To ensure public safety internet of things and convolutional neural network algorithm for a surveillance system enabled with 5G

Chandrasekar Priya[1], Kesavan Kumuthapriya[2], Savarimuthu Sagayamary[3], L. M. Merlin Livingston[4], Marimuthu Venkatesan[5]

[1]Department of Electrical and Electronics Engineering, Sri Sairam Engineering College, Chennai, India
[2]Department of Electronics and Communication Engineering, Tagore Engineering College, Chennai, India
[3]Department of Electronics and Communication Engineering, J.J. College of Engineering and Technology, Tiruchirappalli, India
[4]Department of Computer Science, Saveetha College of Liberal Arts and Sciences, SIMATS University, Chennai, India
[5]Department of Artificial Intelligence and Data Science, Panimalar Engineering College, Chennai, India

Article Info

Article history:

Received Jul 3, 2024
Revised Feb 15, 2025
Accepted Mar 4, 2025

Keywords:

5G connectivity
Public safety
Real-time processing
Smart cities
Surveillance systems

ABSTRACT

Public safety and security are top priorities in the constantly urbanizing society and research develops and implements a smart surveillance system using fifth generation (5G) of wireless communication technology and internet of things (IoT) technologies to improve public safety. It developed a comprehensive and responsive monitoring solution using machine learning methods, especially convolutional neural networks (CNNs). IoT devices, including high-definition cameras, environmental sensors, and drones, are carefully deployed in urban centers, transit hubs, and essential infrastructure. These devices provide data to a central processing unit through the 5G network and CNNs analyze incoming data in real-time. The CNNs are taught to recognize objects, anomalies, faces, and license plates. These tasks help the system identify risks, odd activities, and intriguing people and warn authorities of real-time irregularities and security issues, simplifying emergency responses. Predictive analytics analyzes previous data to forecast security issues, enabling preventative steps and data are protected by strict privacy protections. According to this analysis, 5G-enabled IoT surveillance systems and machine learning may improve public safety, situational awareness, and emergency response times and approach ensures that security advancements respect privacy and integrity.

Corresponding Author:

Chandrasekar Priya
Department of Electrical and Electronics Engineering, Sri Sairam Engineering College
Chennai, India
Email: Priya.eee@sairam.edu.in

1. INTRODUCTION

Events and public places need crowd management, including its definition, importance, and best practices [1] stadia, airports, retail centers, and parks will be shown to need help managing crowds also includes crowd management best practices such as pre-event planning, crowd monitoring and analysis, communication and signage, crowd control procedures, and emergency response. To discover how to handle large crowds in public spaces and events to maintain public safety and advent of smart cities is driven mainly by a desire to improve populations' quality of life via the widespread implementation of technological solutions [2]. Significant technologies and approaches to addressing the challenges people encounter as a consequence of a lack of digitization issues related to public facilities and services and public and personal safety and security are all addressed, with optimal solutions provided. The implementation of intelligent monitoring and early warning systems for public safety machines in developing smart cities [3] utilizes risk management theory as the theoretical foundation and integrates it with the practical context. Specifically, it aims to establish a framework for managing public safety risks within urban refinement management a comprehensive analysis of a typical case is conducted, which involves researching and conducting interviews to understand how communities undertake public safety risk prevention and control.

The research primarily encompasses the robot's overall design and application module design and managing emergencies in a sustainable urban environment, with an emphasis on the internet of things (IoT) and fifth generation (5G) wireless networks discussed in study [4]. The appropriate 5G communication solutions for places hit by disasters or experiencing communications outages and IoT, device-to-device communication, transport networks, cloud and fog computing, drones, and sensor networks for crisis scenarios are possible new communication technologies discussed in [4]. It provides useful information to work together to find technological solutions and use the increasing number of wirelessly connected devices to help maintain communication channels during natural disasters. A comprehensive taxonomy of catastrophe communication systems and findings in a few application areas are presented in the system and also details the essentials needed to set up reliable communications networks. Purpose the state, and the people are very worried about public safety problems due to its design benefits and technological qualities, IoT has captured the attention of many industries and fields as a promising new network technology and industrial mode.

The IoT has grown, and the notion of public safety IoT has been proposed; it has found some use in public safety [5] for regulating public safety has advanced as a result and synthesizes academic research to examine the use of IoT in public safety regulation, identify obstacles to that use, and provide solutions that highlight the field's potential for IoT growth. An intelligent IoT-based interactive sensing and alerting system developed for urban safety leverages mobile phones and Bluetooth low energy (BLE) to find stolen items in an urban area. The urban safety network featured a unique, compact, discrete sensor that combined BLE and radio-based technology. Community users' smartphones and BLE and gateways provide wake-up signals to mobile asset BLE devices [6]. Urban safety users may discover stolen valuables and inform a centralized server using Bluetooth low energy enabled smartphones system was fully tested and proved efficient in providing authorities with current technical methods to improve urban public safety services and administration.

