Real-Time IoT with Edge Computing: Efficiency, Security, and Future Trends

Teresa Guarda[1,2,3(✉)] and Washington Torres[1,2]

[1] Universidad Estatal Península de Santa Elena, La Libertad, Ecuador
tguarda@gmail.com
[2] Facultad de Sistemas y Telecomunicaciones, La Libertad, Ecuador
[3] Algoritmi Centre, University of Minho, Guimarães, Portugal

Abstract. The growth of the Internet of Things (IoT) has increased the need for fast data processing, efficient bandwidth use, and stronger privacy protection. Traditional cloud systems often fall short in these areas, especially for applications that rely on immediate responses. Edge computing helps solve these problems by processing data close to where it is created. This makes systems faster, reduces the load on networks, and keeps sensitive data more secure. This work is a review paper about how edge computing is being used in IoT systems and how it supports real-time actions in areas like healthcare, smart cities, and industrial automation. It also looks at how edge computing works with 5G networks and Artificial Intelligence (AI) to allow devices to make quick decisions on their own. Several case studies show how these technologies improve daily operations and protect personal data. The paper also talks about current challenges such as the cost of setting up edge systems, keeping devices secure, and making sure different devices can work together. Even with these issues, the findings show that edge computing is becoming essential for building smarter and more reliable IoT systems.

Keywords: Edge computing · Internet of Things (IoT) · Real-time Data Processing · Artificial Intelligence · 5G Networks

1 Introduction

The Internet of Things brings together devices and sensors into connected systems that produce large amounts of data throughout the day. In many practical cases, like monitoring equipment, responding to health alerts, or managing traffic, this data needs to be processed right away to support rapid decision-making. Although cloud computing can handle and store massive datasets, it often falls short when immediate action is needed, especially in settings where even a slight delay can cause problems. Sending data back and forth to remote servers can cause delays, which can limit the performance of IoT applications [1].

Edge computing takes a different approach by handling data closer to where it produced, often directly on the device or nearby. This technique shortens the time needed to process information, lowers the strain on network traffic, and reduces how much sensitive data must leave the local environment. This helps reduce wait times, skips over

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2026
O. Gervasi et al. (Eds.): ICCSA 2025 Workshops, LNCS 15889, pp. 106–116, 2026.
https://doi.org/10.1007/978-3-031-97603-2_7

data that isn't needed, and protects sensitive information. It also keeps delays down, uses bandwidth more wisely, and cuts back on how much private data gets sent to the cloud [2].

As more IoT systems are built and used in different areas, edge computing is becoming more important in how these systems are planned. It helps them run faster, stay more secure, and work more efficiently [1].

This paper looks at how edge computing is growing in IoT. It focuses on how it allows data to be processed right where it's needed, keeps personal data more private, and deals with important technical limits. The paper also describes how edge computing connects with tools like artificial intelligence (AI) and 5G networks. Real-world cases from healthcare, smart cities, and industry are included to show how it works in practice.

2 Background

This section establishes the basis for comprehending how edge computing facilitates IoT systems. It explains how processing data closer to where it is generated helps reduce delays, limits the exposure of sensitive information, and increases the dependability of connected devices. These points are important for grasping why edge computing is becoming a practical solution as IoT networks continue to grow (Fig. 1).

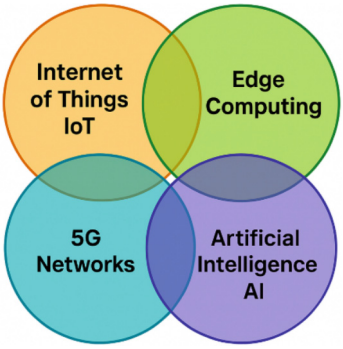

Fig. 1. Figure illustrates the interconnection between the key technologies that enable efficient and real-time IoT systems: Edge Computing enhances the responsiveness of IoT devices, while 5G Networks enable low-latency communication, AI provides intelligent data processing capabilities at the edge, and IoT connects various devices, forming the foundation for seamless and efficient data flow in modern applications.

2.1 Internet of Things (IoT)

The Internet of Things refers to the interconnection of commonplace things, devices, and equipment via networks that facilitate data transmission and reception. Devices within an IoT system may range from a basic temperature sensor to intricate systems such as autonomous vehicles or industrial robots. While working, they gather data that can be

utilized to maintain operational alignment, identify concerns promptly, and facilitate rapid decision-making.

