

Paper Type: Original Article

# Fog Computing in IoT-Driven Smart City Traffic Control Systems

Kumar Sambhav\* 

School of Computer Science Engineering, KIIT University, Bhubaneswar, India; 22052993@kiit.ac.in.

## Citation:

Received: 11 September 2024	Sambhav, K. (2025). Fog computing in IoT-driven smart city traffic control systems. <i>Smart internet of things</i> , 2(1), 35-43.
Revised: 18 November 2024	
Accepted: 13 Junury 2025	

## Abstract

This research investigates the utilization of AI-IoT optimization methods in waste management for smart cities. As urban populations increase, effective waste management becomes essential for ensuring cleanliness, public health, and environmental sustainability. The combination of Artificial Intelligence (AI) with the Internet of Things (IoT) offers innovative strategies for improving waste collection, sorting, and disposal. This paper reviews existing AI-IoT implementations, highlights challenges, and suggests solutions to enhance efficiency, lower costs, and promote sustainable urban development. This study aims to advance the understanding of sustainable waste management practices in smart cities.


**Keywords:** Fog computing, Internet of Things, Smart city, Traffic control, Real-time processing.


## 1 | Introduction

With the rapid increase in urban populations, cities face unprecedented challenges in traffic management. These challenges significantly impact the daily commutes of millions, the efficiency of emergency response services, and the overall sustainability of urban environments. Traditional traffic management systems often struggle to adapt dynamically to fluctuating traffic conditions, leading to increased congestion, higher fuel consumption, and a corresponding rise in greenhouse gas emissions.

IoT-enabled traffic control systems offer a promising solution by facilitating real-time traffic monitoring and adaptive management. By deploying IoT sensors, cameras, and other connected devices across key urban areas, these systems can collect and analyze vast amounts of data, such as vehicle speeds, congestion levels, and environmental conditions. When combined with predictive analytics and machine learning algorithms, IoT-driven systems can optimize traffic flows, adjust traffic signals in real-time, and even provide drivers with alternative routes based on live traffic updates.

 Corresponding Author: 22052993@kiit.ac.in

 <https://doi.org/10.48313/siot.v2i1.243>

 Licensee System Analytics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

However, most IoT implementations rely on cloud-centric architectures, which can introduce limitations, particularly latency and network congestion. The centralized nature of cloud computing means data from IoT devices must travel to and from remote servers, leading to delays that can compromise the effectiveness of real-time traffic management. Additionally, IoT sensors' high volume of data can congest networks, further slowing down response times [1].

Fog computing solves these challenges by decentralizing data processing and moving computation closer to IoT devices at the network's edge. In a fog computing architecture, data is processed on local nodes—such as routers or IoT gateways—reducing the need to send vast amounts of information to a distant cloud. This shift enables near-instantaneous responses, which is crucial for IoT-driven traffic management systems. By leveraging fog computing, cities can implement adaptive traffic control mechanisms, enhancing their ability to manage real-time traffic fluctuations, reduce congestion, and improve response times for emergency vehicles [2].

This combination of IoT and fog computing in traffic management improves urban mobility and contributes to environmental sustainability by reducing fuel consumption and lowering emissions. Integrating these advanced technologies will be essential to building resilient, efficient, and eco-friendly urban infrastructure as cities grow.

## 2 | Literature Review

Fog computing's applications in smart cities are diverse, covering critical aspects like air quality monitoring, energy management, and traffic control. By decentralizing data processing, fog computing brings computation closer to where data is generated, making it especially beneficial for time-sensitive urban applications that rely on IoT networks. This local processing capability enables faster responses, reduces bandwidth demands, and enhances IoT system performance, addressing various issues in modern cities [3].

In air quality monitoring, for example, IoT sensors can be deployed across the city to measure pollution levels, detect harmful gases, and monitor temperature and humidity. These sensors generate vast amounts of data that need quick processing to provide accurate, real-time air quality assessments to residents and city officials. By using fog computing, data from these sensors can be processed at the network's edge, ensuring that local communities receive timely alerts during pollution spikes and enabling quick action to mitigate environmental health risks.

