# Arquitetura Distribuída de Multisensoriamento com ESP32 e MQTT para Monitoramento Inteligente de Data Centers

**Danilo Silva Ramos**[1], **Analucia Schiaffino Morales**[2], **Iwens Gervasio Sene Junior**[1]

[1] Instituto de Informática – Universidade Federal de Goiás (UFG)

[2]Universidade Federal de Santa Catarina (UFSC)

danilo.ramos@ufg.br, analucia.morales@ufsc.br, iwens@ufg.br

***Abstract.*** *A distributed multisensing architecture is proposed for data center monitoring, using autonomous nodes based on ESP32 and MQTT communication with a remote broker. The sensors monitor environmental variables through hierarchical transmission and fault tolerance via local buffers. Configuration is performed via Bluetooth, and the data is integrated into a backend composed of time-series databases and interactive dashboards. The solution provides smart notifications and is designed with a focus on scalability and modularity. Simulated initial tests validate its technical feasibility and indicate strong potential for real-world applications and future incorporation of machine learning techniques for calibration and anomaly detection, as well as functionalities such as physical sensor modularity and over-the-air (OTA) firmware updates.*

***Resumo.*** *Uma arquitetura distribuída de multissensoriamento é proposta para monitoramento de data centers, utilizando nós autônomos baseados em ESP32 e comunicação via MQTT com um broker remoto. Os sensores monitoram variáveis ambientais com transmissão hierárquica e tolerância a falhas por meio de buffers locais. A configuração é realizada via Bluetooth, e os dados são integrados a um backend composto por banco de dados temporais e dashboards interativos. A solução oferece notificações inteligentes, sendo projetada com foco em escalabilidade e modularidade. Testes iniciais simulados validam sua viabilidade técnica e indicam forte potencial para aplicações reais e incorporação futura de técnicas de aprendizado de máquina na calibração e detecção de anomalias. E funcionalidades, como a modularidade física dos sensores e a atualização remota de firmware (OTA).*

## 1. Introdução

Ambientes computacionais críticos, como data centers e salas de servidores, demandam soluções de monitoramento ambiental altamente confiáveis para garantir a continuidade operacional e evitar danos causados por falhas térmicas, instabilidades elétricas ou deterioração da qualidade do ar [TIA 2005, ISO/IEC 2013]. A detecção precoce de anomalias nesses ambientes é fundamental para prevenir interrupções e minimizar prejuízos operacionais.

Nos últimos anos, a adoção de sistemas distribuídos de sensoriamento baseados em dispositivos de baixo custo, como ESP32 e ESP8266, tornou-se uma alternativa viável e eficaz para monitoramento contínuo e granular em ambientes de missão

crítica [Bisignano et al. 2022]. Estruturas segmentadas favorecem a redundância espacial e a resiliência operacional, especialmente quando associadas a arquiteturas tolerantes a falhas que evitam pontos únicos de falha e permitem recuperação distribuída [Grover and Garimella 2018].

Este trabalho propõe um sistema de monitoramento distribuído, modular e escalável, utilizando sensores conectados via MQTT e integrados a um pipeline de coleta e visualização com Telegraf, InfluxDB e Grafana. Cada nó sensor é responsável por um setor do ambiente e opera com armazenamento local para garantir envio posterior em caso de falhas temporárias de conexão.

A adoção de microcontroladores com conectividade de rede tem se mostrado eficiente para aplicações de monitoramento ambiental e industrial, com destaque para o protocolo MQTT devido à sua leveza e confiabilidade em redes com recursos limitados[Hasan and Alhusainy 2018, Cherradi et al. 2016, Corak et al. 2018]. Além disso, o modelo publish/subscribe proporciona escalabilidade e facilita a integração com outras plataformas [Seoane et al. 2021, Vieira et al. 2024].

