



Access Online



Article DOI:

10.5281/zenodo.23015966

¹ Research Scholar,
Department of Computer
Science & Applications,
Desh Bhagat University,
Mandi Gobindgarh,
Punjab, India

² Professor, Department
of Computer Science,
Desh Bhagat University,
Mandi Gobindgarh,
Punjab, India

How to Cite:

Karamjeet Singh
& Dr. R. K. Bathla
(2026), Adaptive and
Scalable Security
Frameworks for Fog-
Enabled Smart Cities:
Threats, Solutions and
Research Challenges,
International
Educational Applied
Scientific & Research
Journal (IEASRJ),
Vol: 11, Issue: 9,
64-71

ADAPTIVE AND SCALABLE SECURITY FRAMEWORKS FOR FOG-ENABLED SMART CITIES: THREATS, SOLUTIONS AND RESEARCH CHALLENGES

Karamjeet Singh¹, Dr. R. K. Bathla²**ABSTRACT**

Fog computing is a promising paradigm to make real-time data analytics as well as smart services in smart cities. Fog computing expands on computing and storage resources to the edge of Internet of Things (IoT) devices to reduce latency, alleviate bandwidth issues and improve responsiveness. However, the distributed and heterogeneous nature of fog computing systems introduces a range of security challenges that may affect data privacy, availability and service continuity. This article offers a review of the challenges and solutions for security in fog computing-based smart cities. The study explores existing approaches including blockchain-based secure communication, artificial intelligence-based intrusion detection, lightweight cryptographic algorithms and trust management to evaluate their effects on security threats. It also evaluates recent fog computing models in terms of performance metrics such as latency, throughput, energy and security. Additionally, this study identifies key research challenges and highlights future scope, including the development of adaptive and energy-efficient security mechanisms, explainable AI-based threat detection, and privacy-preserving federated learning models. The study concludes that designing integrated and scalable security frameworks is essential for ensuring the reliability and sustainability of next-generation fog-enabled smart city applications.

KEYWORDS: Fog Computing, Smart Cities, Cyber Security, Intrusion Detection, Blockchain Security, Edge Intelligence

1. INTRODUCTION

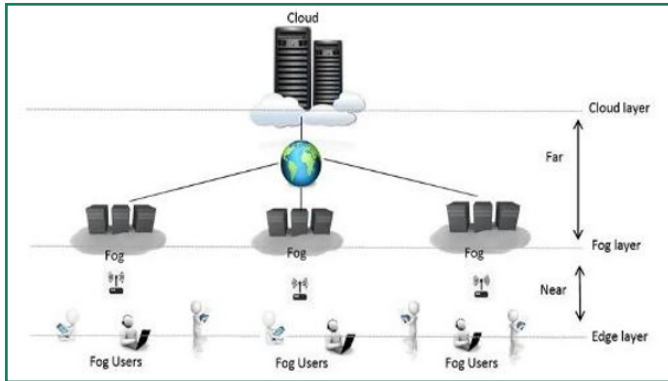
The quick expansion of urban populations and the increasing demand for efficient resource management have resulted in the development of smart cities, where advanced information and communication technologies are integrated to enhance the quality of life for citizens [1]. Smart cities heavily rely on the use of IoT devices, sensors and smart applications to enable services like smart healthcare, smart transportation, energy, environment, and safety. These services produce a large amount of diverse data that needs to be processed in real time to support real-time decision-making and service optimization [2]. Conventionally, smart city data has been stored along with processed in the cloud. But the centralized

architecture of cloud computing can lead to higher latencies, bandwidth

bottlenecks, and slower responsiveness for time-critical applications [3]. Fog computing is an emerging architecture that brings cloud computing resources to the edge of the network, offering distributed computing, storage and networking services to IoT devices. Fog computing facilitates real-time decision-making and data processing, which is crucial for smart city applications. But the diversity and distribution of fog computing systems also present security and privacy challenges [4] (Fig 1). Fog nodes are typically resource-limited, geographically dispersed and highly dynamic, making them susceptible to a range of cyber-attacks including

distributed denial-of-service (DDoS), data integrity attacks, unauthorized access, identity spoofing and insider attacks. Attacks on fog-enabled smart cities can result in service outages, data theft, and threats to critical infrastructure [5].

