**Tema 9 - Computação em Névoa e Internet das Coisas (IoT)**

A Internet das Coisas (IoT, do inglês "Internet of Things") é uma tecnologia que estende a conectividade da internet além dos computadores e dispositivos móveis tradicionais para uma ampla gama de sistemas, dispositivos e ambientes do dia a dia. Através da IoT, objetos físicos são equipados com sensores, atuadores e software que permitem coletar e transmitir dados pela internet, possibilitando que esses objetos se comuniquem e interajam com outros dispositivos e sistemas de maneira autônoma.

A essência da IoT reside na interconexão de dispositivos inteligentes que antes eram isolados, transformando-os em sistemas integrados que podem monitorar, coletar, trocar e analisar dados. Estes dispositivos variam desde aparelhos domésticos comuns, como refrigeradores e lâmpadas, até elementos mais complexos como máquinas industriais e infraestruturas urbanas. Essa interconectividade oferece um novo nível de controle e gestão sobre o mundo físico, tornando possível otimizar processos, melhorar a eficiência, reduzir custos e impactar positivamente a vida das pessoas.

Além de facilitar o controle e a automação, a IoT oferece oportunidades significativas para melhorias em várias áreas, incluindo:

1. **Cidades Inteligentes:** Gestão de tráfego, monitoramento ambiental e serviços públicos podem ser otimizados usando sensores IoT para criar cidades mais sustentáveis e eficientes.
2. **Saúde:** Dispositivos de monitoramento de saúde podem ajudar médicos a acompanhar a condição dos pacientes remotamente, proporcionando diagnósticos mais rápidos e tratamentos personalizados.
3. **Agricultura:** Sensores podem monitorar condições do solo, clima e culturas, guiando os agricultores sobre irrigação e uso de fertilizantes para maximizar a produtividade e sustentabilidade.
4. **Indústria:** A IoT industrial, ou IIoT, utiliza sensores e automação para melhorar a eficiência das operações de manufatura e reduzir os tempos de inatividade das máquinas.

A Internet das Coisas (IoT) está transformando numerosos setores, proporcionando eficiências operacionais inéditas, redução de custos energéticos, melhorias significativas na qualidade de vida e permitindo decisões mais embasadas através de dados coletados em tempo real. Por exemplo, na indústria, a IoT permite monitorar máquinas continuamente, antecipando falhas antes que elas ocorram e reduzindo tanto o tempo de inatividade quanto os custos de manutenção. Nos edifícios inteligentes, os sistemas IoT ajustam o consumo de energia automaticamente, baseando-se em padrões de uso detectados, enquanto no setor de saúde, dispositivos conectados monitoram pacientes com doenças crônicas, alertando os profissionais de saúde sobre possíveis emergências antes que estas ocorram.

No entanto, a IoT também apresenta desafios substanciais. A segurança e a privacidade são preocupações críticas devido ao volume de dados sensíveis coletados e transmitidos pelos dispositivos IoT. A complexidade das redes aumenta com o número de dispositivos conectados, complicando o gerenciamento e a escalabilidade. Além disso, a falta de padrões universais pode limitar a funcionalidade dos dispositivos, dificultando a interoperabilidade entre diferentes sistemas e fabricantes. Os custos iniciais de implementação também podem ser proibitivos, especialmente para pequenas e médias empresas.

A Internet das Coisas (IoT) integra uma série de tecnologias complementares para conectar objetos do ambiente físico ao mundo virtual. Entre os componentes fundamentais da IoT, estão:

