Instituto Superior Tecnológico VICENTE ROCAFUERTE

REVISTA INSTITUTO SUPERIOR TECNOLÓGICO VICENTE ROCAFUERTE (REVISTVR)
Vol. 1 No. 1 – 2025

PATRONES ARQUITECTÓNICOS Y DISPONIBILIDAD EN IMPLEMENTACIONES DE FEDERACIÓN IoT : UNA REVISIÓN SISTEMÁTICA DE LITERATURA

Architectural Patterns and Availability in IoT Federation Implementations: A Systematic Literature Review

Óscar Alfonso Obando Cruz

Nayin Valentino Angúlo Daza

PATRONES ARQUITECTÓNICOS Y DISPONIBILIDAD EN IMPLEMENTACIONES DE FEDERACIÓN IoT : UNA REVISIÓN SISTEMÁTICA DE LITERATURA

Architectural Patterns and Availability in IoT Federation Implementations: A Systematic Literature Review

Nayin Angulo Daza[1] y Óscar Obando Cruz[2]

Como citar: Angulo,Nayin.,Obando,O.(2025).PATRONES ARQUITECTÓNICOS Y DISPONIBILIDAD EN IMPLEMENTACIONES DE FEDERACIÓN IoT : UNA REVISIÓN SISTEMÁTICA DE LITERATURA. *REVISTA INSTITUTO SUPERIOR TECNOLÓGICO VICENTE ROCAFUERTE (REVISTVR)*. 1*(1)*, pp.: 1-22.

RESUMEN

La investigación analizó sistemáticamente la relación entre patrones arquitectónicos y disponibilidad en implementaciones de federación IoT, con el objetivo de identificar y evaluar los patrones predominantes y su impacto en la disponibilidad del sistema, el estudio implementó una metodología PRISMA para la revisión sistemática de literatura científica publicada entre 2019 y 2024, seleccionando 40 estudios relevantes mediante criterios específicos de inclusión y exclusión, el análisis reveló tres patrones arquitectónicos predominantes: microservicios con orquestación distribuida (45% de implementaciones exitosas), arquitecturas event-driven con procesamiento en el borde (30%), y arquitecturas híbridas fog-cloud con federación dinámica (25%), los resultados demostraron que las implementaciones con patrones distribuidos y procesamiento en el borde alcanzaron niveles de disponibilidad superiores al 99.95%, superando significativamente las arquitecturas centralizadas tradicionales, la selección apropiada de patrones arquitectónicos emerge como factor determinante en la disponibilidad de sistemas IoT federados, estableciendo una base

[1] INGENIERO EN SISTEMAS COMPUTACIONALES Instituto Superior Tecnológico Vicente Rocafuerte, Ecuador. Email: oobando@istvr.edu.ec 0009-0008-6354-313X
[2] TECNOLOGO EN REDES Instituto Superior Tecnológico Vicente Rocafuerte, Ecuador. Email: nv.angulo@istvr.edu.ec. 0009-0001-8641-847X.

empírica para futuras implementaciones.

PALABRAS CLAVE: Federación IoT, Patrones Arquitectónicos, Disponibilidad de Sistemas, Computación Distribuida, Arquitectura de Software, Sistemas Resilientes.

ABSTRACT

La investigación analizó sistemáticamente la relación entre patrones arquitectónicos y disponibilidad en implementaciones de federación IoT, con el objetivo de identificar y evaluar los patrones predominantes y su impacto en la disponibilidad del sistema. El estudio implementó una metodología PRISMA para la revisión sistemática de literatura científica publicada entre 2019 y 2024, seleccionando 40 estudios relevantes mediante criterios específicos de inclusión y exclusión. El análisis reveló tres patrones arquitectónicos predominantes: microservicios con orquestación distribuida (45% de implementaciones exitosas), arquitecturas event-driven con procesamiento en el borde (30%), y arquitecturas híbridas fog-cloud con federación dinámica (25%). Los resultados demostraron que las implementaciones con patrones distribuidos y procesamiento en el borde alcanzaron niveles de disponibilidad superiores al 99.95%, superando significativamente las arquitecturas centralizadas tradicionales. La selección apropiada de patrones arquitectónicos emerge como factor determinante en la disponibilidad de sistemas IoT federados, estableciendo una base empírica para futuras implementaciones.

KEYWORDS: IoT Federation, Architectural Patterns, System Availability, Distributed Computing, Software Architecture, Resilient Systems.

INTRODUCCIÓN

El reconocimiento de la actividad humana mediante arquitecturas federadas IoT muestra el potencial transformador de los patrones arquitectónicos en sistemas distribuidos modernos, la implementación de PerFit (Q. Wu et al., 2020), es un marco de trabajo que integra computación en el borde con aprendizaje federado personalizado, que demuestra cómo la selección adecuada de patrones arquitectónicos resuelve desafíos fundamentales en entornos IoT heterogéneos, permitiendo que dispositivos IoT descarguen tareas de aprendizaje a nodos de borde mientras mantienen la privacidad de los datos, empleando un modelo de federación que combina el procesamiento local con la agregación global de modelos, la implementación fue probada con 30 dispositivos diferentes procesando datos de actividad humana, evidencia cómo la arquitectura federada no solo preserva la autonomía operativa de cada nodo sino que también optimiza el rendimiento global del sistema, logrando alta precisión con mínima sobrecarga de comunicación, ejemplificando la importancia crítica de los patrones arquitectónicos en la disponibilidad y eficiencia de sistemas IoT federados (Q. Wu et al., 2020).

Para el año 2030, se espera que el número de dispositivos IoT conectados alcance los 41.100 millones (Rosa Fernández, 2024), un aumento notable desde los 9.500 millones que se estimaban conectados a finales de 2019 (González et al., 2020), lo que se traduce en un crecimiento exponencial de

dispositivos que genera una enorme cantidad de datos, alcanzando los 79.4 zettabytes para 2025 (Khan et al., 2021), resaltando la necesidad de arquitecturas de sistemas distribuidos más eficientes e impulsando la adopción de computación en la niebla (fog) y en el borde (edge) debido al volumen de datos, trasladando el procesamiento más cerca de los dispositivos para reducir la latencia y el consumo de ancho de banda, a la vez que se facilita la gestión de la información (González et al., 2020).

El mercado de la computación en la nube está experimentando un crecimiento significativo y se espera que continúe expandiéndose en los próximos años (Filip Stojanović, 2023), para el 2024, se estimó una facturación de 947.500 millones de dólares en el mercado de IoT, y se proyecta que el número de dispositivos conectados alcance los 41.100 millones para 2030, en cuanto a los hogares inteligentes, se prevé que el número ascienda a 493,5 millones para 2025 (Rosa Fernández, 2024). En España, las empresas están incrementando su inversión en la nube, destinando más del 60% de su presupuesto de TI a esta área y con una previsión de gasto de 6.000 millones de euros en 2024, lo que representa un incremento del 9% con respecto a 2023 (Revista Cloud Computing, 2024), se espera que esta tendencia alcista continúe, superando los 7.500 millones de euros en 2025. Este aumento en la inversión refleja el reconocimiento del cloud como un elemento crítico para la supervivencia y la ventaja competitiva en un entorno empresarial incierto (Martín et al., 2024).

La proliferación de estos dispositivos IoT está transformando las arquitecturas de sistemas, pasando de modelos centralizados a distribuidos (Kim et al., 2023), la tendencia a descentralizar el procesamiento, utilizando la inteligencia artificial (IA) en el borde (González et al., 2020), se presenta como una solución clave, ya que permite a los dispositivos operar de forma más autónoma, la adopción de este modelo ofrece ventajas como una menor latencia, menor uso de banda ancha y mayor eficiencia general del sistema, los datos ya no se transmiten en su totalidad a la nube, sino que se procesan en proximidad a los dispositivos, permitiendo respuestas más rápidas y una mejor gestión de los recursos (González et al., 2020).

El rápido crecimiento de los dispositivos IoT para el 2030, ha llevado a una fragmentación del ecosistema tecnológico (Rosa Fernández, 2024), esta proliferación genera silos de información donde diversas plataformas y sistemas operan de manera aislada, limitando el potencial de las aplicaciones IoT (Kar et al., 2022), la necesidad de un enfoque unificado se vuelve imperativa ante la diversidad de dispositivos, protocolos y plataformas existentes, esta fragmentación no solo dificulta la interoperabilidad, sino que también impide el aprovechamiento completo del valor que estos dispositivos pueden ofrecer cuando se conectan y colaboran entre sí.

En este escenario, la federación de recursos emerge como una solución arquitectónica esencial. Permite la integración coherente de sistemas IoT heterogéneos, manteniendo a la vez su autonomía operativa (Kar et al., 2022). En lugar de imponer una estructura centralizada y rígida, la federación habilita una colaboración flexible y descentralizada entre diferentes dispositivos, plataformas y proveedores (Mostafaei et al., 2020). Este enfoque resulta crucial para superar la fragmentación y los silos de información, permitiendo que los sistemas IoT funcionen de manera coordinada. La federación no es solo una solución tecnológica, sino también una estrategia que reconoce la diversidad inherente del ecosistema IoT.

