Análise de estudo de casos em abordagens pelo mundo da implementação de Internet das Coisas

Thiago Rodrigues de Oliveira[1], Giuliano Prado de Morais Giglio[1]

[1]Centro de Ensino Superior de Juiz de Fora (CES/JF)
Rua Halfeld 1179 – 36.016-000 – Juiz de Fora – MG - Brasil

tro2303@gmail.com, giucontato@gmail.com

Abstract. *The Internet of Things (IoT) is likely to be one of the most important technological advances of the coming years. The main enabling factor of this promising paradigm is the integration of various technologies with identification, detection, network and processing capabilities that enable them to communicate with one another and with other devices and services over the Internet to achieve some goal. This article reports on the current state of research in the Internet of Things, where different views of this paradigm are described, exemplifying its applicability and defining related concepts. The most relevant among them are covered in detail. Based on a careful evaluation of some IoT applications around the world, it was sought to evaluate the most important aspects in the development of applications for this area and the feasibility of it now and in the near future.*

Resumo. *A Internet das Coisas (IoT) provavelmente será um dos avanços tecnológicos mais importantes dos próximos anos. O principal fator habilitador desse paradigma promissor é a integração de várias tecnologias com recursos de identificação, detecção, rede e processamento que lhes permitam se comunicar uns com os outros e com outros dispositivos e serviços pela Internet para atingir algum objetivo. Este artigo relata o estado atual da pesquisa na Internet das Coisas, onde diferentes visões deste paradigma são descritas, exemplificando a sua aplicabilidade e definindo conceitos relacionados. Os mais relevantes entre eles são abordados em detalhes. A partir de uma avaliação criteriosa de algumas aplicações de IoT pelo mundo, procurou-se avaliar os aspectos mais importantes no desenvolvimento de aplicações para esta área e a viabilidade da mesma no momento atual e num futuro próximo.*

1. Introdução

A comunicação por meio da tecnologia é indispensável tanto na atualidade quanto, e principalmente, no futuro. Dentre todas as novas tendências tecnológicas, criações de novos produtos e serviços que ocorrem neste momento, talvez uma das maiores mudanças e uma das mais fundamentais, seja a Internet das Coisas (também conhecida por IoT - *Internet of Things*, em inglês).

A IoT ainda está em processo de amadurecimento, aparentando que irá demorar para acontecer de fato. Levando em consideração que a tecnologia tende-se a desenvolver rapidamente, e considerando-se que a IoT propõe-se ser a próxima

evolução da Internet, esta acaba tendo sua importância, com o papel de prover um grande avanço na capacidade de coletar, analisar e distribuir dados que podem ser transformados em informações, conhecimento e, por fim, sabedoria.

O primeiro dispositivo conectado à internet surgiu em 1990, John Romkey (um dos fundadores do *software* FTP, fornecedor comercial de pilhas TCP / IP e desenvolveu partes cruciais da internet assim como conhecemos hoje) criou o primeiro dispositivo em IoT que é uma torradeira que poderia ser ligada e desligada pela Internet, e a apresentou na INTEROP '89 Conference, feira anual de tecnologia da informação (DEORAS, 2016). A motivação para tal fato saiu na verdade de um desafio lançado a John Romkey pelo presidente da INTEROP na época, Dan Lynch. Lynch prometeu a Romkey que, se a torradeira fosse ligada pela internet, o aparelho seria colocado em exposição durante a conferência.

Diante deste desafio, John Romkey demonstrou o dispositivo no Interop 1990, que com efetividade conectou a torradeira em um computador via rede TCP / IP. O único empecilho, no entanto, é que o pão foi colocado manualmente na torradeira.

No ano seguinte, esse déficit foi corrigido e apresentado na mesma conferência, incluindo um pequeno guindaste robótico no sistema. Esse robô, controlado via internet, pega a fatia de pão e insere na torradeira, automatizando, portanto, o sistema de por completo.