1. **Identificação:** Crucial para a conexão única de objetos à internet, utilizando tecnologias como RFID, NFC (Near Field Communication) e endereçamento IP.
2. **Sensores/Atuadores:** Os sensores coletam dados sobre o contexto dos objetos, que podem ser armazenados ou enviados para data warehouses, nuvens ou outros centros de armazenamento. Os atuadores ajustam ou respondem ao ambiente baseados nos dados coletados.
3. **Comunicação:** Envolve várias técnicas para conectar objetos inteligentes e é vital para a gestão de consumo de energia dos dispositivos. Tecnologias incluem WiFi, Bluetooth, IEEE 802.15.4 e RFID.
4. **Computação:** Abrange unidades de processamento como microcontroladores, processadores e FPGAs, que executam algoritmos localmente nos objetos inteligentes.
5. **Serviços:** A IoT oferece várias classes de serviços:
   1. **Serviços de Identificação:** Mapeiam Entidades Físicas (EF) em Entidades Virtuais (EV), transformando, por exemplo, a temperatura de um local em dados mensuráveis.
   2. **Serviços de Agregação de Dados:** Coletam e resumem dados, sejam eles homogêneos ou heterogêneos, provenientes de objetos inteligentes.
   3. **Serviços de Colaboração e Inteligência:** Utilizam dados agregados para tomar decisões e responder adequadamente aos cenários.
   4. **Serviços de Ubiquidade:** Garantem que serviços de colaboração e inteligência estejam disponíveis em qualquer tempo e lugar.
6. **Semântica:** Trata da extração de conhecimento a partir dos dados coletados, empregando técnicas como Resource Description Framework (RDF), Web Ontology Language (OWL) e Efficient XML Interchange (EXI) para descobrir conhecimentos e utilizar recursos de maneira eficiente.

Os objetos inteligentes são estruturados em torno de quatro componentes principais: processamento/memória, comunicação, energia, e sensores/atuadores, cada um desempenhando funções cruciais para a operacionalidade e eficiência do dispositivo. Conforme pode ser visto na Figura 1:

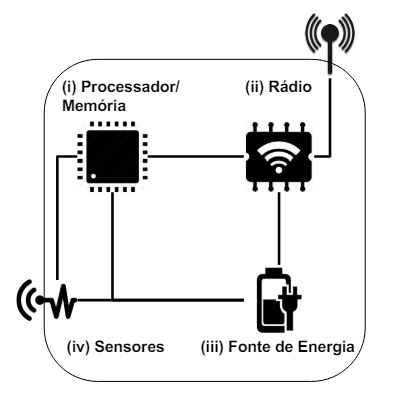


Figura 1: Arquitetura dos dispositivos de IoT.

Primeiramente, a unidade de processamento/memória é essencial, compreendendo uma memória interna utilizada para armazenar dados e programas, juntamente com um microcontrolador e um conversor analógico-digital que processa sinais dos sensores. Essas CPUs, que geralmente têm características similares às de sistemas embarcados, são projetadas para serem energeticamente eficientes e ocuparem o mínimo espaço possível, embora não apresentem alto poder computacional. Muitas vezes, esses sistemas são complementados com memória externa do tipo flash, utilizada para armazenar dados de longo prazo como registros de atividades.

A unidade de comunicação, normalmente sem fio, incorpora rádios de baixo custo e baixa potência, o que implica em comunicações de curto alcance com possíveis perdas frequentes. Esta unidade é fundamental para a conectividade e interatividade dos objetos inteligentes e é frequentemente um foco de estudos detalhados para melhorar a eficiência e o alcance das transmissões.

Quanto à fonte de energia, ela é responsável por alimentar todos os componentes eletrônicos do objeto inteligente. A configuração mais comum inclui uma bateria, que pode ser recarregável ou não, acompanhada de um conversor AC-DC. Inovações como o energy harvesting estão sendo exploradas para capturar energia de fontes alternativas, como solar ou mecânica, convertendo-a em energia elétrica e proporcionando uma autonomia maior aos dispositivos.

Por fim, a unidade de sensores/atuadores é vital para a interação do objeto inteligente com seu ambiente. Os sensores coletam dados sobre diversas grandezas físicas — temperatura, umidade, pressão e presença, por exemplo — permitindo um monitoramento constante e detalhado do ambiente. Os atuadores, por sua vez, realizam ações específicas com base nos dados recebidos ou em comandos externos, podendo ser controlados manual, elétrica ou mecanicamente.