The IoT is a rapidly expanding network of interconnected computing devices and sensors that enables new software and users have demonstrated considerable interest in video analysis for public safety making it one of the most promising application areas [7]. Its services implementation and system design still face challenges, particularly in mobile settings an IoT-enabled public safety service that uses in-car cameras and other sensors to help in surveillance. Industry 4.0, the Industrial IoT, aims to maximize efficiency and output while reducing wasteful downtime and material consumption. Any sector interested in realizing the Industrial IoT's potential should prioritize public safety [8]. It offers a conceptual framework for public safety built on the IoT the method is managing public safety during disasters and crises caused by unanticipated events or attacks. The suggested public safety framework is made to supply and assure recovery from emergency systems for public safety, with a particular focus on alarm development and communication.

a. Problem statement: This 5G-enabled IoT and machine learning with convolutional neural networks (CNNs) monitoring system for public safety aims to combat the continuously shifting nature of current urban security threats are continually changing dangers, lengthy reaction times, and restricted coverage make it difficult for conventional surveillance systems to set up. It highlights the emergency necessity for an advanced and adaptable method of public safety monitoring. Increased population density, greater crime rates, and the need to prepare for unexpected events have all contributed to the need for better security in many modern cities. Due to the inability to quickly identify and react to new threats or occurrences, traditional surveillance systems may need to be up to the task of addressing these concerns to ensure the system upholds people's rights and freedoms, dealing with data privacy problems and ethical concerns about monitoring activities is important. The significance of utilizing 5G networks for data transmission, IoT devices for data collection, and machine learning based on CNN for real-time video analysis to improve threat detection, speed up responses, and provide the honest and open use of surveillance systems and make cities and the public more secure by addressing these issues.
b. Contribution of the paper: Summarize the tri-folded contributions of the paper, which are as follows:
   - This research proposes an innovative 5G-enabled surveillance system that greatly improves public safety and utilizes the benefit of the speed and low latency of 5G networks to transfer data quickly and reliably. It develops an all-encompassing framework for monitoring public areas by integrating IoT devices such as security cameras, environmental sensors, and drones.
   - To identify possible security risks, it uses advanced CNNs for advanced video analysis, enabling real-time object identification, face recognition, and anomaly detection, and the paper's findings,

regulation enforcement, and security professionals will be better equipped to respond quickly to security events.
- This research presents methods for detecting and warning threats in real-time and public is safer due to this feature's ability to respond quickly to possible security problems and privacy regulation, promote monitoring openness, and use data anonymization methods to address ethical issues.

Important advances have been implemented in this work by establishing a 5G-enabled surveillance infrastructure, including IoT devices, integrating intelligent CNN-based video analysis, allowing real-time threat identification, and promoting ethical principles and transparency in public safety operations. A Brazilian public university uses IoT and public safety technology to become a smart campus. It analyzes a public safety system that improves via community interaction [9] and interfaces with several IoT sensors to monitor classroom temperature, student count, and other metrics recorded in components. All this information helps managers grasp emergencies like fires and terrorist strikes faster to stress tests indicated the variation had better reaction times and errors are more manageable, adaptable, and consistent after incorporating components. Public transportation in Bangladesh and throughout the Indian subcontinent requires a reliable real-time monitoring system [4] safety on the way there is essential for the growing population of Bangladesh who are either working or attending school. Society relies heavily on the IoT to keep homes and businesses protected from potential threats and bus company priority is the security of its passengers and drivers; thus, they keep close tabs on all community transportation. One of the most significant public safety applications is road traffic analysis, and the performance of the analysis and detection of traffic incidents may be considerably improved by using a low-compressed or uncompressed video stream [10].

However, the large amount of data makes it difficult to provide a high-definition video stream in real-time and advanced in 5G systems for unmanned aerial vehicle command and control, including the fundamental principles and issues involved in transmitting high-definition videos in real-time. An overview of studies using drones and ground-based analytical systems communicating via a 5G private campus network is provided to IoT and big data technologies are increasingly used for urban public safety management for improved the administration of public safety. However, there are dangers associated with putting it into practice [11] and analyzing the public safety management system under big data and IoT applications and discussing the risks and benefits offered by big data and IoT technology is necessary to increase the application level of big data and IoT technology. Conducive to raising the bar for public safety management, it suggests practical solutions to the challenges that arise when putting big data and the IoT to use in the area of public safety management drones are poised to be crucial in tomorrow's interconnected smart cities. For distributing commodities and products, acting as mobile hot spots for broadband wireless access, and keeping smart cities safe and secure [12].

Future smart cities will rely heavily on drones for various applications, but their widespread usage raises a number of technological and social problems and obstacles, such as in cyber security, privacy, and public safety. While drones have many beneficial applications, they also pose a danger to society since bad actors may utilize them to launch cyber and physical assaults to determine how drones will affect future smart cities regarding security, privacy, and public order. Drone-based cyberattacks are another area where representative data utilization scenarios included under the intelligent connected networks for security and protection initiative aim to construct an innovative framework enabling intelligent interlinking of smart infrastructures, mobile and wearable devices, and applications [13]. This framework is designed to provide a safe environment for the well-being of individuals and platform that has been implemented facilitates the cooperation between individuals and devices to enhance the safety of citizens [14]. This is achieved through the timely reporting of incidents, the ability to adapt to interconnected environments during emergencies, and assisting it enables local authorities and people to respond to these situations effectively. Infrastructure for public safety and security that is smart, networked, and up-to-date is compared to existing IoT frameworks; the proposed system's primary goal is to establish situational awareness via the coordinated efforts of both devices and humans [15].