A persistent difficulty in IoT is the necessity for immediate data processing. A delay, even a little one, might restrict the system's responsiveness and may impact safety, cost, or efficiency in some instances. Conventional cloud computing, despite its capabilities, frequently falters in scenarios demanding rapid responses [3].

2.2 Edge Computing

Edge computing is a type of distributed system that processes data close to where it is generated, rather than sending everything to distant cloud servers [4]. By bringing computation to the edge of the network, this approach reduces delays, uses bandwidth more efficiently, and makes systems more responsive—an advantage for tasks that depend on quick data handling [1, 5]. It has proven especially useful in settings that require real-time processing, like autonomous driving, smart infrastructure, and industrial control. These systems depend on up-to-the-second analysis of sensor data to support fast, accurate decisions [2]. Processing information locally also allows these systems to react quickly without needing constant access to the cloud [6].

In IoT settings, edge computing handles raw data directly at the source. It filters out unnecessary details and forwards only relevant or summarized information to the cloud [1]. This reduces traffic on communication networks and lowers the demand for cloud storage [7]. This approach also helps in remote areas or places with poor connectivity, where cloud access is not always reliable. In these cases, being able to process data locally provides a clear and useful advantage over traditional cloud-based models [8].

2.3 5G Networks and the Internet of Things

5G is especially useful in edge computing because it cuts the time needed to move data between devices. In places where time is critical, such as hospitals or industrial systems, this makes a real difference. Processing data locally, without sending it to distant servers, lets equipment respond right away to changing conditions. This avoids delays that could stop workflows or put safety at risk [2].

In urban areas, 5G connects sensor networks built into roads and public infrastructure. These sensors give up-to-date information that helps city systems act quickly. For example, they can change traffic signals or send maintenance crews when needed. Having timely and reliable data helps cities control traffic better, save energy, and respond faster when public safety is at risk [9].

A key feature that makes 5G stand out is how quickly it moves information. This low delay is especially important when edge computing runs systems that need immediate responses. Low latency is critical for edge computing in situations where a quick reaction is essential. In healthcare or industrial automation, even a short delay can affect how the system works or put safety at risk. Processing data locally helps keep systems stable and able to react fast in these high-pressure settings [2].

2.4 Artificial Intelligence and Edge Computing

Artificial Intelligence (AI) is increasingly being used in edge computing to expand what IoT devices can do. Tools like machine learning (ML) allow data to be processed directly on the device, without needing to send it to the cloud. This makes it possible for IoT systems to react quickly to real-time data and make decisions on the spot [4].

This setup is especially useful in settings where fast responses are essential for example, spotting unusual patterns in patient data, predicting equipment failures before they happen, or helping autonomous vehicles respond to changing road conditions [10]. When AI processes data directly on the device, it reduces the need to send large volumes to the cloud. This not only eases network traffic but also keeps personal information stored locally, where it is less likely to be exposed [4].

In healthcare, edge-based AI can evaluate patient data from wearable devices in real time [11]. It can detect warning signs, such as changes in heart rate or irregular glucose patterns, and send alerts right away, without sharing personal health data beyond the device. By combining AI with edge computing, it is also possible to create systems that adjust while they work. These self-learning systems improve how IoT applications respond over time, making them more efficient and able to handle more complex tasks [12].

3 The Importance of Edge Computing in Internet of Things

As the number of IoT devices grows, so does the volume of data they produce. In cloud-based systems, this data is usually sent to distant servers for processing—a process that can lead to delays and strain network capacity. For applications that rely on immediate feedback, such as autonomous driving, medical monitoring, or industrial control, even small delays can create serious problems. In time-sensitive systems, even a delay of a few milliseconds can lead to missed responses or system errors [2].

Edge computing addresses the problem by enabling data to be processed close to where it is collected, either on the device itself or on a nearby server (Table 1). This reduces transmission time, lowers latency, and allows systems to respond in real time when fast decisions are needed [8].

Edge computing improves bandwidth efficiency by performing local filtering and processing of data before sending only relevant or aggregated information to the cloud [5, 13]. This is critical in environments where connectivity is intermittent or costly, including remote locations or large-scale sensor networks. In agriculture, sensors equipped with IoT technology can track environmental variables like soil moisture, temperature, and humidity [14]. With edge computing, the system can act on that data right away by activating irrigation or issuing alerts without relying on continuous communication with cloud servers.