Os dispositivos de IoT, conforme ilustrado na Figura 1, dependem de fontes de energia para funcionar, sendo as baterias (recarregáveis ou não) as mais comuns. No entanto, essas não são sempre ideais devido à dificuldade de acesso aos dispositivos para substituição, pois muitas vezes estão embutidos em locais de difícil alcance ou não se deseja manipulá-los fisicamente. Assim, é fundamental que tanto o hardware quanto o software sejam otimizados para maximizar a vida útil desses dispositivos.

Uma estratégia promissora para superar os desafios de alimentação é a técnica de colheita de energia a (do inglês Energy Harvesting), que converte energia de fontes externas, como solar, térmica, eólica e cinética, em energia elétrica, armazenando-a em baterias recarregáveis. Esta energia colhida, embora geralmente em pequenas quantidades, é crucial para sustentar as operações dos dispositivos, como comunicação e processamento.

Entretanto, a colheita de energia introduz desafios adicionais, como a necessidade de programar eficientemente as atividades dos dispositivos baseando-se no orçamento de energia disponível. Por exemplo, um dispositivo que precisa operar continuamente, mas só pode captar energia solar durante o dia, deve alternar entre atividades ativas e modos de espera ou baixa potência para equilibrar o uso da energia armazenada com a captada.

Este cenário exige o desenvolvimento de técnicas mais sofisticadas que adaptem as tarefas do dispositivo em função da energia disponível e prevejam a disponibilidade futura baseando-se em padrões passados de colheita de energia. Esta abordagem não só estende a autonomia dos dispositivos como abre caminho para novas pesquisas em gestão inteligente de energia em IoT.

Para efetivamente conectar vários objetos inteligentes à Internet, uma arquitetura flexível é essencial. Diversas propostas de arquiteturas sofisticadas, que atendem às necessidades tanto da academia quanto da indústria, foram desenvolvidas e são frequentemente discutidas na literatura. Um modelo básico comum de arquitetura para IoT é estruturado em três camadas principais: de Percepção, de Rede e de Aplicação, ilustradas pela Figura 2, as quais facilitam a gestão e a escalabilidade dos sistemas.

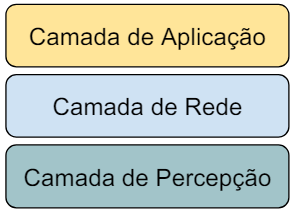


Figura 2: Arquitetura para IoT

A primeira camada, conhecida como camada de percepção, consiste nos objetos inteligentes. Esses objetos estão equipados com sensores que coletam dados do ambiente, como temperatura, umidade, movimento, entre outros, e processam essas informações localmente.

A segunda camada é a camada de rede. Esta camada serve como um ponto central para as tecnologias de comunicação e inclui serviços essenciais de gerenciamento, roteamento e identificação. Sua principal função é assegurar que os dados coletados pelos objetos inteligentes sejam transmitidos de forma eficiente para a próxima camada.

Por fim, a camada de aplicação fica no topo da arquitetura e é responsável por fornecer serviços diretamente aos usuários finais. Aplicações nesta camada podem solicitar dados específicos coletados pelos sensores, como medições de temperatura e umidade, e disponibilizar essas informações para os clientes conforme necessário.

Há uma variedade de tecnologias de comunicação para IoT, cada uma com características distintas adequadas a diferentes necessidades. As principais tecnologias estão sumarizadas abaixo:

