The Indonesian Journal of Computer Science
www.ijcs.net
Volume 15, Issue 2, April 2026
https://doi.org/10.33022/ijcs.v15i2.4879

Smart Surveillance Aided by Fog, Edge and Cloud Computing Architectures: A Critical Review

Glen Lehlohonolo Moepi[1]
moepigl@tut.ac.za[1]
[1]Department of Information and Communication Technology, Tshwane University of Technology, South Africa

Article Information

Received : 14 May 2025
Revised : 1 Mar 2026
Accepted : 5 Mar 2026

Keywords

Fog, Edge, Cloud, Surveillance System, and Internet of Things

Abstract

The rapid growth of the Internet of Things (IoT) has transformed intelligent surveillance systems, creating demands for real-time monitoring, efficient data processing, and reliable decision-making. This review examines the integration of cloud, fog, and edge computing as complementary paradigms for enhancing surveillance. Cloud computing provides large-scale storage, advanced analytics, and centralized management. Fog computing brings computation and networking closer to end devices, reducing latency and optimizing bandwidth. Edge computing enables immediate processing at the source, ensuring rapid responses to security-critical events. Together, these paradigms form a hierarchical, collaborative framework that balances scalability, efficiency, and reliability while overcoming the limitations of standalone approaches. Challenges such as device heterogeneity, interoperability issues, and security risks persist. Future directions include optimized resource allocation, lightweight Artificial Intelligence (AI) for fog and edge nodes, and stronger privacy-preserving mechanisms. The synergy of cloud, fog, and edge computing is expected to drive adaptive, secure, and resilient surveillance in IoT-based smart environments.

A. Introduction

Surveillance systems have become a necessity in day-to-day life, ensuring secure, effective monitoring of system parameters in a dynamic environment. With recent technological advancements, surveillance has shifted from its primary security role to other sectors, such as agriculture, hospitals, and power systems [1, 2]. The use of surveillance in these sectors ensures security and process monitoring. One technology adopted for surveillance across many systems is the Internet of Things (IoT). IoT has become a key innovation in Artificial Intelligence (AI), marking a major shift in modern technological landscapes. In this review, the concept of “things” refers to real-world devices that form interconnected systems through embedded sensors and processors, enabling seamless data exchange between them, which are key components for a surveillance system. These interconnected systems typically consist of two types of nodes: physical and virtual. Physical nodes include sensors, actuators, transmission units, and other embedded or wearable technologies [3]. Virtual nodes, on the other hand, represent software-based elements such as virtual machines or network components that support communication within wireless infrastructures [3, 4].

The Internet of Things (IoT) architecture integrates several essential components, including sensors, actuators, communication protocols, and cloud-based services, which are organized within a layered framework as depicted in Figure 1 [5].

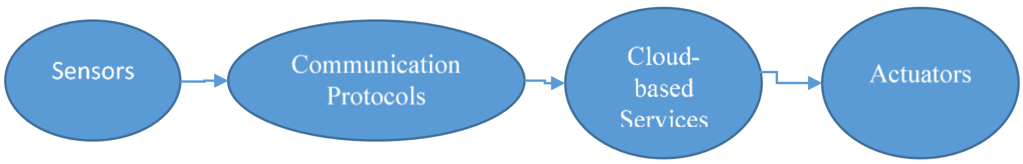

Figure 1. Components of IoT Architecture.

The IoT architecture in Figure 1 can be classified into two distinct forms: the three-layer network and the service network, as shown in Figure 2 [6]. The widely adopted three-layer architecture comprising the perception, network, and application layers supports data collection, secure transmission, analysis, and actionable decision-making for interconnected devices. These layers enable processes such as risk identification, insights generation, and rapid fault resolution [7]. To strengthen these capabilities, IoT surveillance systems often rely on cloud, fog, and edge computing architectures [8]. Cloud computing delivers scalable analytics, device monitoring, and application-specific services across various domains. Meanwhile, fog and edge computing extend computational resources to the network’s edge, ensuring real-time data processing and minimizing latency [9, 10]. As a form of utility computing, cloud services provide flexible, on-demand access to resources with guaranteed scalability and Quality of Service (QoS). Cloud computing is centralized processing and storage on remote data centers.

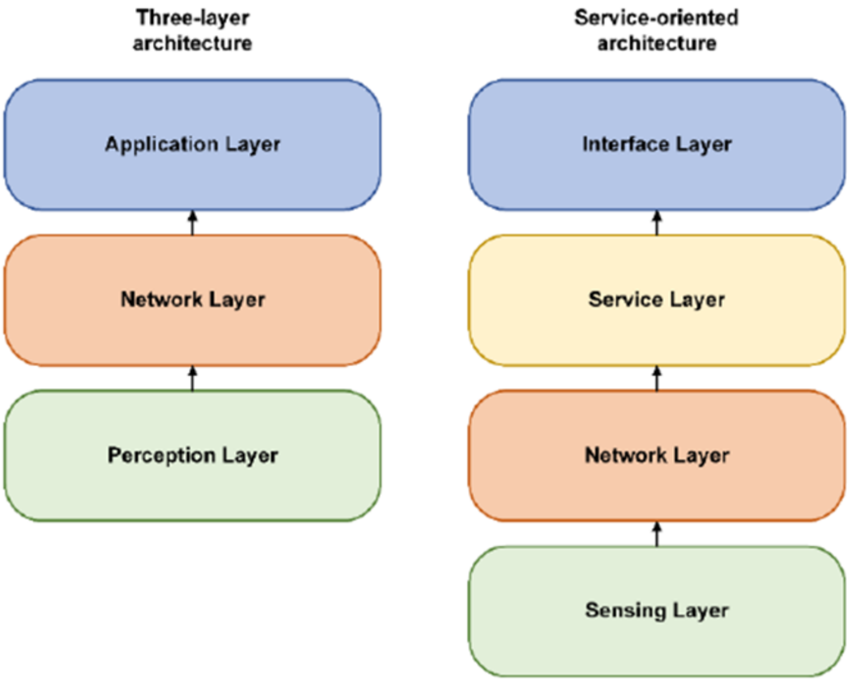

Figure 2. Three-layer architecture and service-oriented architecture of IoT.

Although the use of IoT and cloud computing in intelligent surveillance has evolved along separate paths, their integration has led to the concept of the Cloud of Things. This paradigm, built on core IoT-cloud components, expands connectivity options while reducing data transfer latency from IoT devices to the cloud [11]. In this framework, device-to-cloud interfaces act as transmission endpoints, enabling seamless communication between IoT devices and cloud services. The fusion of these two technologies enhances resource utilization in specific scenarios. Cloud platforms ensure smooth data transfer across the internet, simplifying storage and access, while fog computing extends capabilities by allowing IoT devices to process data locally, make decisions, and then forward only relevant information to the cloud [12]. Both fog and edge computing serve as complementary layers to the cloud, reducing transmission delays. However, they differ in function: fog acts as an intermediary layer between the edge and the cloud, while edge computing emphasises localised, real-time data processing [13].

B. Literature Review

B.1. Cloud, Edge and Fog Computing Architectures

The IoT framework, which underpins surveillance systems, enables devices to communicate and exchange data seamlessly. This functionality enables seamless connectivity between devices and users under diverse conditions, independent of time, location, or participating entities [14, 15, 16]. Through IoT, communication and interaction can occur across multiple systems, networks, services, and communication pathways. Within this framework, cloud computing provides the backbone for linking IoT devices and applications, enabling both device-to-device and application-to-application exchanges [17]. Complementing this, fog and edge computing extend cloud capabilities by introducing distributed architectures composed of interconnected computing resources. These decentralized networks enhance the scalability, responsiveness, and efficiency of IoT communication and data processing [11]. This section describes the detailed architectures of cloud, edge and fog computing with respect to intelligent systems.

