Smart City Insights

www.sci.reapress.com

Smart City Ins. Vol. 2, No. 4 (2025) 214–222.

Paper Type: Original Article

Secure and Scalable Edge Computing Framework for IoT-Enabled Urban Mobility Systems

Javad Pourqasem[1,*], **Mingyue Wang**[2]

[1] Morvarid Intelligent Industrial Systems Research Group, Iran; jpourmail@gmail.com.

[2] School of Computer and Information, Lanzhou University of Technology, China; wang.mingyue9811@gmail.com.

Citation:

Received: 20 February 2025 *Revised: 03 May 2025* *Accepted: 20 June 2025*	Pourqasem, J., & Wang, M. (2025). Secure and scalable edge computing framework for IoT-enabled urban mobility systems. *Smart city insights, 2*(4), 214-222.

Abstract

The demand for efficient urban mobility systems has increased interest in distributed Internet of Things (IoT) applications. Edge computing is a pivotal solution that processes data closer to IoT devices, optimizes real-time responses, and reduces dependency on centralized servers. This paper explores the role of edge computing in urban mobility solutions, focusing on traffic flow optimization, Vehicle-to-Vehicle (V2V) communication, and load distribution among IoT devices. Using edge nodes for decentralized processing enables faster decision-making and reduces network congestion in smart cities. We evaluate the benefits and challenges of edge computing in IoT-based mobility systems and propose frameworks to enhance system scalability and reliability. Our findings reveal that edge computing supports real-time data processing, cost-efficient operations, and scalable urban mobility solutions for future smart cities.

Keywords: Edge computing, Internet of things, Urban mobility, Decentralized processing, Smart city.

1 | Introduction

The surge in urban populations has increased pressure on traditional transportation infrastructures, resulting in widespread traffic congestion, elevated pollution levels, and extended travel times. These challenges demand innovative, data-driven solutions for urban mobility management that operate in real time to alleviate congestion and improve the commuter experience. The rise of the Internet of Things (IoT) has provided a powerful platform for gathering and analyzing data on urban mobility patterns, creating new opportunities for more effective, efficient traffic management systems.

Corresponding Author: jpourmail@gmail.com

https://doi.org/10.22105/sci.v2i4.51

However, centralized cloud-based approaches to processing this vast amount of data often struggle with latency, bandwidth, and privacy issues, making them less than ideal for real-time applications. Edge computing, which processes data locally at or near the data source, has emerged as a viable alternative. By minimizing latency, reducing reliance on the cloud, and enabling localized decision-making, edge computing delivers the speed and flexibility needed for real-time urban mobility solutions. This paper explores the role of edge computing in enhancing IoT-based urban mobility systems, focusing on traffic optimization, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications, and dynamic load balancing [1].

1.1 | The Importance of Edge Computing in Urban Mobility

Edge computing brings computational power closer to IoT devices, enabling faster data processing and direct decision-making at the source. This distributed approach is crucial for real-time applications in urban mobility, such as:

I. Traffic signal management: edge-enabled systems can dynamically adjust traffic light timings based on real-time data analysis, significantly reducing traffic congestion and enhancing traffic flow efficiency.

II. Autonomous vehicle guidance: by processing data locally, edge nodes facilitate real-time updates for autonomous vehicles, enabling them to respond quickly to road conditions, accidents, and unexpected obstacles.

III. Emergency response routing: edge computing enables rapid data processing and optimized rerouting of emergency vehicles, improving response times and enabling efficient navigation through high-traffic areas.

IV. Public transport optimization: edge devices deployed at stations or within vehicles can monitor real-time demand and adjust service schedules accordingly, providing a more responsive and efficient public transportation system [2].

