Journal of Artificial Intelligence and Computing (JAIC)
ISSN (e): 3005-3358
Volume: 3, Number: 2, Pages: 15 - 21, Year: 2025

Towards Resilient Smart Cities: Security, Trust, and Sustainability in Edge Computing - A Survey

Areeb Imtar Chaudary and Irshad Ahmed Sumra

School of Science and Technology (SST), University of Management & Technology, Lahore, 54000, Pakistan
Corresponding author: Areeb Imtar Chaudary (Email: areebimtar@yahoo.com)

Received: 12/07/2025, Revised: 16/11/2025, Accepted: 01/12/2025

***Abstract*—Edge computing has underpinned smart cities by enabling low-latency, localised intelligence for traffic, surveillance, and infrastructure. However, its decentralised, heterogeneous footprint poses severe risks to security, privacy, and environmental sustainability. This paper reviews secure, sustainable edge computing and introduces a unified framework balancing security with ecological constraints. It establishes a threat taxonomy covering expanded attack surfaces, identity flaws, and physical or AI-driven threats, then critically evaluates five core paradigms, AI anomaly detection, blockchain, secure virtualisation, and privacy analytics against latency and resource overhead. Crucially, we assess the environmental toll of these defenses using Energy per Operation (EPO), Energy-Delay Product (EDP), Carbon Intensity (CI), and Lifecycle Energy Use (LEU) metrics. Exposing a critical gap in the literature: the lack of standardised benchmarks for security carbon costs. Finally, we map future frontiers like post-quantum crypto, secure federated learning, digital twins, and edge-native zero-trust, proving that modern urban ecosystems must treat security and sustainability as co-dependent design requirements. The findings emphasise that future smart-city infrastructures must balance security, privacy, performance, and sustainability to achieve resilient and trustworthy edge computing ecosystems.**

***Index Terms*—Edge Computing, Smart Cities, Edge Security, Sustainability, Artificial Intelligence, Blockchain, Trusted Execution Environments, Federated Learning, Privacy Preservation, Post-Quantum Cryptography.**

I. INTRODUCTION

In the modern era, the world is moving toward smart cities. These are being equipped with dense, extensive smart infrastructure, such as smart road sensors, AI-based camera surveillance, smart traffic lights with automated traffic-flow monitoring, and environmental probes and actuators. All such devices continuously generate high-speed data streams. Cloud-based pipelines are used to process these large data streams and extract useful information from raw data. [1-2]. Conventional data centers cause backbone congestion and unsustainable round-trip delays, which in turn disrupt real-time control loops and undermine service-level objectives [3-5].

By moving infrastructure — including computational power, storage, and security controls — closer to physical locations, edge computing delivers substantially lower latency and bandwidth consumption, together with improved security, locality, and privacy [3]. Empirically, edge computing deployments have been shown to reduce request-response delays by 42.5% in highly compact environments and by 66.6% in lightly dense environments. Edge computing is particularly valuable for smart-city functions that are time-critical, such as collision control in smart vehicles, where even a moderate delay could cause severe consequences, including missed deadlines [5-6].

Furthermore, intermittent connectivity issues need not compromise safety. For example, roadside units can act locally and transmit notifications and alerts via V2X while maintaining state consistency using locally optimised, permissioned blockchain mechanisms [7]. Increasingly, intelligence is executed progressively at the local level for visual data analytics, smooth traffic operations, and environmental monitoring [8]. Lightweight machine learning and deep learning models are deployed directly on edge platforms and micro data centres, enabling contextualised decisions with minimal end-to-end latency [9]. To preserve data locality and ensure privacy at scale, federated learning distributes the training process among edge nodes and aggregates model updates rather than processing raw data [10-11], [12]. Sustainability is a primary concern in these architectures: in one green IoT edge model, energy consumption decreased by 21%, routing interruptions decreased by 36%, throughput increased by 15%, end-to-end latency decreased by 12%, and protocol overhead decreased by 52% [13]. Carbon-aware composition and lifecycle assessment further support the alignment of workloads with cleaner energy sources while accounting for embodied and operational impact [14].

