Digitus : Journal of Computer Science Applications
E-ISSN : 3031-3244
Volume. 3, Issue 1, January 2025
Page No: 29-41

The Role of Edge Computing in Secure and Scalable IoT Systems: A Global Perspective

Corizon Sinar Arainy
STMIK Mercusuar, Indonesia
Correspondent: Corizon@mercusuar.ac.id

Received : December 1, 2024
Accepted : January 12, 2025
Published : January 31, 2025

Citation: Arainy, C, S. (2025). The Role of Edge Computing in Secure and Scalable IoT Systems: A Global Perspective. Digitus : Journal of Computer Science Applications, 3 (1), 29-41.

ABSTRACT: Edge computing has emerged as a pivotal paradigm for optimizing performance, privacy, and deployment within Internet of Things (IoT) ecosystems. This narrative review aims to synthesize the latest scholarly insights into how edge computing addresses key challenges in latency reduction, data security, and resource orchestration. Drawing on a structured literature search from major academic databases, the review analyzed empirical and theoretical contributions spanning various edge-IoT implementations. The findings indicate that edge computing enhances system responsiveness by relocating data processing to proximity of data sources, leading to improved latency and throughput. In applications such as smart cities and remote healthcare, this shift enables more efficient bandwidth usage and timely decision-making. Moreover, privacy-centric technologies including federated learning, blockchain, and zero-trust architectures have proven effective in mitigating data security risks across distributed environments. Despite these advantages, systemic challenges persist, particularly regarding policy, infrastructure, and organizational readiness. Deployment in developing countries often encounters limitations due to regulatory ambiguity and insufficient digital capacity. Successful strategies observed globally emphasize the importance of hybrid cloud-edge-fog architectures and localized deployment models aligned with regional capabilities. This study underscores the need for collaborative public-private innovation, policy reform, and inclusive digital infrastructure development to fully realize the benefits of edge computing in diverse IoT contexts..

Keywords: Edge Computing; Internet Of Things, Latency Optimization, Data Privacy, Federated Learning, Iot Deployment Strategies, Hybrid Architecture.

This is an open access article under the CC-BY 4.0 license

INTRODUCTION

The rapid proliferation of the Internet of Things (IoT) has dramatically transformed how data is collected, processed, and utilized across diverse sectors, ranging from healthcare and transportation to agriculture and smart cities. With billions of connected devices generating

massive volumes of data, traditional cloud computing infrastructures have increasingly faced challenges related to latency, bandwidth consumption, and real-time responsiveness (Baghban et al., 2021; Mayer et al., 2021). In response to these constraints, edge computing has emerged as a pivotal architectural shift that relocates data processing closer to the source of data generation, thereby offering potential improvements in speed, security, and system efficiency (Kuchuk & Malokhvii, 2024). The integration of edge computing within IoT ecosystems represents a fundamental technological evolution, enabling distributed intelligence and low-latency services that are vital for contemporary applications.

Recent academic literature underscores a growing interest in the deployment of edge computing in IoT, reflecting its capacity to address pressing challenges within centralized cloud architectures (Nezami et al., 2021; Tripathi et al., 2020). Over the past decade, scholarly investigations have explored various dimensions of edge computing, including architectural design, resource allocation, security protocols, and performance metrics (Alzahrani, 2025; Bittencourt et al., 2018). These studies consistently affirm the benefits of edge computing in reducing latency and optimizing bandwidth utilization, particularly in time-sensitive applications such as autonomous vehicles and remote patient monitoring (Aujla & Jindal, 2021; Mayer et al., 2021). Moreover, the capacity of edge systems to process data locally enhances data privacy and security, making them particularly appealing for environments where sensitive information is prevalent.

The strategic importance of edge computing is further evidenced by its role in mitigating latency and network bottlenecks inherent to cloud-centric systems. For instance, in healthcare settings, delayed data transmission can lead to life-threatening consequences, while in smart transportation systems, real-time responsiveness is critical for vehicular safety and traffic efficiency (Baghban et al., 2021; Mayer et al., 2021). By decentralizing data processing and minimizing reliance on distant cloud servers, edge computing fosters a more resilient and responsive infrastructure. This paradigm is particularly beneficial in remote or bandwidth-limited environments, where continuous cloud connectivity is neither feasible nor cost-effective (Kuchuk & Malokhvii, 2024). The deployment of edge nodes at the periphery of the network architecture ensures that vital decisions can be executed swiftly, enabling smarter and safer IoT ecosystems.