La adopción de una arquitectura federada trae consigo beneficios tangibles, como la compartición controlada de recursos, la interoperabilidad entre sistemas dispares y la optimización en el uso de la infraestructura (Kar et al., 2022). Estos aspectos son vitales para el desarrollo sostenible de soluciones IoT empresariales y gubernamentales. Al permitir que los dispositivos y sistemas compartan datos y capacidades, la federación facilita la creación de aplicaciones más sofisticadas y de mayor valor, mientras que optimiza el uso de los recursos disponibles, reduciendo así los costes y aumentando la

eficiencia. Esta eficiencia es crucial para manejar el volumen de datos y la diversidad de aplicaciones IoT actuales.

Sin embargo, la implementación efectiva de federaciones IoT presenta desafíos significativos, especialmente en términos de disponibilidad y resiliencia del sistema (Xu et al., 2022). Estos aspectos dependen fundamentalmente de los patrones arquitectónicos adoptados. Los sistemas federados deben ser capaces de operar de manera continua, incluso en situaciones de fallo o interrupción en algún componente. Esta necesidad de alta disponibilidad y resistencia es lo que hace que la elección de la arquitectura sea fundamental para garantizar el funcionamiento adecuado de las federaciones IoT. La complejidad de coordinar múltiples entidades heterogéneas en una federación requiere diseños arquitectónicos robustos y adaptables.

La implementación efectiva de federaciones IoT presenta desafíos significativos, especialmente en términos de disponibilidad y resiliencia del sistema, aspectos que, como se mencionó anteriormente, dependen fundamentalmente de los patrones arquitectónicos adoptados. El reto principal radica en asegurar que el sistema federado, compuesto por múltiples entidades heterogéneas, mantenga la operatividad incluso frente a fallos o interrupciones parciales. Esto implica que la arquitectura debe ser capaz de mitigar las consecuencias de fallos individuales en cualquiera de los nodos federados, sin que esto comprometa la disponibilidad general del sistema (González et al., 2020). En otras palabras, la tolerancia a fallos se convierte en un pilar fundamental, requiriendo redundancia en varios niveles y la capacidad de adaptación ante condiciones cambiantes (Alam & Gupta, 2022). Adicionalmente, la naturaleza dinámica de muchos entornos IoT, con dispositivos que pueden ser móviles o intermitentemente activos, añade complejidad a este desafío (Khan et al., 2021).

El desarrollo de arquitecturas federadas en el contexto de IoT ha sido un proceso evolutivo, impulsado por la necesidad de integrar sistemas cada vez más complejos y heterogéneos. Inicialmente, las primeras aproximaciones a la interconexión de dispositivos IoT se caracterizaban por modelos centralizados, donde un único punto de control gestionaba todos los nodos. Sin embargo, este esquema demostró ser poco escalable y vulnerable a fallos únicos (González et al., 2020). A medida que el número de dispositivos crecía y la diversidad de sus funcionalidades aumentaba, se hizo evidente la necesidad de un enfoque más distribuido y flexible que pudiera garantizar la disponibilidad y la resiliencia del sistema (McManus et al., 2024), esta necesidad marcó la transición hacia modelos más descentralizados (Soleymani et al., 2023).

A lo largo del tiempo, se produjo una progresión gradual hacia arquitecturas más sofisticadas, desde las primeras redes de sensores inalámbricos (WSN) hasta los sistemas complejos que se observan hoy en día. La evolución se puede entender a través de las siguientes etapas:

- Arquitecturas de tres capas: Inicialmente, los modelos de tres capas fueron ampliamente adoptados, con una capa de percepción (sensores), una capa de red (transmisión de datos) y una capa de aplicación (procesamiento y servicios) (Kim et al., 2023), esta arquitectura proporcionó una base para la integración de dispositivos, pero aún carecía de la flexibilidad y la descentralización necesarias para manejar grandes volúmenes de datos y la diversidad de aplicaciones (Kar et al., 2022).

- Modelos basados en middleware: El middleware surgió como una solución prometedora, ofreciendo una capa de abstracción que facilitaba la comunicación entre diferentes dispositivos y plataformas (Saxena et al., 2021), es decir, la transición hacia enfoques más sofisticados que buscan la interoperabilidad y la descentralización (McManus et al., 2024), sin embargo, la dependencia de componentes centralizados en muchos modelos de middleware pronto reveló limitaciones en términos de escalabilidad y robustez, ya que un único punto de fallo podía comprometer todo el sistema (Saxena et al., 2021).

- Arquitecturas orientadas a servicios (SOA): Las arquitecturas orientadas a servicios se basaron en la idea de descomponer los sistemas complejos en servicios reutilizables, lo que fomentó la modularidad y la flexibilidad (Javed et al., 2020), aunque mejoró la capacidad de integrar sistemas heterogéneos, la gestión y coordinación de servicios en un entorno federado seguían siendo un desafío (Q. Wu et al., 2020), esto incluye la heterogeneidad de datos, de modelos, de dispositivos, y de comunicación.
- Computación en la niebla (fog computing): La computación en la niebla introdujo una jerarquía de capacidad de cómputo entre los dispositivos de borde y la nube. Esta arquitectura mejoró la latencia, redujo el uso de ancho de banda y acercó el procesamiento a los datos, pero la federación entre nodos niebla seguía siendo un problema a resolver (González et al., 2020).
- Computación en el borde (edge computing): La computación en el borde trasladó el procesamiento y almacenamiento aún más cerca de los dispositivos terminales. Esta arquitectura mejoró aún más la latencia y la eficiencia, pero también introdujo desafíos relacionados con la gestión de dispositivos y la coordinación en entornos altamente distribuidos (Q. Wu et al., 2020).
- Arquitecturas descentralizadas: Los modelos descentralizados abogaron por la autonomía de cada nodo en la red, y la interacción entre ellos, a través de protocolos estandarizados para garantizar la interoperabilidad. Este enfoque proporcionó una mayor resiliencia al eliminar dependencias de componentes centralizados (Lo & Calo, 2023).

La evolución de las arquitecturas federadas se orienta decisivamente hacia modelos descentralizados, autónomos y adaptativos, donde la inteligencia artificial en el borde emerge como componente fundamental para la toma de decisiones locales y la reducción de dependencia de la nube (Q. Wu et al., 2020), esta transformación arquitectónica responde a múltiples necesidades: minimizar la latencia, optimizar los costes de comunicación y fortalecer la privacidad de los datos (Kar et al., 2022), los protocolos de comunicación como MQTT (Hussein & Shujaa, 2020), CoAP (Rizzardi et al., 2022)y DDS (Talcott, 2024) se han convertido en pilares fundamentales para facilitar el intercambio eficiente de datos entre dispositivos heterogéneos en entornos distribuidos. Simultáneamente, el aprendizaje federado se consolida como una técnica esencial que permite el entrenamiento descentralizado de modelos de aprendizaje automático, preservando la privacidad de los datos y fomentando la colaboración efectiva entre dispositivos (Alam & Gupta, 2022), esta convergencia de tecnologías y enfoques arquitectónicos está permitiendo la creación de sistemas IoT más inteligentes y robustos, capaces de adaptarse a entornos dinámicos mientras abordan eficazmente los desafíos inherentes de heterogeneidad y escalabilidad en las aplicaciones IoT modernas (Q. Wu et al., 2020)(Kar et al., 2022).

La disponibilidad sigue siendo un desafío crucial debido a la naturaleza distribuida de estos sistemas (Shieh, 2023). Se requieren mecanismos robustos de tolerancia a fallos y redundancia para asegurar la continuidad operativa. Las arquitecturas modernas emplean replicación de datos y servicios(Javed et al., 2020), detección y recuperación automática de fallos (Alam & Gupta, 2022), y gestión dinámica de recursos (Fé et al., 2022) para mejorar la resiliencia y la disponibilidad. La heterogeneidad de dispositivos y redes añade una complejidad considerable (Chen et al., 2024), demandando protocolos y algoritmos adaptables (Khan et al., 2021).

La implementación de arquitecturas federadas en entornos IoT presenta desafíos multifacéticos que requieren un abordaje sistemático y comprehensivo. La coordinación efectiva entre nodos federados emerge como un reto fundamental, particularmente en aspectos como la sincronización de estados, la gestión de recursos compartidos y la resolución de conflictos en tiempo real (Khan et al., 2021), los requisitos de seguridad y privacidad se vuelven más complejos en un contexto federado, donde los datos atraviesan múltiples dominios administrativos y requieren mecanismos robustos de autenticación, autorización y auditoría (Xu et al., 2022), la garantía de disponibilidad y resiliencia

demanda estrategias sofisticadas de tolerancia a fallos y recuperación, considerando la naturaleza heterogénea y distribuida de los recursos (Q. Wu et al., 2020), la investigación contemporánea se centra en desarrollar soluciones integradas que aborden estos desafíos, incluyendo la estandarización de protocolos de interoperabilidad y el desarrollo de algoritmos adaptativos para la optimización de recursos en entornos heterogéneos (Li et al., 2023).

La transición hacia sistemas IoT federados ha sido impulsada por varios factores clave. El primero es la explosión de dispositivos IoT heterogéneos (González et al., 2020), con una gran diversidad en cuanto a capacidades de procesamiento, almacenamiento y comunicación (Khan et al., 2021). Esto hace que los modelos centralizados, donde todos los datos convergen en un único punto, sean poco escalables y propensos a cuellos de botella. En segundo lugar, la necesidad de integración entre diferentes dominios IoT (Xu et al., 2022), como ciudades inteligentes, industria 4.0, y salud, demanda la capacidad de combinar datos y servicios de múltiples fuentes de forma coordinada. Finalmente, los requisitos de escalabilidad masiva para soportar millones de dispositivos conectados y la gran cantidad de datos que generan hacen indispensable una arquitectura distribuida y flexible (Khan et al., 2021).

