ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Issue–II

March – April 2026

Original Research Article

ENHANCING REAL-TIME SMART DEFENSE SURVEILLANCE THROUGH EDGE INTELLIGENCE AND IOT : KEY CHALLENGES AND PRACTICAL SOLUTIONS

**** Mrs. Sherin Varughese & **Mrs. Anita Yadav***

** Assistant Professor, ** Co-ordinator, Department of Information Technology and Computer Science, Sainath Education Trust's Rajiv Gandhi College of Arts, Commerce & Science, Vashi, Navi Mumbai,*

Abstract:

Edge computing technology is changing rapidly as organizations try to use efficient and intelligent technologies for processing data. From the various literature obtained from recent articles, it can be found that some of the trends related to the future of edge computing are as follows. Edge AI is the term given for the application of artificial intelligence directly to edge devices like sensors, smartphones, cameras, etc., instead of the cloud. Defense surveillance systems need efficient detection of threats in real-time for the security of the nation. However, while using the cloud for surveillance systems, there are many problems related to connectivity.

The paper proposes an Edge-Intelligence-enabled framework for the detection of events in real time from smart defense surveillance systems using IoT. Local processing of data from IoT sensors, cameras, and unmanned devices, integrating AI-driven analytics at the edge layer, enables faster detection of anomalies and intrusions and object tracking with reduced dependency on centralized cloud infrastructure. The proposed approach will enhance situational awareness, reduce network congestion, ensure data privacy, and guarantee operational resilience in dynamic and low-connectivity environments. Based on secondary data analysis, architectural design, key technologies, and implementation challenges of this study reveal the effectiveness of Edge Intelligence in strengthening next-generation defense surveillance systems.

Keywords: *Edge Intelligence, IoT, Defense Surveillance, Real-Time Detection, Edge Computing.*

Introduction:

Edge computing is rapidly advancing as organizations seek faster and more efficient data processing closer to the data source. Global defense systems increasingly depend on automated surveillance to detect threats like intrusions, unauthorized movement, and suspicious activities. Traditional cloud-centric models often fail to meet real-time requirements due to latency and bandwidth constraints. Edge AI — deploying AI models on edge devices — promises faster decision-making by processing data close to the source. This paper synthesizes secondary data to evaluate how IoT and edge AI synergize in defense surveillance systems. Recent literature based on secondary data highlights the growing adoption of Edge AI, where artificial intelligence algorithms are deployed directly on edge devices such as sensors, smart cameras, and IoT gateways instead of relying solely on

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Issue–II

March – April 2026

Original Research Article

centralized cloud servers. This approach reduces latency, bandwidth usage, and dependence on continuous connectivity.

In modern defense surveillance systems, real-time threat detection is critical for ensuring national security. Traditional cloud-based architectures often face delays and connectivity challenges, limiting immediate response capabilities. To address these issues, this paper proposes an Edge Intelligence–enabled framework for real-time event detection in smart defense surveillance systems leveraging IoT. By processing surveillance data locally at the edge, the system enables faster anomaly detection, intrusion identification, and object tracking while enhancing situational awareness, data privacy, and operational resilience. The study is based on secondary data and existing research findings.

Some of the key features of Edge AI involve low latency effects, as the data is processed locally on local devices. For instance, in cases of security and defense, data is sent directly to local devices, which process it locally. Since no data is sent over the internet, the data is processed almost instantly. This is important as, in cases of defense surveillance, low latency effects are very important. Data is sent to the cloud only in important forms. Thus, this feature of Edge AI reduces the data sent over the network. As a result, no congestion of the network occurs, and low costs of communication and better performance of the system ensue. Since most data is held locally, by using Edge AI, sensitive information is not sent over the internet. For instance, security and surveillance information is not sent over the network. Thus, this feature of Edge AI reduces the chances of data breaches. Since data is not sent directly to the servers, these systems of Edge AI operate even in conditions of poor or no internet. Thus, this feature of Edge AI makes these systems very reliable, as in some cases, access to the internet are not available.

Edge AI offers Faster Response Time since the data is processed directly on the devices, and the decisions are taken immediately. It is a very useful approach when it comes to time-sensitive applications like defense and security systems. It offers Better Reliability since, when data is being processed, it is not completely dependent upon the internet. Even when the internet is slow or out for a short period, this system is very effective. It offers Enhanced Data Security as data is processed near its source, resulting in less internet usage for sending data. This minimizes cyber attacks and unauthorized access to data. It enables Efficient Use of Network Resources since data is preferably sent to the cloud in a summarized form, and this minimizes network usage and enhances the performance of the system.