Supporting intelligent connections between humans and entities based on goals and adapting devices to comply with human objectives, profiles, and privacy are all areas where the focus is on tourists. This includes creating the necessary infrastructure to address a number of emergencies, such as health-related issues and missing children in crowded environments [16]. The framework integrates cutting-edge approaches to information representation and connectivity, crowdsourcing, data integration, making choices, and IoT data gathering and analytics are public safety network is crucial to every country's emergency management system for natural or artificial disasters. The method helps first responders manage incidents through information and communication it proposes a computing and communication framework for a future alternate public safety network [17]. IoT for public safety and emergency response infrastructure that is new in form, cost, robustness, reliability, and adaptability [18] to help in the timely rescue of victims, the suggested system may automatically recognize. Emergency relief states brought on by a catastrophe and re-configure it accordingly these networks must be deployed rapidly while remaining completely invisible to end users [19]. The experimentation of 5G technology in the system of public protection and disaster relief use of simulated and cloud-native 5G technologies, along with different architectural and deployment options [20]. It includes feasibility assessments and field trials to verify the performance of 5G infrastructures and applications specific to various industries using long range (LoRa); Radio frequency built a long-range IoT network to protect the general public's safety [21].

The end node uses an Arduino and LoRa and the wireless network gateway is based on a Raspberry Pi data is logged from the gateway into a publicly accessible server and estimates of power consumption and associated costs are used to grade the proposed design. Public safety is evolving in response to the widespread availability of internet-connected device sensors [22] and information needed to make decisions about public safety is often extrapolated using statistical approaches. Connected systems and devices, such as those that make up the IoT, produce a constant flood of data that cannot be processed and mined using conventional methods. The focus of this system is on digital systems and techniques as they relate to public safety it suggests computing public safety as the research of digital systems and procedures that help and protect the public [23]. Safety for everyone is intrinsic to and intertwined with the pursuit of national development for public safety observe as an interdisciplinary research topic, with fundamental competencies including preserving safety for the public and sustaining economic growth and social stability of China's development and innovation over time strategy [24]. Public safety is an interconnected study field in protecting life and maintaining public property, economic growth, and social stability in studying China's medium- and long-term growth plan for engineering, science, and technology [25].

Public safety networks that use unmanned aerial vehicles and the current state of the art regarding unmanned aerial vehicle installation, resource allocation, and security problems connected to vehicle [26]. Public safety solutions should enable broadband voice and data communication and be interconnected, safe, and robust [27]. Development and implementation of modern communications and network technologies in emergency networks to support future security systems are crucial undertakings for Brazilian city of Natal uses technology for public safety to become a smart city [28]. It provides a smart city platform that collects, integrates, analyzes, and shares sensitive citizen and police vehicle data the platform's viability was assessed using a mobile app. Public safety provides communicate, chat, and localization capabilities and bounds of the relevant core 5G architecture; each service has a separate protected network section [29].

2. PROPOSED METHOD

2.1. 5G surveillance workflow

Infrastructure setup is the first step in developing this complex system to set up a system of IoT devices and ensure reliable communication using 5G technology for throughout cities, transportation hubs, and essential infrastructure, IoT devices such as high-definition cameras, drones, and environmental sensors have been placed in important places. These devices are constantly monitoring and relaying data, including video feeds, sensor readings, and information, to a centralized processing unit through the lightning-fast 5G network. The collection and transmission of data is the system's brain using IoT, devices constantly gather data from their environment and send it to the network. Sensors included inside these devices allow for the recording of audio and video as well as other environmental data, including temperature, humidity, and air quality. The low-latency and high-speed 5G network ensures this information will reach the central processing unit quickly and without interruption. The following stage, after data collection, is data processing and analysis. Machine learning methods, especially CNNs excel in tasks requiring the analysis of images and videos, such as item identification and face recognition.

These algorithms analyze incoming data in real time, drawing conclusions about dangers or abnormalities are unauthorized people and vehicles may be seen using object recognition algorithms in limited locations, and people of interest can be identified by face recognition systems. Algorithms that read license plates may be used to keep tabs on suspicious vehicles are system enters real-time analysis and alerts after processing is complete. To identify suspicious or unexpected behavior, the processed data is continually evaluated and to quickly identify potential threats, this kind of real-time analysis is essential. For instance, if the system identifies a person loitering in a prohibited location or a rapid increase in pollution levels, alarms and notifications are sent to the appropriate authorities are security risks may be dealt with quickly due to these notifications, which can be issued by text message, email, or straight to law enforcement. Integration with cloud computing is crucial for the success of this system is essential for storing and analyzing the massive volumes of data IoT devices produce.

It allows the system to grow in size as required due to its scalability and adaptability using cloud-based machine learning models may iteratively improve accuracy by analyzing data from various resources and outputs. Data storage and access are both simplified by cloud integration for video feeds and sensor data are among the information securely maintained on the cloud. This facilitates data security, compliance with data retention regulations, and the examination of data from previous periods are information may be used by authorized staff to conduct checks and trend analyses. The technology uses predictive analytics to improve security further. Patterns and trends in the data are discovered via this process models trained with this data via machine learning may predict security events. For instance, they may notice a spike in activity around a vital infrastructure site during odd hours, suggesting an impending attack with this insight, preventative steps may be taken ahead of time, such as increasing security during peak risk hours.

The privacy considerations remain a primary emphasis of the system and privacy protections are essential for the protection of people's liberties. One method is to anonymize the data so that no individual details are saved or sent to prevent unauthorized access to sensitive data; encryption and secure data transfer methods are used. In addition, the system follows stringent privacy requirements to provide data processing and integration with emergency services is crucial to the success of this system. Integration with law enforcement, fire departments, and emergency medical services is crucial the surveillance system will immediately notify emergency services and provide them with vital data in the case of a crisis or security problem. Combining these systems guarantees that first responders will always have access to the data they need to act effectively and efficiently. Figure 1 block diagram represents a 5G-enabled IoT surveillance system with cloud-based machine learning.