The combination of Artificial Intelligence (AI) and Machine Learning (ML) with edge computing marks a meaningful step forward in the development of these technologies. Running AI models directly on the device allows IoT systems to make decisions based on real-time data [15]. In smart cities, systems are expected to respond to constant shifts in traffic flow, energy usage, and public safety demands. Applying AI at the edge

Table 1. Comparative Overview of Edge Computing Benefits Across IoT Sectors.

Sector	Application Area	Key Benefits	Challenges
Healthcare	Remote monitoring, wearables	Real-time alerts, data privacy, reduced latency	Device security, cost of deployment
Smart Cities	Traffic control, surveillance	Fast response, reduced network load, local insights	Integration across systems
Industrial Automation	Predictive maintenance	Faster diagnostics, low downtime, cost reduction	Interoperability, infrastructure costs
Agriculture	Smart irrigation	Real-time response to sensor data	Rural connectivity, device resilience
Autonomous Vehicles	Real-time navigation	Low latency, on-board decision-making	Data overload, safety certification

gives these systems the ability to adjust based on what is happening locally, improving their performance as they operate over time.

4 Enhancing Privacy and Security with Edge Computing

IoT systems frequently handle personal or sensitive information, and transmitting this data over networks can expose it to unauthorized access [16]. When large volumes of data are stored in one central location, as in most cloud-based systems, they become more attractive and vulnerable to cyberattacks. Even before it reaches the cloud, transmitting personal information across the internet exposes it to interception, which may compromise privacy or security [1].

Edge computing reduces that risk by processing sensitive data locally. Only selected or anonymized information is sent to the cloud, lowering the chance of exposure [2]. For example, in healthcare, wearable devices like smartwatches or ECG monitors can analyses data directly on the device. If they detect signs of concern, such as an irregular heartbeat, alerts can be sent immediately to healthcare staff. Because the system shares only the data that is strictly necessary, it helps protect patient confidentiality and reduces the risk of a [7].

Edge computing also improves system security by embedding protective measures into the devices themselves [16], as summarized in Table 2. These may include secure boot mechanisms, hardware-level authentication, and encryption designed to keep data safe while it is being processed or sent. In the energy sector, for example, smart meters and industrial sensors that handle data locally reduce the risk of intrusion by limiting how much sensitive information leaves the device [1].

Table 2. Key differences between traditional cloud-based and edge computing-based IoT systems in terms of data privacy and security.

Traditional Cloud-Based IoT	Edge Computing-Based IoT
Data collected by IoT devices is transmitted to the cloud for processing	Data is processed locally on the device or nearby edge server
Entire data payload, often including sensitive information, is transferred	Only selected, anonymized, or aggregated data is sent to the cloud
Centralized storage creates a single point of failure	Distributed processing reduces attack surface
High risk of interception during transmission	Local analysis limits exposure and improves response time
Security added at the cloud level	Security mechanisms built into edge devices (e.g., encryption, secure boot)
Slower feedback in time-sensitive cases	Real-time alerts and adaptive system behavior

This approach also supports techniques like differential privacy and data anonymisation. These methods ensure the data sent to the cloud cannot be linked to individual users [8]. These strategies are especially important in fields like finance, where devices handle confidential records and must follow strict data protection rules [2].

5 The Future of Edge Computing in Internet of Things

The growth of edge computing in the Internet of Things (IoT) is closely connected to recent advances in 5G and artificial intelligence. 5G networks, known for their high speed and low delay, are expected to support edge computing by allowing data to be transferred and processed almost instantly.

As illustrated in Fig. 2, edge computing plays a key role between IoT devices and the cloud. Edge nodes equipped with AI and ML tools receive data from local devices, analyses it on-site to support real-time decisions, and send only selected information to the cloud. 5G enables this structure by providing fast, secure, low-latency communication across all layers.

The growing integration of 5G and edge computing is shifting how real-time systems are designed. These technologies are particularly valuable in contexts where delayed decisions carry consequences—including autonomous mobility, remote healthcare procedures, and automated industrial processes [5] (Table 3).

In the case of autonomous vehicles, much of the required processing can now be done on board. By analyzing sensor data directly within the vehicle, edge computing removes the need to consult remote servers before reacting. At the same time, 5G allows continuous, low-latency communication with nearby infrastructure from traffic lights to other cars ensuring that critical information flows fast enough to support safe navigation [1].