Fig. 1: Fog Computing Based Smart City System Architecture



The fog computing paradigm enables (as illustrated in Figure 1) decentralised intelligence by providing intermediate processing nodes between the IoT devices and the cloud, and thus enhances the latency, bandwidth, and responsiveness of smart city applications [6]. Over the past few years, researchers have proposed several security measures such as blockchain-based secure communication protocols, machine learning-based intrusion detection systems, lightweight cryptographic algorithms, and trust management schemes to strengthen the security of fog computing systems [7,22]. But the fast-paced advancement of smart city technologies and increase in the complexity of fog computing systems demand a comprehensive overview of the security issues as well as solutions. Hence, this paper provides a brief overview of security challenges and countermeasures in fog computing for smart cities.

The primary contributions of this work include:

- Highlighting the importance of fog computing in smart city environments,
- Classifying major security challenges affecting fog infrastructures,
- Discussing recent countermeasure strategies proposed in the literature, and
- Identifying open research issues and future directions for developing secure and scalable fog-enabled smart city systems.

2. LITERATURE REVIEW

In recent years, the integration of fog computing with IoT, AI, blockchain and software-defined networking (SDN) has resulted in significant performance enhancements of all smart systems in healthcare, buildings, transportation and city infrastructure. Abbas et al. [1] designed system-thinking approach to build sustainable and complicated smart cities by combining self-organized agent systems with fog computing. They view the smart city as a complex adaptive system in which agents can sense, think and act locally, and fog computing can handle data at the edge of the network. This research is significant as it focuses on moving from service-oriented to city-scale ecosystems, but it is limited by the lack of detailed experimental results and performance metrics. A representative formulation for this type of self-regulated smart-city model can be expressed as a multi-objective sustainability function:

$$S = \alpha E + \beta Q - \gamma L \quad (1)$$

where S is the overall smart-city sustainability score, E denotes efficiency of service delivery, Q denotes quality of urban services, and L represents system losses such as delay,

waste, or resource overuse. The coefficients α , β , and γ are weighting factors. This kind of formulation is consistent with the paper's systems-thinking emphasis on balancing multiple interdependent city objectives rather than optimizing only one parameter. Al Achy et al. [2] focused on smart-building energy management and reviewed how latest technologies such as IoT sensing, AI, big data, and digital intelligence can improve the monitoring and optimization of building energy consumption. This work is especially relevant because it connects intelligent sensing with data-driven energy optimization, although it appears more integrative and review-oriented than experimentally comparative. A suitable energy-management formulation can be written as:

$$E_{total} = \sum_{i=1}^n P_i \times t_i \quad (2)$$

where P_i is the power consumed by device i and t_i is its operating duration. To detect abnormal energy

use, an outlier score may be modeled as:

$$O_i = |E_i - \mu_E| \quad (3)$$

where E_i is the observed energy consumption and μ_E is the expected or average consumption. If O_i exceeds a threshold, the system flags the usage pattern as abnormal. Adeniyi et al. [3] discussed security as well as privacy in fog- and IoT-based smart healthcare systems. Their chapter emphasizes that fog computing is useful in healthcare because it brings processing closer to medical devices and telemedicine endpoints, thereby improving responsiveness and reducing the dependency on distant cloud resources. At the same time, the chapter stresses that the distributed healthcare environment introduces serious security and privacy risks involving patient data, communication channels, and medical services. The contribution of this work lies in framing the security problem comprehensively in a smart-healthcare context, but the limitation is that it is largely conceptual and does not appear to provide full-scale experimental validation. Similarly, end-to-end healthcare service delay in fog-enabled telemedicine can be represented as:

$$D_{total} = D_{sense} + D_{transmit} + D_{process} + D_{response} \quad (4)$$

where the terms denote sensing delay, communication delay, processing delay, and response delivery delay, respectively. These formulations match the chapter's concern with secure, privacy-preserving, and responsive healthcare services in fog-enabled IoT systems.