2 | Literature Review

Edge computing is increasingly recognized as a transformative technology within urban mobility, particularly when integrated with IoT to enable rapid, decentralized data processing. Integrating IoT-based edge computing solutions into urban mobility has attracted significant academic and industry interest, given their potential to address urban traffic congestion, reduce latency, enhance data privacy, and reduce reliance on the cloud. This section reviews the theoretical foundations, practical applications, and challenges associated with edge computing in urban mobility, drawing on recent research across three primary areas: latency reduction and real-time decision-making, Vehicle-to-Everything (V2X) communication, and scalability and load distribution.

2.1 | Edge Computing for Real-time Decision-Making and Latency Reduction

Real-time data processing is central to effective urban mobility management, as delays in decision-making can lead to increased congestion, reduced safety, and suboptimal commuter experiences. Traditional cloud-based IoT frameworks struggle with latency issues due to their reliance on centralized data processing. Edge computing, by contrast, brings processing power closer to data sources—such as traffic sensors, autonomous vehicles, and smart traffic lights—allowing for near-instantaneous data analysis and response [3].

2.2 | Vehicle-to-Everything Communication and Edge Computing

V2X communication, encompassing V2V and V2I interactions, is vital to smart urban mobility ecosystems. V2X communication enables vehicles and roadside infrastructure to share real-time data, facilitating coordinated responses to road conditions, traffic signals, and potential hazards. Traditional V2X systems, however, face latency and bandwidth issues when data is routed through a central cloud. Edge computing offers an alternative by localizing these communication exchanges, improving response times, and reducing data transfer requirements.

V2X-enabled edge nodes can significantly enhance urban mobility by locally processing data from vehicles and infrastructure. For example, when multiple vehicles approach an intersection, edge nodes can coordinate with traffic lights and surrounding vehicles to optimize traffic flow, minimizing the risk of congestion and collisions. Similarly, edge nodes placed at key junctions in urban areas can aggregate data from nearby vehicles and infrastructure, allowing for localized decision-making that would otherwise be delayed by centralized processing [4].

2.3 | Scalability and Load Balancing in Edge Computing for Urban Mobility

Scalability is essential in urban mobility systems, where data volumes can vary significantly depending on traffic density, time of day, and specific urban areas. Edge computing enhances scalability by enabling load balancing and distributing tasks across multiple nodes. Load balancing is particularly valuable in urban environments, where infrastructure must adapt to fluctuations in data flow to maintain service continuity and efficiency.

Several studies highlight the role of edge computing in managing scalability challenges for urban mobility. Mao et al. [5] explored edge computing's load-balancing mechanisms, which redistribute workloads across nodes based on network conditions and availability. Their research demonstrated that when implemented in a distributed network, edge nodes reduce system bottlenecks and prevent overload in high-traffic scenarios. It is especially pertinent in urban mobility, where data surges during peak hours can overwhelm traditional centralized systems.

2.4 | Data Privacy, Security, and Reliability in Edge-Based Urban Mobility Systems

The implementation of edge computing in urban mobility systems also brings data privacy and security challenges, as edge nodes process sensitive data on location, vehicle routes, and commuter behaviors. Edge computing's distributed nature requires robust security measures to protect against data breaches, unauthorized access, and cyberattacks, as these can have severe implications for urban mobility and user privacy.

2.5 | Integration of Machine Learning and AI in Edge Computing for Mobility

Machine Learning (ML) and Artificial Intelligence (AI) are increasingly integrated into edge computing frameworks to improve decision-making capabilities in urban mobility applications. By embedding ML algorithms into edge nodes, systems can perform predictive analysis and adapt to changing conditions in real time, enhancing the overall functionality and efficiency of urban mobility solutions.

More recent studies, such as that by Yan et al. [6] , investigated the use of deep learning algorithms at the edge to enhance real-time analytics for complex urban mobility scenarios. Yan's research highlighted the ability of deep learning models to process large datasets locally, enabling edge nodes to provide insights on traffic density, accident probabilities, and optimal routing. This localized intelligence is particularly beneficial in urban mobility, where dynamic, real-time insights are essential for maintaining safe and efficient transportation networks [6].

