CCTV systems relied on manual observation, which was time-consuming and prone to human error. Surveillance has been made efficient with the introduction of AI, whereby it is now possible to conduct facial recognition and detect anomalies automatically [44], [45]. The developments have improved security functions and enabled real-time detection of threats and suspicious activities. Nonetheless, even with these advancements, the implementation of deep learning models in surveillance practice has been found to have several issues, particularly regarding their transparency and interpretability.

The black-box nature of deep learning models is one of the main issues in AI-based surveillance. These models take large volumes of data and make decisions, yet the rationale behind their results remains obscure [31]. Such in transparency also poses some ethical and legal issues, particularly when AI systems fail to classify people in the right way or produce biased outcomes. These are biases that affect the trust of people in surveillance technology, which should be addressed by creating solutions of XAI to enhance the comprehensibility of the models.

Privacy protection is another important issue of AI-powered surveillance. All the widespread uses of CCTV and facial recognition lead to the question of security of the data and personal rights. Researchers have highlighted the significance of privacy-respecting AI methods, including different privacy and secure federated learning, to address the privacy risk posed by unauthorized access to data [18]. Through such measures, the researcher is hoping that surveillance systems will be effective and remain within the provisions of the law like the GDPR. Researchers have examined methods of fairness-conscious AI, which alter learning algorithms to reduce biases. The techniques are adversarial debiasing, redistribution of weight to training data and integrating equality constraints into model optimization. In order to secure civic trust and prevent the misuse of the technology, it is essential to ensure fairness in AI surveillance.

In addition, the interpretability of AI-based anomaly detection systems in surveillance is an important research interest. Traditional anomaly detection systems examine trends of surveillance data and report suspicious behavior. But unless there are clear explanations of why an operation is taken to be suspicious, security operators may have problems in validating AI generated alerts.

The concept of explainable AI is simply the creation of AI systems that humans can trust and relate to the problem arises. Explainable AI not just sent an alert that somebody is suspicious, even you are also able to explore why the system alerted you about the person who was found suspicious in the first place [40]. It is much simpler to make security teams or legal authorities accountable when individuals can observe and trace the logic of the AI. The analyst can determine whether a call was made and whether it makes sense. The bias of AI is also identified and corrected through this transparency [41]. When an analyst is able to have a look back at the way the AI has been trained, how it makes the specific decisions and alerts.

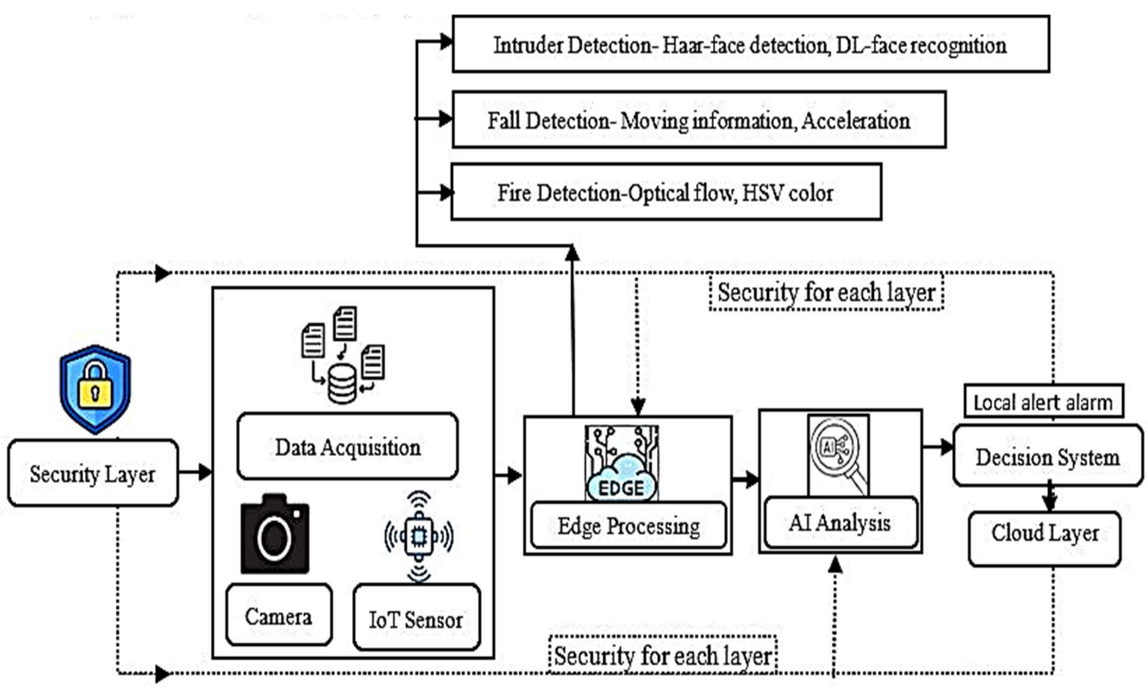

Figure 2 Proposed Pro-surveillance Framework for local alarm.