O termo "Internet das coisas" surgiu em 1999, onde Kevin Ashton do MIT, falava durante uma apresentação para executivos da Procter & Gamble sobre a ideia de se etiquetar eletronicamente os produtos da empresa para facilitar a logística da cadeia de produção, através de identificadores de rádio frequência (*Radio Frequency Identification* - RFID) e assim propôs o termo "Internet das Coisas" (ASHTON, 2009). Dez anos depois escreveu o artigo "A Coisa da Internet das Coisas" para o RFID *Journal*. Segundo Kevin, a "Internet das Coisas" se refere a uma revolução tecnológica que tem como objetivo conectar os equipamentos usados no dia a dia à rede mundial de computadores.

A IoT conecta todos possíveis objetos em potencial para interagirem entre si via internet e proporcionar vida segura para o ser humano.

A IoT propõe-se a conectar o mundo em amplas situações. Hoje em dia, existe uma infraestrutura da Internet onde quer formos e podemos utilizá-la quando quisermos. Dispositivos de computação incorporados estarão expostos à influência da internet. O verdadeiro valor da IoT não tem como proposta somente acender as luzes quando o carro chega à entrada, mas sim interligar os dados que os dispositivos conectados coletam sobre seus usuários. Imaginando-se um hospital com dispositivos conectados, os dados coletados desses dispositivos produzem, por exemplo, informações sobre o *status* dos pacientes e executam análises nas várias máquinas de monitoramento, ajudando o hospital a executar o melhor atendimento possível.

A IoT tenta estabelecer uma conectividade avançada (com a ajuda da Internet) entre esses dispositivos, sistemas ou serviços mencionados, de modo a facilitar a automação em todas as áreas. Entende-se que tudo está conectado e todas as informações interagem umas com as outras através de diferentes domínios de protocolo e aplicações.

O objetivo principal deste trabalho é dar uma perspectiva a respeito da IoT e comparar ao menos cinco iniciativas pelo mundo de implementações deste novo viés, avaliando questões como custo, desempenho, segurança e outros fatores para tentar chegar a um modelo que pudesse aliar baixo custo e grandes chances de sucesso nos projetos. Tem-se, por segundo intuito, promover este trabalho como mais uma referência sobre o assunto, ainda tão escasso em termos de publicações científicas.

Este artigo está organizado em quatro partes. Na primeira, procura-se exemplificar a sua aplicabilidade e definir conceitos relacionados. Na segunda parte, são mostradas tecnologias envolvidas na implementação de aplicações em IoT, tais como equipamentos, linguagens, plataformas, arquiteturas e modelos de desenvolvimento. Na terceira, é realizada uma análise comparativa de implementações, relacionando iniciativas pelo mundo de aplicações dirigidas à IoT. Para finalizar, serão expostas as conclusões a respeito do estudo, quais desafios futuros, além de indicações de trabalhos futuros.

2. Internet das coisas, sua aplicabilidade e conceitos relacionados

Conforme conceito da IoT, definido em (VERMESAN, FRIESS, *et al*., 2009): "Uma infraestrutura de rede dinâmica e global com capacidades de autoconfiguração baseadas em protocolos de comunicação padronizados e interoperáveis nos quais as 'coisas' físicas e virtuais têm identidades, atributos físicos, personalidades virtuais, usam interfaces inteligentes e são completamente integradas na rede de informação. Na IoT é esperado que as 'coisas' se tornem participantes ativas dos negócios e dos processos informacionais e sociais nos quais eles são capazes de interagir e comunicar-se entre eles e com o ambiente através da troca de dados e informação percebida sobre o ambiente, enquanto reagem de forma autônoma aos eventos do 'mundo físico/real' e o influenciam ao iniciar processos que engatilham ações e criam serviços com ou sem intervenção humana direta".

A ideia básica da IoT é que todos os objetos que nos cercam serão parte da rede, interagindo para alcançar um objetivo comum. Portanto, o conceito de IoT visa conectar dispositivos, de tal forma que possam sentir aspectos do mundo real, reportar esses dados ou agir sobre eles. Em oposição à forma como a maioria dos dados na Internet são produzidos e consumidos por pessoas, mais informações seriam produzidas e consumidas por máquinas, comunicando-se entre eles com intuito de melhorar a qualidade de nossas vidas. Os avanços de tecnologia, juntamente com a demanda popular, promoverão a implantação ampla dos serviços da IoT, transformaria radicalmente nossas corporações, comunidades e esferas pessoais.