Some challenges with Edge AI include limited computing power and memory in which the processing power of edge devices is lower compared to cloud servers. Thus, running complex AI models becomes difficult. There are energy constraints because many edge devices depend on limited power sources. Continuous AI processing will reduce energy quickly. It also includes model optimization and deployment complexity: AI models need to be simplified to run effectively on edge devices. Performing updates to multiple device varieties poses a challenge. Device level security threats is another issue where Edge devices might be attacked either physically or digitally. Thus, very strong security measures must be taken.

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Issue–II

March – April 2026

Original Research Article

Literature Review:

Smart surveillance systems incorporate AI, IoT, and edge computing to expand beyond passive video recording into intelligent scene understanding. Hussain et al. provide a comprehensive overview of modern smart surveillance, highlighting the role of edge technologies in expanding functional capabilities like real-time anomaly detection, behavior analysis, and automated alert generation. Godase's study on Edge AI for human activity recognition demonstrates how optimized deep learning models can run on low-power edge devices to classify human behaviors in real-time surveillance with high accuracy (87.3%) while achieving low latency and power consumption — confirming the feasibility of practical EI deployments for smart surveillance

Fernandez et al. (2023) showcase how deep learning-based intrusion detection systems at the edge can provide real-time protection against denial-of-service and other network attacks — a critical requirement for defense surveillance integrity. The reviewed literature underscores the transformative potential of integrating Edge Intelligence with IoT in real-time defense surveillance. While significant progress has been made in latency reduction, distributed analytics, and secure inference, critical challenges remain in balancing performance, security, and scalability.

Research Methodology: This research adopts a secondary data–driven analytical approach to examine how Edge Intelligence and IoT technologies enhance real-time smart defense surveillance systems.

The methodology is designed to critically evaluate existing knowledge and develop an integrated understanding of edge-enabled surveillance architectures in defense environments. The research is based exclusively on secondary data obtained from reliable and recognized academic sources. These include Peer-reviewed journal publications, International conference proceedings Scholarly databases such as IEEE Xplore, SpringerLink, ScienceDirect, MDPI, ACM Digital Library, and Google Scholar. Technical and governmental reports related to defense surveillance technologies. Priority was given to recent publications to ensure that the study reflects current technological developments in edge computing, artificial intelligence, and IoT-based surveillance systems.

Analysis & Discussion: The literature collected was analyzed around a number of dimensions: processing latency, detection accuracy, bandwidth utilization, energy efficiency, system scalability, and security resilience. Low latency is fundamental to defense surveillance in that delayed responses may result in missed threats. It reduces data transmission delays as the data gets analyzed locally at the edge. However, in an environment with a lot of data-for example, many synchronized cameras-the ability of performing consistent ultra-low latency, though achievable, remains tough and requires optimization both at hardware and software levels. The computing power, memory, and energy of edge devices are normally very limited. Performing complex AI models on such devices degrades performance. Techniques like model pruning, quantization, and knowledge distillation are necessary in order to tailor AI models to resource-limited environments.

Due to their distributed nature, distributed surveillance systems form a larger surface that is prone to attacks like cybersecurity attacks involving unapproved access and tampering of information. There is also improved security with federated learning technology since it maintains privacy by ensuring that raw data is locally stored

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Issue–II

March – April 2026

Original Research Article

and that learning is executed locally. Defense surveillance systems may cover wide geographic areas and involve varying devices from different sources. Ensuring seamless communication is crucial for addressing compatibility issues involving the diverse hardware and software capabilities of these systems is essential for implementation considerations. There is also the necessity of updating artificial intelligence models applied in many edge nodes to ensure they effectively counter new threats. Models applied in diverse edge nodes necessitate timely updating to address security threats effectively.

Challenges in Edge-Enabled Defense Surveillance:

Although Edge Intelligence and IoT improve the defense surveillance systems, some problems await solution. For instance, one of the main problems associated with the systems is how to maintain real-time processing. As explained earlier, edge intelligence improves the real-time capabilities of systems through edge computing. However, handling large quantities of data, especially video, in real time is not easy. Secondly, the systems are unable to handle complex tasks due to the constraints associated with them. The devices may lack ample processing ability and battery, thus making them inefficient in handling complex tasks, especially those associated with AI models.

