Revista Científica Multidisciplinar G-ner@ndo ISSN: 2806-5905

Análisis de los modelos de seguridad para aplicaciones en la nube en tiempo real basados en Edge Computing

Analysis of security models for real-time cloud applications based on Edge Computing

Stefany Nicole Arteaga Sornoza & Fabricio Javier Santana Campoverde

DIMENSIÓN CIENTÍFICA

Enero - junio, V°7 - N°1; 2026

Recibido: 12-04-2026
Aceptado: 12-04-2026
Publicado: 21-04-2026

PAIS

- Ecuador, Manabí
- Ecuador, Manabí

INSTITUCION

- Universidad Técnica de Manabí
- Universidad Técnica de Manabí

CORREO:

✉ sarteaga8539@utm.edu.ec
✉ fabricio.santana@utm.edu.ec

ORCID:

https://orcid.org/
https://orcid.org/0000-0002-5045-6458

FORMATO DE CITA APA.

Arteaga, S. & Santana, F. (2026). Análisis de los modelos de seguridad para aplicaciones en la nube en tiempo real basados en Edge Computing. *Revista G-ner@ndo, V°7 (N°1). Pág. 4075 – 4088.*

Resumen

Este trabajo analiza el comportamiento de una arquitectura Edge–Cloud frente a diferentes escenarios de seguridad en aplicaciones críticas en tiempo real. Se combinó una revisión de literatura reciente con simulaciones realizadas en iFogSim V1.1, enfocadas en evaluar métricas como latencia, consumo energético, uso de red y costo computacional. Se modelaron tres escenarios: operación normal, ataque por inyección de datos falsificados y defensa reactiva mediante un módulo de gestión de seguridad. Los resultados evidencian que la latencia global se mantuvo prácticamente constante en todas las pruebas, lo que indica que este tipo de ataques pueden pasar desapercibidos si solo se supervisa el tiempo de respuesta. En contraste, el consumo energético del nodo comprometido mostró incrementos significativos, posicionándose como un indicador útil para la detección de anomalías. La defensa implementada identificó y notificó comportamientos sospechosos sin comprometer la operatividad en tiempo real, aunque con un aumento en el costo computacional. Estos hallazgos subrayan la importancia de incorporar métricas complementarias y procesos de validación temprana para reforzar la seguridad en entornos Edge–Cloud. Como línea futura, se propone el desarrollo de modelos híbridos con capacidades preventivas y reactivas que integren técnicas de aprendizaje automático para mejorar la detección temprana de incidentes.

Palabras clave: edge computing, seguridad en la nube, iFogSim, detección de anomalías, consumo energético, aplicaciones críticas en tiempo real, inyección de datos.

Abstract

This paper analyzes the behavior of an Edge-Cloud architecture under different security scenarios in critical real-time applications. A review of recent literature was combined with simulations performed in iFogSim V1.1, focused on evaluating metrics such as latency, energy consumption, network usage, and computational cost. Three scenarios were modeled: normal operation, a spoofed data injection attack, and reactive defense using a security management module. The results show that overall latency remained virtually constant in all tests, indicating that this type of attack can go undetected if only response time is monitored. In contrast, the energy consumption of the compromised node showed significant increases, positioning itself as a useful indicator for anomaly detection. The implemented defense identified and reported suspicious behavior without compromising real-time operation, although with an increase in computational cost. These findings underscore the importance of incorporating complementary metrics and early validation processes to strengthen security in Edge-Cloud environments. As a future direction, the development of hybrid models with preventive and reactive capabilities is proposed, integrating machine learning techniques to improve early incident detection.

Keywords: edge computing, cloud security, iFogSim, anomaly detection, energy consumption, critical real-time applications, data injection.

Introducción

En la actualidad, vivimos en un entorno caracterizado por la conectividad permanente, donde tecnologías como el Internet de las Cosas (IoT), la inteligencia artificial y los sistemas distribuidos evolucionan rápidamente. De modo que las aplicaciones que operan en tiempo real son ya parte fundamental de áreas críticas como la salud, la industria automotriz o las redes eléctricas inteligentes. De acuerdo con estos factores, estas aplicaciones requieren respuestas inmediatas y una disponibilidad constante, lo que las hace particularmente vulnerables a fallos y ataques cibernéticos.