3 FRAMEWORK FOR PRO-SURVEILLANCE SYSTEM

The proposed surveillance architecture integrates multiple intelligent components to achieve secure, real-time monitoring and decision-making in smart environments. Figure 2 shows the proposed pro-surveillance framework for the local alert system. The process begins with the data acquisition layer, where cameras and IoT sensors continuously collect visual and environmental data from the monitored area. Cameras capture video streams, while IoT sensors gather contextual information such as motion, temperature, or location data. A dedicated security layer is incorporated at the initial stage to ensure secure communication, data confidentiality, and protection against unauthorized access during data collection and transmission.

After data acquisition, the collected information is forwarded to the edge processing layer. The edge processing layer is crucial in the proposed intelligent video surveillance framework, as it processes and filters event-related information before sending it to the AI and cloud layers. Edge devices locally process video streams using adaptive difference imaging, noise removal, frame extraction, erosion calculations, and other techniques to remove redundant and irrelevant information before sending the streams to centralized servers. This helps to save bandwidth, lower latency, and enhance the response speed of the surveillance system, which is crucial in large-scale smart monitoring systems.

The edge layer determines the importance of the events in the surveillance and selectively detects fire detection, intruder detection, loitering detection and fall detection. Depending on the surveillance object, various analytical methods are used. Fire detection includes optical flow and color pattern analysis to identify fire characteristics, while intruder detection uses Haar-like feature extraction and deep learning-based facial recognition to identify unauthorized individuals. In the same way, loitering detection is based on variations in the balance point angle and movement distance to detect suspicious stationary behavior, while fall detection uses motion information and acceleration patterns to detect human falls in emergency situations.

The system filters and processes only relevant surveillance events at the edge, dramatically boosting computational efficiency and alleviating the load on cloud infrastructure. The edge layer is designed to only pass on security relevant data to the upper layer of AI analysis and decision layers for alerts. This distributed processing approach enhances the scalability and reliability of intelligent surveillance systems in smart cities, healthcare facilities, transportation systems and critical infrastructure, as well as accelerates threat response. The processed data is then supplied to the AI analysis module, which employs artificial intelligence and machine learning algorithms for object detection, facial recognition, anomaly detection and behavioral analysis. This layer enhances surveillance efficiency by automatically identifying suspicious activities and extracting meaningful insights from large-scale data streams.

At the final step, the analyzed results are transmitted to the decision system and cloud layer for centralized monitoring, long-term storage and advanced analytics. The decision system generates alerts, supports automated responses and assists security personnel in making accurate operational decisions. The cloud layer further enables scalable storage, remote accessibility and integration with distributed surveillance networks. As illustrated in the framework, security mechanisms are implemented across every layer of the architecture, ensuring end-to-end protection, data integrity and reliable operation of the intelligent surveillance system in modern smart city and critical infrastructure applications.

Pro-Surveillance alert system, which is an explainable AI, is created to improve real-time monitoring by combining intelligent anomaly detection and transparent decision making. This system has an interpretable focus, unlike the traditional black-box models, to create user trust and accountability [31]. It makes sure that it is efficient in its operation as well as ethical in its implementation in surveillance settings by linking automated warnings to explainable reasoning. The suggested surveillance system combines various elements to achieve effective surveillance. It is a combination of detection, tracking, face recognition, anomaly analysis, and explainability capabilities. These modules combined increase accuracy, transparency, and adherence to privacy norms.

The face recognition system leverages advanced deep learning frameworks, including CNNs and transformer networks, to ensure robust identity verification in a surveillance setting. These models are trained on large and mixed datasets to guarantee great accuracy in different settings, such as lighting alterations, masking and stance. The module allows performing accurate matching with enrolled identities by extracting unique facial features and encoding them into discriminative embeddings. The system is also improved by the introduction of Transformer-based models, which help to achieve more global contextual relationships in face data [65]. Therefore, recognition performance improves under more complex real-world conditions. With the latest state-of-the-art XAI techniques, such as SHAP, LIME and counterfactual reasoning, an explainability layer is included in this to ensure transparency and trust in the identification process. SHAP values are useful in determining the contribution of individual facial features to the decision, whereas LIME gives locally interpretable approximations to the model behavior when making specific predictions [78]. Counterfactual explanations introduce a "what-if" element by showing how minor manipulations of facial features may change recognition results. This stratified method enables the system operators and auditors to read and confirm the model decisions, thus reducing biasness and promoting accountability.