* **Ethernet:** Implementado inicialmente em 1983 como padrão IEEE 802.3, o Ethernet é amplamente utilizado em redes locais com fio. Sua popularidade deve-se à simplicidade, facilidade de manutenção e baixo custo. Existem dois tipos de cabos Ethernet: par trançado, que suporta velocidades de até 1 Gbps e é limitado a 100 metros sem repetidores; e fibra óptica, que alcança até 10 Gbps com limitação de até 2000 metros. Ethernet é ideal para dispositivos fixos devido à sua infraestrutura estática.
* **Wi-Fi:** Este é um método de comunicação sem fio extremamente popular, abrangendo ambientes como casas, escritórios e espaços públicos. As versões do padrão IEEE 802.11 variam, com as mais recentes (IEEE 802.11ac) suportando velocidades de 600 Mbps a 1300 Mbps. Apesar de sua conveniência, o Wi-Fi pode não ser ideal para algumas aplicações IoT devido ao seu consumo de energia relativamente alto.
* **ZigBee:** Operando principalmente na frequência 2.4 GHz, o ZigBee é valorizado por seu baixo custo e consumo de energia reduzido, características que o tornam adequado para aplicações que exigem economia de energia e modos de hibernação prolongados. Utiliza a especificação do protocolo IEEE 802.15.4 para camada de enlace.
* **Bluetooth Low Energy (BLE):** Desenvolvido para dispositivos de baixo consumo de energia, o BLE é perfeito para aplicações que utilizam baterias pequenas. Desde sua primeira versão em 2010, o BLE evoluiu para suportar transmissões de dados mais robustas e topologias de rede mais flexíveis, incluindo redes em malha.
* **3G/4G:** Estas tecnologias de telefonia móvel são úteis para cobrir grandes distâncias, embora sejam menos eficientes em termos de energia. São particularmente úteis em locais remotos ou com pouca mobilidade.
* **LoRaWAN:** A especificação LoRaWAN (Long Range Wide Area Network), especificada para redes de área ampla de baixa potência, é ideal para comunicações de longa distância com baixo consumo de energia. Suporta IPv6 e adaptação ao 6LoWPAN, operando sobre uma topologia estrela.
* **Sigfox:** Usando a tecnologia Ultra Narrow Band (UNB), o Sigfox é projetado para aplicações que transmitem pequenas quantidades de dados. Oferece uma cobertura extensa e é uma escolha popular para dispositivos IoT distribuídos amplamente, especialmente em áreas rurais.

A pesquisa em Redes de Sensores Sem Fio (RSSF) tem sido intensa tanto no meio acadêmico quanto na indústria, evidenciando a complexidade de integrar diretamente os protocolos tradicionais da Internet, como a arquitetura TCP/IP, em dispositivos de IoT com recursos limitados. Tais dispositivos exigem protocolos especializados para garantir escalabilidade e robustez, além de possibilitar o processamento em rede, essencial para superar suas limitações físicas.

A arquitetura de internet tradicional não consegue atender às necessidades específicas da IoT, como gerenciar inúmeros dispositivos em uma única sub-rede e operar com eficiência energética limitada. Esse desafio resultou no desenvolvimento de novas abordagens de hardware e software, que muitas vezes dependem de gateways para intermediação. No entanto, essa solução pode centralizar excessivamente a inteligência da rede e criar gargalos operacionais, desviando-se dos princípios de que a inteligência de rede deve estar distribuída.

Para enfrentar esses obstáculos, a Internet Engineering Task Force (IETF) criou grupos focados em redes de baixa potência e com perdas (LLN). O grupo 6LoWPAN padronizou o IPv6 para uso com o padrão IEEE 802.15.4, enquanto o grupo RoLL desenvolveu o protocolo de roteamento RPL, um avanço significativo para o roteamento na IoT.

Além disso, o esgotamento dos endereços IPv4 revelou a falta de escalabilidade deste para a IoT moderna, levando à adoção do IPv6, que expande os endereços para 128 bits, permitindo a conexão de um número muito maior de dispositivos. Ainda assim, o tamanho dos pacotes IPv6 excede o limite de muitos dispositivos de IoT, um desafio mitigado pelo 6LoWPAN através da compressão de pacotes, facilitando a integração eficiente de IPv6 em dispositivos com restrições computacionais.

O protocolo HTTP, desenvolvido para computadores convencionais, não se adequa perfeitamente aos dispositivos de IoT devido às suas limitações computacionais. Para contornar isso, foram desenvolvidos protocolos específicos para dispositivos com baixo poder de processamento, como o CoAP (Constrained Application Protocol) e o MQTT (Message Queue Telemetry Transport).