B.2. Cloud Computing

Cloud computing provides a wide range of digital services, including servers, networking, software, databases, and data analytics, all delivered over the internet. It enables rapid deployment, flexible access to resources, and application-driven solutions [18], rather than relying on local infrastructure. Data is maintained on remote servers managed by third-party providers and accessible globally [13]. Cloud platforms operate under various services and deployment models tailored to different user needs. Deployment strategies encompass private, community, public, and hybrid models, which support individual users, organizations, or multiple institutions simultaneously [19]. This diversity makes cloud computing beneficial across a wide spectrum of users. Its key characteristics include on-demand service provision, scalability, resource pooling, mobility, cost-effectiveness, and multitenancy, making it attractive for both private and public applications [13]. However, despite these benefits, challenges remain, including downtime risks due to regional or regulatory constraints and security or confidentiality issues associated with shared resources [20]. Even so, cloud computing has been widely adopted in domains like digital governance, education, research, and storage solutions, such as surveillance systems [19, 21].

Due to the limited trustworthiness of cloud servers, ensuring data confidentiality is critical. To address this, [22] introduced a privacy-preserving outsourced classification framework. This framework applies proxy homomorphic encryption, based on Gentry's scheme, to protect sensitive information. In practice, multiple data providers submit fully homomorphic ciphertexts to an evaluator ("S"), which stores and processes encrypted data. Working together with a Cryptographic Service Provider (CSP), the evaluator develops a classification model that can perform operations on ciphertexts encrypted with different public keys [13]. This encrypted model is stored within evaluator "S" and later used to deliver secure predictions to clients [23]. Although the algorithm demonstrates semantic efficiency in both encryption and prediction, it lacks clear details regarding evaluator CSP interaction and has relatively high communication costs [24]. Moreover, another challenge lies in selecting suitable cloud services given the abundance of providers. To assist in this decision-making process, researchers have proposed a Neutrosophic Multi-Criteria Decision Analysis (NMCDA) method [13, 25], based on the Analytic Hierarchy Process (AHP). This approach evaluates cloud service quality by incorporating multiple assessment factors. In prior studies, expert panels improved the consistency of evaluation metrics by introducing a bias-mitigation model within a neutrosophic framework [13]. Triangular neutrosophic numbers were used to represent linguistic variables in the comparison matrices, thereby enabling the method to handle imprecision and inconsistency in decision-making. The NMCDA approach has demonstrated practical value for organizations in evaluating cloud services, although adoption is still in its early stages, and large-scale assessments of its effectiveness remain limited.

B.3. Edge Architecture

Edge computing is an integrated paradigm that combines networking, computation, storage, and application functions at the network's edge, located closer to the data source [26]. The computational site in this framework is referred to as an edge node, which may be situated anywhere between the data-generating devices and the central cloud, provided it has networking and processing capabilities [27, 28]. In practical implementations, devices such as smartphones and gateways are frequently cited as edge nodes [28]. While smartphones typically link individuals directly to cloud centers, gateways often connect smart homes to the cloud. The architecture of edge computing generally consists of three layers: the cloud layer, the edge layer, and the end layer, as depicted in Figure 3 [28].

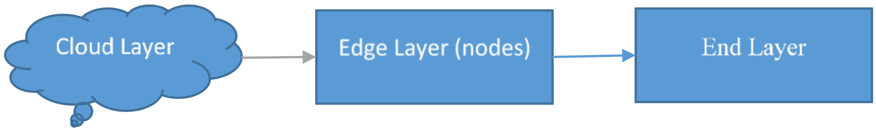

Figure 3. Architecture of Edge Computing.

The cloud layer oversees the scheduling of tasks between nodes and cloud computing centers, guided by policies to ensure efficient service delivery. Unlike purely centralized paradigms, this framework allows data and computational resources to be shared across the network during decision-making rather than transmitting everything to a remote server [29]. The edge layer serves as the central hub for all nodes, extending cloud capabilities toward the edge while continuously relaying information to the cloud layer [30]. It supports low-latency and high-traffic requirements by enabling three primary functions: data caching, local computation, and wireless access [31, 32]. Finally, the end layer, which comprises user devices, collects raw data and forwards it to higher layers for further processing. By distributing computational workloads between cloud servers and edge nodes, edge computing reduces the strain on centralized systems while improving security [33, 34]. This is achieved because most data are processed locally, limiting exposure to external risks. Therefore, any compromise of end devices affects only localized data rather than the entire cloud infrastructure [35]. Furthermore, the decentralized processing helps balance data flow and reduce bottlenecks at cloud centers [36].

However, despite these advantages, some studies [37-41] suggest that edge computing remains underutilised in service management. Improvements are needed in areas such as standardized application naming for consistent communication, addressing, and object identification. Enhanced programmability is also necessary to manage the heterogeneous nature of edge nodes, which complicates the deployment and maintenance of applications across the network.

Currently, edge computing supports a wide range of applications, including privacy preservation, cyberattack detection, and data protection, as well as intelligent transportation, vehicle safety, and resource optimisation [42]. It is also applied in time-sensitive, context-aware domains such as healthcare emergencies and personalized service recommendations. However, the exponential increase in data volumes continues to create challenges in latency-aware distribution. To address this, researchers have proposed a distributed information dissemination model [43]. This model dynamically manages data replication, creating, replacing, or deleting copies based on continuous analysis of data request patterns across edge nodes. Two operational versions are included: the source version, which generates replicas only at the central storage node, and the edge version, which manages replicas across nodes with copies and includes a mechanism for locating them. Empirical results showed a 26% reduction in delays and a 14% decrease in cost relative to non-replicated caching methods. However, the scheme does not guarantee real-time performance, which limits its suitability for critical domains such as autonomous driving and emergency healthcare.

Additionally, the transmission of large data volumes at the edge often introduces latency that conflicts with the real-time requirements of ubiquitous applications. To address this issue, a context-aware data management strategy has been proposed [44]. This method decouples data placement from task scheduling using a multi-level scheduler that allocates resources based on contextual factors. The scheduler not only assigns tasks according to performance requirements but also monitors system status during execution. It adjusts the number of replicas dynamically to balance latency reduction against added storage and management costs. The model integrates four data placement strategies, three task scheduling methods, and three runtime adaptation techniques. Findings indicate that this hybrid approach achieves task response times comparable to those of full replication while significantly reducing overhead [45, 46]. Nonetheless, large-scale deployment and validation of this method remain limited, leaving its real-world applicability an open area for further exploration.

B.4. Fog Computing

The architecture of fog computing integrates computing, storage, networking, and processing services across distributed end devices, distinguishing it from conventional cloud-based systems [47]. By positioning computational and storage resources closer to end users, fog computing bridges the gap between cloud platforms and edge devices [48]. Rather than relying solely on centralized cloud infrastructure, this model enables localized processing, reducing the distance between data generation and data analysis. The system is built on a topology of geographically dispersed nodes that perform computational, storage, and networking functions simultaneously [48, 49]. These devices, referred to as fog nodes, can be positioned wherever network connectivity exists. To qualify as a fog node, a device must be capable of computation, storage, and communication [50]. As illustrated in Figure 4, integrating cloud, fog, and edge computing architectures yields a more comprehensive IoT framework than systems that rely solely on cloud or edge resources, as shown in Figure 5. An effective IoT solution designed to solve real-world problems or enhance organizational value typically requires the combination of all three architectural approaches.