Figure 3 represents a complete process AI based surveillance with their data privacy including local alert alarm. In this figure, the alert generation component is the real-time response mechanism to the system, and it generates instant security alerts when it detects a possible threat or attempts at unauthorized access. These alerts are not a binary output but are backed by explainable decision outputs from the explainability layer. As an example, when a person is identified as hazardous, the system will be able to show which facial features, behavioral patterns, or other environmental factors led to that definition [79]. This not only helps in faster and better-informed decision-making of security personnel, but also offers a verifiable audit trail of post-incident analysis and compliance reporting.

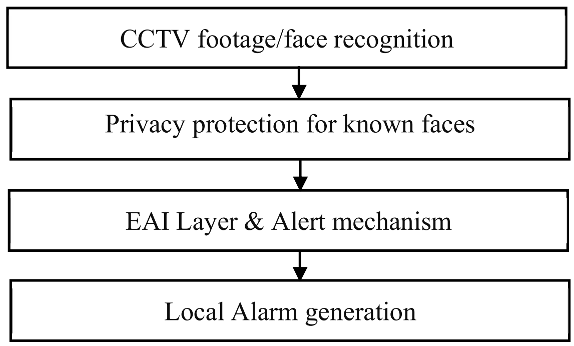

Figure 3: Privacy-aware-based system AI alerts and local alarm generation.

Simultaneously, it has a privacy protection framework in place to secure sensitive biometric information so that it does not violate international data protection laws like GDPR [80]. Such methods as differential privacy is implemented to introduce statistical noise to data so that individuals cannot be identified but still have useful analytical properties. Moreover, federated learning with security minimizes the risks of exposure to data since it allows training models on decentralized data without access to raw facial images. Such a privacy-centric design can make the face recognition system highly effective in its operations and at the same time ethically responsible, which corresponds to the requirements of the law and the trust of people.

4 RESEARCH GAP AND ANALYSIS

The experimental analysis of the suggested pro-surveillance CCTV structure was tailored in such a way that it would evaluate the performance based on a number of dimensions, such as detection and tracking accuracy, face recognition reliability, anomaly detection, explainability, and efficiency of the system. It is also in the context of bias mitigation and privacy compliance, which the study prioritized. The goal was to show that the application of XAI to real time surveillance can improve transparency and fairness without reducing the speed of operations and accuracy of detection.

The various aspects of the framework were addressed using multiple datasets. To ensure face recognition and evaluate fairness, VGGFace2 was used for training and FairFace for testing demographic-specific performance. The datasets of WIDER FACE and MOT17 were used in face detection and tracking, respectively. The UCF-Crime and the ShanghaiTech Campus datasets were trained and tested on anomaly detection models. Also, an in-house CCTV dataset of 18 hours of 720p video recordings of indoors and outdoors settings was gathered, annotated, and subjected to real-life validation. Ethical standards were observed in all in-house data collection, and appropriate signage, storage retention and anonymization rules.

The suggested system integrated several AI modules. Real-time person and face detection was performed using YOLOv8, and object tracking was performed using DeepSORT. ArcFace was used to form the basis of face recognition, and a version was implemented to detect anomalies in a Temporal CNN-Transformer architecture. To provide the ability to read, a framework was used to obtain SHAP, LIME and Grad-CAM to produce the visual and textual explanations of every alert. Descriptions were also provided on the most contributing features, visual heatmaps and counterfactual insights which were created in real time with a small latency.

Video stream decoding at the native frame rates, resizes of frames to the optimum resolution of each of the models, face alignment, and data augmentation was used as preprocessing steps during training. The inferential pipeline was constructed to manipulate incoming frames sequentially- identify and track people, extract face embeddings, detect anomalies, generate explanations and send structured alert data to a message bus to be visualized. Per-stage latency, throughput and resource consumption were performance hooks documented to quantify the overhead caused by the XAI components.

The evaluation metrics have been chosen in order to evaluate accuracy, fairness, explainability, and system performance. MAP, IDF1 and MOTA were used to evaluate object detection and tracking whereas ROC-AUC, TAR and Equal Error Rate (EER) were used to evaluate face recognition performance. The measures of fairness were demographic parity and equalized odds, depending on the subgroups, namely gender and skin tone. Anomaly detection was considered using AUC, F1 score and time-to-detect. The measure of explainability was faithfulness tests including deletion/insertion AUC, localization accuracy, sparsity and time of explanation generation. Lastly, the efficiency of the system was measured as end-to-end latency and frame-per-second throughput and the utilization of GPUs.

Ablation experiments were done to examine how various model structures, video resolutions, frame rates and XAI approaches impact the overall system performance. It has also considered the effect of different fairness mitigation measures, such as reweighting and calibration. Mean results across several random seeds were averaged to obtain statistical strength, and confidence intervals were provided. This holistic experimental procedure was the reason the analysis focused on the technical performance, as well as the ethical aspect of implementing XAI-enabled surveillance systems in practice.