Para (ZCORUM, 2016), a IoT refere-se a dispositivos inteligentes e conectados em casas, negócios e nos ambientes ao nosso redor que têm a capacidade de comunicar-se com outros dispositivos através de uma rede. Esses dispositivos estão emparelhados com sensores coletores de dados para que eles possam comunicar-se uns com os outros como uma maneira de determinar a saúde e o status das coisas, inanimadas ou vivas.

Embora possa-se pensar que a IoT é a comunicação de dispositivo a dispositivo, ao longo de uma rede fechada, tais como o aplicativo para mudar canais em seu dispositivo de TV a cabo ou *smartband* que informa quantos passos você deu hoje. Essa

operação é apenas uma rede interna ou intranet, e não a rede mais ampla habilitada para sensores que conecta uma multidão de coisas com uma multidão de outras coisas. Um aplicativo de aspersão de gramado pode ligar e desligar o sistema de irrigação, ou o aplicativo de contador de passos conta a quantidade de passos realizados e calorias queimadas, porém esses aplicativos não interagem fora dessa rede fechada (CHASE, 2013). É por isso que se cria um aplicativo separado para cada coisa "inteligente". Um aplicativo controla sua porta da garagem, outro controla o irrigador no gramado e assim por diante. Gerenciar todos esses aplicativos seria o equivalente a possuir múltiplos controles remotos, um para cada dispositivo.

Diante desses aspectos apresentados, a IoT apresenta-se como uma rede de dispositivos "inteligentes" implantados. Tal qual um indicador de chuva ou sistema de iluminação que irá coletar dados, onde esses dados coletados serão então disponibilizados para muitas outras aplicações "inteligentes" como, por exemplo, o indicador de chuva comunicar ao sistema de irrigação de gramado por aspersão, que havia uma polegada de chuva na noite anterior e, portanto, ficará desligado no dia atual afim de conservar a água. Um *software* de orçamento doméstico poderia receber os dados sobre a quantidade de água que foi salva e prever o valor da conta de água do mês seguinte. Espera-se que esta verdadeira versão da IoT forneça muito mais valor do que possa ser derivado destas ilhas isoladas de informações (os aplicativos individuais) assim com temos agora.

Segundo a visão de Darnell (DARNELL, 2015), a IoT possui uma definição simples de se entender. Caso observado o conceito da expressão em si, temos uma boa ideia a respeito de ambas as palavras, Internet e coisas. Então, juntando-se as duas, pode-se pensar nisso como "coisas na Internet". Embora isto possa ser verdade até certo ponto, não diz exatamente o que realmente é a IoT e, mais importante, o que isso significa ou os motivos para se estuda-la.

A IoT tenciona-se a tratar a respeito de valores, ideias e oportunidades obtidas por meio da interconectividade de seus mundos físicos e digitais. Dependendo de suas necessidades específicas, o "valor" pode vir de várias formas. Por exemplo, se suas necessidades incluem o rastreamento e monitoramento de frotas de veículos, seu "valor" pode assumir a forma de conformidade do motorista, otimização de rotas, eficiência de combustível melhorada e agendamento mais preciso. Dispositivos conectados instalados em transportes públicos, em faixas ferroviárias e nas estradas, permitem que se receba condições de tráfego em tempo real e prevê contratempos em relação à performance de ônibus, viabilizando a manutenção no momento correto. Em termos de segurança, é possível manter seus entes queridos atualizados a respeito de seu estado atual, através de rastreadores pessoais estão disponíveis, para precisar sua localização atual e status de saúde. Por meio de dispositivos conectados é possível obter-se leituras em tempo real do estado atual do paciente para que médicos e enfermeiros, mesmo quando estão a milhares de quilômetros de distância dos pacientes, prestem atendimento médico efetivo em tempo real.

Em (DARNELL, 2015), menciona-se que a IoT seria basicamente a prática de conectar, monitorar e gerenciar suas "coisas" (ou dispositivos) de forma remota e autônoma. Ou seja, a capacidade de integrar seus dispositivos físicos com seus sistemas digitais, analisar esses dispositivos e os dados entre eles para obter informações sobre o

que está acontecendo no seu ambiente, processar esses eventos e tomar as ações conforme necessário.