3 | Challenges in Implementing Edge Computing for Mobility Solutions

Edge computing has emerged as a transformative technology capable of meeting the rising demands of IoT-enabled mobility systems in smart cities. By processing data closer to its source, edge computing minimizes latency, enhances responsiveness, and supports time-sensitive applications such as traffic control, emergency routing, and autonomous vehicles.

However, despite these benefits, implementing edge computing in large-scale mobility systems introduces multiple technical and operational challenges. These challenges include data privacy and security risks, high infrastructure costs, device heterogeneity and interoperability issues, scalability constraints, network reliability concerns, and the need for skilled personnel to manage complex distributed systems.

3.1 | Data Privacy and Security

Data privacy and security remain the most critical challenges in deploying edge-based mobility solutions. Edge nodes collect and process vast amounts of sensitive data, including real-time location information, vehicle identifiers, and commuter behavior patterns. Because edge devices are often installed in public environments—such as intersections, streetlights, or transport hubs—they are inherently more exposed to physical tampering and cyber threats [7].

Robust, multi-layered security mechanisms are essential. These include strong encryption, authentication, and Intrusion Detection Systems (IDS) capable of operating on resource-limited devices. However, heterogeneous hardware capabilities can lead to inconsistent protection levels across nodes, creating potential vulnerabilities. Implementing adaptive, real-time security frameworks—such as AI-driven intrusion detection or federated learning-based anomaly monitoring—can mitigate risks but also increase complexity and cost [8], [9].

3.2 | Infrastructure and Deployment Costs

Deploying a reliable edge computing infrastructure requires substantial capital investment. Edge nodes must be strategically distributed across the city to minimize latency while maintaining secure and stable connectivity. Each node demands durable, weather-resistant hardware, backup power, and constant network availability [10].

Beyond initial setup, operational costs remain significant, including maintenance, periodic hardware upgrades, and software updates to ensure optimal performance. For developing regions or municipalities with limited budgets, achieving a favorable Return on Investment (ROI) within a reasonable timeframe can be challenging. The economic sustainability of large-scale edge deployment thus depends on careful cost–benefit assessment and incremental rollouts aligned with urban priorities [11].

3.3 | Device Heterogeneity and Interoperability

Smart city ecosystems integrate a diverse range of IoT devices, sensors, and communication protocols, leading to significant interoperability challenges. Variations in vendor standards, data formats, and communication protocols can obstruct seamless data exchange across devices.

Effective mobility applications—such as adaptive traffic control and connected vehicle coordination—require synchronized data sharing between heterogeneous components. To achieve this, developing standardized APIs, adopting open-source middleware, and implementing cross-platform communication frameworks (e.g., MQTT, CoAP, or oneM2M) are critical. Without standardization, integrating new devices into existing networks becomes costly and technically cumbersome, limiting scalability and long-term adaptability [10], [12].

3.4 | Scalability and Network Reliability

Edge-based urban mobility systems must dynamically adjust to varying data loads caused by changes in traffic density, time of day, or emergencies. Unlike cloud systems that scale through centralized resource pooling, edge architectures rely on distributed and resource-constrained nodes. Maintaining consistent performance under fluctuating demand, therefore, requires intelligent load-balancing and task offloading mechanisms [13], [14].

Scalability also depends on network reliability. Urban wireless networks are frequently disrupted by congestion, signal interference, and hardware failures. Ensuring high availability demands redundant edge nodes, predictive maintenance, and self-healing network capabilities driven by AI algorithms. These strategies improve fault tolerance but add design complexity and operational overhead [10].

3.5 | Human Expertise and Operational Complexity

Managing large, distributed edge infrastructures requires skilled personnel capable of configuring, monitoring, and troubleshooting real-time systems. The integration of networking, AI, and cybersecurity expertise is rare and often expensive. Inadequate human capacity can lead to misconfigured systems, downtime, or inefficient use of edge resources. Establishing dedicated training programs and automated orchestration tools (e.g., Kubernetes for edge clusters) can help alleviate this limitation [15].