5 FUTURE DIRECTIONS

This study highlights the importance of implementing explainable artificial intelligence to the AI-powered CCTV surveillance systems, where transparency does not need operational performance. SHAP and LIME had a useful interpretative value and security operators can trace the rationale of each detection or alert. This has been especially applicable in surveillance, where accountability and justification of evidence is paramount. These techniques helped improve confidence in automated decision-making by visualizing the contribution made by features to the models, thus closing the divide between the workings of deep learning models and human cognition.

The other important lesson learned during the study is the reduction of demographic bias during face recognition tasks. The explainability added in the process of assessing the model showed that there are differences in accuracy between gender and racial groups, which can be used to make specific bias reduction actions. Such imbalances will need to be addressed to ethically adopt AI because discriminatory practices and compromised trust in the security systems will be the result of bias in security systems. The enhanced fairness in our framework is in balance with the general AI governance principles, which points to the fact XAI can be both a diagnostic and remedial element to bias in surveillance practice.

The framework provided real-time pro-surveillance warning with a very low computational cost, and so interpretability is not required to be incurred at the cost of efficiency. This is important since often surveillance environments require fast reactions and any delay caused by the explanation generation might undermine its effectiveness. The findings verify that when properly implemented, XAI-enhanced models can provide not only quick notifications but also be easily explainable, and thus, are a good fit in high-stakes and large-scale security systems. The overall outcome of this work justifies the possibility of a Pro-Surveillance approach which considers explainability, fairness, and efficiency as one, coherent framework.

6 CONCLUSION

This study presents a comprehensive analysis of recent research on XAI-driven pro-surveillance CCTV systems, encompassing both efficiency and ethics in their operation. The study covers the concept of explainability integrated into AI-based surveillance. Such frameworks will make decision-making processes transparent. It also emphasized enhancing the level of trust the population has in it, enabling tracing decisions in court and compliance with the new regulatory requirements. This performance-accountability two-pronged approach makes the system a potential way to balance the imperatives of security and civil liberties. Another promising study also focuses on enhancing real-time inference, incorporating more sophisticated privacy-preserving solutions. Although testing the framework's performance across a wide range of deployment settings is necessary to ensure it is scalable and acceptable to society.

Further investigations need to concentrate on the field of intersection between computer vision, deep learning, and XAI, which is an area of innovation for advanced surveillance. There is active exploration in designing interpretable architectures without losing accuracy, finding visualization methods to explore decision paths and finding standardized assessment metrics of explainability. Scalability of the XAI-enabled surveillance, which guarantees that the explanations are consistent and reliable even when scaling to high-volume, real-time surveillance conditions, is also a technical challenge. With cities, organizations, and governments adopting AI as a part of their infrastructure in the field of public safety, the adoption of XAI in surveillance is not only an upgrade, it is a necessity to make sure that technological advancement is consistent with the values and legal principles of society. XAI may add an alarm system to notify people of an outside boundary when required, as a pro-surveillance measure. In addition to this, the use of social models in crowd analysis is still unexplored, where many contributions could be provided.

REFERENCES

[1] N. Choudhry, J. Abawajy, S. Huda, and I. Rao, “A Comprehensive Survey of Machine Learning Methods for Surveillance Videos Anomaly Detection,” IEEE Access, vol. 11, pp. 114680–114713, 2023, doi: 10.1109/ACCESS.2023.3321800.

[2] O. Elharrouss, N. Almaadeed, and S. Al-Maadeed, “A review of video surveillance systems,” J. Vis. Commun. Image Represent., vol. 77, p. 103116, May 2021, doi: 10.1016/j.jvcir.2021.103116.

[3] H. Liu, S. Chen, and N. Kubota, “Intelligent Video Systems and Analytics: A Survey,” IEEE Trans. Ind. Inform., vol. 9, no. 3, pp. 1222–1233, Aug. 2013, doi: 10.1109/TII.2013.2255616.

[4] R. Gunarathne and R. Shakya, Cutting-Edge AI-Powered Real-time Surveillance System for Proactive Threat Detection and Response in Robbery Situations in Sri Lanka. 2023.

[5] G. Sreenu and M. A. Saleem Durai, “Intelligent video surveillance: a review through deep learning techniques for crowd analysis,” J. Big Data, vol. 6, no. 1, p. 48, Jun. 2019, doi: 10.1186/s40537-019-0212-5.

[6] A. D. and M. R.i., “Edge computing based surveillance framework for real time activity recognition,” ICT Express, vol. 7, no. 2, pp. 182–186, Jun. 2021, doi: 10.1016/j.icte.2021.04.010.