The same openness that delivers improved quality and performance also creates opportunities for attackers. Edge nodes are sometimes placed in public spaces rather than trusted, controlled locations. Exposing these devices to physically accessible environments make firmware tampering, side-channel misuse, and malicious task offloading more feasible [15-17]. Modern problems require modern solutions: contemporary edge computing stacks increasingly integrate hardware roots of trust and trusted execution environments to preserve the CIA triad — confidentiality, integrity, and availability — of code and data during execution [18-19]. Finally, reported energy and carbon costs associated with

cryptographic, blockchain, and federated learning techniques vary substantially, sometimes by orders of magnitude, depending on hardware configuration, workload type, and measurement methodology. Because the literature commonly reports results on a per-study basis rather than against platform-independent standards [20-24], comparative reviews are best positioned to clarify this fragmented landscape.

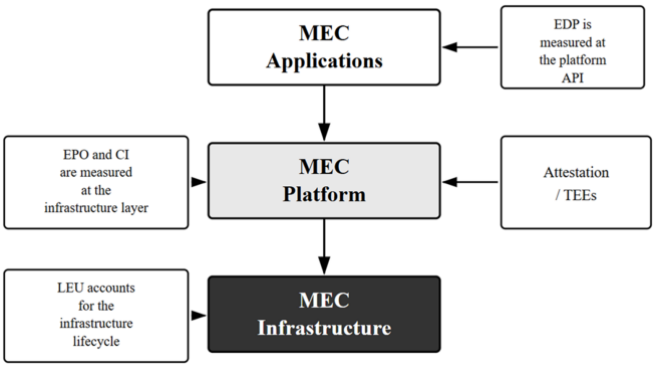

Fig. 1. Edge Computing Layers and Security Zones [1].

This review integrates resilience, digital sovereignty, and sustainability into a single framework for understanding threats and designing defenses in next-generation edge computing for smart cities. It examines current approaches such as AI-based anomaly detection, blockchain-supported access control, and trusted execution environments, focusing on their effects on latency, jitter, resource usage, and real-world readiness. The paper also outlines future research directions, including quantum-resistant cryptography, digital-twin-based risk modelling, and edge-native policy enforcement. Fig. 1 presents the three key deployment layers — infrastructure, platform, and application — alongside their corresponding security zones. In synthesis, this article offers four primary contributions that, taken together, advance the dual objectives of security and sustainability in smart-city edge architectures [25-30].

1) Classification of threats in edge computing: A detailed classification of security threats affecting edge computing in smart-city environments is presented. These threats are categorised into four major groups:

- Larger attack surface
- Data privacy and integrity
- Weaknesses in identity and access management
- New AI-based and physical attacks

This taxonomy helps explain the unique security challenges introduced by the decentralized and diverse nature of edge computing systems.

2) Comparative analysis of security solutions: Five major categories of security solutions are compared: (i) AI-based anomaly detection; (ii) trust and access control based on permissioned blockchain; (iii) trusted execution environments (TEE) and hardware-based trust mechanisms; (iv) secure virtualization and containerization; and (v) privacy-preserving analytics such as Differential Privacy (DP), Homomorphic Encryption (HE), and Secure Multi-Party Computation (SMPC). These approaches are evaluated against three factors: their impact on latency, their resource and energy consumption, and their level of deployment maturity. The study also identifies inconsistencies in how current systems report performance metrics, and introduces a qualitative energy–latency trade-off matrix to help researchers and designers build secure and energy-efficient edge architectures.

3) Sustainable security architecture and performance metrics: A sustainability-focused framework for edge security systems is proposed using standardised metrics. Best practices for measuring and accounting for the additional energy and carbon costs introduced by security mechanisms are also discussed.

4) Future directions for sustainable and secure edge computing: A future research roadmap for secure and sustainable edge computing is provided. The roadmap highlights several important directions, including the use of quantum-resistant cryptography in edge computing, the adoption of federated learning for privacy-preserving collaborative security analysis, the creation of digital-twin-based risk models with sustainability considerations, and the implementation of edge-native, zero-trust policy enforcement. In addition, the need for standardised benchmarking methods is emphasised, given the limited real-world evidence connecting edge security solutions to their energy consumption and sustainability impact.

The rest of this paper is organized as follows. *Section II* reviews related work on the security and sustainability of edge and fog computing. *Section III* describes the ETSI MEC reference architecture used to examine security and sustainability metrics. *Section IV* presents the threat landscape in edge computing. *Section V* discusses the key security mechanisms used in smart-city edge environments. *Section VI* examines sustainable approaches to edge security and compares. *Section VII* concludes the paper.