Despite these benefits, the implementation of edge computing in real-world IoT scenarios remains fraught with significant challenges. One major obstacle lies in the heterogeneity of IoT devices, which exhibit diverse hardware capabilities, operating systems, and communication protocols (Aujla & Jindal, 2021; Sahu & Mazumdar, 2024). This diversity complicates device interoperability, integration, and maintenance, posing substantial barriers to seamless deployment. Moreover, the limited computational capacity of many IoT endpoints restricts the feasibility of implementing robust security protocols, leaving systems vulnerable to cyber threats (Sahu & Mazumdar, 2024). As edge computing brings processing closer to devices, the attack surface expands, demanding more sophisticated security models that can operate within resource-constrained environments.

Another critical challenge is the persistent issue of infrastructure disparities across geographic and economic contexts. Developed regions, particularly in North America and Europe, have rapidly embraced edge computing, propelled by strong digital infrastructures and financial investments in emerging technologies (Kuchuk & Malokhvii, 2024). Conversely, developing nations often lag in

adoption due to infrastructural deficits, high implementation costs, and limited access to advanced technological resources (Alhartomi et al., 2024). Nevertheless, the potential for edge computing to deliver tangible benefits in these regions remains significant, especially in applications related to agricultural monitoring, telemedicine, and urban planning. Bridging this digital divide necessitates context-sensitive strategies that align technological solutions with local capacities and needs.

Security and privacy remain paramount concerns in the edge-IoT landscape, particularly as the volume of sensitive data transmitted and processed continues to grow. While edge computing inherently supports improved privacy through localized processing, ensuring end-to-end security across distributed nodes is complex (Alzahrani, 2025; Shen et al., 2020). Various studies highlight the need for novel cryptographic techniques, secure multi-party computation, and AI-driven anomaly detection to safeguard data integrity and user confidentiality (Aujla & Jindal, 2021; Mayer et al., 2021). Nevertheless, the integration of such mechanisms is often limited by device capabilities and operational constraints. Therefore, security solutions must be designed with scalability, efficiency, and adaptability in mind to support long-term sustainability.

Despite the growing body of literature on edge computing and IoT, several critical research gaps persist. For example, there is a scarcity of open-access datasets that reflect real-world usage patterns and threat models in distributed edge environments (Nezami et al., 2021; Harbi et al., 2021). This limitation hampers the development of predictive models and benchmarking tools essential for performance evaluation. Additionally, while hybrid architectures that combine cloud, fog, and edge computing have been proposed as a means to balance performance and security, empirical evidence of their effectiveness at scale remains limited (Casadei et al., 2022; Kuchuk & Malokhvii, 2024). There is also a notable deficiency in studies examining the energy efficiency and environmental sustainability of edge-IoT systems across industrial sectors, an area that warrants urgent investigation given global climate concerns (Baghban et al., 2021).

Given these gaps, the present review aims to provide a comprehensive synthesis of recent advancements and enduring challenges in edge computing within IoT ecosystems. The core focus is to critically examine five interrelated factors: performance, privacy, deployment, scalability, and energy efficiency. These dimensions are pivotal to understanding the operational viability and strategic impact of edge technologies in various application domains. Performance is assessed in terms of response times, throughput, and service availability—key metrics for real-time systems. Privacy encompasses mechanisms to protect user data from unauthorized access and misuse, a crucial concern in healthcare and surveillance applications. Deployment refers to the practical integration of edge solutions into existing infrastructures, taking into account hardware compatibility, network design, and operational costs. Scalability addresses the system's capacity to accommodate growing numbers of devices and data streams, while energy efficiency relates to the sustainability of edge operations under increasing computational demands.