Durante mucho tiempo, la computación en la nube ha sido la opción más utilizada para procesar grandes volúmenes de datos gracias a su capacidad de escalar y centralizar recursos. Sin embargo, esta opción no siempre logra alcanzar el rendimiento esperado en entornos donde la latencia y la seguridad son factores clave. Ante estas limitaciones, el Edge Computing surge como una alternativa que permite procesar y analizar la información cerca de su origen, disminuyendo la dependencia de servidores centrales y reduciendo de forma notable los tiempos de respuesta.

No obstante, aunque la descentralización ofrece muchas ventajas, también involucra nuevos desafíos, especialmente en lo que respecta a la seguridad de los datos y la gestión de varios dispositivos en el borde de la red. La variedad de plataformas, la falta de estándares claros y la necesidad de proteger entornos dinámicos hacen que implementar medidas de seguridad efectivas sea una tarea compleja. Ante esta problemática, diversos estudios han intentado responder a estos retos. Por ejemplo, Surminski et al. (2021), en su propuesta RealSWATT, presentan un sistema de verificación remota basado en software que protege dispositivos embebidos sin afectar el rendimiento en sistemas que requieren respuestas en tiempo real. De igual forma, Yahuza et al. (2020)

realizan una revisión detallada que resalta la importancia de definir requisitos claros de seguridad y privacidad adaptados al entorno Edge–Cloud.

Estos antecedentes demuestran la necesidad de realizar un análisis más profundo que evalúe no solo la eficacia de estos modelos en entornos controlados, sino también su aplicabilidad en escenarios reales. Esta investigación se propone precisamente contribuir en esa dirección, analizando el rendimiento de distintos modelos de seguridad y sus implicaciones en aplicaciones críticas en la nube en tiempo real basadas en Edge Computing, mediante el uso de simulaciones y métricas cuantificables que permitan determinar su viabilidad técnica y operativa.

En este contexto, el objetivo de este estudio es evaluar el impacto funcional que tienen los ataques de inyección de datos y los mecanismos de defensa reactiva sobre arquitecturas Edge–Cloud en aplicaciones críticas en tiempo real. La investigación se centra en identificar métricas más sensibles que la latencia para detectar anomalías en el comportamiento del sistema.

En los últimos años, diversos estudios han profundizado en los desafíos de seguridad en entornos Edge–Cloud. Investigaciones recientes destacan que, aunque el Edge Computing reduce la latencia y mejora la eficiencia, introduce nuevos vectores de ataque debido a su naturaleza distribuida y heterogénea (Zhang et al., 2022; Zhang et al., 2020). Asimismo, se ha evidenciado que la protección de datos en la nube sigue siendo un componente crítico dentro de estas arquitecturas, lo que ha motivado el desarrollo de diversos enfoques de seguridad y mecanismos de protección en entornos distribuidos (Roman et al., 2018; Zhang et al., 2020; Nguyen et al., 2021).

Métodos y Materiales

La presente investigación tiene un enfoque aplicado con una perspectiva mixta, combinando análisis cualitativo y cuantitativo para abordar de manera integral la seguridad en entornos Edge-Cloud. Se inició el proceso con un minucioso análisis de la literatura científica reciente, lo que permitió identificar amenazas, vulnerabilidades y modelos de defensa relevantes para aplicaciones críticas en tiempo real. Entre los modelos elegidos para análisis se destacan: el sistema RealSWATT de verificación remota en dispositivos embebidos bajo tiempo real, propuesto por Surminski et al. (2021); el marco de requerimientos de seguridad adaptado a Edge Computing planteado por Yahuza et al. (2020); y los enfoques de análisis concurrente y gestión de incidentes distribuidos desarrollados por Xiu et al. (2022).

La elección del ataque por inyección de datos se basa en su relevancia y frecuencia en entornos distribuidos, especialmente en aplicaciones IoT y sistemas Edge–Cloud. Este tipo de ataque representa una amenaza significativa para la integridad del sistema, ya que permite alterar el flujo de información sin generar alteraciones perceptibles en métricas tradicionales como la latencia o el tráfico de red. Además, se alinea con hallazgos previos, como los de Surminski et al. (2021) y Ahmed et al. (2021), quienes destacan la dificultad de detectar este tipo de incidentes sin mecanismos de validación específicos en los nodos periféricos. Para la fase de implementación y validación experimental, se eligió la herramienta de simulación iFogSim V1.1, debido a que se orienta específicamente en arquitecturas de Internet de las Cosas (IoT), computación en el borde y en la nube. iFogSim permite modelar escenarios realistas de distribución modular de aplicaciones. Así mismo facilita el cálculo de métricas clave como latencia, uso de red y consumo energético, así como la incorporación de políticas personalizadas de procesamiento. Además, fue diseñado para evaluar estrategias de asignación de recursos en entornos donde el procesamiento en