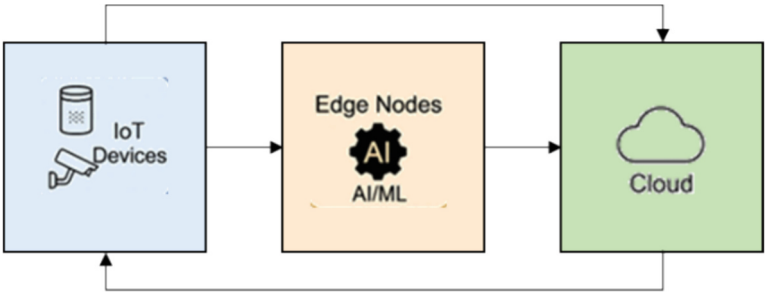

Fig. 2. Integration of Edge Computing, AI, and 5G in IoT Systems.

Table 3. Synergies of Edge Computing with Emerging Technologies

Technology	Role in Edge-IoT Integration	Impact on System Performance
5G	Enables ultra-low latency and high-speed communication	Real-time processing, faster response
Artificial Intelligence	Local data analysis and decision-making at the edge	Autonomous systems, privacy improvements
Cloud Computing	Long-term storage and deeper analytics	Offloads non-urgent processing
ML Ops	Model deployment and maintenance at the edge	Continuous learning, model optimization

Urban systems benefit in similar ways. When edge nodes analyses sensor data locally and 5G handles communication, cities can respond to traffic conditions and service needs almost as they happen. This improves both coordination and public safety, especially in densely monitored areas.

Artificial intelligence, when deployed at the edge, allows systems to respond with more flexibility and independence. Instead of sending all information to the cloud, these systems can analyses patterns locally, adapt to their environment, and act based on what is happening in real time. In industrial settings, this kind of edge-based intelligence makes it possible to spot irregularities before they turn into failures, allowing teams to intervene early and avoid unexpected downtime [17].

Rather than simply speeding up data processing, edge computing is becoming part of the foundation for building smarter, more autonomous systems. It supports real-time adaptation, helps maintain system stability, and reduces reliance on external infrastructure all of which are essential for responsive and resilient IoT operations.

6 Challenges and Trade-Offs

Despite its advantages, edge computing comes with several practical difficulties. One of the core challenges lies in managing devices that are spread across many locations. In contrast to centralized cloud systems, edge environments depend on infrastructure

that can coordinate thousands or even millions of nodes in different places [18]. This distributed nature not only complicates management but also introduces significant heterogeneity in device capabilities and protocols [19, 20] (Table 4).

One of the ongoing difficulties in deploying edge-based IoT systems is getting devices from different manufacturers to function properly within the same environment. In practice, these components are rarely built with interoperability in mind [21]. Many follow their own communication rules, data formats, or hardware configurations [22, 23]. As a result, getting devices from different vendors to operate together often takes more time than initially planned. Integrating these devices frequently encounters setbacks, largely because many of them do not adhere to the same technical standards or communication protocols [24]. In many situations, technical teams end up spending considerable time making manual adjustments to ensure that devices can communicate effectively. This process can involve reconfiguring system parameters, rewriting certain settings, or adding middleware layers to bridge compatibility gaps between components [25]. When the system includes a large number of devices, these interventions tend to escalate quickly, introducing unexpected delays that were not factored into the original project timeline [26].

Even after the system is fully operational, technical mismatches might still cause unexpected behavior, especially under real usage conditions where inconsistencies are more likely to appear than during controlled testing [4].

Security risks also increase when edge devices are placed in locations where it is hard to control physical access. Unlike centralized data centers, these devices may be exposed to theft, tampering, or other types of physical interference. In these situations, security must begin at the device level. Systems need to include strong hardware protections, verified identity credentials, and tools that can detect unexpected behavior in real time. Without this foundation, edge infrastructure becomes easier to breach, both physically and remotely [2].

This exposure raises the risk of tampering, theft, or direct manipulation. Addressing this risk requires more than software-based solutions. It calls for secure hardware, authenticated access, and mechanisms that can detect unauthorized changes in how devices behave. Without these measures, attackers may use these weaknesses, both physically and remotely, to access sensitive data or disrupt system stability [2].

Without these protections, edge nodes can become simple entry points for both physical interference and cyberattacks [2].

Cost is another challenge, especially at the infrastructure level. While edge computing reduces the need for centralized cloud services, it requires investment in local hardware and reliable networks [7]. This can be a major problem for smaller organizations or those in less developed regions, where it is harder to cover the initial costs.

Table 4. Main challenges and trade-offs in edge computing environments, including technical, operational, and economic barriers affecting deployment and maintenance.