A proposta foca na escalabilidade e na flexibilidade da arquitetura, permitindo a adição dinâmica de novos nós e a replicação de medições em setores críticos. Essa abordagem favorece maior resiliência e tolerancia a falhas e simplifica a manutenção da infraestrutura monitorada, em linha com princípios de arquiteturas distribuídas tolerantes a falhas [Grover and Garimella 2018]

A solução tem potencial para elevar o padrão de monitoramento em ambientes computacionais críticos, oferecendo maior confiabilidade, agilidade na resposta a eventos e redução da necessidade de intervenções manuais frequentes. A flexibilidade do sistema também abre possibilidades futuras de integração com técnicas de aprendizado de máquina para calibração automática e detecção de anomalias, como explorado por [Bisignano et al. 2022, Russell et al. 2022].

Este trabalho se diferencia por integrar em uma única solução funcionalidades como modularidade física dos sensores, comunicação MQTT segura, integração com bancos temporais, previsão de atualização OTA e possibilidade de inteligência na borda, embora algumas dessas funcionalidades ainda estejam em fase de implementação. Estas características, somadas à ênfase em tolerância a falhas e notificações inteligentes, contribuem diretamente para uma arquitetura robusta, escalável para monitoramento de data centers.

## 2. Trabalhos Relacionados

Trabalhos como o de Grover e Garimella [Grover and Garimella 2018] discutem arquiteturas IoT com foco em resiliência e tolerância a falhas, destacando a importância da reconfiguração dinâmica de nós e da flexibilidade arquitetural para manter a continuidade do serviço em ambientes distribuídos.

Quanto aos protocolos de comunicação, Hasan [Hasan and Alhusainy 2018] e Seoane et al. [Seoane et al. 2021] avaliam o desempenho e a segurança do MQTT em ambientes IoT, validando sua escolha para sistemas distribuídos com recursos computacionais limitados. Vieira et al. [Vieira et al. 2024] complementam essa análise com estudos de eficiência energética, reforçando a adequação do protocolo para aplicações de monitora-

mento contínuo.

A coleta de dados e o uso de bancos de dados temporais também têm sido amplamente discutidos. [Grzesik and Mrozek 2020] analisam diferentes bancos de dados de séries temporais no contexto de computação de borda, enquanto Cherradi et al. [Cherradi et al. 2016] propõem modelos eficientes de ingestão de dados em redes sensoriais.

Por fim, destaca-se o uso de técnicas de aprendizado de máquina na calibração e detecção de anomalias. [Bisignano et al. 2022] e [Russell et al. 2022] mostram o potencial de modelos leves para calibrar sensores de baixo custo e melhorar a confiabilidade de medições ambientais.

As soluções relacionadas apresentam contribuições relevantes, mas cobrem apenas partes isoladas dos desafios enfrentados em ambientes críticos como data centers. [Grover and Garimella 2018], por exemplo, abordam aspectos de resiliência e tolerância a falhas em arquiteturas distribuídas, mas não tratam de modularidade física nem de integração com bancos de séries temporais. Já [Hasan and Alhusainy 2018] e [Seoane et al. 2021] focam na avaliação de protocolos de comunicação, como MQTT e CoAP, sem propor arquiteturas completas de monitoramento. As contribuições de [Bisignano et al. 2022] se destaca na calibração de sensores e aplicação de inteligência embarcada, porém não abordam comunicação distribuída nem estruturação de backend para coleta e análise contínua. Em contraste, a arquitetura proposta neste trabalho integra múltiplos aspectos em uma única solução: comunicação escalável baseada em MQTT, modularidade física prevista nos nós sensores, backend com bancos de séries temporais, e previsão de algoritmos de inteligência artificial embarcada — todos voltados à robustez e flexibilidade exigidas em data centers. Uma visão comparativa dessas características em relação às soluções existentes está resumida na Tabela 1

**Tabela 1. Comparação da arquitetura proposta com trabalhos relacionados**

| **Características** | **Proposta** | **Grover (2018)** | **Hasan (2018)** | **Bisignano (2022)** |
|---|---|---|---|---|
| Modularidade física | Prevista | Não | Não | Não |
| Comunicação MQTT | Sim | Parcial | Sim | Não |
| Banco temporal | Sim | Não | Não | Não |
| Atualização OTA | Prevista | Não | Não | Não |
| Edge Intelligence | Prevista | Parcial | Não | Sim |
| Tolerância a falhas | Sim | Sim | Não | Parcial |