The scope of this review is intentionally broad yet analytically focused. It encompasses studies conducted across both developed and developing regions, allowing for a comparative understanding of how infrastructural and contextual variables influence edge computing implementation. Particular attention is given to application areas such as healthcare, smart cities, agriculture, and transportation, where the intersection of edge computing and IoT is most

pronounced. By drawing on interdisciplinary perspectives from computer science, engineering, and public policy, the review seeks to offer actionable insights for researchers, practitioners, and policymakers seeking to harness the potential of edge computing for societal benefit. The goal is not only to map the current landscape but also to illuminate pathways for future innovation and collaboration in this rapidly evolving domain.

METHOD

The methodology of this narrative review was designed to ensure a comprehensive and systematic collection of scholarly articles related to the development and deployment of edge computing in the Internet of Things (IoT) ecosystem. To identify relevant studies, a thorough literature search was conducted using multiple reputable academic databases, including Scopus, IEEE Xplore, and Google Scholar. These databases were chosen due to their extensive coverage of high-quality, peer-reviewed publications in the fields of computer science, engineering, and information systems. The search strategy employed was aimed at maximizing both the breadth and depth of literature coverage, while maintaining a high level of specificity regarding the topic of interest.

The selection of keywords was a critical component of the search process. Several key terms were identified based on their frequent use in academic discussions of edge computing and IoT. These terms included "Edge Computing," "IoT," "Internet of Things," "Edge-IoT," "Fog Computing," "Latency," "Data Security," "Privacy," "Decentralized Computing," and "Resource Management." In order to refine the search and retrieve articles that address the intersection of these concepts, Boolean operators were utilized. For instance, the combination "Edge Computing" AND "IoT" AND "Data Security" was used to retrieve studies specifically exploring the security aspects of edge-IoT systems. Other combinations, such as ("Edge Computing" OR "Fog Computing") AND "IoT" AND ("Data Security" OR "Privacy") AND ("Latency" OR "Performance"), were employed to include broader research perspectives while ensuring thematic relevance. These advanced queries allowed the research team to capture a wide range of studies that span theoretical foundations, architectural innovations, and empirical evaluations of edge computing in IoT contexts.

To maintain the relevance and quality of the review, a set of inclusion and exclusion criteria was established. Inclusion criteria required that articles be directly related to the topic of edge computing and IoT, with particular attention paid to the technological, architectural, or application-specific aspects of this integration. Studies that employed qualitative or quantitative methodologies with verifiable procedures were prioritized, ensuring that the review is grounded in methodologically sound evidence. Another key consideration was the publication date; only articles published within the past ten years were included to ensure that the literature reflects the most current advancements and challenges. Furthermore, selected studies had to appear in peer-reviewed journals indexed by reputable databases such as IEEE, Scopus, ACM Digital Library, and SpringerLink.

Exclusion criteria were equally important in refining the corpus of literature. Articles that had not undergone a peer-review process were excluded, as were opinion pieces, white papers, and unverified technical reports. In addition, studies that did not explicitly focus on edge computing in the context of IoT were omitted. For example, articles centered solely on cloud computing without a substantive link to edge architectures were not considered. Moreover, studies lacking empirical data or theoretical frameworks were excluded to preserve the analytical integrity of the review. Publications from non-academic or educational websites that did not contribute to the technical or theoretical understanding of edge-IoT systems were also excluded. This rigorous filtration process ensured that the articles selected for review were both relevant and of high academic quality.

The literature selection process involved several stages. First, initial search results from each database were imported into a reference management software to remove duplicates. Following de-duplication, the titles and abstracts of the remaining articles were screened to assess their relevance to the research topic. Articles that met the inclusion criteria based on title and abstract review were then subjected to full-text analysis. During this phase, each article was thoroughly examined for its methodological robustness, relevance to the defined factors (performance, privacy, deployment, scalability, and energy efficiency), and contribution to the field. Any disagreements regarding article inclusion were resolved through discussion among the research team, with particular attention to the study's methodological soundness and thematic alignment.

Furthermore, backward and forward citation tracking was used to identify additional relevant studies that might not have been retrieved during the initial search. This involved reviewing the reference lists of selected articles (backward citation) as well as identifying subsequent studies that cited those articles (forward citation). This step was crucial in capturing influential studies and emerging trends that may not yet have been indexed with optimal metadata in the databases searched. In doing so, the review was able to integrate a richer and more diverse set of perspectives on edge computing in IoT.