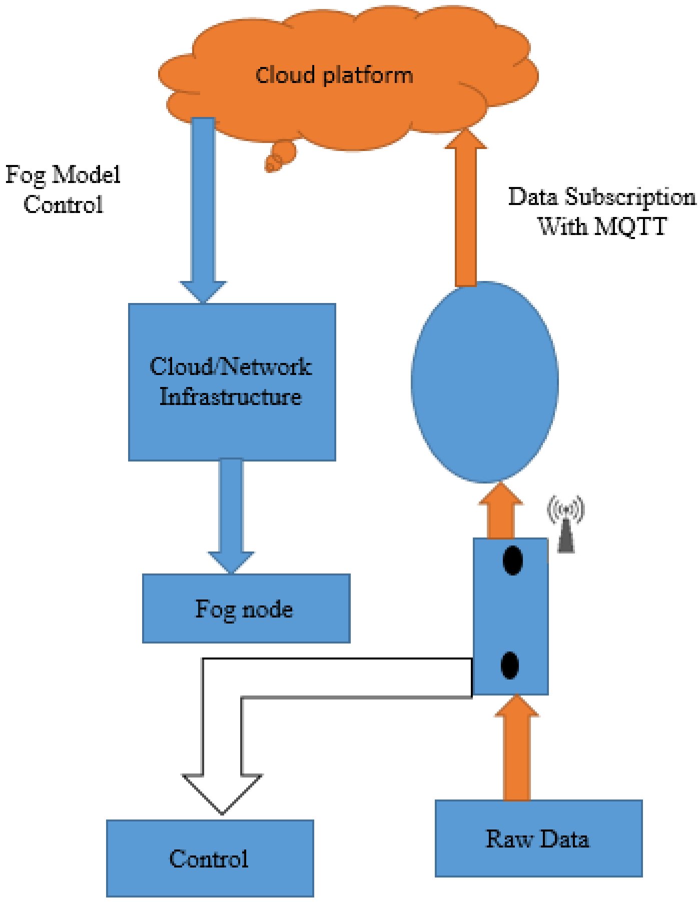

Figure 4. Cloud-edge with Fog Architecture [13].

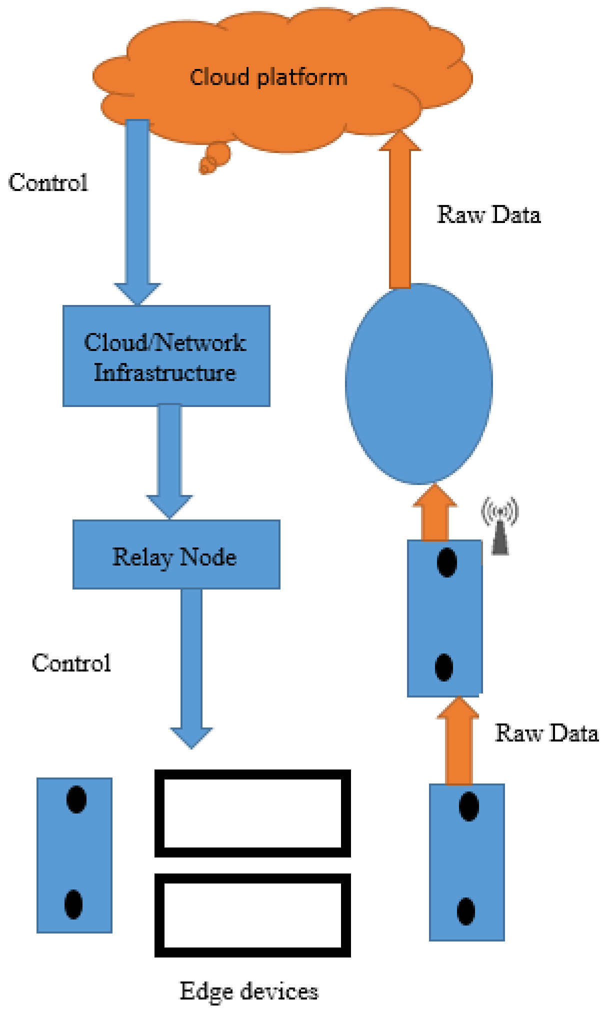

Figure 5. Cloud-Edge without Fog Architecture [13].

Functioning as an intermediary layer, fog computing enhances bandwidth efficiency and privacy by enabling local data processing and responses, which reduces the volume of information transmitted to centralized data centers [50]. This proximity to end-users also helps minimize latency and supports scalability. Nonetheless, operating near the network edge presents challenges, including vulnerability to intruder attacks, authentication difficulties, and exposure to Distributed Denial-of-Service (DDoS) threats [51]. Applications of fog computing span across healthcare, service optimization, web acceleration, road safety, surveillance video analysis, micro–data center resource management, and real-time data processing [52].

However, despite these applications, performance can be hindered by execution delays due to inefficient task scheduling and poor resource allocation [13]. To mitigate these issues, a hybrid bio-inspired algorithm has been introduced in [53]. This method combines Modified Particle Swarm Optimization (MPSO) for balancing workloads among fog nodes with Modified Cat Swarm Optimization (MCSO) to ensure the availability of fog resources. Unlike traditional fog scheduling techniques, the proposed strategy in [53] reduces power consumption, task completion time, response latency, and operational cost. However, its deployment in fog-IoT systems still requires refinement of the model's learning mechanisms to enhance adaptability and robustness. Moreover, in fog environments, users' data, often stored across cloud servers, loses local control and faces heightened privacy risks [13]. Existing privacy-preservation techniques may be inadequate against sophisticated attacks on cloud servers. To address this issue, a three-tier storage model has been proposed in [54] to enhance cloud storage utilisation while maintaining confidentiality. In this approach, user data is distributed across three layers: the cloud server, the fog server, and the local device. Data encoding is performed using the Hash-Solomon coding method, which fragments and partitions data to maximize storage efficiency [54]. Computational intelligence is then applied to determine the proportion of data allocated to each storage layer [55]. Among different coding schemes tested, the Cauchy matrix showed the best performance. Experimental results indicate that this approach achieves efficient encoding and decoding while maintaining overall storage effectiveness. Nonetheless, its scalability in handling large datasets and real-time applications has not been fully validated, raising possible concerns about latency and efficiency in practical deployments.

C. Result and Discussion

C.1. Application of Fog, Edge, and Cloud in Surveillance Systems

The core of Industry 4.0 lies in intelligent transformation enabled by advanced information technologies. Within modern distributed industrial environments, vast amounts of heterogeneous data are generated continuously, offering significant opportunities to enhance operational safety, reliability, and efficiency [56, 57]. Among these data sources, real-time video streams captured by widely deployed surveillance cameras play a critical role in monitoring personnel, equipment, and working environments. However, the ever-increasing scale of video data renders traditional manual monitoring inadequate for timely hazard or risk detection, underscoring the urgent need for intelligent video analysis. With the rapid progress of deep learning techniques [58], video object detection (VOD) based on Convolutional Neural Networks (CNNs) has emerged as a powerful tool for identifying and localizing anomalies in industrial systems. Such anomalies, ranging from unsafe worker practices and equipment malfunctions to unauthorized intrusions, can have severe consequences, placing stringent demands on the End-to-End (E2E) latency of VOD [57].

In other words, detection systems must minimize the delay between frame capture and anomaly recognition to ensure timely responses. However, achieving this goal remains challenging in distributed industrial environments characterized by heterogeneous and resource-limited devices. On the one hand, CNN-based detection algorithms are computationally intensive, often resulting in lengthy processing times when executed on constrained edge devices. On the other hand, relying solely on cloud-based processing introduces high communication latency due to the need to transmit large volumes of raw video data and significant bandwidth consumption. To overcome these limitations, the edge–cloud collaborative intelligence paradigm has gained prominence [59]. This approach distributes computational workloads between edge and cloud infrastructures, reducing latency by enabling edge devices to handle part of the processing while the cloud provides additional computational power. As illustrated in Figure 6 [57], industrial surveillance systems can leverage this framework by collecting video streams via on-site cameras and performing VOD collaboratively across edge and cloud resources, thereby supporting latency-sensitive applications. Despite these advantages, current collaborative strategies [60, 61] still face challenges in delivering real-time video detection with high accuracy under resource-constrained conditions, limiting their direct applicability to industrial surveillance scenarios.