## 3. Arquitetura do Sistema

A arquitetura proposta baseia-se na implementação de nós de sensoriamento autônomos, distribuídos estrategicamente pelo ambiente monitorado. Cada setor ou rack do data center pode contar com uma ou mais unidades dedicadas, otimizando a granularidade da coleta de dados e permitindo cobertura redundante em áreas críticas. Adota-se uma abordagem hierárquica com dois níveis de nós: as unidades de sensores e as unidades agregadoras, com o objetivo de reduzir a sobrecarga da rede e do servidor de destino.

Cada zona monitorada pode contar com uma ou mais unidades de sensoriamento, que operam de forma autônoma e são equipadas com sensores modulares para monitorar

variáveis como temperatura, umidade, pressão, presença de gases, vibração e consumo elétrico dos servidores. Essas unidades são projetadas com conectores destacáveis, o que permite rápida manutenção e reconfiguração. A configuração inicial é feita por meio de uma interface local (bluetooth), sem necessidade de reprogramação manual dos dispositivos [Al-Shareeda et al. 2023].

A comunicação entre as unidades agregadoras e o servidor central segue o modelo publish/subscribe, utilizando o protocolo MQTT com autenticação e criptografia via TLS. O broker MQTT realiza a orquestração das mensagens e deve ser leve e escalável, mesmo em ambientes com alta densidade de sensores [Hasan and Alhusainy 2018, Seoane et al. 2021]. As mensagens são transmitidas em formato JSON, organizadas por tópicos hierárquicos que identificam de forma única cada unidade e sensor, facilitando o roteamento seletivo e o mapeamento com a estrutura física monitorada.

No backend, os dados são processados e armazenados em um banco de dados temporal, por meio de um serviço de intermediação que escuta os dados no broker, realiza eventuais tratamentos e os grava no banco. A escolha por bancos de séries temporais se justifica pela necessidade de análises contínuas, geração de alertas por limiares e construção de dashboards interativos [Grzesik and Mrozek 2020]. Essa estrutura também viabiliza a integração com técnicas de aprendizado de máquina para calibração automática dos sensores, detecção de anomalias e predição de falhas com base em padrões históricos [Cherradi et al. 2016, Grzesik and Mrozek 2020, Bisignano et al. 2022].

A configuração inicial de cada nó é feita via Bluetooth utilizando um aplicativo móvel, permitindo o cadastro de parâmetros como a rede Wi-Fi, modo de operação, autenticação no broker, sensores ativos e seus respectivos limites operacionais. Essa abordagem reduz significativamente o tempo de instalação e simplifica o processo de inicialização dos nós, sendo amplamente adotada em soluções IoT por sua flexibilidade e facilidade de uso [Al-Shareeda et al. 2023].

O sistema incorpora um módulo de notificações inteligentes que classifica os alertas por nível de criticidade e os distribui por múltiplos canais — como e-mail, notificações push ou alarmes sonoros — além de registrá-los no banco de dados. Eventos críticos são direcionados para dispositivos móveis via serviços como o Pushover, garantindo alta taxa de entrega e baixa latência de resposta mesmo em condições adversas da infraestrutura [Mehrotra and Musolesi 2017]

A arquitetura proposta incorpora mecanismos complementares para tolerância a falhas: armazenamento temporário em buffer persistente, redundância de comunicação via redes móveis nas unidades agregadoras e validação cruzada por sensores redundantes em setores críticos. Essas estratégias visam garantir a continuidade da coleta e transmissão mesmo sob falhas transitórias, em conformidade com princípios discutidos em arquiteturas distribuídas e resilientes para IoT e edge computing [Grover and Garimella 2018]. No entanto, há limitações: o buffer possui capacidade restrita, a cobertura de rede alternativa não contempla todos os nós e a validação depende da presença física de sensores duplicados.