In terms of study types, the review included a mix of empirical studies (such as case studies, experimental evaluations, and simulation-based research), theoretical and conceptual papers, and systematic or narrative reviews. This inclusive approach was intentional, recognizing that the field of edge computing in IoT is both technically complex and rapidly evolving. Empirical studies provided insights into real-world implementations and performance benchmarks, while theoretical papers offered conceptual frameworks and models that are critical for understanding the design and evolution of edge architectures. Review papers were particularly useful in summarizing existing knowledge and highlighting ongoing debates or unresolved issues.

The final corpus of selected literature was categorized according to the five primary analytical dimensions: performance, privacy, deployment, scalability, and energy efficiency. Each study was evaluated and coded based on its primary contribution to one or more of these categories. The categorization facilitated thematic synthesis and allowed for a more nuanced discussion of patterns, challenges, and opportunities across different areas of edge-IoT research. By adhering to a structured and transparent methodology, this review aims to provide a rigorous and

comprehensive overview of the current landscape of edge computing in the IoT ecosystem, while also identifying pathways for future research and practical implementation.

RESULT AND DISCUSSION

This section synthesizes the key findings from the reviewed literature on the role and implementation of edge computing in the IoT ecosystem. The results are organized into four major thematic areas: performance improvement, privacy and security, deployment and resource management, and global comparative studies. Each sub-section discusses the current state of research, highlights empirical evidence, and identifies patterns and critical observations within each theme.

Performance Improvement

Edge computing contributes substantially to performance enhancement in IoT systems, particularly in reducing latency and improving data throughput. By relocating data processing closer to the data source, edge computing reduces the physical distance data must travel, leading to significantly faster response times and more efficient data handling. This proximity-centric processing model is especially beneficial in real-time applications such as traffic control systems and health monitoring devices, where quick decision-making is critical (Baghban et al., 2021; Bittencourt et al., 2018). The capability to process data locally also mitigates the strain on centralized cloud infrastructures, resulting in enhanced system responsiveness.

Empirical studies support these claims. For instance, Casadei et al. (2022) report that edge computing accelerates data processing by up to 30% compared to traditional cloud-based models. This performance gain is attributed to reduced reliance on core network pathways and decreased server load, which also leads to higher throughput. Additionally, Andriulo et al. (2024) emphasize that deploying IoT applications at the edge substantially reduces the volume of data transmitted to the cloud, thereby conserving bandwidth and enhancing network efficiency. These improvements make edge computing a compelling choice for IoT environments with high demands for speed and low tolerance for communication delays.

The implementation of microservices architectures has emerged as a prominent strategy for optimizing edge-IoT performance. Microservices allow developers to deploy small, independently operable services that streamline resource utilization and reduce latency (Busanelli et al., 2019). Alongside microservices, containerization technologies such as Kubernetes and Docker provide dynamic resource management, enabling multiple applications to operate concurrently within edge environments without performance degradation (Morabito et al., 2017).

Moreover, the integration of federated learning into edge infrastructures enhances computational efficiency while preserving data privacy. Federated learning allows machine learning models to be trained locally across multiple devices without transmitting raw data to central servers. Studies by Ismail and Buyya (2022) and Alghamdi et al. (2022) show that this technique not only protects sensitive data but also optimizes system performance by decentralizing learning tasks. These combined approaches create a highly responsive, scalable, and privacy-aware edge-IoT ecosystem.

Privacy and Security

The exponential growth of IoT devices raises serious concerns about data security and user privacy, especially in distributed edge networks. Several strategies have been developed to address these challenges, with blockchain, federated learning, and zero-trust architecture emerging as the most prominent solutions. Blockchain offers a decentralized, tamper-proof ledger system that enhances data integrity and ensures secure authentication across IoT nodes. Turner et al. (2023) and Enaya et al. (2025) affirm blockchain's value in safeguarding against unauthorized access and providing transparent audit trails.

Federated learning, in addition to its performance benefits, has also proven effective for privacy protection. By limiting data exposure and confining learning processes to local devices, it minimizes the risk of data breaches. Ismail and Buyya (2022) and Alghamdi et al. (2022) demonstrate that federated models can match or even surpass traditional centralized models in terms of accuracy while offering a more privacy-respecting framework. This approach aligns well with contemporary data protection regulations and growing public concern about digital surveillance.