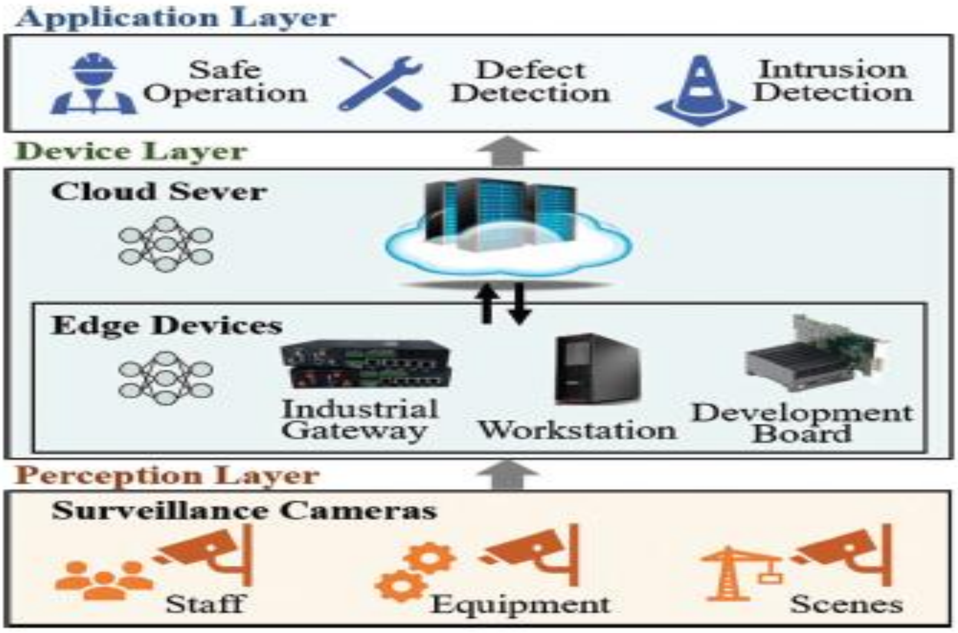

Figure 6. Edge-cloud Collaborative Framework of Industrial Systems [57].

CNN-based object detection algorithms, such as SSD (Single Shot Detector) [62] and YOLO (You Only Look Once) [63], have advanced significantly, enabling the autonomous identification and localization of objects in images. Since video data can be regarded as a sequence of consecutive video frames, an intuitive VOD solution is to directly apply image object detection to each video frame [57]. However, it yields unacceptable processing times due to the complexity of CNN-based detectors, making it impractical for latency-sensitive applications. To address this issue, various methods for increasing VOD processing acceleration have emerged. Researchers in [64, 65] construct lightweight image detectors to reduce processing time, albeit at the cost of reduced accuracy [57]. In addition, references [66-70] leverage spatiotemporal correlations between video frames, running the image detector only on a few selected frames (i.e., keyframes) and applying lightweight techniques to the remaining frames to achieve a good trade-off between speed and accuracy. For example, flow-based methods utilize optical flow predictions [66]. In contrast, memory-guided methods employ temporal models (e.g., long short-term memory [67] and attention [68] to propagate information detected in keyframes to other frames. Benefiting from the rapid advancement of the tracking network (e.g., the state-of-the-art tracking network, SiameseRPN (Region Proposal Network), [69] reaches 160 Frames Per Second (FPS) on GeForce GTX 1080Ti), recent efforts [70] utilize the tracking-assisted method to speed up VOD further. Although they significantly reduce processing time, the approaches are generally cloud-based and incur intolerable bandwidth consumption and communication latency due to the massive volume of data being uploaded.

Edge-based deployment also struggles with real-time demand due to constrained resources, leading to the rise of edge–cloud collaborative video analysis [59], which effectively reduces end-to-end (E2E) latency in distributed systems [57]. The collaborations typically offload partial computation tasks from the cloud to the edge by model partitioning and compression [71]. For example, existing collaborative VOD methods in [60, 61] generally compress video frames at the edge and then process them on the cloud. However, compression significantly affects accuracy (e.g., a 30% reduction in traffic leads to a loss of more than 12% accuracy [61]). Moreover, early exit strategies have gained significant interest recently, utilizing a multi-branch exit model to achieve fast inference while maintaining accuracy [72]. However, branchy network solutions for fast VOD in edge-cloud distributed systems are currently lacking.

Reference [57] proposed a novel tracking-assisted, collaborative, and branchy network to address the above issues. The authors of [57] applied edge and cloud computing to real-time video object detection, using power substation data as a case study. The research addresses computational and communication problems in IoT techniques, which are limited by constraints such as high end-to-end latency and cannot be directly applied to latency-sensitive applications. The authors present a light-weight edge-cloud collaborative branchy Deep Neural Network (DNN), CombiNet, and customize an intelligent edge device, Edge-Vbox, to construct an effective real-time video object detection solution. The approach is validated through a case study of intelligent smart-grid substation operation and maintenance. Experimental results using real-world data demonstrate that the approach significantly outperforms state-of-the-art methods in E2E latency and achieves real-time video object detection with negligible accuracy loss.

Reference [73] utilised fog-edge for health monitoring in Internet of Medical Things (IoMT) systems, achieving optimized latency and enhanced threat resilience. The proposed approach addresses latency and data-protection issues that prevent the use of traditional cloud techniques for real-time monitoring. Both real-world case studies and simulation experiments were employed to validate the proposed framework, with a focus on its ability to reduce latency, enhance data aggregation, and improve scalability. The findings reveal that architecture delivers notable gains compared to cloud-only models, achieving up to 70% lower latency, 30% higher energy efficiency, and a 60% reduction in bandwidth utilisation. Furthermore, the time needed for threat detection is reduced by half, enabling quicker responses to security-related events. Overall, the framework demonstrates a secure, adaptable, and high-performing solution, particularly well-suited for time-critical healthcare applications, including remote patient monitoring and emergency response systems. The authors of [74] introduced an Edge-fog-cloud-based digital twin network for autonomous and distributed structural health monitoring of a mega-dam cluster. The evaluation results show that the seismograph signal detection algorithm achieves a high accuracy of 95%, while the deviation in the virtual model's spatial mapping remains limited to 5%. Additionally, the Structural Health Monitoring (SHM) process operates nearly 9 times faster than traditional manual approaches. This digital twin framework enables efficient, autonomous, and distributed SHM across the mega dam cluster, substantially reducing labour requirements, economic costs, and energy consumption.

C.2. Merits and Challenges of Fog, Edge and Cloud in Surveillance Systems

The convergence of surveillance systems and cloud computing integrates two rapidly advancing technologies with distinct advantages. Surveillance systems typically consist of globally connected devices operating on dynamic infrastructures, but they are often constrained by limited processing power and storage. In contrast, cloud computing provides extensive storage and massive processing capacity [75]. By combining the two, many of the shortcomings of surveillance systems can be mitigated, as the cloud can handle the vast amount of data generated by billions of devices [76]. This integration not only enhances system performance but also creates opportunities for new services and applications through real-world deployment scenarios [77].