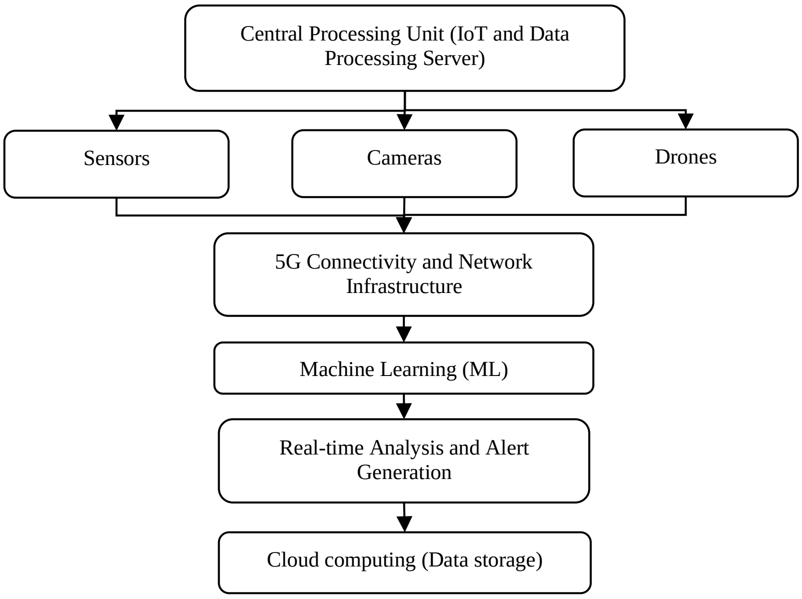
Central Processing Unit (IoT and Data Processing Server)
Sensors
Cameras
Drones
5G Connectivity and Network Infrastructure
Machine Learning (ML)
Real-time Analysis and Alert Generation
Cloud computing (Data storage)

Figure 1. Block diagram of 5G IoT surveillance and cloud ML system

3.2. Key components

3.2.1. Sensors

Passive infrared (PIR) and other motion sensors are often employed to monitor specific regions for human activity these motion detectors are crucial for safety and security and set off other mechanisms, such as cameras and alerts, to detect movement. Changes in the environment that might be harmful can be monitored and identified with the use of environmental sensors such as temperature, humidity, and air quality monitors. Audio surveillance is made possible by sound sensors which record vital acoustic data and heighten the observer's situational awareness with all these sensors working together, the system can better monitor for and react to any threats in real-time.

3.2.2. Camera

The cameras for visual monitoring and various models are available to meet various monitoring requirements are bright and detailed images captured by high-definition cameras allow for reliable identification of people and objects in a scene. For night vision and finding concealed items, thermal cameras are a must-have. Pan-tilt-zoom (PTZ) cameras provide user surveillance due to their remote tilt-and-zoom capabilities. For real-time monitoring, event analysis, and evidence collecting, these cameras' constant acquisition and transmission of visual data is integrated into the system give vital data for security officers to use in assessing situations and taking appropriate action.

3.2.3. Drones

Drones are essential to increasing the monitoring area of the system drones may be connected with cameras to provide aerial surveillance, allowing real-time monitoring of enormous regions, difficult terrain, or inaccessible places from a unique vantage point. Easily deployable, it may survey situations, monitor traffic, and provide an aerial view. Security at borders, disaster relief, and monitoring of vital infrastructure are some areas where drones shine. Integration of drones improves the system's responsiveness to unexpected threats or occurrences by providing crucial data from a viewpoint perspective to supplement ground-based monitoring elements.

3.2.4. 5G Connectivity

5G IoT surveillance systems need modems and routers for smooth data transfer; these devices provide high-speed, low-latency connections as the system's communication infrastructure. Real-time event monitoring and reaction depend on their capacity to quickly and reliably communicate data between IoT devices. The low latency of 5G technology ensures minimum data transfer delays. Security and safety applications need this feature to respond immediately to detected events. High-bandwidth 5G networks can simultaneously transmit large data streams from several sensors and high-resolution cameras are visuals and data-intensive works need this capability.

5G networks' dependability reduces network downtime and disturbances. This dependability ensures that monitoring continues even under difficult situations are scalability of 5G infrastructures makes it ideal for surveillance systems, allowing quick addition of sensors and cameras as operating needs change. 5G networks span urban and rural locations, expanding the monitoring system for security and safety monitoring may be deployed across varied landscapes and places with this extensive coverage. 5G networks use strong encryption and authentication to safeguard data transfer and integrity of surveillance data need this precaution. Figure 2 shows the diagram outlining the key steps involved in IoT-based surveillance. Table 1 algorithm visually represents the operational 5G-enabled IoT surveillance system.