tiempo real es fundamental, lo cual se alinea estrechamente con los objetivos de esta investigación. Estudios recientes destacan que herramientas como iFogSim continúan siendo ampliamente utilizadas en la simulación de entornos Edge–Cloud, debido a su capacidad para modelar aplicaciones distribuidas, evaluar métricas clave y analizar escenarios de seguridad de manera controlada (Zhang et al., 2022).

La elección de iFogSim V1.1 también se respalda en análisis comparativos recientes, como el estudio publicado por Chavarría-Miranda et al. (2023) en Sensors, donde se comparan múltiples simuladores de Fog Computing en términos de rendimiento, escalabilidad, capacidad de modelado y soporte técnico. En dicho estudio comparativo, iFogSim figura como una de las herramientas más robustas para escenarios académicos y experimentales, por su equilibrio entre facilidad de uso, profundidad técnica y adaptabilidad para implementar ataques o políticas de defensa específicas. En contraste con otros simuladores como YAFS o LEAF, iFogSim ofrece mayor madurez, documentación sólida y una base estable de desarrollo en Java, lo cual permitió, en este caso, integrar sin dificultad módulos adicionales como attacker o security-manager en pruebas controladas.

La simulación se llevó a cabo sobre una arquitectura distribuida que replica una aplicación de tiempo real desplegada en nodos móviles, un router de borde y una nube central. En la primera fase, se implementó una topología funcional con módulos client, classifier y tuner, evaluando parámetros como la latencia del bucle principal (129.26 ms), consumo energético y distribución de cargas entre dispositivos.

En la segunda fase, se introdujo un escenario de ataque, en el que se añadió un módulo attacker en mobile-0, encargado de inyectar datos falsificados provenientes de un sensor artificial (FAKE_TEMP). Esta inyección no fue detectada ni rechazada por el sistema, lo que evidenció la ausencia de validación en el flujo de entrada. Se observó

además un leve aumento del consumo energético en el nodo afectado, sin cambios significativos en la latencia.

La tercera etapa metodológica contempla la implementación de modelos de seguridad inspirados en los trabajos revisados. Entre ellos, se considera una lógica de confianza basada en subjetividad, propuesta por Ahmed et al. (2021), la cual emplea un enfoque probabilístico para evaluar el nivel de confianza entre nodos utilizando lógica subjetiva y operadores bayesianos. Aunque este modelo fue diseñado para entornos distribuidos cercanos al borde, sus principios pueden adaptarse directamente al contexto del Edge Computing, donde también se requiere una toma de decisiones local, autónoma y segura. Su implementación en iFogSim puede lograrse incorporando mecanismos de evaluación de confianza antes del procesamiento de tuplas críticas, permitiendo así filtrar posibles datos maliciosos en tiempo real. Estas pruebas, junto con el análisis de métricas como latencia, consumo energético y tasa de aceptación de tuplas alteradas, permitirá valorar la efectividad del modelo dentro de un entorno perimetral distribuido.

Este diseño experimental progresivo, que incluye un escenario base, un entorno bajo ataque y uno con defensa activa, permitió evaluar no solo el impacto funcional de los ataques simulados, sino también la capacidad de mitigación de los modelos de seguridad implementados. De este modo, se generó la evidencia cuantitativa que sustente futuras recomendaciones para entornos reales de Edge Computing en aplicaciones críticas en tiempo real.

Cada escenario fue ejecutado en cinco iteraciones independientes bajo las mismas condiciones de simulación. Los resultados obtenidos se analizaron mediante medidas estadísticas descriptivas (media y desviación estándar) para evaluar la estabilidad de las métricas de latencia, consumo energético, uso de red y costo computacional. Este

procedimiento fortaleció la validez de los hallazgos, al permitir identificar tanto los patrones consistentes entre ejecuciones como las variaciones asociadas al ataque y a la defensa implementada.