Energy management in smart cities also benefits significantly from fog computing. Urban areas rely on complex, interconnected energy grids that balance supply and demand in real time. With IoT-enabled smart meters, energy-efficient lighting, and HVAC systems, cities can gather detailed data on energy usage patterns. Fog computing allows for localized data processing, helping cities make quicker adjustments to energy distribution, reduce power wastage, and improve energy efficiency without overburdening centralized cloud servers. This decentralized approach is essential during peak demand periods, where delays in data processing could lead to power outages or grid instability [4].

One of the most transformative applications of fog computing in smart cities is traffic control and management. Real-time responses are crucial in traffic systems to avoid congestion and improve road safety. With fog computing, traffic data from IoT sensors, cameras, and connected vehicles can be processed at the edge to manage traffic lights dynamically, predict congestion points, and reroute vehicles in real time. This ability to process and act on data locally minimizes cloud processing delays and helps streamline traffic flow, reduce emissions, and decrease travel times. Additionally, emergency routing systems can be enhanced with fog computing by providing near-instantaneous rerouting options for ambulances, fire trucks, and law enforcement vehicles, which can be lifesaving in critical situations.

Studies demonstrate that fog computing can enhance IoT performance by optimizing data flow, reducing latency, and improving system resilience—particularly important for applications demanding real-time responses. By distributing data processing across local nodes rather than relying on distant cloud servers,

cities can ensure that IoT-driven services such as air quality monitoring, energy management, and traffic control respond promptly to current conditions [5].

As smart cities continue to evolve, integrating fog computing with IoT infrastructure will be instrumental in meeting the complex demands of urban life. This approach enables faster, more efficient services and supports the broader goals of sustainability, safety, and livability in increasingly connected urban environments.

### 3 | Challenges in Implementing Fog Computing in Traffic Systems

Despite its numerous advantages, fog computing in smart cities also presents several challenges that must be addressed to realize its full potential. Key issues include data security, resource constraints, and interoperability, all of which impact fog-based systems' efficiency and reliability [6].

#### 3.1 | Data Security

Maintaining data security in fog computing, particularly within smart cities, is a critical challenge that requires careful attention and strategic planning. Fog computing processes sensitive information close to end devices, such as vehicle speeds, congestion levels, and personal navigation routes. This proximity increases the risk of unauthorized access and potential data breaches. The distributed nature of fog nodes makes them easier targets for attackers than centralized cloud systems, which typically have more robust security protocols and monitoring. Unlike cloud infrastructures, where security measures can be applied uniformly, fog nodes often operate autonomously and are geographically dispersed, complicating the implementation of effective security protocols.

The sensitive nature of the data processed in fog computing adds another layer of complexity. For example, traffic data can reveal individual movements and behaviors, while personal navigation data can expose users to privacy breaches if intercepted. Environmental monitoring data may provide insights into community dynamics that could be misused if compromised. Furthermore, fog nodes can be vulnerable to various attacks, including man-in-the-middle attacks, physical tampering, and insider threats. These risks underscore the importance of robust security measures in protecting sensitive information [7].

Compared to centralized cloud systems, fog computing faces unique challenges regarding security. Centralized systems can allocate significant resources to security, enabling comprehensive monitoring and advanced threat detection. They also benefit from standardized security protocols that reduce the risk of vulnerabilities. In contrast, many fog nodes are lightweight devices with limited computational power, which can restrict the implementation of complex security protocols and real-time monitoring solutions. Additionally, the diverse environments in which fog nodes operate complicate the standardization of security measures. In contrast, the dynamic nature of fog networks makes maintaining an updated security posture across the entire network difficult.

Addressing data security in fog computing requires a multifaceted approach. Implementing decentralized encryption standards at various levels—such as data in transit, data at rest, and data in use—ensures that sensitive information is protected from unauthorized access. Lightweight encryption algorithms designed for resource-constrained devices can help maintain performance while providing necessary security. Enhanced node authentication protocols, including multi-factor authentication and digital certificates, should be employed to verify the identity of devices connecting to fog nodes, preventing unauthorized access. Furthermore, establishing a protocol for regular software updates and patches is crucial for addressing vulnerabilities. Automated update mechanisms can ensure that all nodes receive timely updates without manual intervention, enhancing overall network security.