II. BACKGROUND

Edge and fog computing have moved from conceptual models to core infrastructure for latency-sensitive and bandwidth-aware services within smart cities. Early work by Bonomi et al. [3], Shi et al. [2], and Wang et al. [5] established the architectural principles that distinguish edge and fog paradigms from centralized cloud computing — computational proximity, mobility support, and contextual responsiveness. These contributions were largely theoretical; later empirical studies validated the resulting improvements in latency, energy use, and throughput. Security and privacy in edge environments have received extensive survey treatment. Ranaweera et al. [18] classify trust-management, isolation, and data-protection schemes in mobile edge computing. Xiao et al. [17] and Zeyu et al. [30-31] analyse the expanded attack surface of decentralised architectures and the countermeasures available for diverse deployments.

Narrower studies address specific trade-offs: Wu et al. [32] examine classified protection layers, Patil et al. [33] cover end-to-end security costs, and Waguie and Al-Turjman [34] assess AI-driven defenses along with their exposure to adversarial manipulation.

Work on anomaly detection and resource-aware workload allocation runs alongside these efforts. Ahmed et al. [34] survey anomaly-detection methods adapted for edge contexts, and Deng et al. [9] propose optimisation models that jointly minimise latency and energy in fog–cloud systems. Eltanbouly et al. [36] and Abdali et al. [6] measure the overhead of intrusion detection, authentication, and policy enforcement, surfacing trade-offs that higher-level architectural discussions tend to miss.

Privacy preservation and trust-management analytics are now central to secure edge computing. Permissioned blockchains support verifiable identity, access control, and configuration provenance [20], whereas federated learning (FL) enables collaborative model training without exposing raw data [11]. The 2024 standardisation of post-quantum cryptographic primitives by the National Institute of Standards and Technology (NIST) has accelerated research on quantum-resilient edge security. Karakaya and Ulu [22, 35-36] analyse the practicality of deploying these methods under constrained resource and latency conditions.

Several works report measurable benefits of edge computing. Haseeb et al. proposed a green IoT architecture that lowered energy use by 21%, improved throughput by 15%, and reduced delay by 12%. Jararweh et al. achieved latency reductions of up to 62.6% through edge-based offloading in low-density environments. Improvements in latency, bandwidth, air-quality monitoring, and traffic optimisation have been reported in other studies. Swain et al. [37] further introduced game-theoretic orchestration methods to reduce energy consumption and carbon emissions in edge computing networks.

Recent studies have also focused on serverless edge computing, sustainability-driven anomaly detection, and optimization techniques. Ezeugwa [38] highlighted the scalability and manageability benefits of serverless edge systems, though without detailed energy metrics. Yu et al. developed an edge-based anomaly-detection model for sustainable industrial IoT, while Kose et al. [39] applied genetic optimization in healthcare edge environments with promising simulation results.

Despite this progress, several gaps remain. First, reproducible and hardware-independent energy or carbon benchmarks remain limited, and most reported results are platform-specific. Second, although trust mechanisms such as TEEs and blockchain are widely discussed, their actual energy and performance overheads are rarely quantified. Finally, while post-quantum cryptography standards are advancing, their practical integration into resource-constrained edge systems remains largely theoretical, with little real-world evaluation of their impact on energy use, latency, and scalability.

III. ENHANCING EDGE SYSTEM SECURITY AND SUSTAINABILITY USING ETSI MEC

The Multi-access Edge Computing (MEC) reference architecture forms the basis of this study for analysing both security and sustainability in edge systems. It examines security mechanisms such as TPM-based secure boot, TEE-protected application isolation, and blockchain-supported identity and access management, as well as sustainability metrics including Energy per Operation (EPO), Energy-Delay Product (EDP), Carbon Intensity (CI), and Lifecycle Energy Use (LEU).

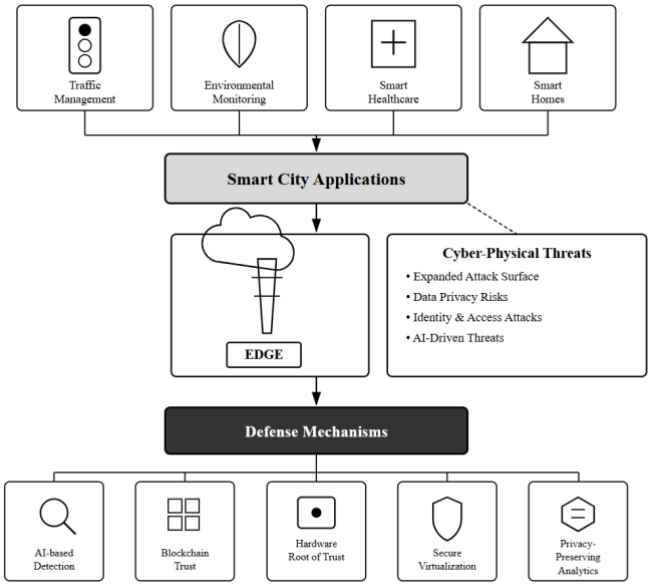

Fig. 2. ETSI MEC architecture with integrated security components [1].