Estão previstas simulações de situações como: perda da conexão Wi-Fi, avaliando o uso e a sincronização do buffer local, bem como eventuais quedas do broker MQTT; falha de sensores, testando a resposta do sistema com redundância sensorial; e falha de

unidades agregadoras, avaliando o impacto local e o isolamento da falha. Cada experimento será analisado quanto à eficácia dos mecanismos de tolerância implementados, utilizando métricas como tempo de recuperação (RTO), taxa de perda de dados.

O objetivo é mensurar o impacto das falhas para embasar estratégias de mitigação das limitações identificadas. Propõe-se a compressão dos dados armazenados localmente para expandir a capacidade do buffer [Hasan and Alhusainy 2018]; a adoção de redes mesh ou protocolos como ESP-NOW para ampliar a cobertura indireta entre sensores [Corak et al. 2018]; e a detecção de anomalias com base em histórico e correlação espacial com sensores vizinhos como alternativa à duplicação física [Bisignano et al. 2022, Russell et al. 2022]. A análise quantitativa desses indicadores permitirá ajustes estruturais e aprimoramentos contínuos nos mecanismos de resiliência do sistema.

A Figura 1 ilustra a arquitetura proposta, mostrando claramente o fluxo de dados entre as unidades de sensoriamento, as unidades agregadoras, o broker MQTT, e o backend com InfluxDB, Telegraf e Grafana. As setas indicam o sentido da comunicação, destacando o fluxo hierárquico desde os sensores até o servidor central, passando pelas unidades agregadoras e broker, culminando na visualização e análise de dados no dashboard

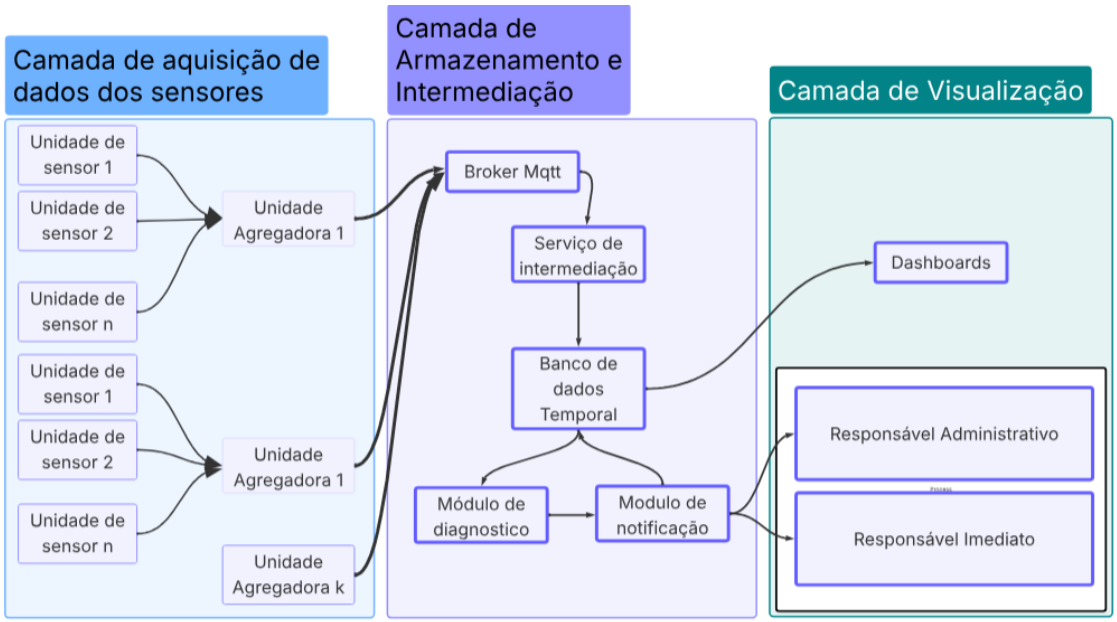


**Figura 1. Arquitetura proposta do sistema de monitoramento distribuído.**

Outra funcionalidade considerada é a atualização remota de firmware (OTA - Over-The-Air), que permite modificações no código, adição de sensores e reconfiguração de parâmetros operacionais sem acesso físico ao dispositivo. Essa capacidade é essencial em ambientes de produção e exige mecanismos de segurança robustos, como autenticação de firmware e verificação de integridade, conforme discutido por Rahman et al. [Rahman et al. 2020].