Intrusion detection and Prevention Systems (IDPS) can safeguard fog computing environments. These systems can monitor network traffic for unusual activity and respond to potential threats in real-time, providing localized monitoring while maintaining central oversight. Additionally, fostering a culture of

security awareness among stakeholders—such as city planners, IoT device manufacturers, and end-users—can significantly reduce the likelihood of human error leading to vulnerabilities.

### 3.2 | Resource Constraints

Another significant challenge of fog computing lies in resource limitations. While capable of local data processing, Fog nodes typically have constrained computational, storage, and power resources compared to centralized cloud servers. These constraints can limit the ability of fog nodes to handle large-scale data processing tasks, especially in dense urban areas where data from thousands of IoT devices must be managed simultaneously. For instance, processing data from numerous IoT sensors, cameras, and connected vehicles requires substantial computational power in traffic management. The limited capacity of fog nodes can lead to delays or even system overloads during peak usage periods, compromising the effectiveness of real-time applications such as adaptive traffic control or emergency routing. To overcome resource limitations, cities can implement load-balancing mechanisms, distribute tasks among multiple fog nodes, or use a hybrid fog-cloud approach, where fog nodes handle time-sensitive processing and offload complex, non-urgent tasks to the cloud [8].

### 3.3 | Interoperability

Interoperability poses a significant challenge for fog computing in smart cities, primarily due to the diverse array of Internet of Things (IoT) devices integrated into these environments. Smart city infrastructures often incorporate devices from various vendors, each with unique communication protocols, data formats, and standards. This fragmentation complicates ensuring compatibility between the fog infrastructure and the many devices it supports. Achieving seamless integration is crucial, as it enables the effective exchange of information and the realization of a cohesive operational framework across the smart city landscape [9].

For example, in traffic management systems, integrating data from various sources, such as sensors, cameras, and connected vehicles, is essential for providing a real-time view of road conditions. This data can be used to optimize traffic flow, enhance safety, and improve urban mobility. However, device protocol and architecture differences can lead to significant integration difficulties. Without a unified approach, organizations may face the challenge of data silos, where information remains isolated within individual systems and cannot be utilized effectively across the network. In many cases, additional middleware may be required to facilitate communication between incompatible devices, adding complexity and potentially introducing latency into the system.

Furthermore, the rapid pace of technological advancement in the IoT space exacerbates the interoperability challenge. As new devices are continually developed and introduced into the ecosystem, ensuring they can seamlessly integrate with existing systems becomes increasingly difficult. This dynamic environment can lead to outdated protocols or systems that struggle to accommodate new technologies, further complicating the interoperability landscape. Moreover, vendors may prioritize their proprietary technologies, resulting in a fragmented ecosystem that hinders the potential benefits of fog computing.

Concerted standardization efforts are essential at both the industry and governmental levels to address these interoperability challenges. Collaborative initiatives involving stakeholders from various sectors can establish common communication protocols and data formats that promote device compatibility. For example, adopting open standards can significantly enhance interoperability by allowing diverse IoT devices to operate harmoniously within a fog network. These standards can provide a framework for device communication, enabling data sharing and collaboration across different systems without extensive middleware.

In addition to standardization, fostering collaboration among device manufacturers, software developers, and city planners is crucial. Engaging in dialogue and partnerships can facilitate sharing best practices and insights, leading to innovative solutions that enhance interoperability. Moreover, developing certification programs for IoT devices can help ensure that products meet established interoperability standards, giving consumers confidence in their compatibility within smart city environments.

Moreover, leveraging emerging technologies such as Artificial Intelligence (AI) and Machine Learning (ML) can enhance interoperability. These technologies can analyze and process data from diverse sources, identifying patterns and relationships that may not be immediately apparent. By implementing AI-driven solutions, smart city operators can enhance their ability to integrate data from various IoT devices, leading to more informed decision-making and improved urban services.