Los cambios arquitectónicos fundamentales representan una transformación paradigmática en el diseño de sistemas IoT. Esta evolución trasciende la simple migración desde arquitecturas centralizadas hacia modelos distribuidos (Q. Wu et al., 2020), implementando un enfoque holístico donde el procesamiento y almacenamiento se distribuyen estratégicamente en una jerarquía de capacidades computacionales (González et al., 2020), la adopción de modelos descentralizados ha introducido conceptos avanzados como la orquestación dinámica de recursos y la auto-organización de nodos, permitiendo que estos operen con autonomía mientras mantienen una colaboración efectiva a través de protocolos estandarizados y mecanismos de consenso distribuido (Khan et al., 2021), este nuevo paradigma arquitectónico facilita la implementación de políticas de calidad de servicio (QoS) más granulares y mecanismos de recuperación ante fallos más robustos.

La transformación en la arquitectura de sistemas IoT ha traído consigo nuevos desafíos operacionales que afectan directamente a cómo gestionamos y utilizamos estos sistemas, imaginemos una ciudad inteligente: la gestión de recursos distribuidos debe coordinar eficientemente desde pequeños sensores de tráfico hasta sistemas complejos de monitorización ambiental, cada uno con sus propias capacidades y necesidades (Kar et al., 2022), esta gestión es similar a dirigir una orquesta donde cada instrumento (dispositivo) debe tocar su parte en el momento preciso, pero con la complejidad adicional de que los músicos (dispositivos) pueden unirse o dejar la orquesta en cualquier momento (Q. Wu et al., 2020).

El procesamiento en tiempo real se ha vuelto crítico en este entorno, por ejemplo, en un sistema de monitorización de salud, la diferencia entre recibir una alerta médica en segundos o en minutos puede ser crucial, estos sistemas deben procesar y entregar información con una rapidez comparable a nuestros reflejos naturales (Kar et al., 2022), la seguridad y privacidad han evolucionado para convertirse en pilares fundamentales, especialmente cuando manejamos datos sensibles (Narkedimilli et al., 2024), es como tener una conversación confidencial en una sala llena de gente: necesitamos asegurarnos de que solo los participantes autorizados puedan entender la información intercambiada (Song et al., 2021).

Pensar en el desafío actual de la heterogeneidad e interoperabilidad es como organizar una conferencia internacional donde los asistentes hablan diferentes idiomas, en el mundo IoT, cada tipo de dispositivo tiene su propia forma de "hablar" - sus protocolos de comunicación, algunos utilizan MQTT, que podríamos comparar con un sistema de mensajería rápida y ligera, mientras otros emplean CoAP, más adecuado para dispositivos con recursos limitados, o DDS, especializado en

comunicaciones en tiempo real (Rizzardi et al., 2022), esta diversidad, aunque enriquecedora, crea un verdadero desafío de "traducción" entre sistemas.

La situación se complica aún más cuando consideramos los diferentes formatos de datos que maneja cada dispositivo, similar a tener documentos escritos en diferentes alfabetos (Chen et al., 2024), por otro lado, un sensor de temperatura puede enviar datos en un formato simple, mientras que una cámara de seguridad inteligente transmite información mucho más compleja, hacer que todos estos dispositivos "se entiendan" entre sí, especialmente en tiempo real, es uno de los mayores retos que enfrentan los arquitectos de sistemas IoT modernos (Khan et al., 2021), es como crear un traductor universal que debe funcionar instantáneamente y sin errores.

Los retos de integración en sistemas IoT federados representan un desafío fundamental en el desarrollo de sistemas distribuidos modernos, la fragmentación actual entre plataformas IoT establece barreras significativas para la interoperabilidad, particularmente cuando se requiere la integración de dispositivos y servicios de diferentes fabricantes (Khan et al., 2021), por otro lado, la sincronización de datos entre nodos federados presenta complejidades adicionales, especialmente en entornos donde múltiples sistemas deben operar de manera coordinada (Q. Wu et al., 2020), un ejemplo ilustrativo se encuentra en los sistemas de gestión de edificios inteligentes, donde la coordinación entre subsistemas de temperatura, seguridad e iluminación debe mantener una operación coherente y sincronizada, independientemente de la diversidad de fabricantes y protocolos de comunicación involucrados.

La gestión de la consistencia de datos en estos sistemas distribuidos emerge como un aspecto crítico que requiere especial atención, el mantenimiento de la coherencia de la información a través de múltiples nodos distribuidos demanda mecanismos sofisticados de sincronización y validación (Javed et al., 2020), esta necesidad se vuelve particularmente crítica en aplicaciones industriales y de atención médica, donde la precisión y la sincronización temporal de los datos pueden tener implicaciones significativas en la operación del sistema."

El análisis del impacto en la disponibilidad de los sistemas IoT federados revela una compleja red de factores interrelacionados que afectan el rendimiento y la confiabilidad del sistema, la gestión de fallos en estos entornos distribuidos presenta desafíos únicos que trascienden los problemas tradicionales de los sistemas centralizados, a diferencia de las arquitecturas monolíticas, donde la detección y resolución de fallos sigue patrones bien definidos, los sistemas federados requieren un enfoque multidimensional para el manejo de errores (Karthikeyan et al., 2023).

Los mecanismos de tolerancia a fallos en sistemas federados deben incorporar estrategias adaptativas que consideren la naturaleza dinámica de los dispositivos IoT, este requerimiento se materializa en la implementación de sistemas redundantes y mecanismos de recuperación que pueden adaptarse a condiciones cambiantes (Javed et al., 2020), los sistemas modernos implementan estrategias de resiliencia que incluyen la replicación de servicios críticos, la distribución geográfica de recursos y la implementación de políticas de failover automático (Legler et al., 2024).

La gestión del mantenimiento de servicios en entornos federados requiere una aproximación sistemática que contemple la diversidad de plataformas y la dispersión geográfica de los recursos, las actualizaciones de software, la configuración de dispositivos y la gestión de parches de seguridad deben ejecutarse de manera coordinada para mantener la integridad del sistema (Fé et al., 2022), esta complejidad se amplifica en escenarios donde los dispositivos operan con diferentes velocidades de procesamiento y capacidades de almacenamiento, requiriendo estrategias de gestión que optimicen el rendimiento mientras mantienen la consistencia del sistema (González et al., 2020).

Los aspectos de latencia y rendimiento emergen como factores críticos adicionales en la disponibilidad de sistemas IoT federados. La coordinación necesaria entre diferentes nodos y dominios introduce desafíos significativos en el rendimiento del sistema (Kar et al., 2022), la latencia se convierte en un factor especialmente crítico en aplicaciones que requieren respuestas en tiempo real o que mantienen requisitos estrictos de alta disponibilidad (Lakhan et al., 2024), este aspecto requiere particular atención en la arquitectura del sistema, donde la distribución eficiente del procesamiento de datos debe equilibrarse cuidadosamente entre el procesamiento local y la coordinación global, la implementación de estrategias de optimización que balanceen estos factores resulta fundamental para mantener niveles aceptables de rendimiento y disponibilidad (González et al., 2020).

El análisis de la evolución de sistemas IoT ha evidenciado que la creciente complejidad y los requisitos de escalabilidad dinámica demandan una aproximación sistemática en el diseño arquitectónico, los modelos tradicionales centralizados resultan insuficientes ante la magnitud y diversidad de los sistemas IoT contemporáneos, lo que fundamenta la necesidad de patrones arquitectónicos robustos y adaptables (Khan et al., 2021), la investigación actual demuestra que la implementación de soluciones estandarizadas y replicables reduce significativamente la complejidad operacional mientras mejora la interoperabilidad entre componentes y plataformas heterogéneas (González et al., 2020).

Los sistemas IoT federados modernos requieren patrones arquitectónicos que exhiban características específicas de adaptabilidad contextual, esta adaptabilidad debe manifestarse en múltiples niveles, desde la capacidad de acomodar diferentes tipos de dispositivos y protocolos de comunicación hasta la habilidad de escalar horizontalmente sin comprometer el rendimiento del sistema (Martín et al., 2024), la implementación de mecanismos robustos para la detección, aislamiento y recuperación de fallos se ha convertido en un requisito fundamental, particularmente en entornos donde la continuidad operacional resulta crítica (Javed et al., 2020).

La investigación actual en patrones arquitectónicos IoT se centra en el desarrollo de marcos de referencia que faciliten la implementación de sistemas escalables y resilientes, estos marcos incorporan principios de diseño que priorizan la modularidad, la cohesión y el bajo acoplamiento, permitiendo la evolución independiente de diferentes componentes del sistema (Fé et al., 2022), la evidencia empírica demuestra que los patrones bien diseñados contribuyen significativamente a la reducción de la complejidad operacional y al mejoramiento de la mantenibilidad del sistema, factores críticos en el contexto de federaciones IoT de gran escala.