Security, too, is a vital factor in this regard. As more devices connect to the network, the potential risk of cyber attacks will be on the rise. This will pose serious threats, such as hacking, data theft, etc., which will incur damage to the reliability of defense surveillance systems.Scaling is yet another problem when it comes to defense surveillance systems, as most systems may have devices from different manufacturers, making communication a complex task.In finalizing the AI models, it is important to remember one critical factor: updating the models will be essential for their continued efficiency and cache value. Updating multiple devices, however, is a complex task.

Practical Solutions and Technological Approaches:

Several solutions can be put in place to resolve the challenges associated with edge-enabled defense surveillance systems. One of the solutions is the development of small AI models. Pruning and quantization are the models used in the development of small AI models. They are effective in reducing the size of the neural networks in the models. By using these models, the AI can be carried out efficiently using the edge devices. Another solution for the edge-enabled defense surveillance system is the integration of edge computing and cloud computing. However, for edge computing with cloud computing, high-speed decisions can be made efficiently by the edge computing-based systems. They can also be integrated using cloud computing for the improvement of the overall system performance. Federated learning is also a useful solution for the edge-enabled defense surveillance system. In the federated learning technique, the local devices are used efficiently. No further data needs to be transmitted for the operation of the AI models.

The bottom line is to make the security of defense surveillance systems strong, preventing cyber-attacks and unauthorized access through techniques such as data encryption, continuous authentication, and AI-based threat detection. Lastly, advanced communication technologies like 5G and emerging 6G networks improve system

ISSN: P-2455-0515
E- 2394-8450

Educreator Research Journal

OPEN ACCESS

Volume–XIII, Issue–II

March – April 2026

Original Research Article

efficiency by increasing the speed of communication and reducing delays, thus supporting real-time surveillance operations.

Conclusion:

These edge-based systems lessen response time and increase operational efficiency, as opposed to traditional cloud-dependent models, by allowing data processing at the source or near the source. By decentralizing, situational awareness is enhanced to provide speed and better-informed decision-making in mission-critical defense environments. Certain challenges around technical and operational aspects remain to be sorted out. The constraints of resources on edge devices, ever-evolving cyber threats, issues of interoperability, and increased complexity in maintaining the AI models in a distributed fashion are concerns for the future.

Overcoming these barriers requires lightweight and optimized AI techniques, hybrid edge–cloud frameworks, privacy-preserving learning methods such as federated learning, and robust security architectures built on encryption and continuous authentication.In conclusion, Edge Intelligence combined with IoT provides a strong foundation for developing responsive, secure, and scalable defense surveillance infrastructures. As communication technologies and AI methods continue to evolve, these systems are expected to become more autonomous, resilient, and capable of adapting to emerging security challenges. Continued research and practical implementation efforts will play a crucial role in realizing their full potential.

References:

1. *Fernandez, M., Lopez, J., & Gomez, A. (2023). Deep learning-based intrusion detection at the edge for secure IoT networks. IEEE Internet of Things Journal, 10(4), 3152–3164.*
2. *Godase, R. (2022). Edge AI for real-time human activity recognition using optimized deep learning models. International Journal of Intelligent Systems and Applications, 14(3), 45–56.*
3. *Hussain, M., Ullah, S., Khan, M. A., & Lee, S. (2021). Smart surveillance systems: A review of edge computing and AI-enabled architectures. IEEE Access, 9, 103598–103615.*
4. *Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637–646.*
5. *Satyanarayanan, M. (2017). The emergence of edge computing. Computer, 50(1), 30–39.*
6. *Zhang, C., & Patel, A. (2020). Security and privacy in IoT-enabled smart surveillance systems: A survey. ACM Computing Surveys, 52(5), 1–36.*
7. *Li, Y., Chen, M., & Yang, Y. (2021). Federated learning for privacy-preserving intelligent IoT applications. IEEE Network, 35(1), 50–56.*
8. *Taleb, T., Samdanis, K., Mada, B., Flinck, H., Dutta, S., & Sabella, D. (2017). On multi-access edge computing: A survey of the emerging 5G network edge architecture and orchestration. IEEE Communications Surveys & Tutorials, 19(3), 1657–1681.*

Cite This Article:

Mrs. Varughese S. & Mrs. Yadav A. (2026). *Enhancing Real-Time Smart Defense Surveillance through Edge Intelligence and IoT : Key Challenges and Practical Solutions.* **In Educreator Research Journal: Vol. XIII (Issue II),** pp. 243-247.