Enquanto que para Wei Quan Liow (LIOW, 2017), a definição de IoT tem-se em uma rede de máquinas e dispositivos inteligentes, tais como *tablets*, *smartwatches* ou mesmo seus refrigeradores, que estão conectados a uma rede comum, como a internet. Embora uma tecnologia nova, em ascensão, a IoT não é algo que devesse-se temer e sim aderir-se às amplas oportunidades e aprimoramentos possibilitados pela IoT para nossas vidas cotidianas. Atualmente já se encontra alguma forma de IoT no cotidiano diário, em termos de uso de *smartphones*, equipamentos de escritório e até mesmo em banheiros.

Em automóveis, os sensores já estão incluídos para melhorar a experiência de condução, proporcionando vários benefícios antes inexistentes. Sensores de frenagem antibloqueio e sensores de pressão de pneus baixos para garantir a segurança. O advento do sistema de alerta de partida da pista propõe extinguir a necessidade de manter o carro na pista. Os carros tendem a se tornar o maior avanço no ecossistema IoT, diretamente conectado à computação em nuvem com o uso de aplicativos móveis, computadores de bordo, chips inteligentes, sensores e tecnologias sem fio (GERLA, *et al*., 2014).

Além dos carros, a IoT encontra-se presente nos dispositivos móveis, como os *smartphones* utilizados atualmente, possuindo recursos como aplicativos, chips e sensores para detectar a localização, fornecimento rotas de direção e alertas de trânsito. Escritórios, casas e portas do hotel podem ser abertos utilizando-se *smartphones* em vez de cartões-chave e chaves normais. Smartphones estão conectados diretamente à internet e é possível conectá-los a outros dispositivos, como relógios, pulseiras inteligentes e monitores de frequência cardíaca. O *smartphone* tende a se tornar o ponto de controle central para os usuários do ecossistema IoT.

Segundo (LIOW, 2017), a IoT não é mais uma ficção científica. Preconiza-se que devesse tratar a IoT, em primeiro lugar, como uma extensão de si próprio para realizar coisas que costumava-se fazer, porém ficando muito mundano para ser executado. Ou, IoT poderia ser uma extensão da própria pessoa para realizar tarefas que costumavam ser muito perigosas e impossíveis de se realizar no passado.

3. Tecnologias para implementação de aplicações em Internet das coisas

A atualização do conceito IoT só pode ser realizado por meio da integração útil de várias tecnologias habilitadoras que cobrem o domínio de *Hardware*, *Software* e aplicativos extremamente robustos em torno de cada domínio de indústrias e setores operacionais (ATZORI, IERA e MORABITO, 2010).

Neste contexto, esta seção apresentará as mais relevantes áreas de tecnologia que possibilitam a utilização da IoT e algumas de suas aplicações.

3.1. Tecnologias de identificação

A função de identificação é mapear um identificador exclusivo para uma entidade de modo a extinguir qualquer ambiguidade. A implantação da IoT exige o

desenvolvimento de novas tecnologias que precisam abordar os esquemas globais de identificação, gerenciamento de identidade, codificação/criptografia de identidade, autenticação e gerenciamento de repositórios, utilizando-se de esquemas de identificação e endereçamento e da criação de serviços de pesquisa de diretórios globais (BANDYOPADHYAY e SEN, 2011).

No contexto descrito acima, um dos componentes mais utilizados da IoT são os sistemas RFID, que são um grande avanço no paradigma de comunicação incorporado, compostos por um ou mais leitores e várias *tags* (etiquetas) RFID que permitem a comunicação de dados sem fio.

Uma *tag* RFID é um pequeno microchip ligado a uma antena, usada tanto para receber o sinal do leitor quanto para transmitir a identificação da *tag*, em uma embalagem que geralmente é semelhante a um adesivo (Figura 1).