Por fim, adota-se o conceito de inteligência na borda (edge intelligence), com a execução de modelos leves de aprendizado de máquina diretamente nos microcontrola-

dores, tanto nas unidades de sensores quanto nas agregadoras, conforme a capacidade dos dispositivos. Isso permite distribuir a lógica de inferência para a borda, reduzindo a latência, o tráfego de rede e a carga sobre o servidor, além de viabilizar a detecção de anomalias em tempo real [Bisignano et al. 2022, Russell et al. 2022].

Assim, é proposto uma solução robusta, escalável e flexível para o monitoramento contínuo de ambientes críticos. Entre as características-chave destacam-se: sensoriamento modular, comunicação leve e segura, análise temporal, notificações inteligentes e possibilidade prevista de reconfiguração remota.

## 4. Estudo de Viabilidade e Experimentação Inicial

A implementação inicial, baseada em simulações controladas, validou a compatibilidade entre componentes, a comunicação via MQTT, e o pipeline completo até o backend. Contudo, testes em ambientes reais, considerando variações de rede, interferências eletromagnéticas e desafios típicos de datacenters, serão conduzidos em etapas posteriores

Foram desenvolvidos nós sensores com microcontroladores *ESP32*, escolhidos por sua conectividade Wi-Fi e Bluetooth integrada, suporte nativo aos protocolos MQTT e ESP-NOW. Neste protótipo inicial, a modularidade física dos sensores ainda não foi implementada, assim como a atualização de firmware remota. O sistema foi validado quanto à configuração inicial dos dispositivos via Bluetooth, utilizando um aplicativo simples de envio de mensagens. Essa abordagem permitiu testar o envio de credenciais de rede e tópicos MQTT de forma simplificada e satisfatória.

Os utilizados sensores são amplamente empregados em contextos ambientais e industriais, os sensores MQ-2, MQ-7, MQ-8 e MQ-135 para detecção de fumaça, monóxido de carbono, hidrogênio e compostos orgânicos voláteis, além dos sensores BMP280 e DS18B20 para medição de temperatura, pressão e umidade. Os sensores apresentaram respostas consistentes durante os testes, com amostragens em intervalos de 1 segundo. A configuração dinâmica dos sensores por Bluetooth, embora prevista, não foi incluída nesta fase, uma vez que os testes focaram na validação geral da arquitetura.

Para avaliar a infraestrutura em um cenário de uso contínuo e com maior densidade de sensores, foi desenvolvido um código em Python para simular várias unidades de sensoriamento. Cada unidade com sensores virtuais de gases, temperatura, umidade e pressão. A Figura 2 apresenta um dashboard simplificado com os valores gerados durante a simulação.

Os dados foram enviados via protocolo MQTT a partir de uma máquina local para o broker hospedado em um servidor remoto, que estava configurado com InfluxDB, Telegraf e Grafana. A figura ilustra os dados armazenados e visualizados no dashboard em tempo real. Apesar do ambiente ser simulado, o experimento permitiu validar toda a cadeia da solução a partir da geração dos dados até sua recepção, armazenamento e visualização, confirmando a viabilidade da arquitetura proposta.

Entretanto este experimento não aborda variações de rede e interferencias diversas existentes em um ambiente de datacenter.