O CoAP, mantido pelo grupo de trabalho IETF Constrained RESTful Environments (CoRE), opera de forma semelhante ao HTTP mas é otimizado para ambientes restritos, utilizando o protocolo UDP para comunicação, o que o torna mais adequado para a IoT, dentre outras razões, por causa do seu menor consumo de energia e a rapidez na transmissão devido a não necessidade de confirmação de recebimento de cada pacote. Suporta métodos semelhantes ao HTTP, como GET, POST, PUT e DELETE, dentro de uma arquitetura RESTful, facilitando a interação entre clientes e servidores através de Uniform Resource Identifiers (URIs). O protocolo estrutura-se em duas camadas: a primeira gerencia a requisição e resposta, e a segunda lida com a detecção de mensagens duplicadas e garante a confiabilidade sobre o UDP. CoAP também suporta tipos de mensagens como confirmable, non-confirmable, reset e acknowledgement, e é possível integrá-lo a navegadores através de extensões como Copper para Firefox.

Por outro lado, o MQTT é projetado para minimizar o consumo de largura de banda e os recursos do dispositivo, utilizando a abordagem de publicar/assinar para a troca de mensagens. Essencial para ambientes com dispositivos extremamente limitados, o MQTT inclui mecanismos de garantia de entrega de mensagens. Ele opera sobre os protocolos de transporte e rede TCP/IP, com cabeçalhos de tamanho fixo ou variável, dependendo da implementação, como o Mosquitto, uma solução open source. No MQTT, os dispositivos se registram em um broker para receber atualizações de publicadores específicos, facilitando uma comunicação eficiente e direcionada dentro de redes de IoT.

À medida que a Internet das Coisas (IoT) se expande, bilhões de dispositivos inteligentes espalhados por diversas localidades geram uma quantidade imensa de dados. Tradicionalmente, esses dados são processados e armazenados na nuvem, o que compensa as limitações de processamento dos dispositivos. Contudo, a infraestrutura de nuvem convencional pode não ser suficiente para as demandas da IoT, especialmente em aplicações industriais e missões críticas que requerem baixa latência e respostas rápidas ao ambiente. Para mitigar esses desafios, tem-se duas soluções: edge computing e fog computing.

O edge computing processa dados no limite da rede, próximo aos dispositivos IoT, evitando a necessidade de enviá-los para data centers remotos, o que reduz significativamente a latência. Esta proximidade é crucial em aplicações sensíveis ao tempo, como monitoramento de saúde e controle de tráfego, onde a rapidez na resposta é essencial. Além disso, processar dados localmente diminui a largura de banda necessária para a transmissão de dados, melhorando a eficiência e reduzindo custos.

A segurança também é reforçada no edge computing, pois menor quantidade de dados transita pela rede, reduzindo as chances de ataques cibernéticos, especialmente em setores industriais onde a proteção de dados é crítica. Adicionalmente, o edge computing facilita análises de dados rápidas e contextuais, permitindo decisões imediatas que podem otimizar operações e melhorar a experiência do usuário, antecipando falhas e ajustando processos em tempo real.

Já a computação de névoa (fog computing) surge como uma solução eficaz para esses desafios, transformando as bordas da rede em uma infraestrutura de computação distribuída. Esse modelo processa dados mais perto dos dispositivos conectados, reduzindo a latência e permitindo análises em tempo real, ideal para ambientes IoT dinâmicos. A computação de névoa também pode integrar inteligência artificial para melhorar a automação e a eficiência das respostas dos sistemas.

Nessa arquitetura, existem os nós de névoa, que são entidades computacionais dotadas de configurações variadas, que incluem servidores, dispositivos de comunicação, cloudlets, estações base e veículos. Tais nós empregam técnicas de virtualização para provisionar recursos, dividindo-os de uma máquina física em máquinas virtuais. Mais recentemente, essa prática evoluiu para o uso de contêineres, que fornecem isolamento no nível do sistema operacional e são mais adequados para a computação em névoa devido à sua capacidade de executar de forma independente da plataforma, facilitando a migração de tarefas entre servidores.