Las características requeridas para estos patrones arquitectónicos deben alinearse con las demandas específicas de los sistemas IoT federados, la adaptabilidad contextual emerge como un requisito fundamental, considerando que cada dominio de aplicación presenta desafíos únicos en términos de procesamiento, latencia y seguridad, por ejemplo, mientras un sistema de monitorización ambiental puede tolerar latencias moderadas, una línea de producción industrial requiere respuestas en tiempo real con tolerancias milimétricas, la gestión robusta de fallos constituye un componente crítico de estos patrones, especialmente considerando la naturaleza distribuida de los sistemas IoT federados, los mecanismos implementados deben abordar tres aspectos fundamentales (González et al., 2020):

- Detección proactiva de anomalías y fallos potenciales.
- Aislamiento efectivo de componentes comprometidos.
- Recuperación automática con mínima interrupción del servicio.

La escalabilidad horizontal representa otro pilar fundamental en el diseño de estos patrones, la capacidad de expandir recursos de manera dinámica debe mantener una relación directa con el rendimiento del sistema (Fé et al., 2022), esta escalabilidad debe complementarse con una

infraestructura adaptativa que responda eficientemente a fluctuaciones en la demanda de recursos (Martín et al., 2024).

Los objetivos de los patrones arquitectónicos en sistemas IoT federados se fundamentan en tres pilares esenciales. Primero, la estandarización que facilita la interoperabilidad y reutilización de componentes, aspecto crítico en sistemas heterogéneos (González et al., 2020), segundo, la mantenibilidad del sistema, que se logra mediante diseños modulares que permiten actualizaciones y correcciones sin afectar la operación global (Javed et al., 2020) y tercero, la optimización de la disponibilidad, especialmente crucial en entornos críticos donde las interrupciones pueden tener consecuencias significativas (Fé et al., 2022), la implementación de estos objetivos requiere estrategias específicas de tolerancia a fallos y gestión de latencia (Martín et al., 2024), los sistemas modernos de IoT federados implementan mecanismos de redundancia y recuperación ante fallos que permiten mantener la continuidad operativa incluso en condiciones adversas (Khan et al., 2021).

La selección de patrones arquitectónicos para sistemas IoT federados requiere una evaluación sistemática basada en criterios técnicos específicos, el primer criterio fundamental es la alineación contextual, que evalúa la compatibilidad del patrón con los requisitos funcionales y no funcionales del sistema, esta evaluación debe considerar aspectos como los tipos de dispositivos involucrados, los protocolos de comunicación requeridos y las restricciones de recursos existentes (González et al., 2020), por otro lado, la viabilidad de implementación constituye el segundo criterio crítico, que debe evaluarse desde múltiples dimensiones, misma que no se limita únicamente a la complejidad técnica del patrón, sino que abarca también la disponibilidad de recursos, la madurez de las tecnologías subyacentes y la existencia de herramientas de soporte adecuadas (Martín et al., 2024), la experiencia empírica demuestra que patrones excesivamente complejos, aunque técnicamente superiores, pueden resultar contraproducentes si su implementación excede las capacidades organizacionales (Khan et al., 2021).

El impacto en la disponibilidad del sistema emerge como el tercer criterio determinante, los patrones seleccionados deben proporcionar mecanismos robustos para garantizar la continuidad operativa, incluyendo estrategias específicas para la tolerancia a fallos, la recuperación automática y la gestión del rendimiento (Javed et al., 2020), esta evaluación debe considerar métricas cuantificables como el tiempo medio entre fallos (MTBF) y el tiempo medio de recuperación (MTTR), la evaluación debe complementarse con un análisis integral de los atributos de calidad del sistema, incluyendo la escalabilidad, mantenibilidad y seguridad. Las herramientas de gestión y monitoreo requeridas por el patrón deben evaluarse en términos de su capacidad para proporcionar visibilidad operativa y facilitar la administración proactiva del sistema (Fé et al., 2022), además, el análisis debe considerar también la capacidad del patrón para adaptarse a futuros cambios en los requisitos del sistema y en las tecnologías subyacentes.

Fundamentación teórica

El marco conceptual de la federación de recursos se basa en una serie de definiciones fundamentales. Desde la perspectiva de sistemas distribuidos, una federación es un conjunto de sistemas o entidades autónomas que colaboran para compartir recursos y servicios, sin estar sujetos a un control centralizado único (S. Wu et al., 2022). Los elementos constitutivos de una federación incluyen los nodos participantes (proveedores y consumidores de recursos), los recursos compartidos (computación, almacenamiento, red, etc.), los mecanismos de coordinación (protocolos de comunicación, acuerdos de servicio) y las políticas de gestión (acceso, seguridad, uso). Las características distintivas de los sistemas federados son la autonomía de los participantes, la heterogeneidad de los recursos, la gestión distribuida y la necesidad de mecanismos de coordinación para la interoperabilidad y la colaboración (Ahmed et al., 2022). Una taxonomía de modelos de federación incluye modelos horizontales (entre proveedores del mismo nivel), verticales (entre

proveedores de diferentes niveles) e híbridos (combinación de ambos) (Kar et al., 2022) (Khan et al., 2021)

En cuanto a los principios operativos de una federación de recursos, la autonomía de los participantes es clave, ya que cada entidad mantiene el control sobre sus propios recursos y políticas (Ahmed et al., 2022). La gestión de recursos distribuidos requiere mecanismos que permitan el descubrimiento, asignación y monitorización de los recursos compartidos en diferentes nodos (González et al., 2020). Los mecanismos de coordinación son esenciales para la comunicación y la colaboración entre los participantes, ya que estos mecanismos deben facilitar la negociación de acuerdos, la transferencia de datos y la sincronización de operaciones. Las políticas de compartición de recursos definen cómo se asignan los recursos entre los participantes, incluyendo aspectos como la priorización, la gestión de la calidad de servicio y las consideraciones económicas (Ahmed et al., 2022).

Los aspectos arquitectónicos esenciales de una federación de recursos incluyen los modelos de referencia, las capas arquitectónicas y los componentes principales. Los modelos de referencia proporcionan una estructura conceptual para el diseño de sistemas federados, como el modelo de capas ITU-T o el modelo de referencia IoT ARM (González et al., 2020), que guían la organización de los componentes y sus interacciones. Las capas arquitectónicas dividen el sistema en niveles funcionales, como la capa de percepción (dispositivos), la capa de red (comunicaciones) y la capa de aplicación (servicios), además de capas de abstracción y gestión. Los componentes principales de una federación incluyen los nodos de borde, los servidores de nube, los brokers, los gestores de recursos y los controladores (Mostafaei et al., 2020). Las interfaces de federación permiten la comunicación y la interoperabilidad entre los diferentes componentes y capas, y estas interfaces son esenciales para el intercambio de datos, la invocación de servicios y la gestión de los recursos (Rizzardi et al., 2022).

Las teorías fundamentales sobre patrones arquitectónicos se construyen sobre una base de definiciones y principios bien establecidos. Un patrón arquitectónico se define como una solución recurrente a un problema de diseño común en un contexto determinado (Javed et al., 2020). La evolución de estos patrones ha acompañado el desarrollo de la ingeniería de software, pasando desde modelos monolíticos hacia arquitecturas más modulares y distribuidas (González et al., 2020). Los principios de diseño arquitectónico, como modularidad, cohesión, acoplamiento y abstracción, son esenciales para crear sistemas robustos y mantenibles (Javed et al., 2020), la categorización de patrones se realiza en función de diferentes criterios, como su ámbito de aplicación (aplicación, dominio, empresa), el nivel de abstracción (arquitectónico, de diseño, idiomático) y la naturaleza del problema que resuelven, además, los criterios de selección de un patrón arquitectónico deben considerar la adecuación al problema específico, la facilidad de implementación, el impacto en la disponibilidad y otros atributos de calidad como la seguridad y la escalabilidad (Chen et al., 2024).

Dentro del ámbito de IoT, varios patrones arquitectónicos han demostrado ser especialmente relevantes. Las arquitecturas basadas en microservicios permiten la construcción de aplicaciones complejas a partir de servicios pequeños e independientes, lo que facilita la escalabilidad y la mantenibilidad (Abdennadher, 2024). Los patrones event-driven son útiles para sistemas reactivos que necesitan responder a eventos en tiempo real, como los sistemas de monitorización y control (González et al., 2020). Las arquitecturas orientadas a servicios (SOA), donde los servicios se coordinan y se promueve la reutilización, son también comunes en entornos IoT, ya que facilitan la integración de diferentes dispositivos y aplicaciones (Javed et al., 2020). Los patrones de escalabilidad, como el escalado horizontal, son fundamentales para manejar el crecimiento del número de dispositivos y la demanda de recursos (Kim et al., 2023). La elección de un patrón específico depende de las necesidades de la aplicación y de los compromisos (trade-offs) que se quieran asumir (Kar et al., 2022) (Chen et al., 2024).

Los aspectos de implementación de patrones arquitectónicos en IoT requieren una consideración cuidadosa. Las estrategias de aplicación deben incluir la selección de las tecnologías adecuadas, como los protocolos de comunicación (MQTT, CoAP) (Hussein & Shujaa, 2020) (Rizzardi et al., 2022), las plataformas de desarrollo y las herramientas de gestión (Javed et al., 2020). Las consideraciones de diseño deben tener en cuenta las limitaciones de los dispositivos IoT, como la capacidad de cómputo, la memoria y la energía (Talcott, 2024). Los compromisos (trade-offs) son inevitables, y a menudo implican la necesidad de equilibrar la funcionalidad, el rendimiento, el costo y la seguridad (Chen et al., 2024). Las métricas de evaluación deben medir la eficiencia del patrón, la disponibilidad del sistema y otros factores relevantes (Kar et al., 2022). Además, es importante considerar la necesidad de herramientas de orquestación y gestión de recursos, así como la adopción de un enfoque basado en FinOps para la optimización de los costos (Revista Cloud Computing, 2024).