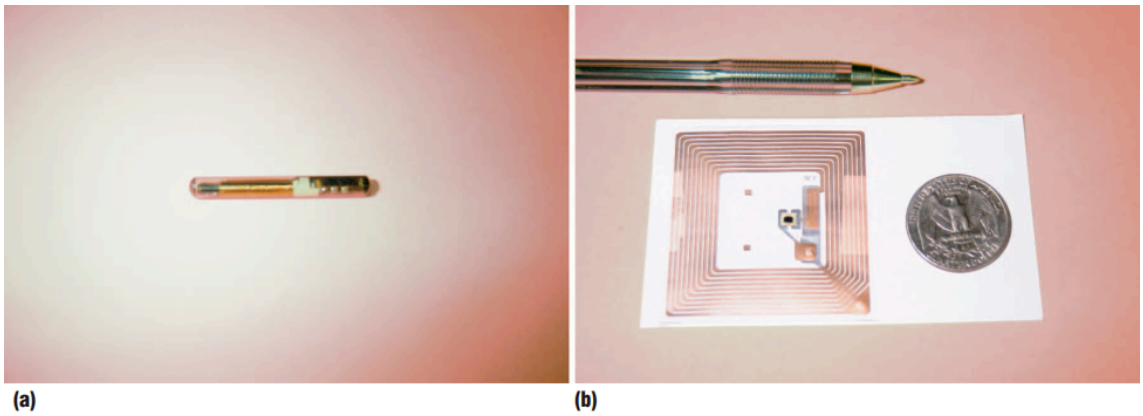

Figura 1. (a) *tag* Trovan de 128 kHz, encapsulada em um frasco de vidro pequeno de aproximadamente 1 cm de comprimento e (b) *tag* Tiris de 13,56 MHz, que possui um substrato de plástico laminar (aproximadamente 5 5 cm) com adesivo para facilitar a fixação em mercadorias.

Fonte: (WANT, 2006)

Existem apenas dois possíveis conceitos de física utilizados pela tecnologia RFID para detecção de *tags* RFID. Eles são: conceito de curta distância (*Near Field Concept*) e conceito de longa distância (*Far Field Concept*).

O acoplamento de curta distância é a abordagem mais direta para a implementação de um sistema RFID passivo. Ao contrário das *tags* de longo alcance, que enviam um campo eletromagnético de propagação, as *tags* de curta distância geram um campo magnético local. São tipicamente menos resistentes e geralmente destinadas a ambientes internos. Como são menos utilizadas, as opções disponíveis para implantação são limitadas.

Os sistemas do longo alcance focam-se na potência real contida no espaço livre, propagando-se por ondas eletromagnéticas. Possuem uma grande variedade de formas e tamanhos, podendo ler *tags* entre em uma distância de alguns centímetros ou até mais de 30 metros, nas condições ideais. Muitas opções estão disponíveis para utilização de uma *tag* de longa distância, como polarização linear ou circular, ganho variável e

opções para uso interno ou externo. Devido ao tamanho da zona de leitura, um problema comum para esse tipo de *tag*, é a leitura de *tags* RFID não intencionais.

As *tags* RFID são utilizadas na rotina diária das pessoas. Alguns exemplos incluem (JUELS, 2005):

- Cartões de proximidade, ou seja, os cartões sem contato usados para construir o acesso.
- *Transponders* automatizados de pagamento de pedágio, pequenas placas montadas em para-brisas de automóveis.
- Chaves de ignição de automóveis, que incluem *tags* RFID como mecanismo contra roubo.
- *Tokens* de pagamento: nos Estados Unidos, o *token SpeedPass* para pagamentos de estações de gasolina. Cartões de crédito sem contato, como o *American Express ExpressPay* e o *Mastercard PayPass*, utilizam RFID.
- Animais de estimação com *tags* RFID implantadas, para facilitar o retorno aos seus proprietários caso eles se percam.

As *tags* atuam como um código de barras eletrônico, caracterizadas por um identificador exclusivo, ajudam na identificação automática de qualquer objeto ligado a elas (podendo também ser aplicados a pessoas ou animais).

O *transponder*, ou a *tag* RFID, utiliza um microchip para armazenar informações, como um código de identificação eletrônico. A unidade de leitura consiste de uma antena e transmissor de rádio com uma capacidade de decodificação anexada a um dispositivo fixo ou portátil. Quando uma etiqueta RFID está dentro do alcance das ondas de rádio emitidas pelo leitor, a *tag* é ativada e começa a enviar dados. O leitor captura esses dados, decodifica-os e os envia de volta por uma rede com ou sem fio para um computador *host* para processamento posterior, como mostra a Figura 2 a seguir.