4 | Proposed Improvements

To address the unique challenges of edge computing in urban mobility, implementing robust security protocols is crucial to protecting sensitive data's privacy, security, and reliability. Data protection becomes paramount as urban mobility systems collect extensive information—from user data to vehicle locations and traffic patterns. Since this data often traverses various nodes, it is especially susceptible to cyber threats. Enhancing security at the edge node level by implementing encryption, Multi-Factor Authentication (MFA), IDS, and routine security audits can significantly improve data security and minimize potential risks.

4.1 | Utilizing Advanced Encryption

One of the cornerstones of data security in urban mobility is encryption, as it renders data inaccessible to unauthorized entities. Advanced encryption methods such as Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA) are essential in safeguarding data in transit and at rest.

AES encryption: AES is a symmetric encryption algorithm widely recognized for its strength and speed. When data is encrypted with AES, the same key is used for both encryption and decryption, making it suitable for real-time data transfer within urban mobility systems. It's known for its high resistance to brute-force attacks. It is particularly useful in securing edge nodes that process continuous data streams from sensors and IoT devices in smart cities. AES's security ensures that the information remains unintelligible without the decryption key, even if a data packet is intercepted [16], [17].

RSA encryption: RSA, an asymmetric encryption method, uses a pair of keys: a public key for encryption and a private key for decryption. It adds a layer of security by ensuring that only the intended recipient, who holds the private key, can access the data. RSA is especially beneficial for applications that require secure data exchange over networks, such as V2V and V2I communication within urban mobility systems. RSA helps prevent unauthorized access to sensitive data exchanged between vehicles and infrastructure [18].

End-to-End Encryption (E2EE): beyond AES and RSA, End-to-End Encryption (E2EE) is crucial for ensuring that data remains secure throughout its journey from source to destination. E2EE protects data from being read by intermediaries within the network, ensuring that only the communicating parties can access the data. It added that a level of security is vital for urban mobility systems, as it provides strong data protection even if the communication network itself is compromised [19], [20].

4.2 | Multi-Factor Authentication

MFA is another critical security measure in safeguarding access to urban mobility systems. MFA requires users to verify their identity using multiple verification factors, typically combining something they know (e.g., a password), something they have (e.g., a mobile device), and something they are (e.g., biometric data).

Passwords and One-Time Passwords (OTPs): traditional methods like passwords are typically combined with One-Time Passwords (OTPs) sent via SMS or email to add an extra layer of protection. OTPs are unique codes generated for each login attempt, making it difficult for attackers to use stolen credentials to gain access [22], [22].

Biometric verification: In addition to OTPs, MFA can include biometric verification, such as fingerprint or facial recognition. Biometric data provides a high level of security because it's nearly impossible for attackers to replicate or steal. It is particularly useful in urban mobility systems where rapid, secure access to data is critical, such as in public transportation apps or real-time traffic monitoring platforms.

Implementing MFA significantly reduces the risk of unauthorized access to sensitive urban mobility systems. By ensuring that only authenticated users can access specific systems or data, MFA can help protect against unauthorized tampering with data, which could otherwise lead to compromised traffic patterns, faulty navigation systems, and data breaches affecting both users and service providers [23], [24].

4.3 | Intrusion Detection Systems

In edge computing, each edge node is a potential vulnerability point. IDS are essential for proactively managing security threats. IDS technology is designed to monitor network traffic continuously and detect suspicious activities or anomalies that may indicate a potential security breach.

Machine learning in IDS: One of the more advanced forms of IDS uses ML algorithms to identify unusual patterns that may signify an intrusion attempt. By learning from historical data, these algorithms become better at identifying potential threats, even those that deviate only slightly from regular traffic patterns. In urban mobility, where the volume and variety of data are substantial, ML-based IDS can adapt to the dynamics of traffic data, detecting even subtle irregularities that could indicate a breach [16], [25].