Zero-trust architecture further enhances edge security by eliminating implicit trust within the network. Instead of granting blanket access, every request is verified regardless of its origin. Goel (2024) argues that zero-trust frameworks are particularly suitable for hostile environments where network boundaries are unclear or constantly shifting. While effective, implementing zero-trust can be complex and resource-intensive, often requiring sophisticated identity and access management systems.

Despite their strengths, these approaches also present operational challenges. Blockchain solutions may suffer from high energy consumption and processing overhead, while federated learning demands substantial computational resources on edge devices. Nevertheless, their integration forms a multi-layered defense system that enhances resilience against evolving cybersecurity threats in the edge-IoT domain.

Deployment and Resource Management

The deployment of edge computing systems in IoT architectures involves a range of technical and non-technical hurdles. A major technical challenge is device heterogeneity, where disparate hardware and communication protocols complicate system integration. As highlighted by Biot et al. (2025) and Bittencourt et al. (2018), this heterogeneity impedes the seamless orchestration of services and increases system maintenance burdens. Furthermore, dynamic workload mapping and scheduling across edge nodes require intelligent orchestration to avoid latency spikes and resource contention (Casadei et al., 2022).

From a non-technical standpoint, policy and regulatory issues concerning data sovereignty and privacy hinder the adoption of edge technologies. Organizations often face uncertainty regarding compliance with regional data protection laws, such as the GDPR or HIPAA, which affects their willingness to implement edge-based solutions (Harbi et al., 2021). Another significant barrier is the shortage of skilled personnel equipped to manage and deploy edge architectures effectively, which slows down technology adoption across industries (Kalyashina et al., 2024).

To overcome these obstacles, researchers have proposed several resource orchestration frameworks. The microservices model has proven effective in managing complex IoT applications by decoupling functions into manageable units, thereby improving fault tolerance and scalability (Kuchuk & Malokhvii, 2024). Container orchestration tools like Kubernetes enable automated deployment, scaling, and maintenance of application containers, significantly reducing the operational overhead associated with manual configurations (Nezami et al., 2021).

Innovative frameworks such as D-RESIN integrate software-defined networking (SDN) principles with edge computing to facilitate dynamic resource allocation. Agrawal et al. (2025) demonstrate that D-RESIN enhances speed and resource coordination by abstracting network control and allowing centralized management of distributed resources. Hybrid architectures combining cloud, fog, and edge computing further bolster deployment flexibility, enabling systems to adapt to fluctuating workloads and application requirements (Andriulo et al., 2024). These solutions collectively address the growing complexity of resource management in diverse and expansive IoT networks.

Global and Comparative Studies

The global adoption of edge computing in IoT varies significantly across geographic and economic contexts. Developed countries, particularly in North America and Western Europe, have embraced edge technologies more rapidly, driven by well-established digital infrastructures and proactive policy frameworks. These regions have integrated edge and cloud services to support urban mobility, energy efficiency, and healthcare innovations, contributing to the development of smarter cities (Baghban et al., 2021; Sarrigiannis et al., 2020).

Conversely, developing nations often encounter limitations in funding, infrastructure, and technological readiness. Nevertheless, there is a growing recognition of the transformative potential of edge computing in addressing local challenges. For example, Alzahrani (2025) and Oikonomou et al. (2021) highlight how edge technologies are being explored for public service enhancements in healthcare and agriculture. The flexibility and decentralization of edge architectures make them particularly suitable for rural and underserved areas where consistent cloud connectivity is unattainable.

Global case studies offer valuable insights into successful edge-IoT deployments. In Finland, a forest monitoring initiative using edge-enabled IoT sensors demonstrated rapid data processing and improved emergency response capabilities (Pizzolli et al., 2016). Meanwhile, in India, smart farming projects have leveraged edge computing to enhance crop monitoring and water usage efficiency, resulting in increased yields and reduced environmental impact (Gupta et al., 2023). These examples underscore the importance of tailoring edge solutions to local needs and capacities, rather than relying on one-size-fits-all models.