However, the transmission of surveillance data to cloud platforms introduces challenges, including unreliable handling of real-time information and heightened privacy concerns. The lack of strict policies and regulations around data protection continues to pose risks to user confidentiality [78]. Ensuring secure and reliable integration of surveillance systems with cloud-based services remains a pressing need. Edge computing further strengthens this ecosystem by decentralizing processing tasks from centralized data centers to local nodes at the network edge [79]. This architecture optimizes the use of nearby resources, allowing faster response times, localized storage, and improved control of IoT-enabled activities.

For IoT-based surveillance systems, edge computing reduces latency and enables faster decision-making by processing data closer to end users. It also supports cost-effective experimentation and analysis. Nonetheless, edge solutions are limited compared to cloud computing, particularly in terms of large-scale computational power and remote accessibility [80]. The combination of IoT-enabled surveillance systems with cloud computing has gained wide adoption due to its ability to store and analyze massive datasets. Yet, challenges remain in supporting highly time-sensitive applications such as gaming, simulation, or video streaming [81]. To address these shortcomings, fog computing has emerged as an intermediary solution. Acting between IoT devices and cloud services, fog computing extends storage and processing capacity closer to the edge while maintaining a virtualized environment for computation, memory, and networking [82]. This makes it particularly effective in managing latency-sensitive tasks, ensuring real-time communication between IoT devices [83].

Moreover, fog computing offers scalability, supporting the exponential growth of IoT networks with billions of devices. However, dynamic changes in IoT environments can disrupt workflow structures, making it difficult for fog systems to adapt effectively [84]. Additional challenges include software and hardware degradation in portable devices, as well as the random distribution of fog nodes across the edge, both of which complicate maintaining an efficient architecture [85]. These issues highlight the need for adaptive and automated solutions to optimize fog resources and sustain reliability in large-scale IoT deployments.

C.3. Future Research in Fog, Edge, and Cloud for Surveillance

The Internet of Things (IoT) has emerged as a rapidly evolving technology that can process vast amounts of data to enable intelligent, automated decision-making without human intervention. It marks a new technological generation characterized by automation and the deployment of AI-enabled devices. The supporting technologies of IoT enable the implementation of practical systems and solutions. By 2021, more than 10 billion IoT devices were active, and forecasts suggest that this number will surpass 25.4 billion by 2030, with applications extending into areas such as smart cities and smart grids [86]. IoT enhances organizational efficiency by improving data collection processes and minimizing human error.

The convergence of IoT with cloud, fog, and edge computing is becoming increasingly significant, offering complementary technologies that ensure successful integration. IoT is regarded as a cornerstone of the future internet, envisioned as a unified communication framework that integrates networks and connected devices into a single IT platform. Cloud computing is positioned as the backbone for managing and analyzing large-scale data streams in this connected ecosystem. According to the 5G Observatory Quarterly Report (2021), global IoT-supported 5G connections increased by 41%, with 124 million new connections added between Q1 and Q2 of 2021, underscoring the growing reliance on cloud-enabled IoT [86].

Researchers also emphasize the role of fog computing, highlighting its potential to reduce operational costs and address critical IoT challenges such as latency, data storage, and traffic management. The fog paradigm is considered essential for building intelligent platforms capable of managing distributed, real-time IoT applications [87]. Edge computing, when integrated with IoT alongside cloud and fog, further strengthens this ecosystem by enabling fast data processing at the source. This reduces latency, optimizes bandwidth usage, improves security, and supports real-time applications that demand instant responses. As a result, the combination of IoT with edge computing is expected to play a critical role in the development of the forthcoming Sixth Generation (6G) communication systems. The synergy between IoT and 6G is projected to bring transformative advancements, including holographic communication, telemedicine, autonomous transportation, smart cities, remote education, and brain-computer interaction technologies [88].

The widespread adoption of IoT is also expected to accelerate as advances in low-cost architectures, communication protocols, and data management capabilities drive down costs. However, cybersecurity remains a major concern. Many IoT devices lack robust protection mechanisms and are not updated regularly, exposing networks to vulnerabilities. To address these challenges, collaborative efforts are needed to establish open standards that ensure security, interoperability, and reliable service delivery. Furthermore, adopting energy-efficient and environmentally friendly technologies will be crucial to reducing power consumption as the IoT ecosystem expands [89].

The reviewed literature highlights the transformative potential of IoT on the Internet of Everything (IoE), shaping future lifestyles, promoting cultural diversity, and enhancing interactions between humans and devices. As IoT integrates more deeply with cloud, fog, and edge computing, it is expected to drive new business models and opportunities. For instance, the Cloud of Things (CoT), merging IoT with cloud computing, can mitigate limitations in scalability, computation, and data accessibility. Edge computing offers superior performance in terms of responsiveness and localized processing, while fog computing addresses latency issues in cloud-based systems by extending resources closer to end-users. This makes fog especially valuable for time-sensitive IoT applications such as gaming, financial trading, streaming, and autonomous systems. Although promising, the seamless integration of fog computing into IoT still faces challenges related to dynamic adaptation and workflow management, underscoring the need for continued research to improve its efficiency and interoperability in next-generation IoT systems.

D. Conclusion

The integration of cloud, fog, and edge computing within IoT-based intelligent surveillance systems has reshaped the way real-time monitoring, analysis, and decision-making are achieved. Cloud computing provides the necessary large-scale storage, advanced analytics, and centralized control, enabling long-term data management and deep learning applications. Complementing this, fog computing brings computational and networking capabilities closer to end devices, reducing latency and enhancing bandwidth utilization while supporting context-aware applications. Edge computing further strengthens the architecture by enabling immediate data processing at the point of collection, thereby ensuring rapid response to critical security events and minimizing dependence on centralized infrastructure. Together, these three paradigms form a hierarchical, collaborative ecosystem that strikes a balance among efficiency, scalability, and reliability. Their combined deployment addresses the limitations of standalone architectures, such as the high latency of cloud-only systems or the resource constraints of edge-only solutions, while unlocking opportunities for adaptive, real-time, and privacy-preserving surveillance. Nonetheless, challenges persist, including heterogeneous device management, security vulnerabilities, and the need for standardised frameworks to ensure interoperability. Future research directions should focus on optimizing resource allocation across the three layers, developing lightweight AI models suitable for edge and fog nodes, and strengthening privacy-preserving mechanisms to build resilient and trustworthy surveillance ecosystems.

With continued advancements, the synergy of cloud, fog, and edge computing will play a pivotal role in realizing intelligent surveillance systems that can support the evolving demands of IoT-driven smart environments. Future studies on the use of fog, edge, and cloud computing in intelligent surveillance should prioritise the development of flexible hybrid systems that can dynamically allocate computational tasks across different layers based on real-time factors such as latency, energy consumption, and network bandwidth. Emphasis should be placed on developing efficient, privacy-aware AI models that can run at the edge, incorporating federated or continual learning to handle evolving environments while safeguarding sensitive data. Additionally, efforts must focus on building secure, fault-tolerant systems that can withstand cyber threats, device failures, and mobile scenarios. The incorporation of diverse sensing modalities (such as video, audio, and thermal data) alongside context-aware processing can significantly improve detection accuracy in complex settings. Lastly, future research should aim to establish scalable, real-world deployment strategies, standardized performance evaluations, and adherence to legal, ethical, and privacy regulations to promote transparency and responsible system use.

E. References

[1] Moepi, G. L., Mathonsi, T. E., Du Plessis, D.P., Muchenje, T. and Tshilongamulenzhe, T.M. (2025). Smart Surveillance Systems: Trends, Challenges and Future Directions. The Indonesian Journal of Computer Science, 14(2), doi: https://doi.org/10.33022/ijcs.v14i2.4802.

[2] Moepi, G. L., and Mathonsi, T. E. (2024). Active Gait System for Real-Time Surveillance Against Cyber-Physical Attacks. International Conference on Cyber Warfare and Security, 19, pp. 602-606, doi: https://doi.org/10.34190/iccws.19.1.2147.