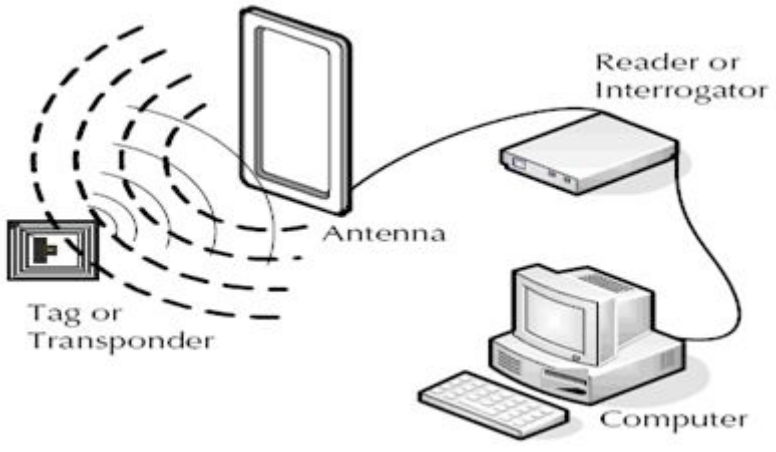

Figura 2. Funcionamento de um sistema de RFID.

Fonte: (AGARWAL, s.d.)

Em consequência disso, os sistemas RFID podem ser usados para monitorar objetos em tempo real, sem a necessidade de estar em linha de visão; permitindo o

mapeamento do mundo real para o mundo virtual (ATZORI, IERA e MORABITO, 2010).

3.2. Tecnologias de sensoriamento

As redes de sensores também desempenham um papel crucial na IoT, podendo cooperar com os sistemas RFID para melhor acompanhar o status das coisas, como por exemplo, sua localização, temperatura, movimentação, etc.

Os recentes avanços tecnológicos em circuitos integrados de baixa potência e comunicações sem fio disponibilizaram dispositivos em miniatura eficientes, como os sensores nós, de baixo custo e de baixa potência para uso em aplicações de sensoriamento remoto. A combinação desses fatores melhorou a viabilidade de utilizar uma rede de sensores (WSN – *Wireless Sensor Networks*) consistindo de um grande número de sensores inteligentes, permitindo a coleta, processamento, análise e disseminação de informações valiosas, reunidas em vários ambientes (AKYILDIZ, *et al*., 2002), atuando como uma ponte adicional entre mundo físico e digital.

As redes de sensores consistem em um certo número (que pode ser muito alto) dos nós de detecção que se comunicam através de múltiplos saltos (*multi-hop*), em redes de sensores sem fio.

As redes de sensores podem consistir diferentes tipos de sensores, capazes de monitorar uma ampla variedade de condições ambientais (AKYILDIZ, *et al*., 2002), incluindo temperatura, umidade, movimento veicular, condições de relâmpago, pressão, condição do solo, níveis de ruído, presença ou ausência de certos tipos de objetos, níveis de estresse mecânico em objetos anexados, e características como velocidade, direção e tamanho de um objeto.

Atualmente, a maioria das soluções de redes de sensores sem fio comercial baseiam-se no padrão IEEE 802.15.4, tecnologia de redes sem fios que tem com objetivo de realizar a interligação de pequenas unidades de comunicações de dados em áreas limitadas, que apresenta uma estrutura definida em camadas: a camada física (oferece uma série de serviços e mecanismos de controle de nível físico essenciais para as camadas superiores da arquitetura) e camada MAC (provê controle coordenado de acesso ao canal físico para a realização das transferências de todos os tipos), para comunicações de baixa taxa de baixa potência em redes de área pessoal sem fio (WPAN).

A facilidade de implantação é influenciada pelo tamanho físico e pelo custo de cada plataforma. Componentes menores usados como nós de sensores, podem ser colocados em mais locais e usados em mais cenários. Abaixo são listadas algumas plataformas de *hardware* da IoT (MAKSIMOVIć, *et al*., 2014):

- Raspberry Pi: é uma placa de computador pequena, poderosa, barata, que possui uma ampla gama de uso. Como é uma placa muito barata, com suporte para uma grande quantidade de periféricos de entrada, saída e de comunicação de rede, é a plataforma perfeita para realização da interface entre dispositivos diferentes, que torna o Raspberry Pi muito adequado para aplicações no conceito IoT.