A arquitetura comum para computação em névoa, descrita por Hu et al., compreende três camadas essenciais:

1. **Camada de nuvem:** Inclui servidores de armazenamento e computação robusta, capazes de armazenar e analisar uma vasta quantidade de dados para diversos serviços de aplicativos, conforme necessário.
2. **Camada de névoa:** Localizada na borda da rede, consiste em uma ampla distribuição de nós de névoa, tanto físicos quanto virtuais, entre a nuvem e os dispositivos finais. Esses nós podem ser móveis ou fixos, com capacidades de processamento, armazenamento temporário e transmissão de dados. Eles também facilitam a conexão e interação com outros nós de névoa próximos.
3. **Camada de dispositivo do usuário (borda):** Esta camada está mais próxima do ambiente físico e do usuário final, incluindo dispositivos e sensores IoT, interagindo diretamente com o ambiente.

A arquitetura de fog computing posiciona uma camada de névoa entre a nuvem e os dispositivos do usuário final. Esta camada consiste em uma variedade de servidores heterogêneos, que variam desde dispositivos dedicados, como servidores e roteadores de borda, até dispositivos temporários como smartphones e sensores avançados. Essa configuração permite que cargas de trabalho que exigem baixa latência ou tempos de resposta rápidos sejam processadas na névoa, enquanto as que necessitam de maior capacidade de processamento continuam a ser direcionadas para a nuvem. Essa abordagem não apenas reduz o congestionamento e os custos associados à computação centralizada, mas também aumenta a segurança ao criptografar dados antes de enviá-los para a nuvem central, garantindo maior proteção ao longo de todo o ciclo.

Além disso, a computação em névoa reduz a dependência da Internet e de conexões de alta qualidade, o que é especialmente valioso em cenários militares onde os recursos são limitados e o uso racional da banda de dados é essencial para o sucesso das operações. A tecnologia 5G ampliará ainda mais as capacidades da computação em névoa, permitindo o processamento de grandes volumes de dados diretamente nos dispositivos de borda, sem necessidade de enviar tudo para a nuvem.

Outra vantagem importante da arquitetura de névoa é a capacidade de localizar usuários de forma mais precisa devido à distribuição geográfica dos nós. Isso permite a alocação de recursos de acordo com a posição geográfica dos dispositivos, melhorando a eficiência das operações e aumentando a segurança dos dados, ao permitir que informações sensíveis sejam processadas e armazenadas localmente, sem exposição desnecessária em redes amplas.

A arquitetura de referência constitui a base principal para a implementação de sistemas em computação em névoa, identificando os componentes funcionais principais e suas interconexões. Essa arquitetura geralmente incorpora interfaces ou APIs que permitem a interação dos blocos funcionais tanto internamente quanto externamente, visando cumprir os objetivos da arquitetura.

As arquiteturas de referência para computação em névoa são desenvolvidas a partir de várias perspectivas e apresentam diferentes níveis de abstração. Uma arquitetura altamente abstrata destaca diferentes tipos de componentes, cada um fornecendo um conjunto de funções e tarefas. Uma arquitetura de nível mais baixo pode detalhar as interações ou procedimentos específicos dentro de uma função destinada a realizar uma tarefa específica. As principais arquiteturas de referência em computação de névoa são: Openfog, Clouds Lab, Cisco-Bonomi e AUT.

A OpenFog, proposta pelo Open Fog Consortium, exemplifica uma arquitetura hierárquica para a computação em névoa. Os nós de névoa, distribuídos em vários níveis hierárquicos, cobrem todas as instalações computacionais entre os pontos finais e os servidores em nuvem. Esses nós se comunicam através de canais com ou sem fio e diferem em parâmetros como capacidades de processamento, habilidades de rede e confiabilidade. Cada camada processa e extrai dados significativos, aumentando a inteligência do sistema. A camada mais baixa realiza a aquisição e normalização de dados, enquanto a camada superior executa filtragem, compressão e transformação de dados. A camada de névoa mais próxima da nuvem transforma os dados coletados em uma base de conhecimento para armazenamento permanente, incrementando a inteligência e capacidade do sistema conforme as camadas se aproximam da nuvem.

Os nós de névoa na borda geralmente requerem menos processamento, comunicação e armazenamento do que os nós em níveis mais altos, mas precisam de aceleradores de entrada e saída maiores para facilitar a ingestão de dados dos sensores. Apesar da emergência da computação em névoa, o modelo centralizado de computação em nuvem continua sendo um componente essencial dos sistemas de computação.