Fig. 2 presents the adapted ETSI MEC architecture used to identify the layers and interfaces at which these metrics can be monitored and evaluated to support more secure, efficient, and sustainable edge deployments. It illustrates an enhanced ETSI MEC architecture with built-in sustainability monitoring points across the infrastructure, platform, and application layers. The framework measures key metrics such as Energy per Operation (EPO), Carbon Intensity (CI), Energy-Delay Product (EDP), and Lifecycle Energy Use (LEU), and also evaluates the overhead caused by security functions such as remote attestation and Trusted Execution Environments (TEEs). These monitoring points help identify the energy, latency, and carbon costs of edge security mechanisms. Overall, the model provides a practical blueprint for building more secure, efficient, and sustainable edge computing systems.

IV. THREATS LANDSCAPE IN EDGE COMPUTING

In smart-city environments, edge computing creates a highly distributed and complex security landscape. Fig. 3 categorises these security challenges into four major areas: (i) broadened attack surface, (ii) data exposure in transit, (iii) identity and access strain, and (iv) emerging attack vectors.

A. Broadened Attack Surface

Compared to centralised cloud infrastructures, edge systems rely on widely distributed nodes that are often placed in public or less secure environments. Devices deployed on poles, streetlights, and other outdoor locations are vulnerable to physical attacks, firmware tampering, hardware inspection, and unauthorised debugging access, which can weaken overall system security and trust [17].

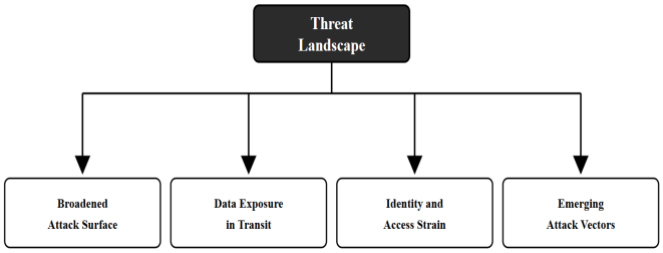

Fig. 3. Threats landscape in edge computing.

Lightweight edge protocols such as 6LoWPAN, RPL, and CoAP reduce communication overhead but also introduce security risks, including replay attacks, sinkhole attacks, and selective forwarding [32]. These threats are amplified by device diversity, irregular software updates, and limited monitoring capabilities. In MEC environments, frequent handovers and real-time operations further expand the attack surface, while side-channel attacks and weak device authentication continue to pose challenges to secure and scalable deployments [19].

B. Data Exposure in Transit

Edge nodes often process sensitive data such as video streams, vehicle telemetry, and biometrics before transmitting it to central systems. If this data is not properly protected during transmission or storage, it becomes vulnerable to interception, manipulation, and the injection of false data, affecting both privacy and integrity [18]. Limited security configurations in lightweight protocols can further expose systems to replay and eavesdropping attacks.

C. Identity and Access Strain

Edge environments are highly dynamic, with sensors, cameras, vehicles, and mobile devices constantly joining, leaving, or moving across networks. Traditional identity systems based on static provisioning and centralized PKIs struggle with this dynamism, often causing delays in certificate management and creating single points of failure [17]. If a central authority becomes unavailable, edge devices may fail to authenticate one another, disrupting critical services. Newer approaches such as decentralized IAM and Zero Trust improve resilience by distributing trust and enforcing continuous verification, often using hardware-based security and local credential checks [7]. However, these methods introduce added latency, management complexity, and scalability challenges that remain insufficiently evaluated in real deployments.

V. KEY SECURITY MECHANISMS IN SMART-CITY EDGE ENVIRONMENTS

Securing edge computing systems in smart cities requires a security-by-design approach built into every layer of the technology stack. Since edge devices process data close to where it is generated, they must balance strong security with sustainability goals such as energy efficiency and reduced carbon emissions. A reliable smart-city edge architecture is built around four key security areas.