Los principios de disponibilidad en sistemas distribuidos se centran en asegurar que los recursos y servicios estén accesibles cuando se necesiten. En sus conceptos fundamentales, la disponibilidad se define como la proporción de tiempo que un sistema está operativo y listo para su uso (Fé et al., 2022). Las métricas de medición incluyen el tiempo medio entre fallos (MTBF), el tiempo medio de reparación (MTTR) y el porcentaje de tiempo de actividad. Los factores que afectan la disponibilidad abarcan fallos de hardware y software, errores humanos, problemas de red, ataques de seguridad y desastres naturales (Shieh, 2023). Los modelos de evaluación utilizan herramientas como redes de Petri estocásticas para analizar el rendimiento y la disponibilidad del sistema (Fé et al., 2022).

Las estrategias de alta disponibilidad son esenciales para mitigar el impacto de estos factores. La redundancia y replicación implican duplicar componentes para que, en caso de fallo, otro componente pueda tomar el control (Javed et al., 2020). El balanceo de carga distribuye el tráfico y las tareas entre varios servidores para evitar la sobrecarga de un único componente, mejorando la eficiencia y la capacidad de respuesta del sistema (Karthikeyan et al., 2023). La recuperación ante fallos incluye mecanismos para detectar, aislar y corregir fallos automáticamente, con el objetivo de restaurar el sistema a un estado operativo en el menor tiempo posible. El monitoreo y detección de fallos son actividades continuas que permiten identificar problemas potenciales antes de que causen interrupciones significativas (Kar et al., 2022).

En el contexto específico de IoT, se presentan desafíos particulares para asegurar la disponibilidad. La gestión de recursos limitados en los dispositivos IoT, como la capacidad de cómputo, la memoria y la energía, requiere estrategias de diseño que minimicen el consumo de recursos. La latencia y conectividad son críticas en entornos IoT, ya que los dispositivos a menudo se encuentran en redes con baja latencia o conectividad intermitente (Q. Wu et al., 2020). La sincronización de estados entre los dispositivos y los servidores es esencial para mantener la coherencia del sistema, pero puede ser difícil de lograr en redes distribuidas (Alam & Gupta, 2022). Finalmente, la consistencia de datos entre los diferentes componentes de un sistema IoT federado es un desafío, especialmente cuando los datos se replican y se distribuyen en varios nodos. La implementación de arquitecturas descentralizadas y la utilización de computación en el borde (edge) y en la niebla (fog) son algunas de las estrategias empleadas para abordar estos desafíos (Javed et al., 2020) (González et al., 2020).

La intersección entre federación, patrones arquitectónicos y disponibilidad es crucial para diseñar sistemas distribuidos robustos y eficientes. Los patrones arquitectónicos influyen directamente en la disponibilidad, ya que una mala elección puede introducir puntos únicos de fallo o cuellos de botella. Las arquitecturas basadas en microservicios, por ejemplo, pueden mejorar la disponibilidad al permitir que un fallo en un servicio no afecte a otros, mientras que un diseño monolítico podría resultar en la caída de todo el sistema (González et al., 2020). La federación introduce complejidades adicionales, ya que la necesidad de coordinación entre entidades autónomas puede afectar la disponibilidad. Las decisiones sobre la arquitectura deben buscar el equilibrio entre la autonomía de los participantes y la capacidad de ofrecer un servicio fiable. En este contexto, las compensaciones

arquitectónicas son inevitables, y es fundamental considerar el impacto en la disponibilidad al seleccionar un patrón o modelo de federación.

La integración de patrones y requisitos de federación requiere coherencia y una estrategia bien definida. La coherencia implica que los patrones seleccionados deben ser compatibles con el modelo de federación y las políticas de compartición de recursos. La optimización de la disponibilidad en sistemas federados exige la implementación de redundancia, balanceo de carga y recuperación ante fallos a nivel de federación (Khan et al., 2021). Esto puede incluir la réplica de servicios, la distribución de datos entre nodos y el diseño de mecanismos de conmutación por error (Kar et al., 2022). Las estrategias de implementación integradas deben abarcar todos los niveles del sistema, desde los dispositivos de borde hasta los servidores de nube, asegurando que la disponibilidad sea una consideración primordial en cada etapa del desarrollo. La capacidad de escalar los recursos según la demanda son fundamentales para mantener la disponibilidad en entornos federados (González et al., 2020).

En la práctica, la evaluación y la selección de patrones y arquitecturas deben basarse en metodologías sólidas. Las metodologías de evaluación incluyen pruebas de carga y estrés, simulación de fallos y análisis de métricas de rendimiento y disponibilidad. Los criterios de selección de patrones deben considerar su impacto en la disponibilidad, la escalabilidad, la seguridad y la eficiencia energética, así como la capacidad de adaptación a los requisitos específicos de la federación. Las métricas de éxito deben definir objetivos claros y medibles para la disponibilidad del sistema, tales como el porcentaje de tiempo de actividad y el tiempo medio de recuperación ante fallos. Los factores de riesgo deben identificarse y gestionarse proactivamente para evitar interrupciones no deseadas (González et al., 2020). La seguridad, la privacidad y la protección de datos son factores críticos (Aouedi et al., 2022).

Las tendencias emergentes en la intersección entre federación, patrones y disponibilidad incluyen nuevos enfoques de integración, tecnologías habilitadoras y direcciones futuras en la investigación. Los nuevos enfoques de integración se centran en arquitecturas descentralizadas, computación en el borde (edge) y la niebla (fog), y el uso de inteligencia artificial para la gestión de recursos y la detección de fallos (Khan et al., 2021). Las tecnologías habilitadoras abarcan nuevos protocolos de comunicación, plataformas de orquestación de servicios y herramientas de monitorización. Estas tecnologías permiten la creación de sistemas federados más flexibles, escalables y disponibles. La federación de recursos en la nube es un tema recurrente (Saxena et al., 2021) (Khan et al., 2021).

Los desafíos pendientes en esta área incluyen la necesidad de estandarización, la gestión de la heterogeneidad, la garantía de la seguridad y la privacidad, y la optimización de la eficiencia energética en sistemas federados a gran escala (González et al., 2020). La estandarización es crucial para facilitar la interoperabilidad y la colaboración entre diferentes proveedores de recursos. La heterogeneidad de dispositivos y plataformas requiere enfoques adaptativos para la gestión de recursos y la comunicación. La seguridad y la privacidad son fundamentales para garantizar la confianza en los sistemas federados. La eficiencia energética es un desafío constante en los dispositivos IoT que requiere el desarrollo de mecanismos de optimización. Las técnicas de aprendizaje federado pueden ser útiles para abordar algunos de estos desafíos (Li et al., 2022).

En este contexto de evolución tecnológica, la revisión de literatura actualizada revela brechas significativas en la comprensión de la relación entre patrones arquitectónicos y disponibilidad en sistemas IoT federados (Q. Wu et al., 2020) (Khan et al., 2021), a pesar de la existencia de estudios que abordan aspectos específicos de la federación IoT, la interacción entre la selección de patrones arquitectónicos y los niveles de disponibilidad alcanzables permanece insuficientemente explorada, investigaciones existentes tienden a hacer énfasis en implementaciones aisladas o en aspectos técnicos particulares, sin proporcionar un marco comprensivo que guíe la selección de patrones

arquitectónicos en función de los requisitos de disponibilidad, lo que dificulta la toma de decisiones informadas en el diseño e implementación de sistemas IoT federados, especialmente cuando se requieren garantías específicas de disponibilidad (Hernan Diazgranados, 2020) (McManus et al., 2024).

Como consecuencia directa de estas brechas en el conocimiento, las implementaciones actuales de federación IoT enfrentan desafíos significativos que no han sido completamente resueltos por las aproximaciones existentes, la heterogeneidad inherente de los dispositivos IoT, combinada con requisitos variables de disponibilidad (Khan et al., 2021), presenta escenarios complejos donde los patrones arquitectónicos tradicionales muestran limitaciones evidentes, los intentos de abordar estos desafíos han producido soluciones parciales que, aunque efectivas en contextos específicos, carecen de la flexibilidad y adaptabilidad necesarias para su aplicación generalizada, la ausencia de un marco unificado que relacione patrones arquitectónicos con métricas de disponibilidad continúa obstaculizando la evolución hacia implementaciones más robustas y resilientes.

Para comprender mejor estas limitaciones, resulta fundamental examinar los casos de estudio documentados, los cuales proporcionan evidencia empírica crucial sobre la efectividad de diferentes aproximaciones arquitectónicas en entornos IoT federados, estas implementaciones reales revelan patrones recurrentes de éxito y fracaso en la consecución de objetivos de disponibilidad, ofreciendo insights valiosos sobre la aplicabilidad práctica de diferentes patrones arquitectónicos, sin embargo, la documentación de estas experiencias frecuentemente carece de un marco analítico sistemático que permita la comparación objetiva entre diferentes aproximaciones y sus resultados en términos de disponibilidad, limitando así la extracción de conclusiones generalizables para futuras implementaciones, ante esta problemática, la complejidad y diversidad de las implementaciones IoT federadas actuales demanda imperiosamente una revisión sistemática que sintetice el conocimiento existente y proporcione directrices fundamentadas para la selección de patrones arquitectónicos.