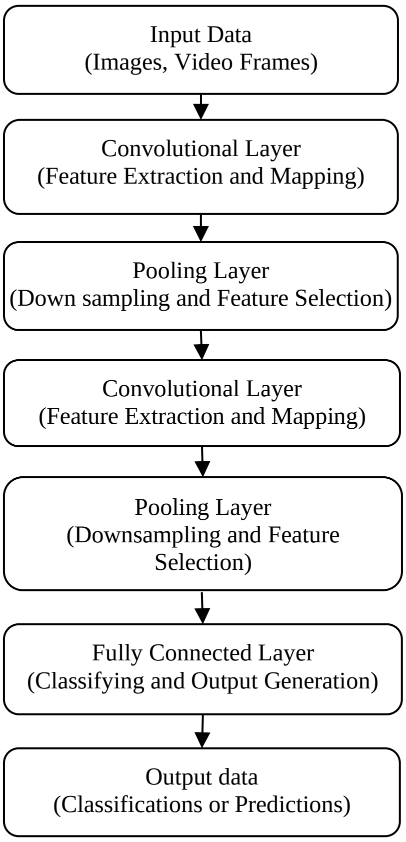
Input Data
(Images, Video Frames)
Convolutional Layer
(Feature Extraction and Mapping)
Pooling Layer
(Down sampling and Feature Selection)
Convolutional Layer
(Feature Extraction and Mapping)
Pooling Layer
(Downsampling and Feature Selection)
Fully Connected Layer
(Classifying and Output Generation)
Output data
(Classifications or Predictions)

Figure 2. CNN model overview

Table 1. Workflow algorithm

Steps	Algorithm
1	Data collection: Gather data from sensors, cameras, and drones.
2	Data transmission: Transmit data over 5G networks
3	Data preprocessing: Enhance data quality through filtering and normalization.
4	Real-time cloud analysis: Analyze data using CNN techniques in real-time.
5	Anomaly detection: Detect and classify events based on predefined criteria.
6	User interface monitoring: Provide real-time monitoring for operators.
7	Response: Trigger appropriate responses to detected events.
8	Data storage: Securely store surveillance data in the cloud.
9	Reporting: Generate detailed anomaly detection reports and analytics.

3.3. Training the CNN model

Critical to the operation of the 5G-enabled IoT surveillance system is the training of the CNN model to identify and categorize objects, people, and patterns of interest within the visual input it analyzes, this CNN model is subjected to intensive training utilizing massive datasets of images and videos. Data collection, preprocessing, and model training are all stages in the training process it creates a large dataset that includes a wide range of potential situations and items for the surveillance system to encounter. Images and videos have been properly categorized and annotated to serve as training material for the model. Figure 2 shows that depending on the specific task a CNN are developed for; it may contain numerous layers of every type and have a very different architectural layout.

The CNN model learns to accurately detect objects and patterns by adjusting its internal parameters continuously during training result of the computational demands of training; high-performance cloud-based computing resources are often used to speed up the learning process. After training, the CNN model is loaded into the surveillance system's main computer, where it performs ongoing analysis of camera feeds. This training, the system can perform object detection and classification in real-time, greatly improving urban security and situational awareness. Table 1 highlights the key steps and the corresponding algorithms used in this system.

3. RESULT AND DISCUSSION

Implementing findings and significant consequences for public security have resulted from deploying the 5G-enabled IoT surveillance system. The revolutionary development of surveillance and situational awareness has started due to the system's capacity to receive, transmit, and analyze data from various IoT devices, such as cameras, sensors, and drones. The system's ability to recognize and follow people, vehicles, and other things of interest in real-time has been vastly enhanced by object detection and face recognition algorithms. The technique has been crucial in effectively responding to security issues in a timely manner and anomaly detection capabilities allow for more preventative action in the face of prospective dangers are quickly identifying automobiles of interest, license plate readers have aided police operations. CNNs have allowed real-time analysis, allowing for more effective monitoring and alerts and faster responses to important incidents the solution now offers scalability and permanent data preservation thanks to cloud storage. Overall, the smart city and critical infrastructure protection applications of the 5G-enabled IoT surveillance systems have improved public safety and opened up new possibilities for data-driven decision-making, urban planning, and resource allocation. The IoT and machine learning technology can revolutionize security and surveillance Table 2 shows some example sensor readings for different sensors installed in a surveillance system.

Table 2. Sensor values

Sensor type	Location	Sample value
Motion sensor	Main entrance	Detected
Temperature sensor	Server room	25 °C
Sound sensor	Lobby	Normal
Environmental sensor	Outdoor area	Humidity: 50% CO2: 400 ppm
GPS data	Surveillance drone	Latitude: 34.0522° N Longitude: 118.2437° W

A 5G-enabled IoT surveillance system, as shown in Table 3, requires a camera values table it provides a brief but thorough overview of the system's camera setup. Camera IDs make it easy to monitor and control several cameras at once the Location field details the accurate coordinates of each camera, allowing for optimal coverage through surveillance. Each camera's status, whether it is online and actively monitoring its assigned region or Offline and maybe experiencing maintenance or technical troubles, is clearly shown in the status column and streamlined setup makes it easier to monitor the cameras and keep the surveillance system running smoothly.

Table 3. Surveillance camera details

Camera ID	Location	Type	Resolution	Status
CAM001	Main entrance	Dome Camera	1080p	Online
CAM002	Parking lot	PTZ Camera	4K	Online
CAM003	Server room	Fixed Camera	720p	Offline
CAM004	Restricted area	Bullet Camera	4K	Online
CAM005	Lobby	Dome Camera	1080p	Online

Table 4 provides an overview of the various CNN models used by the monitoring system is unique name and architecture is used to separate each model. The training time is indicated by the number of epochs, and the learning rate represents the quickly these models learn and batch size describes the many data points are processed in iteration. Indicative of each model performed on a benchmark dataset, accuracy percentages range from 0% to 100% the loss values reflect the success of the model's training, with better results corresponding to smaller loss values. It summarizes key details about the capabilities and limitations of each CNN model used in the monitoring system.