[3] Moepi, G. L., and Mathonsi, T. E. (2024). A Smart Surveillance and Clocking System for Real-Time Monitoring of the Farm Environment. pp. 1-6, doi: https://doi.org/10.1109/ICECET61485.2024.10698031.

[4] da Silva Baiense, J. P., Zdravevski, E., Coelho, P. J. S., Serrano Pires, I. M., and Velez, F. J. Driving Healthcare Monitoring with IoT and Wearable Devices: A Systematic Review.

[5] Dritsas, E., and Trigka, M. (2025). A survey on the applications of cloud computing in the industrial internet of things. Big data and cognitive computing, 9(2), 44.

[6] Dixit, S., and Kaur, U. (2025, July). Three-Tier IoT Structure: Security. In Proceedings of Fourth International Conference on Computing and Communication Networks: ICCCN 2024, 6 (1294), 239. Springer Nature.

[7] Pandey, S., Chaudhary, M., and Tóth, Z. (2025). An investigation on real-time insights: enhancing process control with IoT-enabled sensor networks. Discover Internet of Things, 5(1), 29.

[8] Islam, U., Alatawi, M. N., Alqazzaz, A., Alamro, S., Shah, B., and Moreira, F. (2025). A hybrid fog-edge computing architecture for real-time health monitoring in IoMT systems with optimized latency and threat resilience. Scientific Reports, 15(1), 25655.

[9] Bablu, T. A., and Rashid, M. T. (2025). Edge computing and its impact on real-time data processing for IoT-driven applications. Journal of advanced computing systems, 5(1), pp. 26-43.

[10] Kuchuk, H., and Malokhvii, E. (2024). Integration of IoT with cloud, fog, and edge computing: a review. Advanced Information Systems, 8(2), pp. 65-78.

[11] Ghaseminya, M. M., Eslami, E., Shahzadeh Fazeli, S. A., Abouei, J., Abbasi, E., and Karbassi, S. M. (2025). Advancing cloud virtualization: a comprehensive survey on integrating IoT, Edge, and Fog computing with FaaS for

heterogeneous smart environments: MM Ghaseminya et al. The Journal of Supercomputing, 81(14), 1303.
[12] Al-Atawi, A. A. (2024). Enhancing data management and real-time decision making with IoT, cloud, and fog computing. IET Wireless Sensor Systems, 14(6), pp. 539-562.
[13] Ahmed, S. F., Shawon, S. S., Afrin, S., Rafa, S. J., Hoque, M., and Gandomi, A. H. (2025). Optimising Internet of Things (IoT) Performance Through Cloud, Fog and Edge Computing Architecture. IET Wireless Sensor Systems, 15(1), e70016.
[14] Uzoka, A., Cadet, E., and Ojukwu, P. U. (2024). The role of telecommunications in enabling Internet of Things (IoT) connectivity and applications. Comprehensive Research and Reviews in Science and Technology, 2(02), pp. 055-073.
[15] Semary, H. E., Al-Karawi, K. A., Abdelwahab, M. M., and Elshabrawy, A. M. (2024). A Review on Internet of Things (IoT)-related disabilities and their implications. Journal of Disability Research, 3(2), 20240012.
[16] Adibi, S., Rajabifard, A., Shojaei, D., and Wickramasinghe, N. (2024). Enhancing healthcare through sensor-enabled digital twins in smart environments: A comprehensive analysis. Sensors, 24(9), 2793.
[17] Rehman, M. U., Zoha, A., Jamshed, M. A., and Ramzan, N. (Eds.). (2024). Multimodal Intelligent Sensing in Modern Applications. John Wiley and Sons.
[18] Gomathi, B., Balaji, B., Kumar, V. R., Abouhawwash, M., Aljahdali, S., Masud, M. and Kuchuk, N. (2022), "Multi-Objective optimization of energy aware virtual machine placement in cloud data center", Intelligent Automation and Soft Computing, vol. 33(3), pp. 1771–1785, doi: https://doi.org/10.32604/iasc.2022.024052.
[19] Petrovska, I., Kuchuk, H. and Mozhaiev, M. (2022), "Features of the distribution of computing resources in cloud systems", 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), doi: https://doi.org/10.1109/khpiweek57572.2022.9916459.
[20] Soni, P. K., and Dhurwe, H. (2024). Challenges and Open Issues in Cloud Computing Services. In Advanced Computing Techniques for Optimization in Cloud, pp. 19-37. Chapman and Hall/CRC.
[21] Thavi, R., Jhaveri, R., Narwane, V., Gardas, B., and Jafari Navimipour, N. (2024). Role of cloud computing technology in the education sector. Journal of Engineering, Design and Technology, 22(1), pp. 182-213.
[22] Li, P., Li, J., Huang, Z., Gao, C., Chen, W. and Chen, K. (2017), "Privacy-preserving outsourced classification in cloud computing", Cluster Computing, vol. 21(1), pp. 277–286, doi: https://doi.org/10.1007/s10586-017-0849-9.
[23] Kathole, A. B., Vhatkar, K. N., Goyal, A., Kaushik, S., Mirge, A. S., Jain, P., ... and Islam, M. T. (2024). Secure federated cloud storage protection strategy using hybrid heuristic attribute-based encryption with permissioned blockchain. IEEE Access.
[24] Cao, B., Xiao, S., Shi, L., Wang, T., Chen, J., Wang, J., and Liu, E. (2025). Web 3.0: A Survey on the Architectures, Enabling Technologies, Applications, and Challenges. IEEE Communications Surveys and Tutorials.

[25] Abdel-Basset, M., Mohamed, M. and Chang, V. (2018), "NMCDA: A framework for evaluating cloud computing services", Future Generation Computer Systems, vol. 86, pp. 12–29, doi: https://doi.org/10.1016/j.future.2018.03.014.
[26] Wang, R., Yan, J., Wang, D., Wang, H. and Yang, Q. (2018), "Knowledge-Centric edge computing based on virtualized D2D communication systems", IEEE Comm. Magazine, vol. 56(5), pp. 32–38, doi: https://doi.org/10.1109/mcom.2018.1700876.
[27] Khatatneh, K., Nawafleh, O. and Al-Utaibi, D. (2020), "The Emergence of Edge Computing Technology over Cloud Computing", International Journal of P2P Network Trends and Technology, vol. 10(2), pp. 1–5, doi: https://doi.org/10.14445/22492615/ijptt-v10i2p401.
[28] Rimal, B. P., Van, D. P. and Maier, M. (2017), "Cloudlet enhanced Fiber-Wireless access networks for Mobile-Edge Computing", IEEE Transactions on Wireless Communications, vol. 16(6), pp. 3601–3618, doi: https://doi.org/10.1109/twc.2017.2685578 .
[29] S Alsaffar, Q., and Ayed, L. B. (2024). Heterogeneous Resources in Infrastructures of the Edge Network Paradigm: A Comprehensive Review. Karbala International Journal of Modern Science, 10(2), 15.
[30] Carvalho, A., Riordan, D., and Walsh, J. (2024). A novel edge platform streamlining connectivity between modern edge devices and the cloud. Future Internet, 16(4), 111.
[31] Mousavi Jalali, S. M., and Rezaei, F. (2025). IoT data caching and scheduling in heterogeneous mobile networks by exploiting mobility and transient data characteristics. Peer-to-Peer Networking and Applications, 18(4), 167.
[32] Li, Z., Shrestha, S., Song, Z., and Tilevich, E. (2024, July). Edge Cache on WiFi Access Points: Millisecond-Level App Latency Almost for Free. In 2024 IEEE 44th International Conference on Distributed Computing Systems (ICDCS), pp. 601-612. IEEE.
[33] Wang, F., Xu, J., Wang, X. and Cui, S. (2018), "Joint offloading and computing optimization in wireless powered Mobile-Edge computing systems", IEEE Transactions on Wireless Communications, vol. 17(3), pp. 1784–1797, doi: https://doi.org/10.1109/twc.2017.2785305
[34] Ficili, I., Giacobbe, M., Tricomi, G., and Puliafito, A. (2025). From sensors to data intelligence: Leveraging IoT, cloud, and edge computing with AI. Sensors, 25(6), 1763.
[35] Bhattacharya, T., Peddi, A. V., Ponaganti, S., and Veeramalla, S. T. (2025). A survey on various security protocols of edge computing. The Journal of Supercomputing, 81(1), 310.
[36] Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M. and Wu, D. (2020), "Edge Computing in Industrial Internet of Things: architecture, advances and challenges", IEEE Communications Surveys and Tutorials, vol. 22(4), pp. 2462–2488, doi: https://doi.org/10.1109/comst.2020.3009103
[37] Veeramachaneni, V. (2025). Edge computing: Architecture, applications, and future challenges in a decentralized era. Recent trends in computer graphics and multimedia technology, 7(1), pp. 8-23.