1. AI-Based Threat Detection

Edge devices increasingly use lightweight machine learning models to monitor system behavior and detect unusual activity in real time. These models establish normal operating patterns and can identify threats such as sensor tampering, unauthorized access, or abnormal network traffic. Anomaly-detection techniques allow devices to react quickly without sending all data to centralized servers.

Federated Learning (FL) further strengthens privacy by enabling multiple devices to train shared models without exchanging raw data. However, FL systems can still face risks such as data poisoning and inference attacks, necessitating additional protections like differential privacy and secure aggregation.

2. Decentralised Trust Through Blockchain

Traditional centralised security systems often create single points of failure. Blockchain and distributed ledger technologies provide a decentralised alternative by creating tamper-resistant records of transactions and device activities. Smart contracts can also automate security policies across large networks of connected devices.

Permissioned blockchains are generally more suitable for smart cities because they offer lower latency and consume less energy than public, permissionless systems. Despite these advantages, further research is needed to measure the actual energy, latency, and carbon costs of blockchain-based security solutions on edge devices.

3. Hardware-Based Security and Secure Virtualization

Strong security must begin at the hardware level. Technologies such as Trusted Platform Modules (TPMs), secure boot mechanisms, and hardware roots of trust help verify system integrity from startup through application execution. Trusted Execution Environments (TEEs), including ARM TrustZone and Intel SGX, provide isolated spaces where sensitive operations can run securely even if the operating system is compromised. Physically Unclonable Functions (PUFs) further enhance security by generating unique hardware identities without storing permanent secret keys.

In addition, lightweight virtualization technologies such as microVMs and containers isolate applications and limit the impact of security breaches. Combined with continuous monitoring, encryption, and runtime attestation, these mechanisms improve resilience against attacks.

4. Privacy-Preserving Data Analytics

Smart-city applications often rely on data sharing while also needing to protect citizen privacy. Several privacy-preserving techniques support this goal. Differential Privacy (DP) adds controlled noise to datasets to prevent individual identification. Homomorphic Encryption (HE) allows computations to be performed on encrypted data, while Secure Multiparty Computation (SMPC) enables multiple parties to collaborate without revealing sensitive information.

Although these approaches provide strong privacy guarantees, they require significant computational resources and can introduce performance and energy overheads.

VI. SUSTAINABLE APPROACHES TO EDGE SECURITY

Security solutions deployed at the edge should not only be effective but also sustainable over the long term. Overlooking factors such as energy consumption, carbon emissions, and hardware lifecycle impacts can undermine the efficiency benefits typically associated with edge computing. In some cases, these neglected costs may even outweigh the advantages of processing data closer to the source. Recent studies highlight three key requirements for ensuring sustainable edge security. First, security hardware and communication protocols should be evaluated using comprehensive lifecycle assessments. This approach helps account for the environmental impact of manufacturing, deployment, operation, and disposal, preventing embodied carbon emissions from being hidden behind seemingly low operational power consumption [14].

The studies presented in Table I illustrate the diverse approaches being explored to strengthen security in edge computing environments. Research has examined the use of artificial intelligence for intelligent threat detection and response [9], federated learning for privacy-preserving analytics [11], and blockchain-based frameworks for decentralized trust management and secure data sharing [24]. Other works have focused on hardware-assisted protection through trusted execution environments [18], privacy-enhancing techniques such as homomorphic encryption [23], and emerging post-quantum cryptographic solutions designed to address future security threats [21].

In addition, comprehensive surveys have identified key vulnerabilities, attack vectors, and defense mechanisms across edge and multi-access edge computing architectures [16]. Collectively, these studies highlight that achieving robust edge security requires integrating multiple complementary technologies while carefully addressing performance overhead, scalability, implementation complexity, and resource constraints.