The accuracy of a monitoring system over many months is shown visually in Figure 3 metrics are broken down and explained, including accuracy, precision, recall, F1 score, false positives, false negatives, and detection time. Monitoring these key performance indicators over time allows users to evaluate the system's capability to identify and react to security incidents. The monitoring system may be optimized, and new insights gained due to the graph's potential to highlight trends, improvements, and areas for improvement.

Table 4. Performance metrics of CNN models

CNN model name	Architecture	Training epochs	Learning rate	Batch size	Accuracy (%)	Loss
Model A	ResNet-50	100	0.001	32	95.2	0.12
Model B	MobileNetV2	80	0.0005	64	93.8	0.18
Model C	InceptionV3	120	0.0002	48	96.5	0.09
Model D	VGG-16	60	0.0001	128	91.7	0.23
Model E	EfficientNet-B0	90	0.0003	16	97.1	0.15

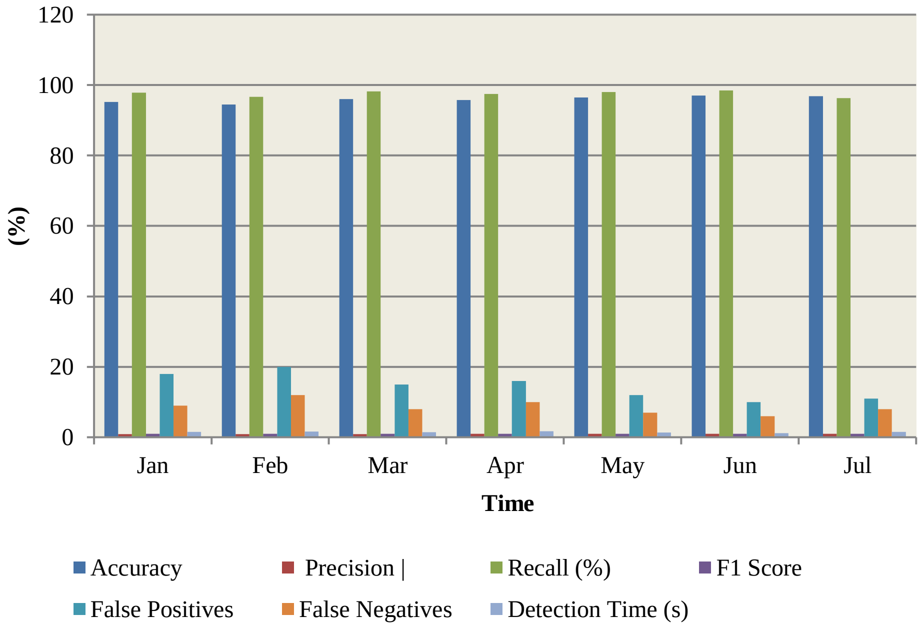

Figure 3. Monthly performance trends in surveillance system

The security and surveillance industries have found many uses for this technology since it is essential for monitoring public areas, key infrastructure, and private assets are fundamental role in designing smart cities is its ability to improve public safety by monitoring transportation, public spaces, and critical infrastructure. Additionally, it allows for extensive monitoring in industrial settings, which is essential for the protection and productivity of production operations and the safeguarding of expensive equipment. In today's connected and security-conscious world, this system is invaluable because it can give a viewpoint perspective of monitored regions, increase situational awareness, and permit quick responses.

4. CONCLUSION

The 5G-enabled IoT monitoring system is a major step forward in protecting the public for latest technology, such as 5G network connection, IoT devices, machine learning algorithms, and real-time analytic capabilities, are included in one system for maximum coverage in monitoring and identifying any dangers. Using several IoT devices, including cameras, sensors, drones, and innovative machine-learning algorithms, the system accomplishes remarkable feats are key features that improve its capacity to recognize and react to security events immediately and correctly include object detection face recognition, anomaly detection, and license plate identification. CNN provides real-time analysis, improving monitoring and shortening the lag between detecting and reacting to key events using cloud-based nature of the system's storage provides both scalability and longevity. In addition to ensuring the safety of cities and essential infrastructure, the system provides the framework for data-driven decision-making and the distribution of scarce resources. With the ability to monitor in real-time, get insights from data, and trigger a quick response, this 5G-enabled IoT surveillance system is a potent instrument for improving public safety and security. The potential for this to improve public safety and promote urban growth is huge, and it highlights the way we've come to use technology for protection.

REFERENCES

[1] T. Daware and T. Dhote, "Enhancing public safety through real-time crowd density analysis and management," in *2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA)*, Aug. 2023, pp. 1040–1046, doi: 10.1109/ICIRCA57980.2023.10220731.

[2] M. A. Jabbar, S. Tiwari, and F. Ortiz-Rodriguez, *Smart urban computing applications*. New York: River Publishers, 2022, doi: 10.1201/9781003373247.

[3] Y. Sha, M. Li, H. Xu, S. Zhang, and T. Feng, "Smart city public safety intelligent early warning and detection," *Scientific Programming*, vol. 2022, pp. 1–11, Jun. 2022, doi: 10.1155/2022/7552601.