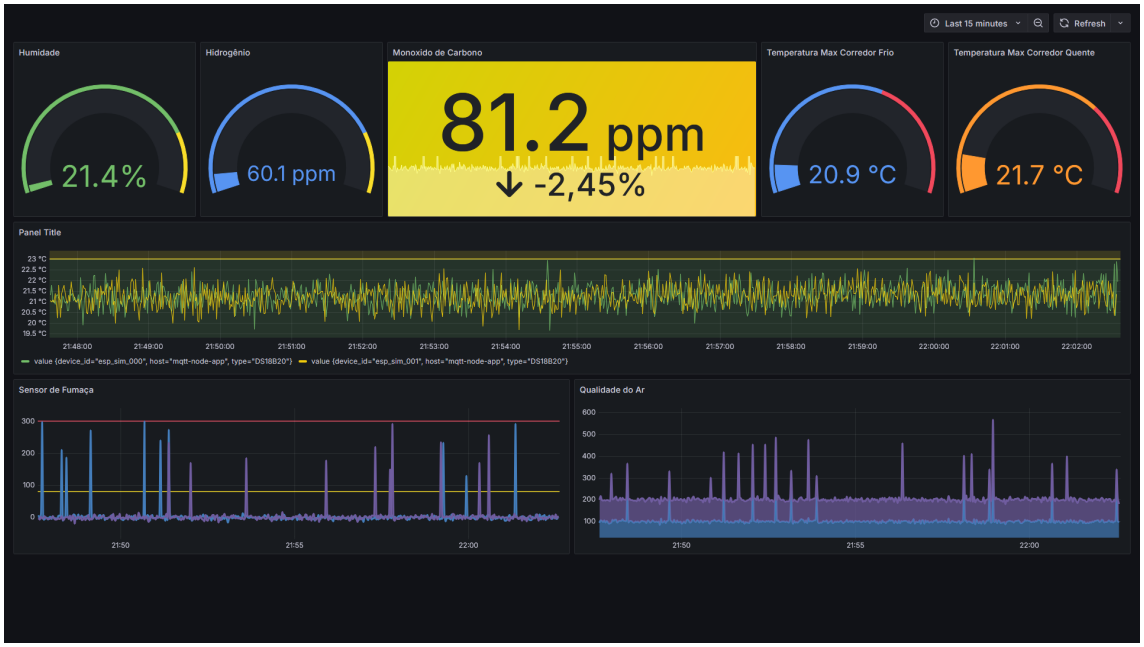


**Figura 2. Dashboard gerado a partir dos dados simulados dos sensores.**

Adicionalmente, a Figura 3 apresenta um gráfico de latência de entrega das mensagens para cenários com 10, 50 e 100 nós sensores simulados, operando por 5 minutos cada. Observa-se que, à medida que o número de sensores aumenta, há um crescimento significativo na quantidade de mensagens com latência acima do esperado.

Em ambientes de data center, onde a rápida detecção de anomalias é crítica para evitar falhas operacionais, atrasos superiores a alguns segundos na entrega de mensagens podem comprometer a eficácia de ações preventivas. Por isso, a latência deve ser cuidadosamente monitorada e mitigada com estratégias de agregação e processamento local.

Esse resultado reforça a importância de estratégias como a agregação local de dados — reduzindo a quantidade de mensagens individuais transmitidas — e o uso de modelos embarcados para pré-processamento e filtragem antes do envio. Para evidenciar as variações de latência, a simulação utilizou propositalmente um servidor remoto localizado nos Estados Unidos, enquanto os sensores simulados estavam no Brasil. Essa escolha não compromete os objetivos do teste, que busca justamente avaliar o impacto do aumento da carga sensorial sobre a infraestrutura de comunicação e armazenamento.