- Arduino: Plataforma de computação física de código aberto, baseada em uma placa de microcontrolador simples. Ele pode receber entrada de uma variedade de sensores, possibilitando interação ambiental, como controle de luzes, motores e outros atuadores. O microcontrolador na placa de *hardware* pode ser programado usando a linguagem de programação Arduino e o Ambiente de Desenvolvimento Integrado Arduino (IDE - *Arduino Integrated Development Environment*).
- Udoo: Mini computador que pode ser usado tanto no Android como no Linux. Pode-se dizer que Udoo procura trazer os melhores elementos de Raspberry Pi e Arduino em um único mini-computador. O Udoo possui os melhores desempenhos entre as plataformas de hardware IoT consideradas, mas ao mesmo tempo seu preço é bastante alto.

3.3. Tecnologias de comunicação

O paradigma de comunicação são as redes de sensores sem fio (WSN - *Wireless Sensor Networks*), que por meio de cobertura via rádio, não requer a presença de um leitor (a comunicação é *peer-to-peer*, enquanto que é assimétrica para os outros tipos de sistemas).

Um RFID ativo (leitores RFID ativos possuem seu próprio suprimento de bateria e podem instanciar uma comunicação) é quase o mesmo que os nós WSN de extremidade inferior, com capacidade de processamento e armazenamento limitados. Os dados do sensor são compartilhados entre nós de sensores e enviados para um sistema distribuído ou centralizado para análise.

Normalmente, um nó (*hardware* do núcleo WSN) contém interfaces de sensores, unidades de processamento, unidades de transceptor e fonte de energia. São compostos de múltiplos conversores A/D para interface de sensores, e os nós sensores mais modernos têm a capacidade de se comunicar utilizando uma banda de frequência, tornando-os mais versáteis (AKYILDIZ, *et al*., 2002).

A maneira pela qual os dados são encaminhados de volta para o usuário nas redes WSN segue a arquitetura especificada na Figura 3. O sensor nó detecta os dados no ambiente e esses dados são encaminhados dos nós até chegar à um *gateway* (*sink*) de Sensores de rede integrados sem fio (WINS - *Wireless integrated network sensors*), que se comunica com o usuário através de serviços de rede convencionais, como a Internet.

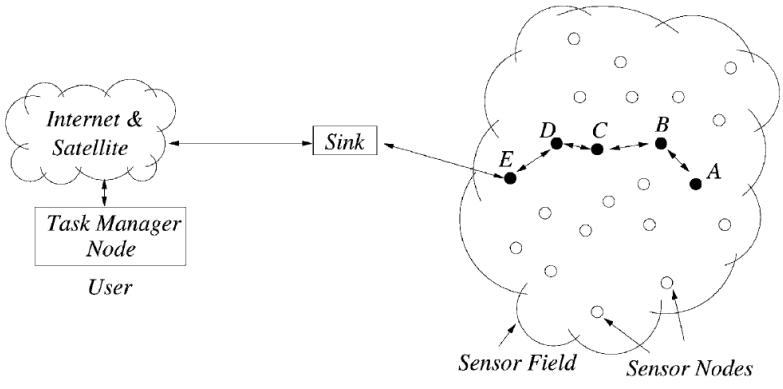

Figura 3. Sensores nós espalhados em um campo de sensoriamento.

Fonte: (AKYILDIZ, et al., 2002)

Os nós em uma WSN precisam comunicar entre si para que possam transmitir dados de maneira única ou em *multi-hop* para uma estação base. A pilha de comunicação no nó do coletor deve ser capaz de interagir com o mundo exterior através da Internet.

Como características das atividades de padronização mais relevantes, pode-se encontrar o uso extensivo da tecnologia ZigBee para permitir ambientes com ubiquidade (FERREIRA, DIAS CANEDO e DE SOUSA, 2013).