[7] S. Nikkath Bushra, G. Shobana, K. Uma Maheswari, and N. Subramanian, “Smart Video Survillance Based Weapon Identification Using Yolov5,” in 2022 International Conference on Electronic Systems and Intelligent Computing (ICESIC), Chennai, India: IEEE, Apr. 2022, pp. 351–357. doi: 10.1109/ICESIC53714.2022.9783499.

[8] A. T.-Y. Chen, M. Biglari-Abhari, and K. I.-K. Wang, “Fusing Appearance and Spatio-Temporal Models for Person Re-Identification and Tracking,” J. Imaging, vol. 6, no. 5, p. 27, May 2020, doi: 10.3390/jimaging6050027.

[9] R. C. Gonzalez and R. E. Woods, Digital image processing. New York, NY: Pearson, 2018.

[10] M. Valera and S. A. Velastin, “Intelligent distributed surveillance systems: a review,” IEEE Proc. - Vis. Image Signal Process., vol. 152, no. 2, pp. 192–204, Apr. 2005, doi: 10.1049/ip-vis:20041147.

[11] W. Hu, T. Tan, L. Wang, and S. Maybank, “A Survey on Visual Surveillance of Object Motion and Behaviors,” IEEE Trans. Syst. Man Cybern. Part C Appl. Rev., vol. 34, no. 3, pp. 334–352, Aug. 2004, doi: 10.1109/TSMCC.2004.829274.

[12] W. Hu, T. Tan, L. Wang, and S. Maybank, “A survey on visual surveillance of object motion and behaviors,” IEEE Trans. Syst. Man Cybern. Part C Appl. Rev., vol. 34, no. 3, pp. 334–352, Aug. 2004, doi: 10.1109/TSMCC.2004.829274.

[13] R. Szeliski, Computer Vision: Algorithms and Applications. Springer Nature, 2022.

[14] M. T. Bhatti, M. G. Khan, M. Aslam, and M. J. Fiaz, “Weapon Detection in Real-Time CCTV Videos Using Deep Learning,” IEEE Access, vol. 9, pp. 34366–34382, 2021, doi: 10.1109/ACCESS.2021.3059170.

[15] M. Elhamod and M. D. Levine, “Automated Real-Time Detection of Potentially Suspicious Behavior in Public Transport Areas,” IEEE Trans. Intell. Transp. Syst., vol. 14, no. 2, pp. 688–699, Jun. 2013, doi: 10.1109/TITS.2012.2228640.

[16] A. B. Rashid and M. A. K. Kausik, “AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications,” Hybrid Adv., vol. 7, p. 100277, Dec. 2024, doi: 10.1016/j.hybadv.2024.100277.

[17] P. R. Brandao, “The Impact of Artificial Intelligence on Modern Society,” AI, vol. 6, no. 8, p. 190, Aug. 2025, doi: 10.3390/ai6080190.