Real-time threat detection and response: the real-time nature of IDS is essential for urban mobility systems, enabling immediate responses to security threats. For example, if an IDS detects an anomaly in data traffic at an edge node, it can initiate automated responses, such as alerting system administrators or isolating the compromised node. This real-time reaction helps prevent the attack's spread, limiting the network's potential damage [9], [26].

4.4 | Regular Security Audits and Updates

While implementing strong security protocols is critical, maintaining them is equally important. Regular security audits and updates ensure that the urban mobility edge computing system remains resilient against evolving cyber threats [27], [28].

Conducting security audits: systematically examining systems to identify and address vulnerabilities. These audits cover both software and hardware components and can identify gaps in current security measures. By conducting regular audits, urban mobility systems can identify potential weaknesses before attackers exploit them. Security audits also allow organizations to assess the effectiveness of existing protocols and make improvements as needed [9], [29].

Security patches and updates: It is vital to regularly update all software and hardware components with the latest security patches. Cybercriminals often exploit known vulnerabilities in outdated software or firmware. By staying up to date, urban mobility systems can prevent attackers from using well-known tactics to infiltrate them. For example, operating systems, firmware on IoT devices, and applications require frequent updates to address security loopholes. Additionally, when new threats emerge, developers often release patches designed to counter them, ensuring that systems remain protected.

Zero-day vulnerability response: urban mobility systems are exposed to zero-day vulnerabilities, in which cyber threats target unknown or unpatched weaknesses. By monitoring industry trends and participating in

cybersecurity networks, urban mobility providers can quickly stay aware of emerging threats and apply necessary countermeasures [9], [30].

5 | Conclusion

Edge computing represents a transformative approach for IoT-driven urban mobility systems, fundamentally reshaping how cities manage transportation and mobility services. By processing data closer to the source, edge computing significantly reduces latency, enhances real-time responsiveness, and enables scalable, decentralized processing. These advantages are particularly pertinent in applications that demand rapid data processing, such as traffic management, autonomous vehicle routing, and public transport optimization.

Analyzing vast amounts of data in real-time is crucial for urban mobility systems that rely on timely decision-making. For instance, edge computing can enable traffic management systems to dynamically adjust traffic signals based on current congestion levels, thereby optimizing traffic flow and reducing travel times. Similarly, autonomous vehicles benefit from low-latency data processing, allowing them to make quick decisions in response to their immediate environment, enhancing safety and efficiency.

Furthermore, the decentralized nature of edge computing empowers cities to scale their mobility solutions more effectively. As urban populations grow and the number of IoT devices increases, the ability to distribute processing tasks across multiple edge nodes alleviates the burden on central cloud infrastructures. This decentralization improves performance and facilitates the integration of new technologies, making urban mobility systems more adaptable to changing demands.

However, several challenges must be addressed to maximize the effectiveness of edge computing in urban mobility. Security concerns are paramount, as edge nodes can become targets of cyberattacks. Ensuring robust security protocols and the monitoring of these devices is essential to protecting sensitive data and maintaining public trust in urban mobility solutions. Additionally, scalability and infrastructure challenges need to be addressed to ensure cities can effectively deploy edge computing technologies. Investments in connectivity, power supply, and interoperable systems are crucial to creating a resilient urban mobility ecosystem.

In summary, this paper highlights the potential and limitations of edge computing for urban mobility. As cities strive to become smarter and more efficient, understanding the implications of edge computing will be vital for future research and development in smart city technologies. By leveraging the advantages of edge computing while proactively addressing its challenges, urban areas can create more responsive, secure, and efficient mobility systems that meet the needs of their inhabitants.