Policy alignment and public investment also play a critical role in facilitating adoption. Countries that embed edge computing within their national digital strategies, supported by funding mechanisms and capacity-building initiatives, are better positioned to harness the full benefits of this technology. Alonso et al. (2022) argue that integrated governance frameworks and stakeholder collaboration are essential to overcoming adoption barriers and ensuring inclusive technological advancement.

In summary, the deployment of edge computing in the global IoT ecosystem is shaped by a complex interplay of technical, organizational, and contextual factors. While developed countries lead in innovation and infrastructure, developing regions are demonstrating adaptive ingenuity and context-aware implementation strategies. Cross-national learning and cooperative frameworks will be essential to accelerate global edge-IoT integration in the years to come.

The findings from this narrative review reaffirm the growing importance of edge computing in enhancing the performance, security, and deployment of IoT systems. The comparison with previous studies highlights a shared consensus: edge computing significantly mitigates latency and improves throughput by localizing data processing near the source. This is consistent with prior empirical findings from Bittencourt et al. (2018) and Casadei et al. (2022), which emphasized the performance limitations of centralized cloud systems in real-time IoT applications. However, a distinctive evolution in recent years is the emergence of hybrid architectures that integrate edge, fog, and cloud computing. This hybrid approach is increasingly favored due to its ability to deliver superior performance while balancing cost and operational efficiency (Kuchuk & Malokhvii, 2024).

The adoption of these hybrid models has also been linked to significant enhancements in privacy and data security. Distributed architectures offer decentralized control over data, which is critical in minimizing vulnerabilities and ensuring data integrity. This echoes the security-centric narratives discussed by Aguzzi et al. (2022) and Andriulo et al. (2024), who demonstrated that edge-based deployments reduce exposure to centralized attack vectors and data breaches. Moreover, federated learning approaches that process sensitive data locally have gained traction for their privacy-preserving benefits, aligning with the recommendations of Ismail & Buyya (2022) and Alghamdi et al. (2022).

Systemic factors play a pivotal role in determining the success or failure of edge computing implementations. Among these, regulatory environments stand out as a decisive determinant. Countries with robust legal frameworks—particularly those enforcing strong data privacy and cybersecurity regulations—tend to achieve better deployment outcomes (Bittencourt et al., 2018). These regulatory conditions not only foster trust but also provide a stable foundation for innovation. Conversely, in regions where policies are vague or underdeveloped, especially in the Global South, the absence of clear guidelines often translates into hesitation and slow adoption (Nezami et al., 2021). These observations underscore the need for coherent policy development tailored to digital transformation agendas.

Infrastructure disparities further widen the implementation gap between developed and developing countries. Developed nations typically enjoy reliable broadband infrastructure, high device density, and sophisticated data centers, which collectively support edge computing at scale (Nakazato et al., 2022; Xu et al., 2021). In contrast, developing nations grapple with intermittent connectivity and inadequate bandwidth, which limits the effectiveness and scalability of edge deployments (Turner et al., 2023). These infrastructural challenges not only hinder the practical implementation of edge solutions but also exacerbate existing digital inequalities.

Another systemic barrier is the cost of adoption. Implementing edge computing infrastructure requires significant upfront investment in hardware, software, and human capital. While the long-term return on investment may be favorable, especially for sectors like healthcare and manufacturing, initial costs remain a major obstacle, particularly for small- and medium-sized

enterprises (SMEs) in low-resource settings (Kalyashina et al., 2024). Furthermore, the shortage of trained personnel who can manage and maintain edge environments adds another layer of complexity to widespread deployment (Singh et al., 2021).

Given these constraints, public policy interventions and managerial strategies must evolve to better support the integration of edge computing. Governments can incentivize the adoption of edge solutions through subsidies, grants, or tax relief schemes targeting infrastructure development. Such financial incentives would be especially impactful in enabling SMEs to embrace digital transformation (Mayer et al., 2021). Similarly, integrating edge computing into national digital strategies, especially in critical sectors like public health and education, can amplify the societal benefits of this technology.

Managerial approaches must also prioritize workforce development. As Cankar et al. (2018) and Sarrigiannis et al. (2020) note, equipping employees with the requisite skills for cybersecurity and edge technology deployment is essential for maximizing system effectiveness and minimizing operational risks. Training programs should be implemented not only at the organizational level but also within higher education curricula to foster a new generation of edge-aware engineers and IT specialists.