### 3.4 | Addressing the Challenges

Addressing the challenges posed by fog computing in smart cities necessitates a multi-faceted approach that encompasses various strategies tailored to specific issues such as data security, resource constraints, and interoperability. Each challenge requires targeted solutions to ensure that fog computing can function effectively and contribute meaningfully to urban environments [10].

**\*\*For data security\*\***, cities can implement a combination of edge security measures that focus on protecting sensitive information at the source where data is generated. This can include local encryption techniques, which ensure that data is encrypted before it even leaves the device, thus reducing the risk of unauthorized access during transmission. Additionally, identity-based authentication can strengthen access control, ensuring only verified devices and users can interact with the fog nodes. Regular security updates across all fog nodes are critical; these updates can patch vulnerabilities, enhance security protocols, and keep the system resilient against emerging threats. By creating a proactive security posture, cities can better safeguard the vast amounts of sensitive data processed in fog environments.

**\*\*Managing resource constraints\*\*** presents another significant challenge that requires strategic planning and innovative solutions. Cities can adopt more efficient processing algorithms designed to optimize the use of computational resources at the edge. Techniques such as workload distribution can help balance the load across multiple fog nodes, ensuring that no single node becomes a bottleneck. This involves dynamically allocating tasks based on each node's capabilities and current workload, which can enhance overall system performance. Furthermore, integrating hybrid cloud-fog architectures can provide a flexible framework where data processing can occur either on the fog nodes or in the centralized cloud, depending on the requirements of specific applications. This hybrid approach allows for better resource management while leveraging the strengths of both cloud and fog computing.

**\*\*Interoperability\*\*** is another crucial area requiring focused efforts to enable seamless communication among the diverse IoT devices deployed in smart cities. Establishing industry-wide standards and encouraging government regulation can play a pivotal role in promoting compatibility among different systems. By advocating for developing open-source protocols tailored for IoT devices, cities can ensure that devices from various manufacturers can operate harmoniously within the fog network. Open standards facilitate integration and foster innovation, as developers can build applications that leverage a wide range of devices and data sources without being restricted by proprietary technologies.

As fog computing technology evolves, ongoing efforts to overcome these challenges will be crucial for enabling secure, efficient, and scalable IoT-driven applications. Collaboration among city planners, technology providers, and regulatory bodies will be essential in creating a conducive environment for the growth of fog computing solutions. By sharing knowledge and best practices, stakeholders can better address the unique challenges of their local contexts while contributing to the broader advancement of smart city initiatives.

Successfully tackling these issues will unlock the potential of fog computing to enhance urban living. By delivering faster, smarter, and more sustainable services across smart cities, fog computing can play a transformative role in improving the quality of life for residents. Enhanced traffic management systems, more efficient waste collection, and responsive energy management are examples of how fog computing can contribute to smarter urban environments. Ultimately, the ability to harness the power of fog computing will not only support the development of innovative applications but also lay the foundation for resilient, adaptable, and thriving smart cities in the future.



## 4| Limitations of Fog Computing for Smart City Traffic

While fog computing offers clear benefits for traffic management systems, it also has limitations that can impact the performance and reliability of real-time traffic management. Two significant challenges include dependency on specific hardware and the potential for fog node overload, which can affect data processing and decision-making accuracy and responsiveness [11].

### 4.1| Hardware Dependency

To enable edge data processing, fog computing in traffic systems often relies on specialized hardware, such as local routers, switches, and IoT gateways. This dependency on specific hardware can limit the flexibility and scalability of fog-based systems. Traffic management applications require consistent, reliable processing power to handle the high volumes of data generated by sensors, cameras, and other connected devices monitoring real-time traffic conditions. However, fog nodes have finite processing and storage capacities, and replacing or upgrading this hardware can be challenging due to compatibility and cost constraints.

Additionally, hardware failure at key fog nodes can disrupt the entire system. For instance, if a node responsible for processing traffic data in a high-traffic area experiences a malfunction, it could lead to delays in data processing, ineffective traffic light control, and an increased risk of congestion. To mitigate these issues, traffic management systems need redundancy strategies, such as backup fog nodes or hybrid architectures that offload some processing to cloud servers when hardware fails. Investing in robust, scalable, and easily upgradable hardware is also essential to ensure that traffic systems can adapt to changes in data volume and demand over time.