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] Raj, M. (In Peess). IoT-based urban mobility solutions for traffic congestion. *Computational engineering and technology innovations*. https://doi.org/10.48314/ceti.vi.44

[2] Sood, S. K. (2021). Smart vehicular traffic management: An edge cloud centric IoT based framework. *Internet of things*, *14*, 100140. https://doi.org/10.1016/j.iot.2019.100140

[3] Abdullah, M. F. A., Yogarayan, S., Razak, S. F. A., Azman, A., Amin, A. H. M., & Salleh, M. (2023). Edge computing for vehicle to everything: A short review. *F1000Research*, *10*, 1104. https://doi.org/10.12688/f1000research.73269.4

[4] Bréhon--Grataloup, L., Kacimi, R., & Beylot, A.-L. (2022). Mobile edge computing for V2X architectures and applications: A survey. *Computer networks*, *206*, 108797. https://doi.org/10.1016/j.comnet.2022.108797

[5] Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017). A survey on mobile edge computing: The communication perspective. *IEEE communications surveys & tutorials*, *19*(4), 2322–2358. https://doi.org/10.1109/COMST.2017.2745201

[6] Yan, G., Liu, K., Liu, C., & Zhang, J. (2024). Edge intelligence for internet of vehicles: A survey. *IEEE transactions on consumer electronics*, *70*(2), 4858–4877. https://doi.org/10.1109/TCE.2024.3378509

[7] Gheorghe, C., & Soica, A. (2025). Revolutionizing urban mobility: A systematic review of AI, IoT, and predictive analytics in adaptive traffic control systems for road networks. *Electronics (2079-9292)*, *14*(4), 719. https://doi.org/10.3390/electronics14040719

[8] Patra, B., Tamrakar, A., & Sharma, R. (2019). Edge computing: Evolution, challenges, and future directions. *Turkish journal of computer and mathematics education vol*, *10*(1), 741–745. https://doi.org/10.61841/turcomat.v10i1.14603

[9] Kong, L., Tan, J., Huang, J., Chen, G., Wang, S., Jin, X., … & Das, S. K. (2022). Edge-computing-driven internet of things: A survey. *ACM computing surveys*, *55*(8), 1–41. https://doi.org/10.1145/3555308

[10] Sheikh, A. M., Islam, M. R., Habaebi, M. H., Zabidi, S. A., Bin Najeeb, A. R., & Kabbani, A. (2025). A survey on edge computing (EC) security challenges: Classification, threats, and mitigation strategies. *Future internet*, *17*(4), 175. https://doi.org/10.3390/fi17040175

[11] Trigka, M., & Dritsas, E. (2025). Edge and cloud computing in smart cities. *Future internet*, *17*(3), 118. https://doi.org/10.3390/fi17030118

[12] Madamori, O., Max-Onakpoya, E., Erhardt, G. D., & Baker, C. E. (2021). Enabling opportunistic low-cost smart cities by using tactical edge node placement. *2021 16th annual conference on wireless on-demand network systems and services conference (WONS)* (pp. 1–8). IEEE. https://doi.org/10.23919/WONS51326.2021.9415579

[13] Zreikat, A. I., AlArnaout, Z., Abadleh, A., Elbasi, E., & Mostafa, N. (2025). The integration of the internet of things (IoT) applications into 5G networks: A review and analysis. *Computers*, *14*(7), 250. https://doi.org/10.3390/computers14070250

[14] Mahbub, M., & Shubair, R. M. (2023). Contemporary advances in multi-access edge computing: A survey of fundamentals, architecture, technologies, deployment cases, security, challenges, and directions. *Journal of network and computer applications*, *219*, 103726. https://doi.org/10.1016/j.jnca.2023.103726

[15] Mahomed, A. S., & Saha, A. K. (2025). Unleashing the potential of 5G for smart cities: A focus on real-time digital twin integration. *Smart cities*, *8*(2), 70. https://doi.org/10.3390/smartcities8020070

[16] Ferrag, M. A., Friha, O., Kantarci, B., Tihanyi, N., Cordeiro, L., Debbah, M., … & Choo, K. K. R. (2023). Edge learning for 6G-enabled internet of things: A comprehensive survey of vulnerabilities, datasets, and defenses. *IEEE communications surveys & tutorials*, *25*(4), 2654–2713. https://doi.org/10.1109/COMST.2023.3317242