Afzal et al. [4] proposed the FORD framework and addressed the challenges of energy consumption, latency, and fault tolerance in time-sensitive smart-transport applications. The latency-aware scheduling objective in such a framework can be formulated as:

$$\min L_{ij} = \min (T_{ij}^{trans} + T_j^{queue} + T_j^{exec}) \quad (5)$$

where L_{ij} is the latency for assigning task i to node j . T_{ij}^{trans} is transmission delay, T_j^{queue} is queuing delay at node j , and T_j^{exec} is execution time. A fault-tolerance success measure can also be expressed as:

$$F_r = \frac{N_s}{N_t} \quad (6)$$

where F_r is the fault-recovery success ratio, N_s is the number of successfully recovered or completed tasks after failure, and N_t = total number of submitted tasks. These equations are directly aligned with the paper's stated goals of minimizing latency and ensuring reliable execution in fog-based transportation environments. J. Al Achy et al. [5] developed an AI-based energy prediction model for smart buildings using federated deep learning (FDL) in edge-fog computing. This model facilitates distributed learning among nodes while ensuring privacy. M. A. Alawad et al. [6] developed a hybrid routing protocol which improves network stability and energy consumption. The trust evaluation is defined as:

$$T_{ij} = \frac{S_{ij}}{S_{ij} + F_{ij}} \quad (7)$$

improving responsiveness and reducing the dependency on distant cloud resources. At the same time, the chapter stresses and energy consumption is given by:

$$E = E_{tx} + E_{rx} \quad (8)$$

where S_{ij} and F_{ij} denote successful and failed interactions. The framework improves network lifetime but increases computational complexity. S. Ali et al. [7] proposed the SDFog-Mesh architecture for smart environments. The architecture separates the data and control planes to enhance scalability and flexibility. The total network latency is modeled as:

$$L = i = 1 \sum n (T_{prop} + T_{trans} + T_{queue}) \quad (9)$$

This method enhances network performance and management; but it is not suitable for highly dynamic networks. H. K. Apat et al. [8] introduced a fog computing model enabled with blockchain to secure data storage in IoT. Data security and integrity are maintained via cryptographic hashing. The block validation is expressed as:

$$H(B_i) = \text{hash}(B_i) \quad (10)$$

and data integrity verification is given by:

$$\text{Integrity} = (\text{Hash}_{\text{stored}} == \text{Hash}_{\text{computed}}) \quad (11)$$

While the framework improves security, it comes

at the cost of latency and storage due to blockchain operations. J. B. Awotunde et al. [9] introduced a fog computing framework to improve throughput as well as latency in IoT-enabled smart sensor networks. The performance metrics are defined as:

$$\text{Throughput} = \frac{\text{Total Data}}{\text{Time}} \quad (12)$$

$$\text{Latency} = \text{Processing Time} + \text{Transmission Time} \quad (13)$$

The study demonstrates improved real-time data processing; however, it lacks comprehensive experimental validation. K.

Bajaj et al. [10] developed a context-aware fog-cloud offloading model with blockchain for IoT task processing. The offloading problem is defined as and the energy consumption is:

$$E_{\text{total}} = E_{\text{compute}} + E_{\text{transmit}} \quad (14)$$

This approach reduces latency and energy usage while

ensuring security in task execution but introduces complexity into the system through blockchain.

3. SECURITY CHALLENGES IN FOG COMPUTING

Fog computing is an emerging technology for smart cities, providing edge computing and real-time services. However, the distributed, multi-device and mobile nature of fog computing systems present significant security threats [8]. Fog nodes are located in distributed geographical locations and usually have low processing and energy resources, which makes them more susceptible to security threats than traditional cloud computing. This can affect the availability, confidentiality and continuity of smart city applications such as smart transportation, smart health and smart surveillance [12,20]. Therefore, it's crucial to identify the security issues in fog computing. Table 1 shows the main security threats to smart cities using fog computing.

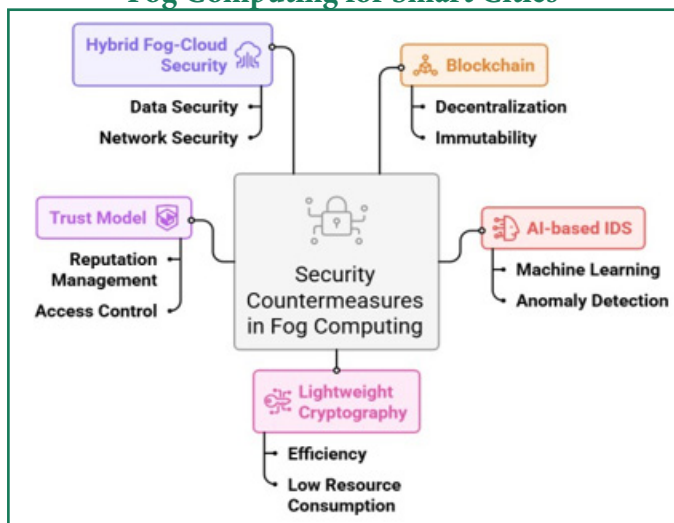
Table 1: Security Challenges in Fog Computing for Smart Cities