### 4.2| Fog Node Overload

Fog node overload is another major limitation in traffic systems, particularly in densely populated urban areas where IoT devices continuously generate vast amounts of data. Each fog node has limited computational capacity, and during peak times—such as rush hours or special events—these nodes may struggle to process all incoming data in real-time. Overloaded fog nodes can delay data processing, compromising the system's ability to manage traffic flows, adjust traffic lights, or reroute vehicles promptly. These delays can have significant consequences in critical situations, such as emergency vehicle routing.

Overloaded fog nodes may also lead to inaccuracies in decision-making. When nodes are overburdened, data might be processed in batches or prioritized based on urgency, potentially resulting in missed or delayed information updates. This prioritization could mean less critical data, such as minor congestion in low-priority areas, might be overlooked, leading to unexpected bottlenecks. To alleviate overload, traffic management systems can implement load-balancing algorithms that distribute tasks among multiple nodes and offload non-urgent processing to the cloud, allowing nodes to focus on real-time critical data.

### 4.3| Addressing the Limitations

To address hardware dependency and fog node overload, cities can adopt a hybrid approach combining fog and cloud computing. In such a setup, fog nodes handle high-priority, real-time data, while more intensive or time-insensitive tasks are offloaded to centralized cloud servers. This hybrid model ensures that the fog nodes focus on immediate traffic control needs while the cloud processes predictive analytics or historical data analysis, reducing the risk of overload.

Regular hardware upgrades and scalable, modular fog nodes can also address hardware dependency, allowing traffic systems to accommodate increased data volumes and process power-intensive tasks. Implementing predictive load management algorithms can further optimize data distribution across fog nodes, reducing the likelihood of overload during peak times.

## 5 | Proposed Improvements

To enhance the effectiveness and reliability of fog computing in smart city traffic systems, several strategies can be implemented to address key challenges related to data security, resource management, and interoperability. By strengthening these areas, cities can improve their traffic management systems' responsiveness, security, and scalability.

### Enhanced security protocols

Security is paramount in fog computing, especially given the sensitivity of traffic data and the need to protect against cyber threats. End-to-end encryption ensures that data remains protected from unauthorized access as it travels from IoT devices to fog nodes and other connected systems. This encryption minimizes the risk of data tampering and interception by securing communication channels. Additionally, real-time threat detection systems—enabled by AI-driven monitoring tools—can analyze network traffic patterns to identify potential security breaches or anomalies. By detecting threats as they occur, these systems can quickly isolate compromised nodes, prevent the spread of malware, and ensure that critical traffic data remains uncompromised. Implementing enhanced security protocols across all fog nodes builds a more robust, resilient traffic management system and increases public trust in smart city technologies [12].

### Adaptive load balancing

Adaptive load balancing is crucial for preventing fog node overload, especially in high-density urban areas where traffic management systems generate substantial data during peak hours. By optimizing the distribution of tasks across multiple fog nodes, adaptive load balancing reduces the risk of system bottlenecks and ensures that all nodes operate within their capacity limits. This can be achieved using dynamic load-balancing algorithms that continuously monitor node workloads and redistribute tasks based on current traffic levels, processing demands, and available resources. When the network experiences peak load, less time-sensitive tasks can be delayed or sent to cloud servers, allowing fog nodes to focus on real-time critical data processing. This dynamic approach to load balancing enhances the system's ability to respond efficiently to fluctuating data volumes, ultimately improving the accuracy and timeliness of traffic-related decision-making.