[38] Rafique, W., Qi, L., Yaqoob, I., Imran, M., Rasool, R. U., and Dou, W. (2020). Complementing IoT services through software defined networking and edge computing: A comprehensive survey. IEEE Communications Surveys and Tutorials, 22(3), pp. 1761-1804.
[39] Sharma, M., Tomar, A., and Hazra, A. (2024). Edge computing for industry 5.0: Fundamental, applications, and research challenges. IEEE Internet of Things Journal, 11(11), pp. 19070-19093.
[40] Khan, L. U., Yaqoob, I., Tran, N. H., Kazmi, S. A., Dang, T. N., and Hong, C. S. (2020). Edge-computing-enabled smart cities: A comprehensive survey. IEEE Internet of Things journal, 7(10), 10200-10232.
[41] Porambage, P., Okwuibe, J., Liyanage, M., Ylianttila, M., and Taleb, T. (2018). Survey on multi-access edge computing for internet of things realization. IEEE Communications Surveys and Tutorials, 20(4), pp. 2961-2991.
[42] Khan, W. Z., Ahmed, E., Hakak, S., Yaqoob, I. and Ahmed, A. (2019), "Edge computing: A survey", Future Generation Computer Systems, vol 97, pp. 219–235, doi: https://doi.org/10.1016/j.future.2019.02.050 .
[43] Yin, Y. and Deng, L. (2022), "A dynamic decentralized strategy of replica placement on edge computing", International Journal of Distributed Sensor Networks, vol.18(8), 155013292211150, doi: https://doi.org/10.1177/15501329221115064.
[44] Breitbach, M., Schäfer, D., Edinger, J. and Becker, C. (2019), "Context-Aware Data and Task Placement in Edge Computing Environments", 2019 IEEE Int. Conf. Pervasive Comput. Commun. PerCom, doi: https://doi.org/10.1109/percom.2019.8767386.
[45] Ihsan, R., and Zeebaree, S. R. (2025). Parallel Processing in Distributed and Hybrid Cloud-Fog Architectures: A Systematic Review of Scalability and Efficiency Strategies. The Indonesian Journal of Computer Science, 14(1).
[46] Islam, U., Alatawi, M. N., Alqazzaz, A., Alamro, S., Shah, B., and Moreira, F. (2025). A hybrid fog-edge computing architecture for real-time health monitoring in IoMT systems with optimized latency and threat resilience. Scientific Reports, 15(1), 25655.
[47] Verma, M., Bhardwaj, N. and Yadav, A. K. (2016), "Real-time efficient scheduling algorithm for load balancing in FOG computing environment", International Journal of Information Technology and Computer Science, vol. 8(4), pp. 1–10, doi: https://doi.org/10.5815/ijitcs.2016.04.01.
[48] Hunko, M., Tkachov, V., Kovalenko, A. and Kuchuk, H. (2023), "Advantages of Fog Computing: A Comparative Analysis with Cloud Computing for Enhanced Edge Computing Capabilities", 2023 IEEE 4th KhPI Week on Advanced Technology, KhPI Week 2023 - Conference Proceedings, 02-06 October 2023, Code 194480, doi: https://doi.org/10.1109/khpiweek61412.2023.10312948.
[49] Meruje Ferreira, L. M., Coelho, F., and Pereira, J. (2024). Databases in edge and fog environments: A survey. ACM Computing Surveys, 56(11), 1-40.
[50] Kraemer, F. A., Bråten, A. E., Tamkittikhun, N., and Palma, D. (2017), "FOG Computing in Healthcare–A Review and Discussion, IEEE Access, vol. 5, pp. 9.206–9.222, doi: https://doi.org/10.1109/access.2017.2704100.

[51] Atlam, H. F., Walters, R. J. and Wills, G. (2018), "Fog Computing and the Internet of Things: a review", Big Data and Cognitive Computing, vol. 2(2), doi: https://doi.org/10.3390/bdcc2020010.

[52] Nuthalapati, A. (2024). Cloud data center performance optimization through machine learning-based workload forecasting and energy efficiency. International Journal of Science and Research Archive, 13(02), pp. 2353-2361.

[53] Rafique, H., Shah, M. A., Islam, S. U., Maqsood, T., Khan, S. and Maple, C. (2019), "A novel Bio-Inspired Hybrid Algorithm (NBIHA) for efficient resource management in Fog computing", IEEE Access, vol. 7, pp. 115.760–115.773, doi: https://doi.org/10.1109/access.2019.2924958.

[54] Wang, T., Zhou, J., Chen, X., Wang, G., Liu, A. and Liu, Y. (2018), "A Three-Layer privacy preserving cloud storage scheme based on computational intelligence in FOG computing", IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2(1), pp. 3–12, doi: https://doi.org/10.1109/tetci.2017.2764109

[55] De Donno, M., Tange, K. and Dragoni, N. (2019), "Foundations and evolution of modern computing paradigms: cloud, IoT, edge, and FOG", IEEE Access, vol. 7, pp. 150.936–150.948, doi: https://doi.org/10.1109/access.2019.2947652

[56] Bisio, A. I., Garibotto, C., Grattarola, A., Lavagetto, F., and Sciarrone, A. (2018). Exploiting context-aware capabilities over the Internet of Things for Industry 4.0 applications. IEEE Netw., vol. 32, no. 3, pp. 101–107, doi: 10.1109/MNET.2018.1700355.

[57] Guo, S., Zhao, C., Yang, S., Liang, Y., Wang, Y., and Han, Q. (2025). Edge-Cloud Collaborative Real-Time Video Object Detection for Industrial Surveillance Systems. IEEE Intelligent Systems.

[58] LeCun, Y., Bengio, Y., and Hinton, G. (2015). Deep learning. Nature, vol. 521, no. 7553, pp. 436–444, 2015,doi: 10.1038/nature14539.

[59] Han Q. et al. (2022). ECCvideo: A scalable edge cloud collaborative video analysis system. IEEE Intell. Syst., vol. 38, no. 1, pp. 34–44, doi: 10.1109/MIS.2022.3214614.

[60] Kim, S., Ko, K., Ko, H., and Leung, V. C. M. (2021). Edge-networkassisted real-time object detection framework for autonomous driving. IEEE Netw., vol. 35, no. 1, pp. 177–183, doi: 10.1109/MNET.011.2000248.

[61] J. Ren, Y. Guo, D. Zhang, Q. Liu, and Y. Zhang, "Distributed and efficient object detection in edge computing: Challenges and solutions," IEEE Netw., vol. 32, no. 6, pp. 137–143, Nov./Dec.2018, doi: 10.1109/ MNET.2018.1700415.