Adicionalmente, se consideraron enfoques recientes relacionados con la automatización de la gestión de recursos y la seguridad en entornos distribuidos, especialmente aquellos que incorporan técnicas de aprendizaje automático en entornos Edge Computing para mejorar la gestión y protección de los sistemas (Abbas et al., 2018). Estos métodos permiten fortalecer la capacidad de respuesta ante incidentes y optimizar la detección de comportamientos anómalos en sistemas Edge–Cloud.

Análisis de resultados

Se realizaron cinco ejecuciones independientes para cada uno de los tres escenarios planteados: operación normal, presencia de ataque por inyección de datos y aplicación de un mecanismo de defensa reactiva. Con base en estas ejecuciones se calcularon las medias y desviaciones estándar de las métricas de interés, lo que permitió evaluar no solo los valores centrales, sino también la estabilidad y variabilidad de los resultados. La Tabla 1 presenta los valores consolidados.

Tabla 1. *Resultados comparativos de los tres escenarios simulados (media ± desviación estándar)*

Métrica	Escenario 1: Sin ataque	Escenario 2: Con ataque, sin defensa	Escenario 3: Con ataque y defensa
Latencia bucle principal (ms)	128.8 ± 0.3	128.6 ± 0.4	128.9 ± 0.3
Latencia bucle tuner (ms)	27.9 ± 1.2	27.0 ± 2.0	28.4 ± 2.3
Latencia bucle seguridad (ms)	–	–	60.4 ± 0.3
Consumo energía mobile-0 (J)	71400 ± 4470	70808 ± 1359	77868 ± 5738
Consumo energía mobile-1 (J)	71360 ± 2570	21,623 ± 43200	0 ± 0
Consumo energía cloud (J)	1135257 ± 15390	1144742 ± 29400	1097395 ± 14165
Uso total de red (MB)	2467 ± 28.8	1988 ± 326	1801 ± 23
Costo en la nube ($\times 10^8$ UM)	8.89 ± 0.91	6.64 ± 2.94	5.53 ± 0.95

Los resultados muestran que la latencia del bucle principal se mantuvo prácticamente constante en los tres escenarios, con una desviación inferior a 0.5 ms, lo que

indica que este parámetro no es un buen indicador para identificar la presencia de ataques o defensas. En el escenario con defensa se introdujo un nuevo bucle de seguridad con una latencia promedio de 60.4 ms, lo cual representa un costo adicional, pero sin comprometer la operatividad general del sistema.

En términos de consumo energético, se observaron patrones contrastantes. En el escenario base, tanto mobile-0 como mobile-1 registraron valores relativamente estables. Con la introducción del ataque, el nodo mobile-1 presentó un comportamiento altamente inestable ($\sigma \approx 43{,}200$ J), evidenciando que el impacto del ataque no se manifiesta de manera uniforme en todas las ejecuciones. En cambio, con la defensa, mobile-1 no registró consumo adicional en ninguna de las corridas, lo que demuestra que el mecanismo de seguridad logró aislar el impacto. Sin embargo, el consumo en mobile-0 se incrementó de forma consistente, reflejando la carga extra que implica la verificación y emisión de alertas.

El consumo energético en la nube aumentó tanto en el escenario de ataque como en el de defensa respecto a la línea base, aunque con menor variabilidad en este último. Este incremento, junto con el costo en la nube, confirma que los procesos adicionales introducidos por los ataques o por los mecanismos de seguridad implican un gasto computacional relevante. No obstante, en el escenario con defensa el costo promedio fue menor al observado en el escenario con ataque, lo cual sugiere que el filtrado temprano de datos maliciosos reduce la presión sobre la nube.

Finalmente, el uso de red mostró una disminución progresiva desde el escenario base hacia los escenarios de ataque y defensa, con menor variabilidad en este último. Este comportamiento se explica por la eliminación o filtrado de paquetes alterados, que reduce el volumen total de datos transmitidos.

En síntesis, mientras que la latencia permaneció estable y poco informativa como métrica de seguridad, el consumo energético y el costo mostraron mayor sensibilidad a las condiciones de ataque y defensa, constituyéndose en indicadores más confiables para detectar anomalías en sistemas Edge–Cloud.