[17] Spadaccino, P., & Cuomo, F. (2020). *Intrusion detection systems for iot: Opportunities and challenges offered by edge computing and machine learning*. https://arxiv.org/abs/2012.01174

[18] Alotaibi, A., Aldawghan, H., & Aljughaiman, A. (2025). A review of the authentication techniques for internet of things devices in smart cities: Opportunities, challenges, and future directions. *Sensors*, *25*(6), 1649. https://doi.org/10.3390/s25061649

[19] Gușiță, B., Anton, A. A., Stângaciu, C. S., Stănescu, D., Găină, L. I., & Micea, M. V. (2025). Securing IoT edge: A survey on lightweight cryptography, anonymous routing and communication protocol enhancements. *International journal of information security*, *24*(3), 149. https://doi.org/10.1007/s10207-025-01071-7

[20] Kumar, S., Hu, Y., Andersen, M. P., Popa, R. A., & Culler, D. E. (2019). *JEDI: many-to-many end-to-end encryption and key delegation for IoT*. https://arxiv.org/abs/1905.13369

[21] Varugu, R. B., & Kumar, G. A. (2023). *A survey on iot device authentication and anomaly detection for cyber security using machine learning* [presentation]. Proceedings of the 5th international conference on communication and information processing (ICCIP)-2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4798899

[22] Tran-Truong, P. T., Pham, M. Q., Son, H. X., Nguyen, D. L., Nguyen, M. B., Tran, K. L., ... & Nguyen, A. T. (2025). A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis. *Journal of systems architecture*, *162*, 103402. https://doi.org/10.1016/j.sysarc.2025.103402

[23] Rahman, M. M., Al Shakil, S., & Mustakim, M. R. (2025). A survey on intrusion detection system in IoT networks. *Cyber security and applications*, *3*, 100082. https://doi.org/10.1016/j.csa.2024.100082

[24] Čižiūnienė, K., Prokopovič, M., Zaranka, J., & Matijošius, J. (2024). Biometric breakthroughs for sustainable travel: Transforming public transportation through secure identification. *Sustainability*, *16*(12), 5071. https://doi.org/10.3390/su16125071

[25] Lien, C. W., & Vhaduri, S. (2023). Challenges and opportunities of biometric user authentication in the age of iot: A survey. *ACM computing surveys*, *56*(1), 1–37. https://doi.org/10.1145/3603705

[26] Umar, H. G. A., Yasmeen, I., Aoun, M., Mazhar, T., Khan, M. A., Jaghdam, I. H., & Hamam, H. (2025). Energy-efficient deep learning-based intrusion detection system for edge computing: A novel DNN-KDQ model. *Journal of cloud computing*, *14*(1), 32. https://doi.org/10.1186/s13677-025-00762-9

[27] Singh, A. (2025). Real time intrusion detection in edge computing using machine learning techniques. *Turkish journal of engineering*, *9*(2), 385–393. https://doi.org/10.31127/tuje.1516046

[28] Tung, N. T., Nam, P. M., & Tin, P. T. (2021). Performance evaluation of a two-way relay network with energy harvesting and hardware noises. *Digital communications and networks*, *7*(1), 45–54. https://doi.org/10.1016/j.dcan.2020.04.003

[29] Fazeldehkordi, E., & Grønli, T.-M. (2022). A survey of security architectures for edge computing-based IoT. *IoT*, *3*(3), 332–365. https://doi.org/10.3390/iot3030019

[30] Sha, K., Yang, T. A., Wei, W., & Davari, S. (2020). A survey of edge computing-based designs for IoT security. *Digital communications and networks*, *6*(2), 195–202. https://doi.org/10.1016/j.dcan.2019.08.006

[31] Sasi, T., Lashkari, A. H., Lu, R., Xiong, P., & Iqbal, S. (2024). A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. *Journal of information and intelligence*, *2*(6), 455–513. https://doi.org/10.1016/j.jiixd.2023.12.001