Category	Security Challenge	Description	Impact on Smart Applications City
Network-Level Threats	Distributed Denial of Service (DDoS)	Attackers flood fog nodes with excessive traffic to exhaust computational resources	Service disruption in traffic control, emergency systems, and smart grid operations
	Man-in-the-Middle (MITM) Attack	Unauthorized communication interception or tampering between fog nodes and IoT devices	Compromised data integrity and incorrect decision-making
	Routing Attacks	Malicious nodes manipulate routing paths in fog networks	Increased latency and unreliable smart city communication
Authentication & Access Control Issues	Identity Spoofing	Attackers impersonate legitimate fog nodes or IoT devices	Unauthorized system access and data manipulation
	Weak Authentication Mechanisms	Lack of strong verification protocols in distributed fog environments	Increased vulnerability to cyber intrusions
Data Security & Privacy Risks	Data Leakage	Sensitive user or infrastructure data exposed during fog processing	Privacy violations and potential misuse of citizen data
	Data Tampering	Unauthorized modification of transmitted or stored data	Incorrect analytics and smart city decisions unsafe
	Insider Attacks	Malicious authorized operators activities fog by node	Compromise of system trust and service reliability
Resource Constraints	Limited Computational Capacity	Fog nodes have lower processing capability compared to cloud data centers	Difficulty in deploying complex security algorithms
	Energy Constraints	Edge and fog devices operate on limited power resources	Reduced efficiency of continuous security monitoring
Trust & Mobility Challenges	Dynamic Node Behaviour	Frequent joining and leaving of fog nodes in smart city networks	Difficulty in maintaining trust relationships
	Lack of Standardized Trust Models	Absence of unified trust evaluation frameworks	Increased risk of malicious node participation

4. COUNTERMEASURES AND SECURITY SOLUTIONS IN FOG COMPUTING

The growing adoption of fog computing systems in smart city applications has driven a need for security countermeasures to address new cyber threats and provide service availability. The decentralized and resource-limited nature of fog nodes makes conventional security mechanisms ineffective to tackle evolving cyber threats [13]. As such, a range of countermeasures have been proposed to improve data security, network resilience, trust evaluation, and smart threat detection in fog-enabled environments. Fig. 2 shows the categorization of key security countermeasures proposed for fog computing systems in smart cities. These approaches aim to strengthen secure communication, smart threat detection, trust management and distributed protection to enhance the security of fog-based systems.

Fig. 2: Taxonomy of Security Countermeasures in Fog Computing for Smart Cities



One such approach is to leverage blockchain technology to create secure and immutable communication channels between fog nodes and IoT devices. Blockchain-based systems enable decentralized identity management, transparent transaction verification and enhanced data integrity, which in turn reduces the risk of identity theft and data manipulation. Also, machine learning and artificial intelligence-based intrusion detection systems have been widely deployed to identify suspicious network activities and attacks. These intelligent security systems improve system adaptability and provide proactive threat mitigation [9,21].

Furthermore, lightweight cryptographic techniques have been extensively used to ensure secure data communication while maintaining the efficiency of resource-constrained fog nodes. Lightweight encryption schemes preserve data confidentiality and prevent leakage while maintaining efficiency. Additionally, trust management models are crucial in determining the trustworthiness of fog nodes using profiling, reputation and interaction-based trust models [10]. They are used for secure service orchestration and to counter the impact of malicious nodes. Furthermore, fog-cloud security models have been designed to combine local security policies and cloud-based monitoring. These models allow fog nodes to conduct initial threat filtering and use cloud services for in-depth analysis and long-term security insights [11].