TABLE I. COMPARATIVE REVIEW OF REPRESENTATIVE STUDIES RELATED TO EDGE COMPUTING SECURITY

Ref.	Study Focus	Major Contribution	Key Limitations	Relevance to Edge Security
[9]	Machine Learning-Based Smart Traffic Management	Demonstrates the integration of AI and IoT for adaptive traffic monitoring and decision-making in smart-city environments.	Focuses primarily on application performance rather than comprehensive security evaluation.	Highlights the potential of AI-driven threat and anomaly detection at the edge.
[11]	Federated Learning for Distributed Systems	Introduces a communication-efficient federated learning framework that enables decentralized model training without centralized data collection.	Vulnerable to model-poisoning and inference attacks; requires frequent synchronization.	Provides a foundation for privacy-preserving security analytics in edge environments.
[16]	Edge Computing Security Survey	Presents a comprehensive analysis of security threats, vulnerabilities, and defense mechanisms in edge computing.	Primarily conceptual; lacks implementation-specific performance analysis.	Serves as a benchmark reference for understanding edge security challenges.
[17]	Multi-Access Edge Computing (MEC) Security	Reviews security and privacy concerns in MEC architectures, including authentication and access-control issues.	Limited discussion of emerging post-quantum security solutions.	Identifies critical attack surfaces and mitigation strategies in MEC deployments.
[18]	Trusted Execution Environments (TEEs)	Explains hardware-assisted secure execution and isolation mechanisms for protecting sensitive workloads.	Susceptible to certain side-channel and hardware-based attacks.	Enables secure boot, attestation, and trusted application execution.
[19]	Blockchain for Edge of Things	Investigates blockchain-based trust management and decentralized security models for edge ecosystems.	Consensus mechanisms may introduce latency and resource overhead.	Strengthens trust, data integrity, and access control across distributed edge nodes.
[21]	Post-Quantum Security for Edge Computing	Surveys quantum-resistant cryptographic approaches suitable for next-generation edge infrastructures.	Many proposed algorithms remain computationally expensive for constrained devices.	Addresses future security requirements against quantum-enabled attacks.
[23]	Homomorphic Encryption	Introduces practical homomorphic encryption techniques that support computation over encrypted data.	Significant computational and energy overhead.	Enables privacy-preserving data processing in edge and IoT systems.
[24]	Blockchain-Assisted Homomorphic Encryption	Combines blockchain and homomorphic encryption to enhance privacy protection in edge computing environments.	Increased implementation complexity and processing requirements.	Demonstrates secure data sharing and collaborative analytics.
[32]	Artificial Intelligence for Edge Security	Reviews AI-driven security mechanisms including intrusion detection, anomaly detection, and automated threat response.	Effectiveness depends heavily on training data quality and model robustness.	Supports intelligent and adaptive security management in dynamic edge networks.

The future of smart-city edge security depends on balancing protection with operational efficiency. Security solutions should not undermine the sustainability benefits that edge computing aims to deliver. Future research should focus on evaluating security mechanisms using measurable indicators such as Energy per Operation (EPO), Energy-Delay Product (EDP), Carbon Intensity (CI), and Lifecycle Energy Use (LEU).

Ultimately, successful smart-city security strategies will be those that provide strong protection while maintaining energy efficiency, scalability, and environmental sustainability. As edge computing becomes increasingly central to smart-city ecosystems, greater attention is being given to the interconnected challenges of security, privacy, and sustainability. Current research trends emphasize the

development of decentralized and efficient solutions that can protect sensitive data, support real-time decision-making, and minimize environmental impact, while operating effectively on the diverse and resource-limited devices that characterize modern edge environments. Overall, the literature reflects a growing shift toward security frameworks that balance performance, privacy protection, and long-term sustainability.

VII. CONCLUSION

Edge computing has emerged as a key enabler of smart-city development, supporting real-time data processing, intelligent decision-making, and improved service reliability. Despite these advantages, the distributed nature of edge environments creates significant challenges related to security, privacy, and sustainability. This review examined the major threats facing edge infrastructures and evaluated a range of security approaches, including artificial intelligence, blockchain, trusted hardware mechanisms, secure virtualization, and privacy-preserving analytics. The analysis highlighted both the benefits and trade-offs of these technologies in terms of protection capabilities, resource requirements, and practical deployment considerations. Furthermore, sustainability aspects such as energy consumption and environmental impact were considered to emphasize the importance of developing security solutions that are both effective and environmentally responsible. Looking ahead, emerging areas such as post-quantum cryptography, secure federated learning, digital twin technologies, and edge-native governance frameworks offer promising directions for future research. Overall, building secure, trustworthy, and sustainable edge ecosystems will require continued collaboration among researchers, industry stakeholders, and policymakers.

FUNDING STATEMENT

The author(s) received no specific funding for this study.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest to report regarding the present study.

AUTHOR CONTRIBUTIONS

Conceptualization, methodology, validation, writing—original draft preparation, writing—review and editing, A.I.C.

INSTITUTIONAL REVIEW BOARD STATEMENT

Not applicable.

INFORMED CONSENT STATEMENT

Not applicable.

DATA AVAILABILITY STATEMENT

Data is available on reasonable request.