O software do sistema é dividido em três camadas: serviço de aplicação, suporte de aplicação e gestão de nós com software de interligação. O suporte de aplicação engloba um amplo espectro de softwares utilizados e compartilhados por várias aplicações, incluindo mecanismos de execução, serviços de segurança, barramento de mensagens e eventos, armazenamento de aplicativos e ferramentas e frameworks analíticos. A camada de software de interligação inclui sistema operacional, drivers, firmware, sistema de arquivos, virtualização e contêineres.

Os nós de névoa também podem ser interconectados em uma topologia de malha para proporcionar balanceamento de carga, resiliência, tolerância a falhas, compartilhamento de dados e minimização da comunicação com a nuvem. Cada nó precisa implementar mecanismos de segurança adequados e agentes de gerenciamento, além de suportar várias funções como rede, computação, aceleração, armazenamento e controle de sensores e atuadores.

A Clouds Lab Architecture é outra arquitetura de referência para computação em névoa que propõe cinco camadas: acesso, rede, serviços e recursos de nuvem, gerenciamento de recursos definido por software e aplicações IoT. Na camada mais baixa estão os dispositivos finais, incluindo sensores, dispositivos de borda e gateways, que fornecem conectividade através da camada de rede. A camada de nuvem oferece a plataforma computacional para gerenciar recursos e aplicações IoT.

A camada de gerenciamento de recursos definido por software é crucial para a arquitetura, pois gerencia e orquestra todos os recursos de forma a simplificar a tomada de decisões. Esta camada inclui serviços intermediários que otimizam o uso dos recursos de nuvem e névoa para aplicações IoT, com o objetivo de melhorar o desempenho das aplicações e reduzir atrasos, garantindo assim qualidade de serviço.

A última camada abriga as aplicações IoT que utilizam a computação em névoa para fornecer serviços inteligentes e inovadores aos usuários finais.

No que tange ao Gerenciamento de Recursos Definido por Software, a camada é composta por oito blocos funcionais essenciais:

1. **Alocação de Fluxos e Tarefas:** Monitora recursos disponíveis na névoa e na nuvem para alocar tarefas e fluxos apropriados, em colaboração com o serviço de Provisão de Recursos.
2. **Base de Conhecimento:** Armazena informações históricas sobre alocação de recursos e tipos de demanda para refinar a eficiência dos algoritmos.
3. **Previsão de Desempenho:** Utiliza dados da Base de Conhecimento para estimar o desempenho dos recursos que serão utilizados pelo sistema de provisão de recursos.
4. **Monitoramento:** Acompanha o desempenho e o status das aplicações.
5. **Perfilamento:** Constrói e mantém perfis de recursos e aplicações com base nas informações da Base de Conhecimento.
6. **Provisão de Recursos:** Responsável por alocar recursos de névoa, nuvem e rede para hospedar as aplicações de maneira dinâmica.
7. **Segurança:** Executa autenticação, autorização e criptografia para proteger os dados e as transações.

Outra arquitetura de referência, Cisco-Bonomi, foi proposta por Bonomi et al. [1], e consiste em cinco componentes principais: a Camada de Recursos Físicos Heterogêneos, a Camada de Abstração de Névoa, a Camada de Orquestração de Serviço de Névoa, Serviços de IoT e Barramento de Mensagem Distribuída [3]. Neste modelo a Camada de Recursos Físicos contém todos os hardwares envolvidos na névoa incluindo servidores, roteadores, pontos de acesso, sensores, etc. A Camada de Abstração tem a responsabilidade de ocultar a natureza heterogênea dos dispositivos, e fornecer uma interface programável a fim de permitir o gerenciamento dos recursos. A Camada de Orquestração de Serviço foi projetada para gerenciar o ambiente distribuído e fazer a orquestração dos serviços. O Barramento de Mensagens é responsável por transportar mensagem entre a orquestração e o gerenciamento, já os Serviços de IoT contém as aplicações disponibilizadas para os clientes. Assim sendo, similar a arquitetura Cloud Labs, o modelo Cisco-Bonomi apresenta componentes abstratos, no qual a hierarquia das camadas não representa a diferença na complexidade de computação, e sim níveis de complexidade na abstração dos recursos. Na camada mais baixa está o hardware e nas camadas superiores estão as aplicações, sendo que nas camadas intermediárias estão os mecanismos de orquestração e gerenciamento dos recursos.