Challenge Area	Description	Consequences
Distributed Device Management	Managing a large number of geographically dispersed nodes with heterogeneous capabilities and protocols	Complex infrastructure coordination and increased maintenance effort
Interoperability Issues	Difficulty in integrating devices from different vendors due to non-standard communication protocols and data formats	Delays in deployment due to manual configuration and middleware requirements
Post-Deployment Issues	Unexpected behavior may occur under real-world usage, despite successful testing	Operational instability and performance degradation in live environments
Physical Security Risks	Edge nodes in remote or unsecured locations are vulnerable to theft and tampering	Greater risk of unauthorized physical access and damage
Cybersecurity Vulnerabilities	Lack of secure hardware, identity credentials, and real-time monitoring increases vulnerability to cyberattacks	Potential data breaches and system compromise
Infrastructure Costs	High initial investment in local infrastructure poses a challenge for small or under-resourced organizations	Limited adoption in budget constrained or developing regions

7 Conclusions

Edge computing is becoming a core part of how the Internet of Things (IoT) is growing. It allows devices to handle data close to where it's collected, which helps systems act in real time, lowers delays, and adds better protection for sensitive information. With this local processing, IoT devices can react quickly to events, run more efficiently, and keep user data safer. When combined with new technologies like 5G and Artificial Intelligence (AI), edge computing gives IoT systems even greater potential. This technology can be applied in real ways across several areas, including autonomous vehicles, health monitoring, city infrastructure, and industrial operations. But there are still important issues to work through. These include managing a large number of devices spread across different locations, protecting those devices from security threats, and handling the high costs involved in setting up the required systems. As these challenges are gradually addressed, edge computing is expected to keep playing a strong role in helping IoT systems become more reliable, quicker to respond, and better at keeping data safe in many different settings.

One area that still needs more attention is how to make edge-based IoT systems easier to integrate when the devices involved don't follow the same standards. This remains

a practical challenge in many real deployments. At the same time, there's a need for simpler, more adaptable security solutions especially for devices with limited computing resources, where traditional models often don't apply. We still don't fully understand how these systems behave once they're placed in environments where conditions can't be controlled. What works in testing doesn't always hold in real-world use. Watching how they respond over time to stress, faults, or changing inputs could help uncover the kinds of problems that don't show up in short-term trials. These challenges go beyond technical engineering. Addressing them will likely require input from other fields as well, especially if we expect edge computing to support systems that people can rely on systems that remain clear, secure, and manageable, even as they grow more complex.

References

1. Zhang, J., Fan, B.: Edge computing in information technology: enhancing real-time data processing for IoT applications. Artif. Intell. Digit. Technol. **1**(1), 1–19 (2024). https://doi.org/10.70088/3852aq53
2. Anarbayevich, A.: Harnessing edge computing for enhanced security and efficiency in IoT networks. Am. J. Appl. Sci. Technol. **4**(3), 18–23 (2024). https://doi.org/10.37547/ajast/volume04issue03-04
3. Jha, D.N., et al.: IoTSim-edge: a simulation for modeling the behavior of Internet of Things and edge computing environments. Softw. Pract. Exp. **50**(6), 844–867 (2020). https://doi.org/10.1002/spe.2787
4. Bhanage, S., Patil, S.: Edge computing technology: revolutionizing daily existence. Int. Res. J. Mod. Eng. Technol. Sci. **6**(6), 1–3 (2024). https://doi.org/10.56726/irjmets52305
5. Jaddoa, A., Sakellari, G., Panaousis, E., Loukas, G., Sarigiannidis, P.G.: Dynamic decision support for resource offloading in heterogeneous Internet of Things environments. Simul. Model. Pract. Theory **101**, 1–13 (2020). https://doi.org/10.1016/j.simpat.2019.102019
6. Patel, U.: Edge computing and its role in IoT: analyze how edge computing is transforming IoT by processing data at the edge of the network, reducing latency and enhancing data security. Int. J. Innov. Sci. Res. Technol. **9**, 1751–1756 (2024). https://doi.org/10.38124/ijisrt/ijisrt24may791
7. Nalayini, P., Sudha, M., Egamberdieva, S., K.S., V.S., Rajkumar, R.: Edge computing in the era of IoT: enhancing data processing and reducing latency for smart applications. Nanotechnol. Percept. **20**(6), 145–154 (2024). https://nano-ntp.com/index.php/nano/article/view/2497/1874
8. Mohsin, M., Shahrouzi, S., Perera: Composing efficient computational models for real-time processing on next-generation edge-computing platforms. IEEE Access **12**, 24905–24932 (2024). https://doi.org/10.1109/access.2024.3365652
9. Mohit, M.: The role of edge computing in IOT: enhancing real time data processing capabilities. Int. J. Adv. Res. Electr. Electron. Instrum. Eng. **6**(12), 8811–8819 (2017). https://doi.org/10.15662/ijareeie.2017.0612002
10. Dec, G., et al.: Role of academics in transferring knowledge and skills on artificial intelligence, Internet of Things and edge computing. Sensors **22**(7), 1–34 (2022). https://doi.org/10.3390/s22072496
11. Subramanian, S.: IoT and edge computing for smart manufacturing: architecture and future trends. Int. J. Eng. Comput. Sci. **13**(10), 26504–26522 (2024). https://doi.org/10.18535/ijecs/v13i10.4922
12. Pasupuleti, M.: AI-enabled edge computing: revolutionizing IoT with real-time optimization. Int. J. Acad. Ind. Res. Innov. **4**(11), 29–64 (2024). https://doi.org/10.62311/nesx/46687

13. Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L.: Edge computing: vision and challenges. IEEE Internet Things J. **3**(5), 637–646 (2016). https://doi.org/10.1109/JIOT.2016.2579198
14. Wolfert, S., Ge, L., Verdouw, C., Bogaardt, M.J.: Big data in smart farming–a review. Agric. Syst. **153**, 69–80 (2017). https://doi.org/10.1016/j.agsy.2017.01.023
15. Algarni, S., El-Samie, F.E.: Energy-efficient distributed edge computing to assist dense Internet of Things. Future Internet **17**(1), 1–23 (2025). https://doi.org/10.3390/fi17010037
16. Gudnavar, A., Naregal, K.: Edge computing in Internet of Things (IoT): enhancing IoT ecosystems through distributed intelligence. AIBTIA **2**(3), 1–7 (2023). https://doi.org/10.46610/aibtia.2023.v02i03.001
17. Gambheer, R., Bhat, M.S.: Optimized compressed sensing for IoT: advanced algorithms for efficient sparse signal reconstruction in edge devices. IEEE Access **12**, 63610–63617 (2024). https://doi.org/10.1109/access.2024.3396494
18. Ren, J., Zhang, D., He, S.Z., Li, T.: A survey on end-edge-cloud orchestrated network computing paradigms. ACM Comput. Surv. **52**(6), 1–36 (2019). https://doi.org/10.1145/3362031
19. AlQerm, I., Wang, J., Pan, J., Liu, Y.: BEHAVE: behavior-aware, intelligent and fair resource management for heterogeneous edge-IoT systems. EEE Trans. Mob. Comput. **21**(11), 3852–3865 (2021). https://doi.org/10.48550/arxiv.2103.11043
20. Contreras, L., Bernardos, C.: Overview of architectural alternatives for the integration of ETSI MEC environments from different administrative domains. Electronics **9**(9), 1–20 (2020). https://doi.org/10.3390/electronics9091392
21. Niu, X., et al.: Workload allocation mechanism for minimum service delay in edge computing-based power Internet of Things. IEEE Access **7**, 83771–83784 (2019). https://doi.org/10.1109/access.2019.2920325
22. Ali, M., Anjum, A., Rana, O., Zamani, A.R., Balouek-Thomert, D., Parashar, M.: RES: real-time video stream analytics using edge enhanced clouds. IEEE Trans. Cloud Comput. **10**, 792–804 (2020). https://doi.org/10.1109/tcc.2020.2991748
23. Mukhtar, N., Mehrabi, A., Kong, Y., Anjum, A.: Edge enhanced deep learning system for IoT edge device security analytics. Concurr. Comput. Pract. Exp. **35**(13), e6764 (2021). https://doi.org/10.1002/cpe.6764
24. Das, A., Wazid, M., Yannam, A., Rodrigues, J., Park, Y.: Provably secure ECC-based device access control and key agreement protocol for IoT environment. IEEE Access **7**, 55382–55397 (20219). https://doi.org/10.1109/access.2019.2912998
25. Liu, L., Kang, L., Li, X., Zhou, Z.: Service reliability based on fault prediction and container migration in edge computing. Appl. Sci. **13**(23) (2023). https://doi.org/10.3390/app132312865
26. Peng, K., Liu, P., Peng, T., Huang, Q.: Security-aware computation offloading for mobile edge computing-enabled smart city. J. Cloud Comput. Adv. Syst. Appl., 1–13 (2021). https://doi.org/10.1186/s13677-021-00262-6