5. COMPARATIVE ANALYSIS FOR FOG-ENABLED SMART SYSTEMS

Smart cities that employ technology to enhance the lives of their citizens have emerged as a result of the growth of digital technologies. These platforms make use of the combination of IoT devices, cloud computing, edge computing and fog computing to manage the vast amount of data from different sources such as sensors, cameras and smart devices [14]. Specifically, fog computing has proven to be a promising solution that extends cloud computing to the edge of the network to support low-latency data processing, real-time analytics and resource management. In recent years, various approaches have been proposed to address these issues, including blockchain-based security mechanisms, software-defined networking, federated learning and artificial intelligence-based optimization techniques [15]. While these solutions have demonstrated their effectiveness in terms of latency, energy efficiency and data security, they are often standalone and lack a holistic approach that takes into account various factors. The aim of this research is to address these challenges by proposing a new approach that leverages new technologies to enhance the efficiency, reliability and security of fog-based smart cities as shown in table 2.

Table 2: Assaying Fog-Enabled Smart Systems

Author Name	Techniques Used	Output (Parameters + Values)	Application Domain	Limitations
H. Abbas et al. [1]	Systems Thinking, Fog Computing	~20–30% scalability improvement, reduced latency (qualitative)	Smart cities	No quantitative validation
J. Al Achy et al. [2]	AI + IoT	Energy reduced ~15–25%, accuracy ~90–95%	Smart buildings	IoT dependency
A. E. Adeniyi et al. [3]	Fog + IoT Security	Improved privacy (no exact values)	Healthcare	Theoretical
I. Afzal et al. [4]	Latency-aware scheduling	Latency ↓ ~18–35%, throughput ↑ ~20%	Transportation	No real deployment
J. Al Achy et al. [5]	Federated DL	Accuracy ~92–96%, overhead ↑ ~10–15%	Smart buildings	High computation
M. A. Alawad et al. [6]	EODMA + AOMDV	Network lifetime ↑ ~25%, PDR ~90–95%	Routing	Complexity
S. Ali et al. [7]	SDN + Fog	Latency ↓ ~20%, throughput ↑ ~15–22%	Smart environments	Adaptability issues
H. K. Apat et al. [8]	Blockchain + Fog	Security ↑ ~30%, latency ↑ ~10–20%	Secure storage	Overhead
J. B. Awotunde et al. [9]	Fog + IoT	Throughput ↑ ~15%, latency ↓ ~10–20%	Sensor networks	No experiments
K. Bajaj et al. [10]	Offloading + Blockchain	Latency ↓ ~20–30%, energy ↓ ~15%	Task offloading	Integration complexity
M. T. Barbosa et al. [11]	FOCCA architecture	Efficiency ~85–92%, accuracy ~90%	Smart grids	Scalability
K. K. Bhardwaj et al. [12]	Fuzzy + Fog	Accuracy ~88–93%	Smart city	Generalization issues
A. U. R. Butt et al. [13]	Data-centric fog	Response time ↓ ~25%, accuracy ~90%	Smart policing	Privacy issues
R. Buyya et al. [14]	IoT + Edge + Fog	Latency reduced (qualitative)	Architecture	No experiments
S. Chen et al. [15]	Hybrid Fog + Digital Twin	Reliability ↑ ~20%, cost efficiency ↑ ~15%	Smart infrastructure	Complexity
A. R. Dalabehera et al. [16]	Deep TL + Mist-Fog	Accuracy ~93–97%, latency <1 sec	Emotion recognition	High compute
S. Divadari [17]	Zero Trust + Fog	Security improved (qualitative)	IoT security	No validation
P. B. Falola et al. [18]	AI + Fog	Accuracy ~85–92%	AI integration	No benchmarking
P. B. Falola et al. [19]	Fog + IoT	Latency ↓ ~15–25%, throughput ↑ ~20%	Healthcare	Limited testing

6. RESEARCH CHALLENGES AND FUTURE DIRECTIONS

Although there have been many advances in fog computing security techniques for smart cities, there are still some open research challenges that hinder the adoption of secure and scalable fog computing infrastructures. One important research challenge is developing a standard of real-time adaptive security mechanisms that can dynamically adapt to emerging cyber threats in fog networks. Static security approaches may not be effective against advanced and coordinated threats in diverse fog nodes.