[18] C. Fontes, E. Hohma, C. C. Corrigan, and C. Lütge, “AI-powered public surveillance systems: why we (might) need them and how we want them,” Technol. Soc., vol. 71, p. 102137, Nov. 2022, doi: 10.1016/j.techsoc.2022.102137.
[19] R. Cucchiara, “Multimedia surveillance systems,” in Proceedings of the third ACM international workshop on Video surveillance & sensor networks, in VSSN ’05. New York, NY, USA: Association for Computing Machinery, Nov. 2005, pp. 3–10. doi: 10.1145/1099396.1099399.
[20] A. Wakefield, “The Public Surveillance Functions of Private Security,” Surveill. Soc., vol. 2, no. 4, 2004, doi: 10.24908/ss.v2i4.3362.
[21] A. Geron, Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems, Third Edition, Third edition. Shroff/O’Reilly, 2022.
[22] C. V. Amrutha, C. Jyotsna, and J. Amudha, “Deep Learning Approach for Suspicious Activity Detection from Surveillance Video,” in 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Mar. 2020, pp. 335–339. doi: 10.1109/ICIMIA48430.2020.9074920.
[23] R. Golande, R. Bhapkar, A. Nalawade, A. Rashinkar, and S. Mane, “Weapon Detection System: Real-Time Object Recognition for Threat Detection,” Int. J. Res. Appl. Sci. Eng. Technol., vol. 13, no. 3, pp. 3514–3521, Mar. 2025, doi: 10.22214/ijraset.2025.68105.
[24] T. Ko, “A survey on behavior analysis in video surveillance for homeland security applications,” in 2008 37th IEEE Applied Imagery Pattern Recognition Workshop, Washington, DC, USA: IEEE, 2008, pp. 1–8. doi: 10.1109/AIPR.2008.4906450.
[25] Z. Xue et al., “Large-batch Optimization for Dense Visual Predictions: Training Faster R-CNN in 4.2 Minutes,” Adv. Neural Inf. Process. Syst., vol. 35, pp. 18694–18706, Dec. 2022.
[26] A. Singh, S. Bhatt, V. Nayak, and M. Shah, “Automation of surveillance systems using deep learning and facial recognition,” Int. J. Syst. Assur. Eng. Manag., vol. 14, no. Suppl 1, pp. 236–245, 2023, doi: 10.1007/s13198-022-01844-6.
[27] A. Rego, A. Canovas, J. M. Jiménez, and J. Lloret, “An Intelligent System for Video Surveillance in IoT Environments,” IEEE Access, vol. 6, pp. 31580–31598, 2018, doi: 10.1109/ACCESS.2018.2842034.
[28] Q. Chen, K. Fan, K. Zhang, H. Wang, H. Li, and Y. Yang, “Privacy-preserving searchable encryption in the intelligent edge computing,” Comput. Commun., vol. 164, pp. 31–41, Dec. 2020, doi: 10.1016/j.comcom.2020.09.012.
[29] V. L. Raposo, “When facial recognition does not ‘recognise’: erroneous identifications and resulting liabilities,” AI Soc., vol. 39, no. 4, pp. 1857–1869, Feb. 2023, doi: 10.1007/s00146-023-01634-z.
[30] H.-B. Kim, N. Choi, H.-J. Kwon, and H. Kim, “Surveillance System for Real-Time High-Precision Recognition of Criminal Faces From Wild Videos,” IEEE Access, vol. 11, pp. 56066–56082, 2023, doi: 10.1109/ACCESS.2023.3282451.
[31] T. Qamar and N. Z. Bawany, “Understanding the black-box: towards interpretable and reliable deep learning models,” PeerJ Comput. Sci., vol. 9, p. e1629, Nov. 2023, doi: 10.7717/peerj-cs.1629.
[32] T. Ramon, E. Chris, W. Olabiyi, and B. Favor, “AI-powered surveillance systems and anomaly detection,” Jan. 2025.
[33] A. R. Niemeijer, B. J. M. Frederiks, I. I. Riphagen, J. Legemaate, J. A. Eefsting, and C. M. P. M. Hertogh, “Ethical and practical concerns of surveillance technologies in residential care for people with dementia or intellectual disabilities: an overview of the literature,” Int. Psychogeriatr., vol. 22, no. 7, pp. 1129–1142, Nov. 2010, doi: 10.1017/S1041610210000037.
[34] R. Iphofen, “Ethical Issues in Surveillance and Privacy,” in Hostile Intent and Counter-Terrorism, CRC Press, 2015.
[35] C. Paul, “Ethical and Legal Implications of AI-Driven Surveillance: Balancing Security and Privacy in a Regulated Environment,” May 2024.
[36] A. Adadi and M. Berrada, “Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence

(XAI)," IEEE Access, vol. 6, pp. 52138–52160, 2018, doi: 10.1109/ACCESS.2018.2870052.
[37] M. Hanief Wani and A. R. Faridi, "Deep learning-based video surveillance system for suspicious activity detection," J Intell Fuzzy Syst, vol. 47, no. 1–2, pp. 71–82, Jan. 2024, doi: 10.3233/JIFS-234365.
[38] A. Fine, E. R. Berthelot, and S. Marsh, "Public Perceptions of Judges' Use of AI Tools in Courtroom Decision-Making: An Examination of Legitimacy, Fairness, Trust, and Procedural Justice," Behav. Sci., vol. 15, no. 4, p. 476, Apr. 2025, doi: 10.3390/bs15040476.
[39] M. Kattnig, A. Angerschmid, T. Reichel, and R. Kern, "Assessing trustworthy AI: Technical and legal perspectives of fairness in AI," Comput. Law Secur. Rev., vol. 55, p. 106053, Nov. 2024, doi: 10.1016/j.clsr.2024.106053.
[40] K. Barsagade, S. Tabhane, V. Satpute, and V. Kamble, "Suspicious Activity Detection Using Deep Learning Approach," in 2023 1st International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP), Mar. 2023, pp. 1–6. doi: 10.1109/IHCSP56702.2023.10127155.
[41] V. Z. Mohale and I. C. Obagbuwa, "A systematic review on the integration of explainable artificial intelligence in intrusion detection systems to enhancing transparency and interpretability in cybersecurity," Front. Artif. Intell., vol. 8, p. 1526221, Jan. 2025, doi: 10.3389/frai.2025.1526221.
[42] S. Caton and C. Haas, "Fairness in Machine Learning: A Survey," ACM Comput Surv, vol. 56, no. 7, p. 166:1-166:38, Apr. 2024, doi: 10.1145/3616865.
[43] M. Cristani, R. Raghavendra, A. Del Bue, and V. Murino, "Human behavior analysis in video surveillance: A Social Signal Processing perspective," Neurocomputing, vol. 100, pp. 86–97, Jan. 2013, doi: 10.1016/j.neucom.2011.12.038.
[44] R. Sardar et al., "Challenges in detecting security threats in WoT: a systematic literature review," Artif. Intell. Rev., vol. 58, no. 7, p. 196, Apr. 2025, doi: 10.1007/s10462-025-11176-z.
[45] A. Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations," in Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, in TrustED '16. New York, NY, USA: Association for Computing Machinery, Oct. 2016, pp. 45–54. doi: 10.1145/2995289.2995290.
[46] E. Boone, F. Ellis, L. Sullivan, and M. Wilson, "Advancing Machine Learning Through Automated Feature Discovery," pp. 1–10, Jul. 2025.
[47] L. Di, M. Mola, G. Neri, and E. Viarani, "A rule-based tracking system for video surveillance applications," Jan. 2002.
[48] A. A. Ahmed and M. Echi, "Hawk-Eye: An AI-Powered Threat Detector for Intelligent Surveillance Cameras," IEEE Access, vol. 9, pp. 63283–63293, 2021, doi: 10.1109/ACCESS.2021.3074319.
[49] T. Saheb, "'Ethically contentious aspects of artificial intelligence surveillance: a social science perspective,'" AI Ethics, vol. 3, no. 2, pp. 369–379, Jul. 2022, doi: 10.1007/s43681-022-00196-y.
[50] D. Minh, H. X. Wang, Y. F. Li, and T. N. Nguyen, "Explainable artificial intelligence: a comprehensive review," Artif. Intell. Rev., vol. 55, no. 5, pp. 3503–3568, Nov. 2021, doi: 10.1007/s10462-021-10088-y.
[51] A. Barredo Arrieta et al., "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," Inf. Fusion, vol. 58, pp. 82–115, Jun. 2020, doi: 10.1016/j.inffus.2019.12.012.
[52] T. Singh, "AI-Driven Surveillance Technologies and Human Rights: Balancing Security and Privacy," Sep. 2024, pp. 703–717. doi: 10.1007/978-981-97-3690-4_53.
[53] H. Choung, P. David, and T.-W. Ling, "Acceptance of Ai-Powered Technology in Surveillance Scenarios: Role of Trust, Security, and Privacy Perceptions," 2024, Social Science Research Network, Rochester, NY: 4724446. Accessed: Apr. 04, 2026. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4724446
[54] R. Rodrigues, "Legal and human rights issues of AI: Gaps, challenges and vulnerabilities," J. Responsible Technol., vol. 4, p. 100005, Dec. 2020, doi: 10.1016/j.jrt.2020.100005.

[55] M. Irshad et al., "City Vision: CCTV Images Based Public Surveillance Model," in 2021 International Conference on Electronic Information Technology and Smart Agriculture (ICEITSA), Dec. 2021, pp. 416–420. doi: 10.1109/ICEITSA54226.2021.00085.

[56] S. Yao et al., "From lab to field: Real-world evaluation of an AI-driven Smart Video Solution to enhance community safety," Internet Things, vol. 33, p. 101716, Sep. 2025, doi: 10.1016/j.iot.2025.101716.

[57] P. R. Kalluri, W. Agnew, M. Cheng, K. Owens, L. Soldaini, and A. Birhane, "Computer-vision research powers surveillance technology," Nature, vol. 643, no. 8070, pp. 73–79, Jul. 2025, doi: 10.1038/s41586-025-08972-6.

[58] B. R. Ardabili et al., "Understanding Policy and Technical Aspects of AI-Enabled Smart Video Surveillance to Address Public Safety," Feb. 08, 2023, arXiv: arXiv:2302.04310. doi: 10.48550/arXiv.2302.04310.

[59] R. Chatterjee, A. Chatterjee, M. R. Pradhan, B. Acharya, and T. Choudhury, "A Deep Learning-Based Efficient Firearms Monitoring Technique for Building Secure Smart Cities," IEEE Access, vol. 11, pp. 37515–37524, 2023, doi: 10.1109/ACCESS.2023.3266514.

[60] K. Nguyen, T. Fernando, C. Fookes, and S. Sridharan, "Physical Adversarial Attacks for Surveillance: A Survey," IEEE Trans. Neural Netw. Learn. Syst., vol. 35, no. 12, pp. 17036–17056, Dec. 2024, doi: 10.1109/TNNLS.2023.3321432.

[61] S. Y. Mohammed, "Architecture review: Two-stage and one-stage object detection," Frankl. Open, vol. 12, p. 100322, Sep. 2025, doi: 10.1016/j.fraope.2025.100322.

[62] W. J. Yun et al., "Cooperative Multiagent Deep Reinforcement Learning for Reliable Surveillance via Autonomous Multi-UAV Control," IEEE Trans. Ind. Inform., vol. 18, no. 10, pp. 7086–7096, Oct. 2022, doi: 10.1109/TII.2022.3143175.