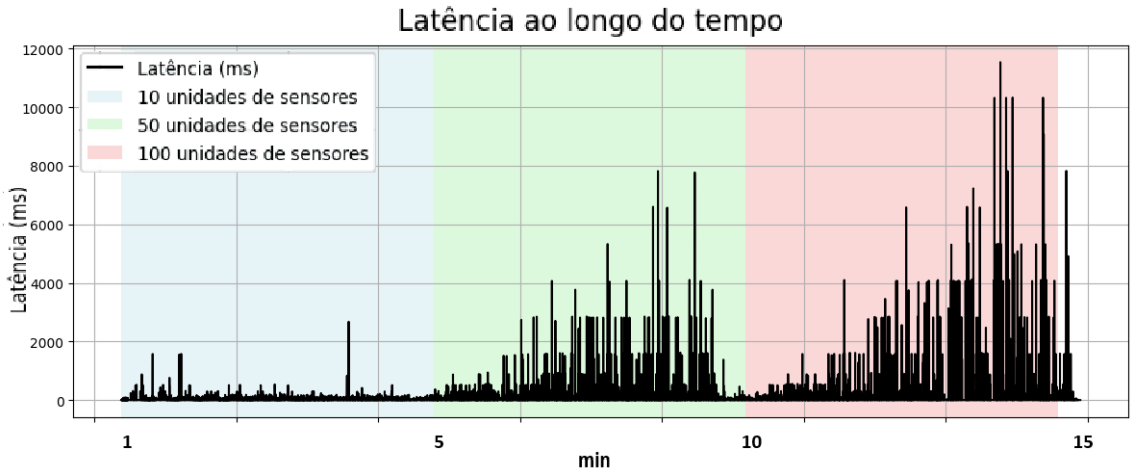


**Figura 3. Gráfico de latência para diferentes quantidades de sensores simulados.**

As mensagens publicadas seguiram o formato JSON e foram transmitidas ao broker Mosquitto com autenticação simples por token. Um exemplo ilustrativo da estrutura dessas mensagens pode ser visto na Figura 4.

A infraestrutura de backend foi implementada utilizando contêineres Docker, abrangendo o broker MQTT Mosquitto, o banco de dados temporal InfluxDB, o Telegraf como serviço de intermediação para ingestão de dados, e o Grafana para visualização das métricas. Essa abordagem containerizada proporciona portabilidade, modularidade e facilidade de implantação da solução, tanto em servidores dedicados quanto em ambientes cloud ou serverless.

```
{
  "device_id": "sensor_esp32_001",
  "timestamp": 1712005123456,
  "type": "BME280",
  "slot": 1,
  "sensor_id": "bme280_temp",
  "value": 24.7
}
```

**Figura 4. Exemplo de mensagem JSON enviada por um nó sensor.**

Os experimentos iniciais confirmaram a viabilidade técnica da arquitetura proposta, validando com sucesso a integração com os serviços de backend baseados em containers Docker.

## 5. Conclusão

Este trabalho apresentou uma arquitetura distribuída de multissensoriamento para monitoramento ambiental e operacional de data centers, com foco em modularidade, escalabilidade e confiabilidade. A proposta combina unidades de sensoriamento e agregação que se comunicam hierarquicamente com um servidor central por meio de um modelo

publish/subscribe, utilizando o protocolo MQTT. A arquitetura foi concebida para otimizar o tráfego de rede e garantir resiliência frente a falhas de conectividade, por meio de estratégias como buffers locais, redundância de sensores e canais de notificação inteligentes.

A implementação do protótipo validou a viabilidade técnica da proposta, demonstrando a estabilidade da comunicação entre dispositivos, a correta integração com os serviços de backend e a consistência das leituras dos sensores, mesmo sob diferentes cargas simuladas. A utilização de uma infraestrutura containerizada reforçou a portabilidade da solução e seu potencial de adoção em ambientes reais, favorecendo a escalabilidade e a manutenção modular.

Como trabalhos futuros, destacam-se a implementação da atualização remota de firmware (OTA), essencial para manutenção escalável e reconfiguração dinâmica dos nós, e a incorporação de algoritmos embarcados para pré-processamento dos dados e detecção de anomalias na borda. Essas funcionalidades, embora ainda não validadas, estão previstas na arquitetura e podem ser integradas sem a necessidade de reformulações estruturais. Também está prevista a realização de testes de campo em ambientes reais de data center, com simulações de falhas físicas (como perda de conectividade, falha de sensores e interrupções de energia), a fim de validar os mecanismos de tolerância a falhas em condições reais de operação.