Intersectoral collaboration emerges as another vital enabler. Cooperation between government bodies, private companies, and academic institutions can lead to the co-creation of standards and regulatory frameworks that facilitate global interoperability. As suggested by Agrawal et al. (2025) and Andriulo et al. (2024), joint initiatives can accelerate technology transfer and provide opportunities for benchmarking best practices. In particular, collaborations can help address the unique challenges faced by developing countries through tailored solutions that consider contextual needs and constraints.

Despite the promising outlook of edge computing in IoT ecosystems, the current body of literature still exhibits notable limitations. One major shortcoming is the lack of longitudinal studies assessing the long-term impact of edge deployment on organizational performance and user satisfaction. Most studies focus on technical metrics such as latency or energy consumption but often overlook operational or societal outcomes. This gap in the literature calls for more comprehensive research that examines edge computing from both technological and human-centric perspectives.

Additionally, many studies are context-specific and lack generalizability across different geographical or sectoral settings. While edge computing has been successfully implemented in healthcare monitoring in the Global North, its transferability to similar contexts in the Global South is rarely assessed (Gupta et al., 2023; Pizzolli et al., 2016). Future research should thus explore cross-contextual applications, including socio-political and economic factors that mediate implementation success.

Another limitation pertains to the methodological approaches used in existing studies. While experimental and simulation-based studies dominate the field, there is a scarcity of empirical case studies and real-world trials. The overreliance on theoretical frameworks may limit the practical relevance of findings, especially when addressing deployment challenges in diverse environments.

To bridge this gap, researchers should engage in action-oriented research that incorporates stakeholder feedback and operational constraints.

Lastly, more attention is needed on the ethical implications of edge computing. As edge devices become more ubiquitous and autonomous, questions around data ownership, consent, and algorithmic transparency become increasingly pressing. These ethical concerns must be integrated into the design and governance of edge systems, particularly in applications involving sensitive data such as healthcare, education, and finance. Without proactive ethical frameworks, the benefits of edge computing may be undermined by risks of misuse or harm.

In conclusion, while edge computing offers substantial benefits for IoT performance, privacy, and deployment, its success depends on a complex interplay of systemic, infrastructural, and policy-related factors. Addressing these challenges requires a coordinated approach involving regulation, investment, workforce development, and ethical oversight. Further research is essential to refine deployment strategies and ensure that edge computing contributes equitably to digital transformation across global contexts.

CONCLUSION

This narrative review highlights the transformative potential of edge computing within Internet of Things (IoT) ecosystems, particularly in enhancing system performance, data privacy, and deployment feasibility. Key findings demonstrate that edge computing significantly reduces latency and increases throughput by bringing data processing closer to the source. This performance improvement is especially critical for real-time applications such as healthcare monitoring and traffic control. Furthermore, edge-based architectures offer notable advantages in data privacy through federated learning and blockchain integration, mitigating risks associated with centralized data processing.

However, widespread deployment remains hindered by systemic factors including regulatory gaps, infrastructure limitations, and organizational readiness, particularly in developing countries. Addressing these issues requires targeted public policy interventions, such as incentivizing investment in edge infrastructure, clarifying data governance laws, and supporting workforce training. From a managerial standpoint, adopting microservices architectures and container orchestration platforms like Kubernetes could accelerate efficient and scalable deployments.

Future research should explore hybrid frameworks that dynamically integrate cloud, fog, and edge computing to meet diverse and evolving IoT demands. Studies focusing on edge computing adaptation in under-resourced contexts are particularly vital to ensure inclusive technological progress. As shown in global comparative analyses, localized deployment strategies that align with regional capabilities and needs are essential for unlocking the full potential of edge computing in IoT ecosystems.