Por fim, Habibi et al. [2] propuseram uma arquitetura de referência para computação em névoa (AUT), baseada em padrões de função de rede virtualizada (FRV) e redes definidas por software (SDN). Nesse modelo existem cinco componentes principais [3], os quais são: (i) camada de infraestrutura, (ii) camada de abstração de recursos, (iii) controle e gerenciamento, (iv) aplicativos e serviços e (v) camada de orquestração. Nessa arquitetura os equipamentos estão na camada de infraestrutura, a heterogeneidade dos equipamentos é abstraída através da camada de abstração que fornece APIs de alto nível para que as camadas subsequentes possam utilizar os recursos.

Nessa arquitetura os equipamentos estão na camada de infraestrutura, a heterogeneidade dos equipamentos é abstraída através da camada de abstração que fornece APIs de alto nível para que as camadas subsequentes possam utilizar os recursos.

Essa utilização é feita por meio de controle e gerenciamento de componentes de rede e controladores de redes definidas por software (SDN), e pela orquestração dos serviços, na qual, dentro da gama de serviços, estão as funções de rede virtualizadas. Os modelos, Clouds Lab, Cisco-Bonomi e AUT, possuem uma característica em comum que é a abstração por níveis, nos quais os níveis mais baixos estão próximos ao hardware, e os níveis mais altos são as aplicações. É importante observar que nessas arquiteturas, os hardwares que compõem cada nó da névoa são gerenciados por uma camada de abstração. Para isso, os componentes de orquestração nas camadas superiores alocam os serviços sobre o hardware de maneira transparente, ou seja, os nós não são tratados como elementos da arquitetura de forma individualizada, eles são absorvidos pela camada de abstração, que assume a responsabilidade de fornecer os recursos para as camadas superiores.

A expansão da Internet das Coisas (IoT) e a integração crescente com a computação em névoa revelam um futuro tecnológico promissor e desafiador. As IoT está redefinindo a maneira como interagimos com o mundo físico ao conectar uma infinidade de dispositivos inteligentes capazes de gerar, compartilhar e processar dados em tempo real, otimizando processos em diversas áreas como saúde, indústria e agricultura. Enquanto isso, a computação em névoa oferece a infraestrutura necessária para processar e analisar esses dados perto de sua fonte, minimizando a latência e maximizando a eficiência, o que é essencial para aplicações críticas que demandam respostas rápidas e precisas. A colaboração entre IoT e computação em névoa não apenas facilita uma gestão mais inteligente e autônoma dos dispositivos conectados, mas também impulsiona inovações em serviços automatizados e inteligência distribuída. Contudo, desafios como segurança, privacidade e escalabilidade continuam sendo obstáculos significativos que exigem soluções inovadoras e robustas para garantir a sustentabilidade e eficácia dessa integração tecnológica no longo prazo.

**Referências**

<https://pt.wikipedia.org/wiki/Fog_computing>

[1] Bonomi, Flavio, Rodolfo Milito, Preethi Natarajan e Jiang Zhu: Fog computing: A platform for internet of things and analytics. Em Big data and internet of things: A roadmap for smart environments, páginas 169–186. Springer, 2014. 17

[2] Habibi, Pooyan, Soroush Baharlooei, Mohammd Farhoudi, Sepehr Kazemian e Siavash Khorsandi: Virtualized sdn-based end-to-end reference architecture for fog networking. Em 2018 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), páginas 61–66. IEEE, 2018. 17

**Pasta de livros:**

internet-das-coisas.pdf

Fog\_Computing\_A\_Comprehensive\_Architectural\_Survey.pdf

2022\_MarcosFranciscodaSilva.pdf