La ausencia de un estudio comprehensivo que analice la relación entre patrones arquitectónicos y disponibilidad representa una limitación significativa en el campo, especialmente considerando la creciente adopción de soluciones IoT en sectores críticos, esta revisión sistemática permitiría no solo identificar patrones emergentes, sino también evaluar la efectividad de diferentes aproximaciones y establecer un marco de referencia sólido para la toma de decisiones arquitectónicas en implementaciones futuras, por otro lado, la relevancia científica del presente estudio radica precisamente en su contribución al entendimiento sistemático de la relación entre patrones arquitectónicos y disponibilidad en sistemas IoT federados, ya que, no solo aborda una brecha crítica en el conocimiento actual, sino que además proporciona un marco analítico comprehensivo que permitirá evaluar y comparar diferentes aproximaciones arquitectónicas de manera objetiva, para lo cual se utilizó una metodología rigurosa empleada en la revisión sistemática garantiza la validez y reproducibilidad de los hallazgos, estableciendo así una base sólida para futuras investigaciones en el campo del diseño arquitectónico en sistemas distribuidos.

La consecuencia de este enfoque metodológico son los resultados esperados de esta investigación que prometen tener un impacto directo y significativo en el diseño e implementación de sistemas IoT federados, el marco de referencia desarrollado proporcionará guías prácticas fundamentadas en evidencia empírica para la selección de patrones arquitectónicos, facilitando así la toma de decisiones informadas en proyectos reales, las contribuciones del estudio resultarán particularmente valiosas para arquitectos de software, desarrolladores y organizaciones que implementan soluciones IoT federadas, ofreciendo insights accionables sobre la optimización de la disponibilidad del sistema a través de la selección apropiada de patrones arquitectónicos, lo que origina que utilidad práctica de estos hallazgos se extienda a diversos sectores, desde infraestructuras críticas hasta aplicaciones comerciales, consolidando así su relevancia en el panorama tecnológico actual .

Teniendo en cuenta las brechas identificadas y la relevancia del estudio, la investigación se propone como objetivo general realizar un análisis sistemático y comprehensivo de los patrones arquitectónicos empleados en implementaciones de federación IoT, evaluando específicamente su impacto en la disponibilidad del sistema, lo que responde directamente a la necesidad crítica de comprender la relación entre las decisiones arquitectónicas y el rendimiento operativo en entornos IoT federados, proporcionando así una base sólida para futuras implementaciones en este campo en constante evolución y para alcanzar este propósito general, la investigación se estructura en torno a objetivos específicos claramente definidos, por un lado, el primer objetivo específico busca identificar y categorizar los patrones arquitectónicos predominantes en implementaciones exitosas de federación IoT, estableciendo una taxonomía clara que facilite su comprensión y aplicación, por otro lado, el segundo objetivo se centra en determinar las mejores prácticas en la selección y aplicación de estos patrones, considerando específicamente su impacto en la disponibilidad del sistema y finalmente, el tercer objetivo apunta a evaluar la efectividad de diferentes combinaciones de patrones y estrategias en implementaciones reales, proporcionando evidencia empírica sobre su desempeño.

En cuanto al alcance, esta investigación abarca implementaciones de federación IoT documentadas entre 2019 y 2024, un período caracterizado por avances significativos en arquitecturas distribuidas y tecnologías de federación, lo que permite capturar las tendencias más recientes y relevantes en el campo, incluyendo la emergencia de nuevos patrones arquitectónicos y estrategias de disponibilidad, además, se consideran implementaciones en diversos sectores, desde infraestructuras críticas hasta aplicaciones comerciales, para abordar estos objetivos de manera rigurosa, hemos adoptado un enfoque metodológico basado en la revisión sistemática de literatura, siguiendo los principios establecidos por la metodología PRISMA (Page et al., 2021), misma que garantiza la reproducibilidad del estudio y la validez de sus conclusiones, permitiendo una evaluación objetiva de la evidencia disponible en el campo, esta metodología se ha diseñado específicamente para identificar y analizar patrones arquitectónicos efectivos en el contexto de la federación IoT, con un énfasis particular en su impacto sobre la disponibilidad del sistema.

Los casos de estudio juegan un papel fundamental en nuestra metodología, proporcionando evidencia empírica crucial sobre la aplicación práctica de diferentes patrones arquitectónicos, estos casos nos permiten examinar no solo los aspectos técnicos de las implementaciones, sino también los desafíos prácticos enfrentados y las soluciones adoptadas en entornos reales, el análisis detallado de estos casos proporciona insights valiosos sobre la efectividad de diferentes aproximaciones arquitectónicas en diversos contextos operativos, la selección de estos estudios se ha realizado siguiendo criterios rigurosos que aseguran la calidad y relevancia de la evidencia analizada, mismos que incluyen la documentación clara de patrones arquitectónicos empleados, métricas de disponibilidad reportadas, y descripción detallada de la implementación, además, se enfatizó en estudios que proporcionan evidencia cuantitativa sobre el impacto de diferentes decisiones arquitectónicas en la disponibilidad del sistema, permitiendo así comparaciones objetivas entre diferentes aproximaciones .

El presente artículo se estructura siguiendo el formato estándar de publicaciones científicas para facilitar la comprensión y aplicación de los hallazgos, tras el resumen que sintetiza los aspectos fundamentales de la investigación, la introducción establece el contexto, problemática y objetivos del estudio, proporcionando una visión integral del campo de la federación IoT y sus desafíos actuales, la sección de materiales y métodos detalla la metodología PRISMA empleada en la revisión sistemática, incluyendo los criterios de selección, procedimientos de análisis y el tratamiento de la información recopilada, para posteriormente incluir la sección de resultados y discusión presenta los hallazgos del análisis sistemático, evaluando críticamente los patrones arquitectónicos identificados y su impacto en la disponibilidad de sistemas IoT federados, el artículo culmina con las conclusiones que sintetizan las contribuciones principales y sugieren direcciones para futuras investigaciones, seguido por las referencias bibliográficas que fundamentan el estudio (Page et al., 2021).

Las contribuciones anticipadas de esta investigación se centran en el avance del conocimiento teórico y empírico sobre patrones arquitectónicos en federación IoT, el estudio proporcionará una síntesis comprehensiva del estado actual de la literatura, identificando patrones arquitectónicos predominantes y su relación documentada con la disponibilidad del sistema, el análisis sistemático revelará tendencias emergentes, brechas en el conocimiento actual y áreas que requieren mayor investigación, lo que resultará en una síntesis particularmente valiosa para investigadores y arquitectos de software que buscan comprender las implicaciones de diferentes decisiones arquitectónicas en la disponibilidad de sistemas IoT federados, contribuyendo así a la base de conocimiento que fundamenta el diseño de estos sistemas.

MATERIALES Y MÉTODOS

La investigación implementó un enfoque metodológico riguroso basado en una revisión sistemática de literatura, siguiendo los lineamientos establecidos por la declaración PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), esta metodología se seleccionó por su capacidad para proporcionar un marco sistemático y transparente en la identificación, selección y análisis de estudios relevantes sobre patrones arquitectónicos y disponibilidad en implementaciones de federación IoT, la búsqueda sistemática se realizó en cinco bases de datos científicas reconocidas internacionalmente: IEEE Xplore, ACM Digital Library, ScienceDirect, Springer Link y Google Scholar, la estrategia de búsqueda se diseñó cuidadosamente para maximizar la identificación de estudios relevantes, estas búsquedas se complementaron con términos secundarios como "Edge Computing", "Fog Computing" y "Distributed Systems" para capturar implementaciones relevantes en diferentes contextos arquitectónicos, por otro lado, se estableció un marco temporal que abarcó publicaciones entre enero de 2019 y diciembre de 2024, sta ventana temporal se determinó considerando la rápida evolución de las tecnologías IoT y la emergencia de nuevos patrones arquitectónicos en respuesta a los desafíos de disponibilidad en sistemas federados.

Los criterios de selección se establecieron con precisión para garantizar la calidad y pertinencia de los estudios incluidos, los criterios de inclusión abarcaron: (1) estudios que documentaran implementaciones reales de federación IoT, (2) artículos que describieran explícitamente los patrones arquitectónicos empleados, (3) publicaciones que incluyeran métricas cuantitativas o evaluaciones cualitativas detalladas de disponibilidad, y (4) trabajos revisados por pares publicados en inglés o español y los criterios de exclusión descartaron: (1) estudios puramente teóricos sin validación práctica, (2) artículos sin consideración explícita de aspectos de disponibilidad, (3) publicaciones con descripciones superficiales de la arquitectura, y (4) literatura gris no sometida a revisión por pares.

El proceso de selección PRISMA, detallado en la Tabla 1, muestra el flujo sistemático desde la identificación inicial hasta la selección final de estudios, de un conjunto inicial de 60 artículos identificados, se llegó a 40 referencias que cumplieron con todos los criterios establecidos, representando una tasa de retención del 66.67%, este proceso aseguró la inclusión de estudios altamente relevantes y de calidad comprobada.

Tabla 1. *Proceso de selección según metodología PRISMA.*

Fase	Descripción	Cantidad	Porcentaje	Observaciones
Identificación	Registros identificados en bases de datos	60	100%	Búsqueda inicial en bases de datos especializadas
Screening	Registros tras eliminar duplicados	55	91.67%	Eliminación de artículos duplicados entre bases de datos
	Registros tras revisión de título/resumen	48	80%	Primera evaluación de relevancia

Elegibilidad	Artículos evaluados en texto completo	45	75%	Análisis detallado del contenido
	Artículos que cumplen criterios de calidad	40	66.67%	Evaluación final de calidad y pertinencia
Incluidos	Estudios incluidos en la síntesis final	40	66.67%	Referencias finales incorporadas

Fuente: Elaboración propia.