### Standardized protocols for interoperability

Interoperability is essential for seamless communication between IoT devices and fog infrastructure, given the wide variety of devices and protocols used in smart city traffic systems. Establishing standardized communication protocols for IoT and fog computing can greatly enhance system interoperability, allowing devices from different manufacturers to communicate effectively. Standardized protocols, such as the Message Queuing Telemetry Transport (MQTT) and Constrained Application Protocol (CoAP), facilitate efficient data exchange, reduce integration complexity, and promote compatibility across different components. Standardization efforts can also extend to data formats, ensuring that traffic data from various sources can be aggregated and processed without requiring extensive data transformation. Adopting these standards enhances the scalability of fog-enabled traffic systems, reduces integration costs, and simplifies the incorporation of new devices as cities expand their smart infrastructure.

### Additional enhancements

In addition to these core strategies, further improvements can be made to optimize fog computing in traffic systems:

- I. Predictive analytics: leveraging predictive models to analyze historical and real-time data can help fog nodes anticipate traffic patterns and proactively manage congestion.
- II. Edge AI integration: embedding AI capabilities at the edge allows fog nodes to make autonomous decisions, such as rerouting traffic or adjusting signal timings, without relying on centralized processing.
- III. Redundancy and failover mechanisms: incorporating backup nodes and failover systems can enhance reliability, ensuring uninterrupted service even if some fog nodes go offline.

## 6 | Conclusion

Fog computing plays a transformative role in IoT-driven traffic control within smart cities by addressing critical challenges such as latency and bandwidth limitations. Unlike traditional cloud-centric architectures, fog computing brings data processing closer to IoT devices, enabling near-instantaneous analysis and decision-making. This local processing capability is essential for real-time traffic management applications that require quick response times, such as dynamic traffic light adjustments, congestion prediction, and emergency vehicle routing. By reducing the need to send large volumes of data to distant cloud servers, fog computing mitigates network congestion and bandwidth constraints, leading to faster, more efficient traffic control.

Our study explores the advantages and limitations of integrating fog computing into urban traffic systems, aiming to offer a balanced perspective on its application in smart cities. Key benefits include reduced latency, enhanced system scalability, and the ability to handle high-frequency data generated by numerous IoT devices. Fog nodes, deployed at strategic locations throughout the city, allow traffic management systems to adapt rapidly to real-time traffic fluctuations, improving traffic flow and reducing congestion. This decentralized architecture also enables a more scalable approach to traffic control, as fog nodes can be added or upgraded to support growing urban populations and increased IoT data volumes.

However, our study also highlights some limitations of fog-based traffic control systems. These include dependency on specific hardware, which can affect system flexibility and increase maintenance costs, and potential fog node overload during peak traffic times, which may compromise the system's real-time responsiveness. Security is another critical concern, as fog nodes are distributed across urban environments and may be vulnerable to unauthorized access. Ensuring secure data transmission and device authentication is essential to maintaining the integrity and privacy of traffic data. Interoperability is an additional challenge, as smart city infrastructure typically consists of IoT devices from multiple vendors, making seamless data integration complex without standardized protocols.

These findings offer a foundational perspective on integrating fog computing in urban traffic management, providing valuable insights for future research in smart city development. Further studies can build on this work by exploring advanced load-balancing techniques, developing more resilient security protocols, and establishing open standards to enhance interoperability among diverse IoT devices. Additionally, investigating AI-driven predictive analytics at the edge can further optimize fog computing's role in traffic systems, enabling more proactive and adaptive traffic control.

Our study thus lays the groundwork for continued exploration of fog computing in smart cities, emphasizing its potential to create responsive, efficient, and sustainable urban traffic management systems. By addressing both the benefits and challenges, this research contributes to developing robust frameworks that can guide the deployment of fog-enabled IoT solutions in cities worldwide, ultimately advancing the vision of smarter, safer, and more resilient urban environments.

## Acknowledgment

The author gratefully acknowledges the support provided by KIIT University, which has been instrumental in facilitating this research. The resources and encouragement from the university have significantly contributed to the development and execution of this study on fog computing in smart city traffic systems. Additionally, the author extends heartfelt thanks to the faculty and mentors from the School of Computer Science Engineering, whose guidance, expertise, and insights have been invaluable throughout the research process. Their constructive feedback and encouragement have enriched this study, helping shape its findings and conclusions and laying a solid foundation for future research.