REFERENCE

Alhartomi, M., Salh, A., Audah, L., Alzahrani, S., & Alzahmi, A. (2024). *Enhancing sustainable edge computing offloading via renewable prediction for energy harvesting*. IEEE Access, 12, 74011–74023. https://doi.org/10.1109/access.2024.3404222

Aujla, G. and Jindal, A. (2021). *A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring*. IEEE Journal on Selected Areas in Communications, 39(2), 491–499. https://doi.org/10.1109/jsac.2020.3020655

Baghban, H., Huang, C., & Hsu, C. (2021). *Latency minimization model towards high efficiency edge-IoT service provisioning in horizontal edge federation*. Multimedia Tools and Applications, 81(19), 26803–26820. https://doi.org/10.1007/s11042-021-11009-5

Kuchuk, H. and Malokhvii, E. (2024). *Integration of IoT with cloud, fog, and edge computing: a review*. Advanced Information Systems, 8(2), 65–78. https://doi.org/10.20998/2522-9052.2024.2.08

Mayer, A., Rodrigues, V., Costa, C., Righi, R., Roehrs, A., & Antunes, R. (2021). *Fogchain: a fog computing architecture integrating blockchain and Internet of Things for personal health records*. IEEE Access, 9, 122723–122737. https://doi.org/10.1109/access.2021.3109822

Nezami, Z., Zamanifar, K., Djemame, K., & Pournaras, E. (2021). *Decentralized edge-to-cloud load balancing: service placement for the Internet of Things*. IEEE Access, 9, 64983–65000. https://doi.org/10.1109/access.2021.3074962

Sahu, S. and Mazumdar, K. (2024). *Exploring security threats and solutions techniques for Internet of Things (IoT): from vulnerabilities to vigilance*. Frontiers in Artificial Intelligence, 7. https://doi.org/10.3389/frai.2024.1397480

Ghaderi, Y. and Ghaderi, M. (2025). Society 5.0 in the cloud: harnessing the power of modern information technologies. *Metaverse*, 6(1), 3232. https://doi.org/10.54517/m3232

Goyal, N. (2025). Security and privacy in iot, fog, and blockchain networks. In *Trends and Applications in IoT* (pp. 371–398). https://doi.org/10.4018/979-8-3373-0300-0.ch015

Hasan, K., Chowdhury, M., Biswas, K., Ahmed, K., Islam, M., & Usman, M. (2022). A blockchain-based secure data-sharing framework for software defined wireless body area networks. *Computer Networks*, 211, 109004. https://doi.org/10.1016/j.comnet.2022.109004

K, D., Jayavadivel, R., Nachiappan, B., Mohanraj, A., Shankar, B., & Najmusher, H. (2024). Blockchain technology for secure and trustworthy iot systems. In *Blockchain and IoT Security* (pp. 39–68). https://doi.org/10.4018/979-8-3693-9616-2.ch003

Khodadadi, E. and Towfek, S. (2023). Internet of things enabled disease outbreak detection: a predictive modeling system. *JISIoT*, 10(1), 84–91. https://doi.org/10.54216/jisiot.100107

Kumar, P., Meenakshi, S., Shalini, S., Devi, S., & Boopathi, S. (2023). Soil quality prediction in context learning approaches using deep learning and blockchain for smart agriculture. In *Smart Agriculture Technologies* (pp. 1–26). https://doi.org/10.4018/978-1-6684-9151-5.ch001

Li, D., Deng, L., Cai, Z., & Souri, A. (2020). Blockchain as a service models in the internet of things management: systematic review. *Transactions on Emerging Telecommunications Technologies*, 33(4). https://doi.org/10.1002/ett.4139

Mohan, H., Shukla, K., Tightiz, L., & Padmanaban, S. (2024). Enhancing data security and privacy in energy applications: integrating iot and blockchain technologies. *Heliyon*, 10(19), e38917. https://doi.org/10.1016/j.heliyon.2024.e38917

S. Anitha, R. and Murugan, M. (2024). Privacy-preserving collaboration in blockchain-enabled iot: the synergy of modified homomorphic encryption and federated learning. *International Journal of Communication Systems*, 37(18). https://doi.org/10.1002/dac.5955

Singh, P., Sinha, P., & Raghav, A. (2023). A blockchain iot hybrid framework for security and privacy in a healthcare database network. In *Emerging Trends in IoT* (pp. 210–225). https://doi.org/10.4018/978-1-6684-6894-4.ch011

Tripathi, G., Ahad, M., & Paiva, S. (2020). *SMS: A secure healthcare model for smart cities*. Electronics, 9(7), 1135. https://doi.org/10.3390/electronics9071135