Como parte do desenvolvimento contínuo da arquitetura, está prevista a implementação da funcionalidade de atualização remota de firmware (OTA - Over-The-Air). Essa funcionalidade permitirá reconfigurações operacionais e correções de segurança sem necessidade de acesso físico aos dispositivos. O sistema será adaptado para suportar atualizações assíncronas com verificação de integridade, autenticação do firmware e rollback seguro em caso de falha. O processo será validado em ambiente de data center com múltiplos nós, avaliando-se métricas como taxa de sucesso da atualização, tempo médio por nó e impacto na operação durante o processo, conforme orientações de estudos recentes sobre segurança em OTA [Rahman et al. 2020].

Finalmente, pretende-se expandir o número de nós operacionais, realizar testes prolongados em ambientes reais, aprimorar os mecanismos de notificação e avaliar o impacto do uso de inteligência embarcada sobre a latência e o consumo energético da solução. Com essas evoluções, espera-se contribuir para o desenvolvimento de uma plataforma robusta, adaptável e de baixo custo para o monitoramento inteligente de data centers e outras infraestruturas críticas.

## Referências


Al-Shareeda, M. A., Ali, M., Manickam, S., and Karuppayah, S. (2023). Bluetooth low energy for internet of things: Review, challenges, and open issues. *Indonesian Journal of Electrical Engineering and Computer Science*, 31(2):1182–1189.

Bisignano, D., Chiodi, A., Ferrari, R., and Flammini, F. (2022). Low-cost air quality monitoring and calibration using machine learning: A survey. *Sensors*, 22(13):5040.

Cherradi, B., El Bouziri, A., and Boulmakoul, A. (2016). Smart data collection based on iot protocols. *Procedia Computer Science*, 83:1204–1210.

Corak, J., Mihaljevic, B., and Stojanovic, M. (2018). Comparative analysis of iot communication protocols. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 582–586. IEEE.

Grover, J. and Garimella, S. (2018). Reliable and fault-tolerant iot-edge architecture. In *2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 1733–1738. IEEE.

Grzesik, B. and Mrozek, D. (2020). Comparative analysis of time series databases in the context of edge computing for low power sensor networks. In *ICCS 2020*, volume 12139 of *Lecture Notes in Computer Science*, pages 574–588. Springer.

Hasan, H. M. and Alhusainy, B. K. (2018). Evaluation of mqtt protocol for iot based industrial automation. *International Journal of Engineering and Technology*, 7(4.19):106–109.

ISO/IEC (2013). ISO/IEC 27031:2013 – Information technology – Security techniques – Guidelines for ICT readiness for business continuity. Publicada pela ABNT como NBR ISO/IEC 27031.

Mehrotra, A. and Musolesi, M. (2017). Intelligent notification systems: A survey of the state of the art and research challenges. *arXiv preprint arXiv:1711.10171*.

Rahman, M. M., Islam, M. A., and Kwak, K. S. (2020). Secure over-the-air firmware updates for internet of things devices: A survey. *Journal of Network and Computer Applications*, 102:102702.

Russell, L., Zito, R., and Williamson, L. (2022). Calibration of low-cost gas sensors using artificial neural networks. *Atmosphere*, 13(3):478.

Seoane, S. P., Hernández-Ramos, J. L., Jara, A. J., and Skarmeta, A. F. (2021). Performance evaluation of coap and mqtt with security support for iot environments. *Computer Networks*, 197:108278.

TIA (2005). ANSI/TIA-942: Telecommunications Infrastructure Standard for Data Centers. Disponível em: `https://www.tiaonline.org`.

Vieira, L., Souza, T., and Queiroz, G. (2024). Análise de desempenho e eficiência energética dos protocolos mqtt e coap no contexto de iot. In *Anais do XXXVIII Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2024)*. SBC.