[62] W. Liu et al., "SSD: Single shot multibox detector," in Proc. Eur. Conf. Comput. Vision, 2015, pp. 21–37.

[63] J. Redmon and A. Farhadi, "Yolov3: An incremental improvement," 2018, arXiv:1804.02767.

[64] C. Wang, A. Bochkovskiy, and H.-Y. M. Liao, "Yolov7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors," 2022, arXiv:2207.02696.

[65] S. Liang et al., "Edge YOLO: Real-time intelligent object detection system based on edge-cloud cooperation in autonomous vehicles," IEEE Trans. Intell.

Transp. Syst., vol. 23, no. 12, pp. 25,345–25,360, Dec. 2022, doi: 10.1109/TITS.2022.3158253.
[66] X. Zhu, Y. Xiong, J. Dai, L. Yuan, and Y. Wei, "Deep feature flow for video recognition," in Proc. IEEE Comput. Vision Pattern Recognit., 2017, pp. 4141–4150, doi: 10.1109/CVPR.2017.441.
[67] M. Liu and M. Zhu, "Mobile video object detection with temporally-aware feature maps," in Proc. IEEE Comput. Vision Pattern Recognit., 2018, pp. 5686–5695, doi: 10.1109/CVPR.2018.00596.
[68] Q. Qi, X. Wang, T. Hou, Y. Yan, and H. Wang, "FastVODNet: A real-time and high-accuracy video object detector," IEEE Trans. Intell. Transp. Syst., vol. 23, no. 11, pp. 20,926–20,942, Nov. 2022, doi: 10.1109/ TITS.2022.3176721.
[69] B. Li, J. Yan, W. Wu, Z. Zhu, and X. Hu, "High performance visual tracking with Siamese region proposal network," in Proc. IEEE Comput. Vision Pattern Recognit., 2018, pp. 8971–8980, doi: 10.1109/CVPR.2018.00935.
[70] W. Yang, B. Liu, W. Li and N. Yu, "Tracking assisted faster video object detection," in IEEE Int. Conf. Multimed. Expo, 2019, pp. 1750–1755, doi: 10.1109/ ICME.2019.00301.
[71] Y. Su, W. Fan, L. Gao, L. Qiao, Y. Liu, and F. Wu, "Joint DNN partition and resource allocation optimization for energy-constrained hierarchical edge-cloud systems, IEEE Trans. Veh. Technol., vol. 72, no. 3, pp. 3930–3944, Mar. 2023, doi: 10.1109/TVT.2022.3219058.
[72] H. P. Rahmath, V. Srivastava, K. Chaurasia, R. G. Pacheco, and S. Rodrigo, "Early-exit deep neural network-a comprehensive survey," ACM Comput. Surv., vol. 57, no. 3, pp. 1–37, 2024.
[73] Islam, U., Alatawi, M. N., Alqazzaz, A., Alamro, S., Shah, B., and Moreira, F. (2025). A hybrid fog-edge computing architecture for real-time health monitoring in IoMT systems with optimized latency and threat resilience. Scientific Reports, 15(1), 25655.
[74] Li, Y., Kong, Q., Xiong, B., Chi, F., Qu, Y., and Wang, C. (2025). Edge-fog-cloud-based digital twin network for autonomous and distributed structural health monitoring of a mega dam cluster. Automation in Construction, 172, 106050.
[75] Zhou, J., Leppänen, T., Harjula, E., Ylianttila, M., Ojala, T., Chen, Y., Jin, H. and Yang, L. T. (2013), "CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing", 2013 IEEE 17th Int. Conf. Comput. Support. Coop. Work Des. CSCWD 2013, doi: https://doi.org/10.1109/cscwd.2013.6581037
[76] Díáz, M., Martin, C. L. and Rubio, B. (2016), "State-of-the-art, challenges, and open issues in the integration of Internet of Things and cloud computing", Journal of Network and Computer Applications, vol. 67, pp. 99–117, doi: https://doi.org/10.1016/j.jnca.2016.01.010
[77] Suciu, G., Vulpe, A., Halunga, S., Fratu, O., Todoran, G. and Suciu, V. (2013), "Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things", 19th Int. Conf. Control Syst. Comput. Sci. CSCS 2013, doi: https://doi.org/10.1109/cscs.2013.58
[78] Atlam, H. F., Alenezi, A., Alharthi, A., Walters, R. J. and Wills, G. (2017), "Integration of Cloud Computing with Internet of Things: Challenges and Open Issues", 2017 IEEE Int. Conf. Internet Things, IEEE Green Comput.

Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data, doi: https://doi.org/10.1109/ithings-greencom-cpscom-smartdata.2017.105
[79] Hamdan, S., Ayyash, M. and Almajali, S. (2020), "Edge-Computing Architectures for Internet of Things Applications: A survey", Sensors, vol. 20(22), 6441, doi: https://doi.org/10.3390/s20226441
[80] Naveen, S. and Kounte, M. R. (2019), "Key Technologies and challenges in IoT Edge Computing", 2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), doi: https://doi.org/10.1109/i-smac47947.2019.9032541
[81] Mouradian, C., Naboulsi, D., Yangui, S., Glitho, R., Morrow, M. and Polakos, P. (2018), "A comprehensive survey on FoG Computing: State-of-the-Art and Research challenges", IEEE Communications Surveys and Tutorials, vol. 20(1), pp. 416–464, doi: https://doi.org/10.1109/comst.2017.2771153
[82] Agarwal, S., Yadav, S. and Yadav, A. K. (2016), "An efficient architecture and algorithm for resource provisioning in Fog computing", International Journal of Information Engineering and Electronic Business, vol. 8(1), pp. 48–61, doi: https://doi.org/10.5815/ijieeb.2016.01.06
[83] Atlam, H. F., Walters, R. J. and Wills, G. (2018), "Fog Computing and the Internet of Things: a review", Big Data and Cognitive Computing, vol. 2(2), doi: https://doi.org/10.3390/bdcc2020010
[84] Luan, T. H., Gao, L., Li, Z., Xiang, Y., Wei, G. and Sun, L. (2015), "Fog Computing: focusing on mobile users at the edge", arXiv (Cornell University), doi: https://doi.org/10.48550/arxiv.1502.01815
[85] Sabireen, H. and Venkataraman, N. (2021), A" Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges", ICT Express, vol. 7(2), pp. 162–176, doi: https://doi.org/10.1016/j.icte.2021.05.004
[86] Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R. and Lin, J. C. (2022), "Applications of wireless sensor networks and Internet of Things Frameworks in the Industry Revolution 4.0: A Systematic Literature review", Sensors, vol. 22(6), 2087, doi: https://doi.org/10.3390/s22062087
[87] Gedeon, J., Brandherm, F., Egert, R., Grube, T. and Mühlhäuser, M. (2019), "What the fog? Edge Computing revisited: promises, applications and future challenges", IEEE Access, 7, pp. 152.847–152.878, doi: https://doi.org/10.1109/access.2019.2948399
[88] Malik, U. M., Javed, M. A., Zeadally, S. and Islam, S. U. (2022). Energy-Efficient FOG Computing for 6G-Enabled Massive IoT: Recent trends and future opportunities. IEEE Internet of Things Journal, 9(16), 14572–14594, doi: https://doi.org/10.1109/jiot.2021.3068056
[89] Imoize, A. L., Adedeji, O., Tandiya, N. and Shetty, S. (2021). 6G Enabled Smart Infrastructure for Sustainable Society: Opportunities, Challenges, and Research Roadmap. Sensors, 21(5), 1709, doi: https://doi.org/10.3390/s21051709