## Author Contributions

Aditya Tulsyan: Conceptualization of the study, data analysis, methodology development, software integration, and manuscript preparation. The author has read and approved the published version of the manuscript.

## Funding

This research received no external funding.

## Data Availability

Data supporting the findings can be made available upon request from the corresponding author.

## Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

## References

- [1] Mohapatra, H., & Rath, A. K. (2020). Survey on fault tolerance-based clustering evolution in WSN. *IET networks*, 9(4), 145–155. <https://doi.org/10.1049/iet-net.2019.0155>
- [2] Mohapatra, H., & Rath, A. K. (2019). Detection and avoidance of water loss through municipality taps in India by using smart taps and ICT. *IET wireless sensor systems*, 9(6), 447–457. <https://doi.org/10.1049/iet-wss.2019.0081>
- [3] Rehan, H. (2023). Internet of Things (IoT) in smart cities: Enhancing urban living through technology. *Journal of engineering and technology*, 5(1), 1–16. <https://www.researchgate.net>
- [4] Tang, B., Chen, Z., Hefferman, G., Pei, S., Wei, T., He, H., & Yang, Q. (2017). Incorporating intelligence in fog computing for big data analysis in smart cities. *IEEE transactions on industrial informatics*, 13(5), 2140–2150. <https://doi.org/10.1109/TII.2017.2679740>
- [5] Li, X., Liu, Y., Ji, H., Zhang, H., & Leung, V. C. M. (2019). Optimizing resources allocation for fog computing-based Internet of Things networks. *IEEE access*, 7, 64907–64922. <https://doi.org/10.1109/ACCESS.2019.2917557>
- [6] Bouzarkouna, I., Sahnoun, M. H., Sghaier, N., Baudry, D., & Gout, C. (2018). Challenges facing the industrial implementation of fog computing. In *2018 IEEE 6th international conference on future internet of things and cloud (FiCloud)* (pp. 341–348). IEEE. <https://doi.org/10.1109/FiCloud.2018.00056>
- [7] Miracle, N. O. (2024). The importance of network security in protecting sensitive data and information. *International journal of research and innovation in applied science*, 9(6), 259–270. [https://www.academia.edu/download/116668702/THE\\_IMPORTANCE\\_OF\\_NETWORK\\_SECURITY\\_IN\\_PROTECTING\\_SENSITIVE\\_DATA\\_AND\\_INFORMATION.pdf](https://www.academia.edu/download/116668702/THE_IMPORTANCE_OF_NETWORK_SECURITY_IN_PROTECTING_SENSITIVE_DATA_AND_INFORMATION.pdf)
- [8] Hong, C. H., & Varghese, B. (2019). Resource management in fog/edge computing: a survey on architectures, infrastructure, and algorithms. *ACM computing surveys (csur)*, 52(5), 1–37. <https://doi.org/10.1145/3326066>
- [9] Huaranga-Junco, E., González-Gerpe, S., Castillo-Cara, M., Cimmino, A., & García-Castro, R. (2024). From cloud and fog computing to federated-fog computing: a comparative analysis of computational resources in real-time IoT applications based on semantic interoperability. *Future Generation Computer Systems*, 159, 134–150. <https://doi.org/10.1016/j.future.2024.05.001>
- [10] Ni, J., Zhang, K., Lin, X., & Shen, X. (2017). Securing fog computing for internet of things applications: Challenges and solutions. *IEEE communications surveys & tutorials*, 20(1), 601–628. <https://doi.org/10.1109/COMST.2017.2762345>
- [11] Ning, Z., Huang, J., & Wang, X. (2019). Vehicular fog computing: enabling real-time traffic management for smart cities. *IEEE wireless communications*, 26(1), 87–93. <https://doi.org/10.1109/MWC.2019.1700441>
- [12] Haseeb, K., Saba, T., Rehman, A., Ahmed, Z., Song, H. H., & Wang, H. H. (2022). Trust management with fault-tolerant supervised routing for smart cities using internet of things. *IEEE internet of things journal*, 9(22), 22608–22617. <https://doi.org/10.1109/JIOT.2022.3184632>