[4] V. Sangeetha *et al.*, "Breast cancer prediction using genetic algorithm and sand cat swarm optimization algorithm," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 37, no. 2, pp. 849–858, Feb. 2025, doi: 10.11591/ijeecs.v37.i2.pp849-858.

[5] Y. Ma, C. Wu, K. Ping, H. Chen, and C. Jiang, "Internet of things applications in public safety management: a survey," *Library Hi Tech*, vol. 38, no. 1, pp. 133–144, Dec. 2018, doi: 10.1108/LHT-12-2017-0275.

[6] S. K. Sekar *et al.*, "Random forest algorithm with hill climbing algorithm to improve intrusion detection at endpoint and network," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 37, no. 1, pp. 134–142, Jan. 2025, doi: 10.11591/ijeecs.v37.i1.pp134-142.

[7] L. Liu, X. Zhang, Q. Zhang, A. Weinert, Y. Wang, and W. Shi, "AutoVAPS," in *Proceedings of the Fourth Workshop on International Science of Smart City Operations and Platforms Engineering*, Apr. 2019, pp. 41–47, doi: 10.1145/3313237.3313303.

[8] I. A. Dahlan, M. B. G. Putra, S. H. Supangkat, F. Hidayat, F. F. Lubis, and F. Hamami, "Real-time passenger social distance monitoring with video analytics using deep learning in railway station," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 26, no. 2, pp. 773–784, 2022, doi: 10.11591/ijeecs.v26.i2.pp773-784.

[9] M. R. Sudha *et al.*, "Predictive modeling for healthcare worker well-being with cloud computing and machine learning for stress management," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 15, no. 1, pp. 1218–1228, Feb. 2025, doi: 10.11591/ijece.v15i1.pp1218-1228.

[10] G. Thahniyath *et al.*, "Cloud based prediction of epileptic seizures using real-time electroencephalograms analysis," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 5, pp. 6047–6056, Oct. 2024, doi: 10.11591/ijece.v14i5.pp6047-6056.

[11] E. Vattapparamban, I. Guvenc, A. I. Yurekli, K. Akkaya, and S. Uluagac, "Drones for smart cities: issues in cybersecurity, privacy, and public safety," in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, Sep. 2016, pp. 216–221, doi: 10.1109/IWCMC.2016.7577060.

[12] C. Chatzigeorgiou, M. Feidakis, D. G. Kogias, and C. Z. Patrikakis, "Increasing safety and security in public places using IoT devices," in *2020 IEEE 6th World Forum on Internet of Things (WF-IoT)*, Jun. 2020, pp. 1–2, doi: 10.1109/WF-IoT48130.2020.9221458.

[13] P. Radhakrishnan *et al.*, "DoS attack detection and hill climbing based optimal forwarder selection," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 36, no. 2, pp. 882–891, Nov. 2024, doi: 10.11591/ijeecs.v36.i2.pp882-891.

[14] N. Mohankumar *et al.*, "Advancing chronic pain relief cloud-based remote management with machine learning in healthcare," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 37, no. 2, pp. 1042–1052, Feb. 2025, doi: 10.11591/ijeecs.v37.i2.pp1042-1052.

[15] Y. Liu *et al.*, "Design and implementation of community safety management oriented public information platform for a smart

city," in *2017 Forum on Cooperative Positioning and Service (CPGPS)*, May 2017, pp. 330–332, doi: 10.1109/CPGPS.2017.8075149.

[16] L. Amodu, O. Odiboh, S. Usaini, D. Yartey, and T. Ekanem, "Data on security implications of the adoption of internet of things by public relations professionals," *Data in Brief*, vol. 27, p. 104663, Dec. 2019, doi: 10.1016/j.dib.2019.104663.

[17] A. Buzachis, M. Fazio, A. Galletta, A. Celesti, and M. Villari, "Infrastructureless IoT-as-a-service for public safety and disaster response," in *2019 7th International Conference on Future Internet of Things and Cloud (FiCloud)*, Aug. 2019, pp. 133–140, doi: 10.1109/FiCloud.2019.00026.

[18] H. Hildmann and E. Kovacs, "Using unmanned aerial vehicles (UAVs) as mobile sensing platforms (MSPs) for disaster response, civil security and public safety," *Drones*, vol. 3, no. 3, p. 59, Jul. 2019, doi: 10.3390/drones3030059.

[19] M. Volk and J. Sterle, "5G experimentation for public safety: technologies, facilities and use cases," *IEEE Access*, vol. 9, pp. 41184–41217, 2021, doi: 10.1109/ACCESS.2021.3064405.

[20] P. S. Ramapraba *et al.*, "Implementing cloud computing in drug discovery and telemedicine for quantitative structure-activity relationship analysis," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 15, no. 1, pp. 1132–1141, Feb. 2025, doi: 10.11591/ijece.v15i1.pp1132-1141.

[21] B. Tekinerdogan, Ö. Köksal, and T. Çelik, "System architecture design of IoT-based smart cities," *Applied Sciences*, vol. 13, no. 7, p. 4173, Mar. 2023, doi: 10.3390/app13074173.

[22] A. D. Johnson, M. M. Lee, and S. Tronson, "Public safety and protection by design: opportunities and challenges for IoT and data science," *Women Securing the Future with TIPPSS for IoT: Trust, Identity, Privacy, Protection, Safety, Security for the Internet of Things*, pp. 119–129, 2019, doi: 10.1007/978-3-030-15705-0_9.