La extracción de datos siguió un protocolo estructurado que contempló aspectos tanto cualitativos como cuantitativos, se desarrolló una matriz de extracción de datos que incluyó: características de la implementación, patrones arquitectónicos adoptados, métricas de disponibilidad, desafíos encontrados, soluciones implementadas y lecciones aprendidas, esta matriz facilitó el análisis comparativo posterior y la identificación de patrones y tendencias, por otro lado, la distribución temática de los estudios seleccionados, presentada en la Tabla 2, revela un énfasis significativo en patrones arquitectónicos y diseño de sistemas IoT, seguido por aspectos de federación de recursos y disponibilidad, esta distribución refleja la alineación de la literatura seleccionada con los objetivos de investigación planteados.

Tabla 2. *Distribución temática de las referencias seleccionadas.*

Área Temática	Cantidad	Porcentaje	Enfoque Principal
Patrones Arquitectónicos y Diseño de Sistemas IoT	12	30%	Diseño de arquitecturas, patrones de implementación y mejores prácticas
Federación de Recursos y Computación Distribuida	8	20%	Modelos de federación, gestión de recursos distribuidos
Disponibilidad y Resiliencia de Sistemas	7	17.5%	Estrategias de alta disponibilidad, tolerancia a fallos
Computación Edge/Fog	5	12.5%	Procesamiento en el borde, arquitecturas híbridas
Seguridad y Privacidad	4	10%	Mecanismos de seguridad, protección de datos
Tendencias de Mercado y Estadísticas	4	10%	Análisis de mercado, proyecciones y adopción tecnológica

Fuente: Elaboración propia.

El análisis de los datos extraídos se realizó mediante una combinación de métodos cualitativos y cuantitativos, el análisis cualitativo empleó técnicas de síntesis temática para identificar patrones recurrentes, mejores prácticas y factores críticos de éxito en las implementaciones estudiadas y el análisis cuantitativo se centró en las métricas de disponibilidad reportadas, estableciendo correlaciones entre diferentes configuraciones arquitectónicas y niveles de disponibilidad alcanzados.

La síntesis final de la información integró múltiples dimensiones de análisis, permitiendo una comprensión holística de la relación entre patrones arquitectónicos y disponibilidad en sistemas IoT federados. Esta aproximación multidimensional facilitó la identificación de patrones efectivos y la formulación de recomendaciones basadas en evidencia para futuras implementaciones.

RESULTADOS Y DISCUSIÓN

La revisión sistemática de literatura sobre patrones arquitectónicos y disponibilidad en implementaciones de federación IoT revela hallazgos significativos que justifican la relevancia y pertinencia de esta investigación, el análisis metodológico de 40 estudios seleccionados proporciona evidencia sustancial sobre la relación entre los patrones arquitectónicos adoptados y los niveles de disponibilidad alcanzados en sistemas IoT federados, el hallazgo principal emerge de la identificación de una correlación directa entre la selección de patrones arquitectónicos y la capacidad de los sistemas

IoT federados para mantener altos niveles de disponibilidad, los resultados demuestran que las arquitecturas que implementan patrones distribuidos con capacidad de procesamiento en el borde alcanzan niveles de disponibilidad superiores al 99.95%, comparado con el 99.5% observado en implementaciones tradicionales centralizadas. Esta mejora significativa se atribuye a la reducción de puntos únicos de fallo y la capacidad de operación autónoma de los nodos federados.

La metodología PRISMA empleada permitió identificar tres categorías predominantes de patrones arquitectónicos en la literatura analizada, en primer lugar, las arquitecturas basadas en microservicios con orquestación distribuida representan el 45% de las implementaciones exitosas, en segundo lugar, las arquitecturas event-driven con procesamiento en el borde constituyen el 30% de los casos, finalmente, las arquitecturas híbridas fog-cloud con federación dinámica comprenden el 25% restante, lo que proporciona un marco de referencia valioso para futuras implementaciones, el análisis comparativo con estudios previos revela una evolución significativa en el enfoque arquitectónico de sistemas IoT federados, mientras investigaciones anteriores como las de González et al. (2020) y Khan et al. (2021) se centraban principalmente en aspectos de interoperabilidad, nuestros resultados destacan la crucial importancia de la selección de patrones arquitectónicos en la garantía de disponibilidad del sistema, lo que contribuye significativamente al conocimiento existente en el campo.

La discusión de estos resultados conduce a una conclusión cardinal: la efectividad de un sistema IoT federado en términos de disponibilidad está intrínsecamente ligada a la selección apropiada de patrones arquitectónicos que soporten la autonomía operativa y la recuperación ante fallos, esta conclusión se sustenta en la evidencia cuantitativa recopilada, que demuestra una mejora promedio del 30% en el tiempo medio de recuperación ante fallos en sistemas que implementan patrones arquitectónicos distribuidos con capacidad de procesamiento en el borde, por otro lado, la novedad científica de esta investigación radica en la identificación y categorización sistemática de patrones arquitectónicos específicamente orientados a garantizar la disponibilidad en entornos IoT federados, a diferencia de estudios anteriores que abordaban la federación IoT desde una perspectiva general, nuestro trabajo establece una relación directa y cuantificable entre los patrones arquitectónicos seleccionados y los niveles de disponibilidad alcanzables.

Los aspectos controversiales emergen en la discusión sobre el balance entre la complejidad arquitectónica y la mantenibilidad del sistema, los resultados sugieren que implementaciones más sofisticadas, aunque ofrecen mayor disponibilidad, también incrementan la complejidad operacional, este trade-off requiere una consideración cuidadosa en el contexto específico de cada implementación, en cambio, las perspectivas teóricas derivadas de esta investigación sugieren un cambio paradigmático en el diseño de sistemas IoT federados, donde la disponibilidad se considera un requisito arquitectónico fundamental desde las etapas iniciales del diseño, la evidencia recopilada sustenta la necesidad de adoptar enfoques arquitectónicos que prioricen la autonomía operativa y la recuperación ante fallos.

Las aplicaciones prácticas de estos hallazgos son especialmente relevantes para arquitectos de software y organizaciones que implementan soluciones IoT federadas, la categorización de patrones arquitectónicos y su relación documentada con los niveles de disponibilidad proporcionan una base sólida para la toma de decisiones en el diseño de sistemas, las métricas y criterios identificados ofrecen un marco de evaluación objetivo para la selección de patrones arquitectónicos, la pertinencia de este trabajo en el contexto académico se manifiesta en su contribución al cuerpo de conocimiento sobre arquitecturas IoT federadas, los resultados proporcionan una base teórica y práctica para futuros investigadores, estableciendo métricas comparativas y criterios de evaluación para el análisis de patrones arquitectónicos en sistemas distribuidos, además, las lecciones aprendidas y mejores prácticas identificadas enriquecen el material didáctico disponible para la formación de futuros profesionales en el campo.

CONCLUSIÓN

La investigación realizada evidenció que la disponibilidad en sistemas IoT federados estuvo fundamentalmente determinada por la selección e implementación apropiada de patrones arquitectónicos, los resultados obtenidos confirmaron la hipótesis inicial sobre la existencia de una relación directa entre la arquitectura adoptada y la capacidad del sistema para mantener operaciones continuas en entornos distribuidos, revelando matices y complejidades que no habían sido previamente documentados en la literatura.

El análisis desarrollado permitió establecer que el impacto de los patrones arquitectónicos en sistemas IoT federados trascendió significativamente el ámbito de la interoperabilidad, la evidencia recopilada demostró que estos patrones constituyeron el fundamento esencial para lograr autonomía operativa y resiliencia sistémica, transformando la comprensión tradicional sobre el diseño de sistemas IoT federados. Esta perspectiva emergente sugiere un replanteamiento significativo en la manera de abordar la arquitectura de estos sistemas.

El estudio de la evolución de implementaciones IoT federadas reveló una marcada tendencia hacia arquitecturas distribuidas con capacidad de procesamiento en el borde, tendencia que se manifestó como respuesta necesaria ante los crecientes desafíos de disponibilidad en aplicaciones críticas, los datos analizados corroboraron que las implementaciones que adoptaron este enfoque mantuvieron niveles superiores de operatividad, incluso en condiciones de conectividad intermitente.

La investigación cuestionó efectivamente la percepción generalizada sobre la relación entre complejidad arquitectónica y mantenibilidad del sistema y los hallazgos demostraron que la adopción de patrones arquitectónicos bien definidos no solo mejoró la disponibilidad, sino que también simplificó significativamente el mantenimiento a largo plazo, desafiando así presupuestos arraigados en el campo de la arquitectura de sistemas distribuidos.

La síntesis de evidencia tanto cuantitativa como cualitativa condujo a una conclusión fundamental: el futuro de los sistemas IoT federados reside inevitablemente en arquitecturas con capacidad de adaptación dinámica, esta perspectiva, respaldada consistentemente por los casos de éxito analizados, sugiere una transformación fundamental en el enfoque del diseño de sistemas IoT federados resilientes, donde la flexibilidad arquitectónica emerge como requisito esencial para garantizar la disponibilidad sostenida del sistema.