REFERENCES

[1] M. Mrabet and M. Sliti, “Towards Secure, Trustworthy and Sustainable Edge Computing for Smart Cities: Innovative Strategies and Future Prospects,” *IEEE Access*, vol. 4, DOI 10.1109/ACCESS.2025.3602390, 2025.

[2] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, “Edge computing: Vision and challenges,” IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637–646, 2016.

[3] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, “Fog computing and its role in the internet of things,” in Proc. 1st ACM Workshop on Mobile Cloud Computing (MCC), Helsinki, Finland, pp. 13–16, Aug. 2012.

[4] T. Wang, Z. Peng, S. Wen, G. Wang, B. Wang, and A. Liu, “A survey of fog computing in wireless sensor networks: Concepts, frameworks, applications and issues,” Ad Hoc & Sensor Wireless Networks, vol. 44, pp. 109–130, 2019.

[5] T.-A. N. Abdali, R. Hassan, A. H. M. Aman, and Q. N. Nguyen, “Fog computing advancement: Concept, architecture, applications, advantages, and open issues,” IEEE Access, vol. 9, pp. 75961–75980, 2021.

[6] Y. Jararweh, S. Otoum, and I. Al Ridhawi, “Trustworthy and sustainable smart city services at the edge,” Sustainable Cities and Society, vol. 62, 2020.

[7] R. Deng, R. Lu, C. Lai, T. Luan, and H. Liang, “Optimal workload allocation in fog–cloud computing toward balanced delay and power consumption,” IEEE Internet of Things Journal, vol. 3, no. 6, pp. 1171–1181, 2016.

[8] E. Androulaki, A. Barger, V. Bortnikov, et al., “Hyperledger fabric: A distributed operating system for permissioned blockchains,” in Proc. 13th EuroSys, Porto, Portugal, 2018.

[9] M. Kumar, K. Raju, D. Kumar, N. Goyal, S. Verma, and A. Singh, “An efficient framework using visual recognition for IoT-based smart city surveillance,” Multimedia Tools and Applications, vol. 80, pp. 31277–31295, 2021.

[10] U. Lilhore, A. Imoize, C.-T. Li, et al., “Design and implementation of an ML- and IoT-based adaptive traffic-management system for smart cities,” Sensors, vol. 22, no. 1, 2022.

[11] Z. Zheng, Y. Zhou, Y. Sun, Z. Wang, B. Liu, and K. Li, “Applications of federated learning in smart cities: Recent advances, taxonomy, and open challenges,” Connection Science, vol. 34, no. 1, pp. 1–28, 2022.

[12] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. Arcas, “Communication-efficient learning of deep networks from decentralized data,” in Proc. Int. Conf. Artificial Intelligence and Statistics (AISTATS), Fort Lauderdale, FL, USA, pp. 1273–1282, 2017.

[13] K. Haseeb, I. Ud Din, A. Almogren, I. Ahmed, and M. Guizani, “Intelligent and secure edge-enabled computing model for sustainable cities using green internet of things,” Sustainable Cities and Society, vol. 68, 2021.

[14] C. Berville, C. Croitoru, and F. Bode, “Life-cycle analysis in the context of smart cities,” in E3S Web of Conferences, vol. 480, 2025.

[15] Y. Kim, U. Gupta, A. McCrabb, et al., “Greenscale: Carbon-aware systems for edge computing,” arXiv:2304.00404, 2023.

[16] K. Ma and Y. Zhou, “A comprehensive quantitative lifecycle cost and environmental impact analysis model for computing infrastructure,” MethodsX, vol. 13, 2024.

[17] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, “Edge computing security: State of the art and challenges,” Proceedings of the IEEE, vol. 107, no. 8, pp. 1608–1631, 2019.

[18] P. Ranaweera, A. Jurcut, and M. Liyanage, “Survey on multi-access edge computing security and privacy,” IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1078–1124, 2021.

[19] M. Sabt, M. Achemlal, and A. Bouabdallah, “Trusted execution environment: What it is, and what it is not,” in Proc. IEEE TrustCom/BigDataSE/ISPA, Helsinki, Finland, pp. 57–64, 2015.

[20] T. Gadekallu, V. Pham, D. Nguyen, et al., “Blockchain for edge of things: Applications, opportunities, and challenges,” IEEE Internet of Things Journal, vol. 9, no. 2, pp. 964–988, 2021.