[23] P. A. M, C. M. Reddy, A. Anbarasi, N. Mohankumar, I. M.V, and S. Murugan, "Cloud-based road safety for real-time vehicle rash driving alerts with random forest algorithm," in *2024 3rd International Conference for Innovation in Technology (INOCON)*, Mar. 2024, pp. 1–6, doi: 10.1109/INOCON60754.2024.10511316.

[24] B. J. Ganesh, P. Vijayan, V. Vaidehi, S. Murugan, R. Meenakshi, and M. Rajmohan, "SVM-based predictive modeling of drowsiness in hospital staff for occupational safety solution via IoT infrastructure," in *2024 2nd International Conference on Computer, Communication and Control (IC4)*, Feb. 2024, pp. 1–5, doi: 10.1109/IC457434.2024.10486429.

[25] S. Srinivasan, S. LK, T. Alavanthar, C. Srinivasan, S. Murugan, and S. Sujatha, "IoT-enabled horticultural lighting for optimizing plant growth and agriculture operations," in *2024 2nd International Conference on Networking and Communications (ICNWC)*, Apr. 2024, pp. 1–7, doi: 10.1109/ICNWC60771.2024.10537484.

[26] R. Raman, P. R. Parvathy, P. Sapra, V. B. Sonule, and S. Murugan, "Robotic weed control and biodiversity preservation: IoT solutions for sustainable farming," in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Nov. 2023, pp. 112–117, doi: 10.1109/ICECA58529.2023.10395531.

[27] P. Maheswari, S. Gowriswari, S. Balasubramani, A. Ramesh Babu, J. NK, and S. Murugan, "Intelligent headlights for adapting beam patterns with Raspberry Pi and convolutional neural networks," in *2024 2nd International Conference on Device Intelligence, Computing and Communication Technologies (DICCT)*, Mar. 2024, pp. 182–187, doi: 10.1109/DICCT61038.2024.10533159.

[28] M. D. A. Hasan, K. Balasubadra, G. Vadivel, N. Arunfred, M. V Ishwarya, and S. Murugan, "IoT-driven image recognition for microplastic analysis in water systems using convolutional neural networks," in *2024 2nd International Conference on Computer, Communication and Control (IC4)*, Feb. 2024, pp. 1–6, doi: 10.1109/IC457434.2024.10486490.

[29] M. S. Kumar, H. Azath, A. K. Velmurugan, K. Padmanaban, and M. Subbiah, "Prediction of Alzheimer's disease using hybrid machine learning technique," in *AIP Conference Proceedings*, 2023, p. 20091, doi: 10.1063/5.0110283.

BIOGRAPHIES OF AUTHORS

Chandrasekar Priya is an associate professor in the Department of EEE, Sri Sai Ram Engineering College, Chennai. Completed UG – BE Instrumentation and Control Engineering from Madras University, PG – ME – Control and Instrumentation Engineering from Anna University. She completed PhD in the Faculty of Electrical Engineering with Specialization in Process Control from Anna University in Jan 2017. Obtained Guide ship in Anna University and currently a Recognized Supervisor in Faculty of Electrical Engineering. Reference No: 3330016, Date: 30.01.2019. Research interest includes controller design, optimization, soft computing techniques, automation. She can be contacted at email: priya.eee@sairam.edu.in.

Kesavan Kumuthapriya is presently serving as the associate professor in the Department of Electronics and Communication Engineering, Tagore Engineering College, Rathinamagalam, Vandalur-Kelambakkam Road, Chennai, Tamil Nadu, India. She graduated in electronics and communication engineering from the University of Madras in 1999, received masters in applied electronics in December 2000 respectively from University of Madras, Chennai, India. She is having over 21 years of teaching experience. Her field of interest is bio medical and wireless communication. She is a Fellow of IETE, Life Member of ISTE and IAENG Membership. She has published more than 22 papers in the International/National conferences/journals. She can be contacted at email: kumuthapriya875@gmail.com.

Savarimuthu Sagayamary received her B.E. in electronics and communication engineering from M.A.R College of Engineering and Technology (Anna University) in 2016 and her M.E. from Mother Teresa College of Engineering and Technology (Anna University) in 2019. At present, she is working as an assistant professor at J.J college of Engineering and Technology, Trichy. The author has total experience are 5 years. Her area of interest VLSI systems and digital electronics and communication. She can be contacted at email: sagayamsavarimuthu@gmail.com.

L. M. Merlin Livingston is a professor, Department of Electronics and Communication Engineering, Jeppiaar Institute of Technology, Chennai. She is a dedicated educator and a passionate researcher in electronics. She has been actively engaged in academic and research endeavours for more than twenty years, making substantial contributions to the scholarly community. Her research interests encompass a wide range of topics in electronics and communication engineering, with a specific focus on digital image processing. She has deeply engaged in research areas such as embedded systems, IoT, communication systems, and signal processing. She has authored and co-authored numerous research papers in renowned journals and conferences. She can be contacted at email: merlinlivingston@yahoo.com.

Marimuthu Venkatesan is an assistant professor in the Department of Artificial Intelligence and Data Science, Panimalar Engineering College, Chennai. He had completed his M.E (CSE) from Anna University 2012. He had completed his B.E. (CSE) from Annamalai University 2010.His areas of research include machine learning and deep learning. He can be contacted at email: venkatesan5488@gmail.com. His profile can be found on linkedin.com/in/venkatesan-m-mari-67b5209b, https://ResearchID.co/rid64644.