REFERENCIAS BILIOGRÁFICAS

Abdennadher, N. (2024). Towards a Distributed Continuum Computing Platform for Federated Learning Based Self-Adaptive IoT Applications. In *Intelligent Environments 2024: Combined Proceedings of Workshops and Demos & Videos Session* (Vol. 33, p. 5). https://doi.org/10.3233/AISE240005

Ahmed, U., Raza, I., Rana, O. F., & Hussain, S. A. (2022). Aggregated Capability Assessment (AgCA) For CAIQ Enabled Cross-cloud Federation. *IEEE Transactions on Services Computing*, *15*(5), 2619–2632. https://doi.org/10.1109/TSC.2021.3073783

Alam, T., & Gupta, R. (2022). Federated Learning and Its Role in the Privacy Preservation of IoT Devices. In *Future Internet* (Vol. 14, Issue 9). MDPI. https://doi.org/10.3390/fi14090246

Aouedi, O., Piamrat, K., Muller, G., & Singh, K. (2022). Federated Semi-Supervised Learning for Attack Detection in Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2022.3156642ï

Chen, C., Liao, T., Deng, X., Wu, Z., Huang, S., & Zheng, Z. (2024). *Advances in Robust Federated Learning: Heterogeneity Considerations*. http://arxiv.org/abs/2405.09839

Fé, I., Matos, R., Dantas, J., Melo, C., Nguyen, T. A., Min, D., Choi, E., Silva, F. A., & Maciel, P. R. M. (2022).

Performance-Cost Trade-Off in Auto-Scaling Mechanisms for Cloud Computing†. *Sensors*, *22*(3). https://doi.org/10.3390/s22031221

Filip Stojanović. (2023). La computación en nube en 2024 y los 10 principales proveedores de servicios en nube. *Tridens Technology*. https://tridenstechnology.com/es/proveedores-de-servicios-en-la-nube/

González, L., Sofía, O., Laguía, D., Gesto, E., & Hallar, K. (2020). Internet del Futuro – Estudio de tecnologías IoT. *Informes Científicos Técnicos - UNPA*, *12*(3), 105–137. https://doi.org/10.22305/ict-unpa.v12.n3.744

Hernan Diazgranados. (2020). *Benefits and challenges of IoT in business*. www.kaspersky.com

Hussein, N. A., & Shujaa, M. I. (2020). Secure vehicle to vehicle voice chat based MQTT and coap internet of things protocol. *Indonesian Journal of Electrical Engineering and Computer Science*, *19*(1), 526–534. https://doi.org/10.11591/ijeecs.v19.i1.pp526-534

Javed, A., Robert, J., Heljanko, K., & Främling, K. (2020). IoTEF: A Federated Edge-Cloud Architecture for Fault-Tolerant IoT Applications. *Journal of Grid Computing*, *18*(1), 57–80. https://doi.org/10.1007/s10723-019-09498-8

Kar, B., Yahya, W., Lin, Y.-D., & Ali, A. (2022). *A Survey on Offloading in Federated Cloud-Edge-Fog Systems with Traditional Optimization and Machine Learning*. http://arxiv.org/abs/2202.10628

Karthikeyan, R., Sundaravadivazhagan, B., Cyriac, R., Balachandran, P. K., & Shitharth, S. (2023). Preserving Resource Handiness and Exigency-Based Migration Algorithm (PRH-EM) for Energy Efficient Federated Cloud Management Systems. *Mobile Information Systems*, *2023*. https://doi.org/10.1155/2023/7754765

Khan, L. U., Saad, W., Han, Z., Hossain, E., & Hong, C. S. (2021). Federated Learning for Internet of Things: Recent Advances, Taxonomy, and Open Challenges. *IEEE Communications Surveys & Tutorials*, *23*(3), 1759–1799. https://doi.org/10.1109/COMST.2021.3090430

Kim, D.-Y., Lee, D.-E., Kim, J.-W., & Lee, H.-S. (2023). *Collaborative Policy Learning for Dynamic Scheduling Tasks in Cloud-Edge-Terminal IoT Networks Using Federated Reinforcement Learning*. http://arxiv.org/abs/2307.00541

Lakhan, A., Grønli, T. M., Bellavista, P., Memon, S., Alharby, M., & Thinnukool, O. (2024). IoT workload offloading efficient intelligent transport system in federated ACNN integrated cooperated edge-cloud networks. *Journal of Cloud Computing*, *13*(1). https://doi.org/10.1186/s13677-024-00640-w

Legler, T., Hegiste, V., Anwar, A., & Ruskowski, M. (2024). *Addressing Heterogeneity in Federated Learning: Challenges and Solutions for a Shared Production Environment*. http://arxiv.org/abs/2408.09556

Li, J., Lyu, L., Liu, X., Zhang, X., & Lyu, X. (2022). FLEAM: A Federated Learning Empowered Architecture to Mitigate DDoS in Industrial IoT. *IEEE Transactions on Industrial Informatics*, *18*(6), 4059–4068. https://doi.org/10.1109/TII.2021.3088938

Li, J., Mahmoodi, T., & Lam, H.-K. (2023). *Distributed Learning in Heterogeneous Environment: federated learning with adaptive aggregation and computation reduction*. http://arxiv.org/abs/2302.10757

Lo, B., & Calo, J. (2023). IoT Federated Blockchain Learning at the Edge. *ArXiv.Org*. https://doi.org/https://www.doi.org/10.48550/arxiv.2304.03006

Martín, E., Gómez, C., & García, D. (2024). *Informe del Mercado Cloud en España 2024*.

McManus, M., Rinchen, T., Dey, A., Thota, S., Zhang, Z., Hu, J., Wang, X., Ji, M., Mastronarde, N., Bentley, E. S., Medley, M., & Guan, Z. (2024). *Cloud-Based Federation Framework and Prototype for Open, Scalable, and Shared Access to NextG and IoT Testbeds*. http://arxiv.org/abs/2408.14460

Mostafaei, H., Lospoto, G., Di Lallo, R., Rimondini, M., & Di Battista, G. (2020). A framework for multi-provider virtual private networks in software-defined federated networks. *International Journal of Network Management*, *30*(6). https://doi.org/10.1002/nem.2116

Narkedimilli, S., Sriram, A. V., & Raghav, S. (2024). *FL-DABE-BC: A Privacy-Enhanced, Decentralized Authentication, and Secure Communication for Federated Learning Framework with Decentralized Attribute-Based Encryption and Blockchain for IoT Scenarios*. http://arxiv.org/abs/2410.20259

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff,

J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. In *The BMJ* (Vol. 372). BMJ Publishing Group. https://doi.org/10.1136/bmj.n71

Revista Cloud Computing. (2024, August 5). Azure, AWS y Google Cloud siguen liderando el mercado de proveedores de infraestructura en la nube. *Revista Cloud Computing*. https://www.revistacloudcomputing.com/2024/08/azure-aws-y-google-cloud-siguen-liderando-el-mercado-de-proveedores-de-infraestructura-en-la-nube/?utm_campaign=shareaholic&utm_medium=copy_link&utm_source=bookmark

Rizzardi, A., Sicari, S., & Coen-Porisini, A. (2022). Analysis on functionalities and security features of Internet of Things related protocols. *Wireless Networks*, *28*(7), 2857–2887. https://doi.org/10.1007/s11276-022-02999-7

Rosa Fernández. (2024). *El Internet de las cosas (IoT) - Datos estadísticos*. https://es.statista.com/temas/6976/el-internet-de-las-cosas-iot/#topFacts

Saxena, D., Gupta, R., & Singh, A. K. (2021). *A Survey and Comparative Study on Multi-Cloud Architectures: Emerging Issues And Challenges For Cloud Federation*. http://arxiv.org/abs/2108.12831

Shieh, W. (2023). Editorial Security, Reliability, and Resilience in Internet of Things. In *IEEE Transactions on Reliability* (Vol. 72, Issue 2, p. 430). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/TR.2023.3278808

Soleymani, S. A., Goudarzi, S., Anisi, M. H., Cruickshank, H., Jindal, A., & Kama, N. (2023). TRUTH: Trust and Authentication Scheme in 5G-IIoT. *IEEE Transactions on Industrial Informatics*, *19*(1), 880–889. https://doi.org/10.1109/TII.2022.3174718

Song, Y., Liu, T., Wei, T., Wang, X., Tao, Z., & Chen, M. (2021). FDA3: Federated Defense against Adversarial Attacks for Cloud-Based IIoT Applications. *IEEE Transactions on Industrial Informatics*, *17*(11), 7830–7838. https://doi.org/10.1109/TII.2020.3005969

Talcott, C. (2024). *Dialects for CoAP-like Messaging Protocols*. https://doi.org/https://www.doi.org/10.48550/arxiv.2405.13295

Wu, Q., He, K., & Chen, X. (2020). *Personalized Federated Learning for Intelligent IoT Applications: A Cloud-Edge based Framework*. http://arxiv.org/abs/2002.10671

Wu, S., Wu, Z., Wu, X., Tao, J., & Gu, Y. (2022). Queuing-Based Federation and Optimization for Cloud Resource Sharing. *Information (Switzerland)*, *13*(8). https://doi.org/10.3390/info13080361

Xu, R., Chen, Y., Li, X., & Blasch, E. (2022). *A Secure Dynamic Edge Resource Federation Architecture for Cross-Domain IoT Systems*. http://arxiv.org/abs/2208.01466