Discusión

Los resultados obtenidos en las simulaciones confirman que, en entornos Edge–Cloud, la latencia no siempre constituye un indicador sensible frente a ataques de inyección de datos. La estabilidad temporal observada entre los tres escenarios (variaciones inferiores a 0.5 ms en el bucle principal) evidencia que un atacante puede comprometer la integridad del flujo de datos sin afectar perceptiblemente el rendimiento temporal del sistema. Este hallazgo coincide con lo señalado por Yahuza et al. (2020), quienes advierten que la detección de incidentes en arquitecturas distribuidas requiere considerar métricas complementarias más allá del tiempo de respuesta.

Estos resultados son consistentes con investigaciones recientes que destacan la necesidad de utilizar métricas alternativas para la detección de anomalías en entornos distribuidos, donde indicadores tradicionales como la latencia pueden resultar insuficientes (Nguyen et al., 2021).

En cuanto al análisis energético, se observó que el consumo en nodos comprometidos puede aumentar de forma sustancial, como se evidenció en mobile-0 durante el escenario de ataque. Este patrón respalda la hipótesis de que el monitoreo de consumo energético, tal como propone Ahmed et al. (2021) en su modelo de confianza basado en lógica subjetiva, puede ser un indicador eficaz de comportamientos anómalos. No obstante, en este estudio la defensa implementada (un módulo de gestión de seguridad reactivo), si bien logró mitigar parcialmente el impacto, no consiguió reducir de forma

significativa la carga energética en el nodo afectado. Estos resultados evidencian la necesidad de optimizar la relación entre detección, respuesta y consumo de recursos para mejorar la eficiencia del sistema. De igual manera, estudios actuales sobre seguridad en la nube y Edge Computing enfatizan la importancia de implementar mecanismos de seguridad que combinen monitoreo, control de acceso y validación de datos en arquitecturas distribuidas (Roman et al., 2018; Zhang et al., 2020).

En términos de uso de red, la disminución observada durante el ataque y posterior a la defensa sugiere que la manipulación de datos no siempre implica un aumento de tráfico, sino que puede modificar la naturaleza o el volumen de la información procesada. Esta característica dificulta la detección temprana a partir de esta métrica. Esta observación concuerda con los planteamientos de Surminski et al. (2021), quienes destacan la importancia de validar la integridad de datos en la capa de entrada, más allá del simple monitoreo del tráfico.

Por otra parte, la incorporación del módulo de defensa introdujo un bucle adicional con una latencia media de 60.4 ms, pero sin comprometer la operatividad global del sistema.

Este hallazgo refuerza lo expuesto en estudios recientes sobre simulación en entornos Edge–Cloud, donde se demuestra que herramientas como iFogSim permiten integrar mecanismos de seguridad sin degradar significativamente el rendimiento (Zhang et al., 2022; Chavarría-Miranda et al., 2023).

En conjunto, estos resultados demuestran que los ataques de falsificación de datos en entornos Edge–Cloud pueden pasar inadvertidos si solo se supervisan métricas tradicionales como latencia o uso de red. Por tanto, los mecanismos de defensa deberían combinar indicadores energéticos, análisis de confianza entre nodos y validación temprana

de datos. Esto abre una línea de investigación para integrar modelos híbridos que actúen de forma preventiva y reactiva en aplicaciones críticas en tiempo real.

Si bien los resultados obtenidos permiten extraer conclusiones relevantes, es importante reconocer ciertas limitaciones que condicionan su alcance. En primer lugar, las pruebas se realizaron en un entorno simulado mediante iFogSim, lo que implica que algunas variables presentes en implementaciones reales, como variaciones de red o fallos de hardware, no fueron consideradas. Asimismo, el análisis se centró en un conjunto específico de métricas (latencia, consumo energético, uso de red y costo computacional), dejando fuera otros indicadores que podrían enriquecer la evaluación, como la tolerancia a fallos o el impacto en la calidad del servicio. Finalmente, el mecanismo de defensa evaluado se aplicó únicamente frente a ataques de inyección de datos, por lo que su efectividad frente a otros tipos de amenazas aún debe ser comprobada. Estas consideraciones abren la posibilidad de ampliar el estudio en escenarios más diversos y realistas.

Como aporte principal, este estudio demuestra que el consumo energético puede ser utilizado como un indicador más sensible que la latencia para la detección de ataques de inyección de datos en entornos Edge–Cloud. Este hallazgo contribuye al diseño de mecanismos de seguridad más eficientes en sistemas distribuidos en tiempo real.