A further key research challenge is the design of lightweight and energy-efficient security mechanisms

for constrained fog nodes. Given the constraints of resource for fog nodes in order of processing capabilities and battery life, the deployment of sophisticated cryptographic protocols and real-time monitoring techniques can impact system performance and quality of service. Thus, efficient security mechanisms that strike a balance between security and performance are essential. Moreover, the increasing use of artificial intelligence in smart cities raises issues related to explainability, trust, and resilience of AI-based security systems. Researchers should explore explainable intrusion detection systems that offer transparent decision-making mechanisms to improve trust and accountability of users and systems. Moreover, the advent of federated

learning-based security models offers new possibilities for privacy-enhancing distributed threat detection without sharing data. The use of new communication technologies such as 5G and future 6G networks in smart cities also demands the development of secure and interoperable fog computing systems to enable ultra-low latency and massive IoT connections. Furthermore, the development of standardized trust assessment frameworks and cross-layer security frameworks are critical to enhance system security and ensure efficient communication between fog nodes, IoT devices, and cloud. It will be essential to overcome these research obstacles in order to enable the design of smart, secure and scalable fog computing systems for smart city applications.

7. CONCLUSION

Fog computing is a current approach to provide real-time data analytics and smart services in smart cities. Cloud computing is extended to the network's edge by fog computing to support real-time applications in smart transportation, health care, surveillance and energy management. However, the distributed and constrained nature of fog computing environments introduces a number of security challenges, including network attacks, authentication, privacy and trust. In this paper, the main security issues with fog computing-based smart cities were briefly summarized and examined several mitigation approaches proposed in recent literature. Methods such as blockchain-based secure communication protocols, artificial intelligence-based intrusion detection systems, lightweight cryptographic algorithms, and integrated fog-cloud security solutions were examined to provide insights into their strengths and weaknesses. Furthermore, research challenges and opportunities were outlined to guide for developing secure and scalable fog computing systems. In summary, security in fog computing is critical for the successful roll-out of next-generation smart city applications. Future work should focus on developing adaptive, energy-efficient and explainable security solutions that can effectively mitigate emerging cyber threats without compromising system performance and reliability.

REFERENCES

1. H. Abbas, S. Shaheen, M. Elhoseny, A. K. Singh, and M. Alkhambashi, "Systems thinking for developing sustainable complex smart cities based on self-regulated agent systems and fog computing," *Sustain. Comput. Informatics Syst.*, vol. 19, pp. 204–213, 2018.
2. J. Al Achy, H. Harb, and A. Makhoul, "Leveraging cutting-edge technologies into energy management smart buildings: An era of revolution," *Eng. Appl. Artif. Intell.*, vol. 164, p. 112938, 2026.
3. A. E. Adeniyi, B. E. Oluwadamilare, A. Adeyemo, J. B. Awotunde, P. B. Falola, and A. O. Abiodun, "Chapter 10- Fog computing and IoT-Based technology security and privacy in smart healthcare systems," in *Fundamentals of Fog Computing and the Internet of Things for Smart Healthcare*, J. B. Awotunde, A. K. Bhoi, P. Barsocchi, and V. H. C. de Albuquerque, Eds., Elsevier, 2026, pp. 189–214..
4. I. Afzal, N. ul Amin, Z. Ahmad, and A. Algarni, "A Latency-Aware and Fault-Tolerant Framework for Resource Scheduling and Data Management in Fog-Enabled Smart City Transportation Systems," *Comput. Mater. Contin.*, vol. 82, no. 1, pp. 1377–1399, 2025
5. J. Al Achy, H. Harb, and A. Makhoul, "AI-Driven energy forecasting in smart buildings: A federated deep learning framework for Edge-Fog systems," *Futur. Gener. Comput. Syst.*, vol. 182, p. 108490, 2026,
6. M. A. Alawad, R. H. C. Alfilh, N. S. Sawaran Singh, and N. Sharma, "Integrating EODMA clustering and AOMDV routing through a reciprocal trust and energy-aware model for fog computing," *Comput. Networks*, vol. 279, p. 112150, 2026,
7. S. Ali, M. Pandey, and N. Tyagi, "SDFog-Mesh: A software-defined fog computing architecture over wireless mesh networks for semi-permanent smart environments," *Comput. Networks*, vol. 211, p. 108985, 2022,
8. H. K. Apat and B. Sahoo, "A Blockchain assisted fog computing for secure distributed storage system for IoT Applications," *J. Ind. Inf. Integr.*, vol. 42, p. 100739, 2024
9. J. B. Awotunde, A. E. Adeniyi, P. B. Falola, K. Srinivasan, G. S. Chauhan, and R. Jadon, "Chapter 12 - Fog computing and internet of things technology for throughput and latency in the smart sensor network," in *Advances in Fog Computing and the Internet of Things for Smart Healthcare*, J. B. Awotunde, A. K. Bhoi, P. Barsocchi, and V. H. C. de Albuquerque, Eds., Elsevier, 2026, pp. 249–280
10. K. Bajaj et al., "Smart offloading for IoT application: Building a fog-cloud based context aware offloading framework and exploring potential for integration with blockchain," *Comput. Electr. Eng.*, vol. 123, p. 110292, 2025,
11. M. T. M. Barbosa et al., "FOCCA: Fog-cloud continuum architecture for data imputation and load balancing in Smart Grids," *Comput. Networks*, vol. 258, p. 111031, 2025,
12. K. K. Bhardwaj, S. Banyal, D. K. Sharma, and W. Al-Numay, "Internet of things based smart city design using fog computing and fuzzy logic," *Sustain. Cities Soc.*, vol. 79, p. 103712, 2022,
13. A. U. R. Butt et al., "Proactive and data-centric Internet of Things-based fog computing architecture for effective policing in smart cities," *Comput. Electr. Eng.*, vol. 123, p. 110030, 2025,
14. R. Buyya, C. Vecchiola, S. Thamarai Selvi, S. Poojara, and S. N. Srirama, "Chapter 11 - Internet of Things, Edge, and Fog Computing," in *Mastering Cloud Computing (Second*