[63] L. Tan, T. Huangfu, L. Wu, and W. Chen, "Comparison of YOLO v3, Faster R-CNN, and SSD for Real-Time Pill Identification," Jul. 30, 2021, Research Square. doi: 10.21203/rs.3.rs-668895/v1.

[64] S. Hangaragi, T. Singh, and N. N, "Face Detection and Recognition Using Face Mesh and Deep Neural Network," Procedia Comput. Sci., vol. 218, pp. 741–749, Jan. 2023, doi: 10.1016/j.procs.2023.01.054.

[65] D. Nimma et al., "Object detection in real-time video surveillance using attention based transformer-YOLOv8 model," Alex. Eng. J., vol. 118, pp. 482–495, Apr. 2025, doi: 10.1016/j.aej.2025.01.032.

[66] E. Boone, F. Ellis, L. Sullivan, and M. Wilson, "Advancing Machine Learning Through Automated Feature Discovery," Jul. 2025.

[67] Z. Omiotek and U. Zhunissova, "Dangerous Items Detection in Surveillance Camera Images Using Faster R-CNN," Jun. 17, 2024, Computer Science and Mathematics. doi: 10.20944/preprints202406.1090.v1.

[68] C. Conde, D. Moctezuma, I. Martín De Diego, and E. Cabello, "HoGG: Gabor and HoG-based human detection for surveillance in non-controlled environments," Neurocomputing, vol. 100, pp. 19–30, Jan. 2013, doi: 10.1016/j.neucom.2011.12.037.

[69] C. Paul, "Ethical and Legal Implications of AI-Driven Surveillance: Balancing Security and Privacy in a Regulated Environment," May 2024.

[70] S. Afra and R. Alhajj, "Early warning system: From face recognition by surveillance cameras to social media analysis to detecting suspicious people," Phys. Stat. Mech. Its Appl., vol. 540, p. 123151, Feb. 2020, doi: 10.1016/j.physa.2019.123151.

[71] Y. Qian, "Face recognition technology for video surveillance integrated with particle swarm optimization algorithm," Int. J. Intell. Netw., vol. 5, pp. 145–153, Jan. 2024, doi: 10.1016/j.ijin.2024.02.008.

[72] C.-H. Chuan, R. Sun, S. Tian, and W.-H. S. Tsai, "EXplainable Artificial Intelligence (XAI) for facilitating recognition of algorithmic bias: An experiment from imposed users' perspectives," Telemat. Inform., vol. 91, p. 102135, Jul. 2024, doi: 10.1016/j.tele.2024.102135.

[73] H. Jeon, H. Kim, D. Kim, and J. Kim, "PASS-CCTV: Proactive Anomaly surveillance system for CCTV footage analysis in adverse environmental conditions," Expert Syst. Appl., vol. 254, p. 124391, Nov. 2024, doi: 10.1016/j.eswa.2024.124391.

[74] W. Sultani, C. Chen, and M. Shah, “Real-World Anomaly Detection in Surveillance Videos,” in 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT: IEEE, Jun. 2018, pp. 6479–6488. doi: 10.1109/CVPR.2018.00678.

[75] D. Gowsikhaa, S. Abirami, and R. Baskaran, “Automated human behavior analysis from surveillance videos: a survey,” Artif Intell Rev, vol. 42, no. 4, pp. 747–765, Dec. 14, doi: 10.1007/s10462-012-9341-3.

[76] D. Volosevici and G. D. Isbasoiu, “Surveillance as a Socio-Technical System: Behavioral Impacts and Self-Regulation in Monitored Environments,” Systems, vol. 13, no. 7, p. 614, Jul. 2025, doi: 10.3390/systems13070614.

[77] T. Singh, “AI-Driven Surveillance Technologies and Human Rights: Balancing Security and Privacy,” Sep. 2024. doi: 10.1007/978-981-97-3690-4_53.

[78] “Explainable AI for Intrusion Detection Systems: LIME and SHAP Applicability on Multi-Layer Perceptron,” ResearchGate, doi: 10.1109/ACCESS.2024.3368377.

[79] L. M. Wastupranata, S. G. Kong, and L. Wang, “Deep Learning for Abnormal Human Behavior Detection in Surveillance Videos—A Survey,” Electronics, vol. 13, no. 13, p. 2579, Jun. 2024, doi: 10.3390/electronics13132579.

[80] M. Ben Ayed, S. Elkosantini, S. A. Alshaya, and M. Abid, “Suspicious Behavior Recognition Based on Face Features,” IEEE Access, vol. 7, pp. 149952–149958, 2019, doi: 10.1109/ACCESS.2019.2947338.