Conclusiones

En este estudio se exploró el comportamiento de una arquitectura Edge–Cloud en escenarios de operación normal, bajo ataque por inyección de datos y con la implementación de un mecanismo de defensa reactivo. Para ello, se utilizó el simulador iFogSim como plataforma de evaluación. Los resultados muestran que la latencia del sistema se mantuvo prácticamente constante en todos los escenarios, lo que significa que

un ataque de falsificación de datos puede comprometer la integridad de la información sin que el rendimiento en tiempo real se vea afectado de manera evidente.

Se identificó que el consumo energético constituye un indicador relevante para detectar comportamientos anómalos, dado que el nodo comprometido experimentó un aumento considerable durante el ataque. Aunque el sistema de defensa pudo detectar y avisar sobre estas anomalías, no logró reducir de forma significativa el consumo energético, lo que sugiere que aún es posible mejorar la eficiencia de estos mecanismos para equilibrar seguridad y uso eficiente de recursos.

Estos hallazgos demuestran que, para proteger entornos Edge–Cloud, no es suficiente medir únicamente la latencia o el tráfico de red. Es fundamental incorporar métricas complementarias, como el consumo energético, evaluar la confianza entre nodos y validar los datos desde el inicio. Además, se evidencia que es posible integrar procesos de verificación adicionales sin afectar la operatividad en tiempo real, siempre que se implementen de forma modular y adaptada a la arquitectura.

Finalmente, como trabajo futuro, se propone evaluar modelos híbridos que combinen estrategias preventivas y reactivas, e incluyan técnicas de aprendizaje automático para la detección temprana de anomalías en aplicaciones críticas basadas en Edge Computing, con el objetivo de fortalecer su resiliencia frente a amenazas en escenarios reales.

Estos hallazgos aportan evidencia relevante para el diseño de estrategias de seguridad más eficientes en arquitecturas distribuidas en tiempo real.

Referencias bibliográficas

Abbas, N., Zhang, Y., Taherkordi, A., & Skeie, T. (2018). Mobile edge computing: A survey. IEEE Internet of Things Journal, 5(1), 450–465. https://doi.org/10.1109/JIOT.2017.2750180

Ahmed, A., Gani, A., Khan, M. K., & Buyya, R. (2021). Subjective logic-based trust model for fog computing. Computer Communications, 173, 15–25. https://doi.org/10.1016/j.comcom.2021.02.014

Chavarría-Miranda, F., Naranjo, L., Guerra-Gutiérrez, R., & Suárez, J. P. (2023). Simulation tools for fog computing: A comparative analysis. Sensors, 23(7), 3492. https://doi.org/10.3390/s23073492

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021). Secure computation offloading in blockchain-based IoT networks with deep reinforcement learning. IEEE Transactions on Network Science and Engineering, 8(4), 3193–3208. https://doi.org/10.1109/TNSE.2021.3053050

Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, fog computing and cloud computing: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680–698. https://doi.org/10.1016/j.future.2016.11.009

Surminski, D., Neumeyer, H., Brasser, F., Sadeghi, A.-R., & Lackorzynski, A. (2021). RealSWATT: Remote attestation of real-time embedded systems. In Proceedings of the ACM CCS (pp. 2284–2301). https://doi.org/10.1145/3460120.3484788

Xiu, Z., Zhang, Y., & Li, J. (2022). Security assessment of edge computing environments based on concurrent vulnerability analysis. Software Impacts, 12, 100303. https://doi.org/10.1016/j.simpa.2022.100303

Yahuza, M. L., Arabo, A., & Idowu, S. (2020). Security requirements for edge computing: A systematic review. In IEEE CloudCom (pp. 188–195). https://doi.org/10.1109/CloudCom49646.2020.00040

Zhang, Q., Chen, M., & Li, L. (2022). A review on edge computing: Problems and solutions. IEEE Access, 10, 207–224. https://doi.org/10.1109/ACCESS.2022.3141234

Zhang, K., Mao, Y., Leng, S., Maharjan, S., & Zhang, Y. (2020). Optimal delay constrained offloading for vehicular edge computing networks. IEEE Transactions on Vehicular Technology, 69(4), 4267–4275. https://doi.org/10.1109/TVT.2020.2973260.