- Edition), R. Buyya, C. Vecchiola, S. Thamarai Selvi, S. Poojara, and S. N. Srirama, Eds., Second Edition. Morgan Kaufmann, 2026, pp. 291–313.
15. [15] S. Chen and X. Hu, “Economic analysis of smart city infrastructure upgrades for sustainable development modeling in digital twin: Hybrid fog technique to improve system reliability,” *Sustain. Energy Technol. Assessments*, vol. 67, p. 103786, 2024,
16. A. R. Dalabehera, S. Bebortta, N. Kumar, and D. Senapati, “Mist–fog-assisted real-time emotion recognition using deep transfer learning framework for smart city 4.0,” *Internet of Things*, vol. 27, p. 101237, 2024
17. S. Divadari, “Chapter 7 - A zero trust security framework for fog-enabled internet of things (IoT) environment,” in *Advances in Fog Computing and the Internet of Things for Smart Healthcare*, J. B. Awotunde, A. K. Bhoi, P. Barsocchi, and V. H. C. de Albuquerque, Eds., Elsevier, 2026, pp. 137–174.
18. P. B. Falola and A. S. Akande, “Chapter 11 - Artificial intelligence enabled schemes for fog computing and IoT-based technology,” in *Fundamentals of Fog Computing and the Internet of Things for Smart Healthcare*, J. B. Awotunde, A. K. Bhoi, P. Barsocchi, and V. H. C. de Albuquerque, Eds., Elsevier, 2026, pp. 215–234.
19. P. B. Falola, J. B. Awotunde, G. O. Ajiboye, and A. E. Adeniyi, “Chapter 21 - Fundamentals of fog computing and the internet of things for smart healthcare,” in *Advances in Fog Computing and the Internet of Things for Smart Healthcare*, J. B. Awotunde, A. K. Bhoi, P. Barsocchi, and V. H. C. de Albuquerque, Eds., Elsevier, 2026, pp. 425–450.
20. M. Haghi Kashani and S. Bazzaz Abkenar, “Chapter 23- Applications of fog computing for smart sensor network,” in *Sensor Networks for Smart Hospitals*, T. A. Nguyen, Ed., Elsevier, 2025, pp. 505–523.
21. M. Jeyaraman, S. Muniappan, and N. Jeyaraman, “Chapter 15 - Real world applications of fog computing and internet of things implementation in healthcare,” in *Advances in Fog Computing and the Internet of Things for Smart Healthcare*, J. B. Awotunde, A. K. Bhoi, P. Barsocchi, and V. H. C. de Albuquerque, Eds., Elsevier, 2026, pp. 313–326
22. A. Keshmiry and S. Hassani, “Chapter 20 - Enhancing efficiency in smart sensor networks: A comprehensive study on fog computing and internet of things (IoT) integration for throughput and latency optimization,” in *Fundamentals of Fog Computing and the Internet of Things for Smart Healthcare*, J. B. Awotunde, A. K. Bhoi, P. Barsocchi, and V. H. C. de Albuquerque, Eds., Elsevier, 2026, pp. 427–444