[21] National Institute of Standards and Technology, “NIST releases first 3 finalized post-quantum encryption standards,” 2024. Accessed: Jul. 25, 2025. [Online]. Available: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[22] A. Karakaya and A. Ulu, “A survey on post-quantum-based approaches for edge computing security,” Wiley Interdisciplinary Reviews: Computational Statistics, vol. 16, no. 3, 2024.

[23] S. Hoque, A. Aydeger, and E. Zeydan, “Exploring post-quantum cryptography with quantum key distribution for sustainable mobile network architecture design,” in Proc. 4th Workshop on Performance & Energy Efficiency in Concurrent and Distributed Systems, Edinburgh, UK, 2024.

[24] J. Cheon, A. Kim, M. Kim, and Y. Song, “Homomorphic encryption for arithmetic of approximate numbers,” in Proc. Advances in Cryptology – ASIACRYPT 2017, vol. 10624 of LNCS, Hong Kong, China, pp. 409–437, Springer, 2017.

[25] J. Liao, H. Wang, and J. Wu, “A multikey fully homomorphic encryption privacy-protection protocol based on blockchain for edge computing systems,” Concurrency and Computation: Practice and Experience, vol. 35, no. 2, 2023.

[26] X. He, D. Chen, N. Zhang, H. Dai, and K. Yu, “Integration of blockchain and edge computing in internet of things: A survey,” arXiv:2205.13160, 2022.

[27] S. Mishra, N. Kumar, B. Rao, B. Brahmendra, and L. Teja, “Role of federated learning in edge computing: A survey,” Journal of Autonomous Intelligence, 2023.

[28] S. Lu, Z. Zhang, and M. Papaefthymiou, “A 1.25 pJ/bit 0.048 mm² AES core with DPA resistance for IoT devices,” in Proc. IEEE Asian Solid-State Circuits Conf. (A-SSCC), Seoul, Korea, pp. 66–68, 2017.

[29] C. Hung and W. Hsu, “Power consumption and calculation requirement analysis of AES for wireless sensor and IoT networks,” Sensors, vol. 18, no. 6, 2018.

[30] Z. Huangfu, G. Xia, Z. Wang, and Y. Sen, “Survey on edge computing security,” in Proc. Int. Conf. Big Data, Artificial Intelligence and IoT Engineering (ICBAIE), Fuzhou, China, pp. 96–105, 2020.

[31] W. Wu, Q. Zhang, and H. Wang, “Edge computing security protection from the perspective of classified protection of cybersecurity,” in Proc. Int. Conf. Information Science and Control Engineering (ICISCE), Shanghai, China, pp. 278–281, 2019.

[32] K. Patil, S. Gupta, A. Nair, and V. Gutte, “Cloud, fog and edge computing: Security and privacy concerns,” International Journal for Research in Applied Science and Engineering Technology, vol. 10, no. 5, pp. 181–189, 2022.

[33] F. Waguie and F. Al-Turjman, “Artificial intelligence for edge computing security: A survey,” in Proc. Int. Conf. Artificial Intelligence in Everything (AIE), Istanbul, Turkey, pp. 446–450, 2022.

[34] M. Ahmed, A. Mahmood, and J. Hu, “A survey of network anomaly detection techniques,” Journal of Network and Computer Applications, vol. 60, pp. 19–31, 2016.

[35] S. Eltanbouly, M. Bashendy, N. Alnaimi, Z. Chkirbene, and A. Erbad, “Machine learning techniques for network anomaly detection: A survey,” in Proc. IEEE Int. Conf. Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, pp. 156–162, 2020.

[36] M. Mukherjee, R. Matam, C. Mavromoustakis, et al., “Intelligent edge computing: Security and privacy challenges,” IEEE Communications Magazine, vol. 58, no. 9, pp. 26–31, 2020.

[37] S. Alkaabi, M. Gregory, and S. Li, “Multi-access edge computing handover strategies, management, and challenges: A review,” IEEE Access, vol. 12, pp. 4660–4673, 2024.

[38] S. Swain, K. Chakravarty, A. Jena, and et al., “Green edge computing sustainability using a game theoretic approach,” in Proc. 15th Int. Conf. Computing Communication and Networking Technologies (ICCCNT), (Kharagpur, India), pp. 1–5, 2024.

[39] X. Yu, X. Yang, Q. Tan, C. Shan, and Z. Lv, “An edge computing-based anomaly detection method in IoT industrial sustainability,” *Applied Soft Computing*, vol. 128, 2022.