O ZigBee é uma tecnologia de padrão global para comunicação sem fio entre dispositivos IoT em uma área restrita e dentro de uma faixa de 100m, como em uma casa ou edifício. Possui vantagens significativas em sistemas complexos que permitem produtos de monitoramento e controle confiáveis, econômicos, de baixa potência, sem fio, permitindo a melhor utilização de controle sem fio e das redes de sensores nas aplicações de IoT.

3.4. Middleware

A camada de *middleware*, camada de software interposta entre os níveis tecnológico e de aplicação é um mecanismo que tem como objetivo combinar infraestrutura cibernética com uma arquitetura orientada a serviços (SOA - *Service Oriented Architecture*), que apesar desta já ter sido ultrapassada por novas tecnologias, ainda possui bastante aplicabilidade.

O middleware é um mecanismo para combinar a infra-estrutura cibernética com uma arquitetura SOA e redes de sensores para fornecer acesso a recursos de sensores heterogêneos de maneira independente de implantação. Baseia-se nas camadas de Aplicação, Composição do Serviço, Gerenciamento de Serviço, Abstração de objetos e Objetos (ATZORI, IERA e MORABITO, 2010).

Como observado na Figura 4 abaixo, as aplicações estão no topo da arquitetura, exportando todas as funcionalidades do sistema para o usuário final. A camada de Composição do serviço fornece as funcionalidades para a composição de serviços únicos oferecidos por objetos em rede para criar aplicativos específicos. No Gerenciamento de serviços as principais estão as funções que se espera que estejam disponíveis para cada objeto e que permitam seu gerenciamento no cenário IoT. Existe a necessidade da camada de Abstração capaz de harmonizar o acesso aos diferentes dispositivos com um idioma e procedimento comuns. Por fim, a camada de objetos, onde estão cada objeto na rede.

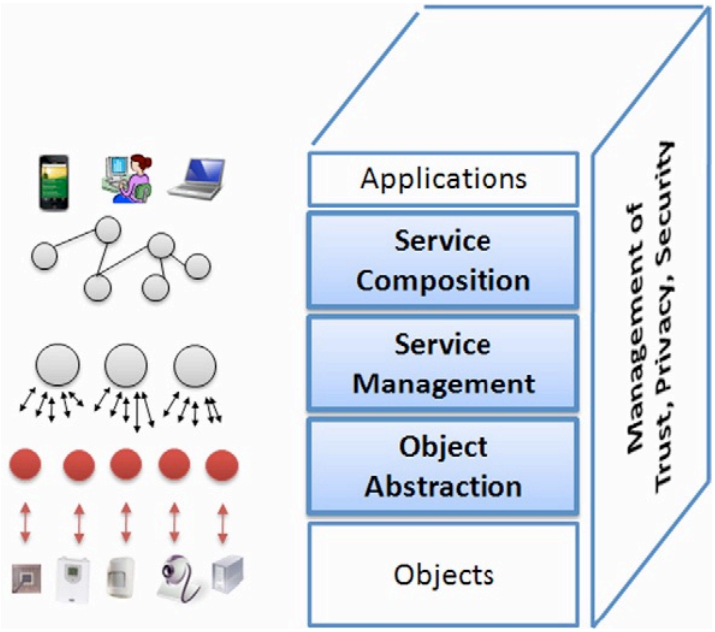

Figura 4. Camada *middleware* entre as aplicações e os objetos, conforme arquitetura SOA.

Fonte: (ATZORI, IERA e MORABITO, 2010)

A *middleware* é composta de redes de sensores com finalidade de fornecer acesso a recursos de sensores heterogêneos de maneira independente de implantação, baseado na ideia de isolar recursos que podem ser utilizados por várias aplicações. Sua característica de isolar os recursos de diferentes tecnologias é fundamental para isentar o programador de questões que não são diretamente pertinentes ao seu foco, que é o desenvolvimento da aplicação específica habilitada pelas infraestruturas IoT.

A adoção dos princípios SOA permite a decomposição de sistemas complexos em aplicações que consistem em um ecossistema de componentes mais simples e bem definidos, através da utilização de interfaces comuns e protocolos padrões, oferece uma visão horizontal de um sistema empresarial. Desta forma, o desenvolvimento de processos empresariais habilitados pela SOA é o resultado do processo de elaboração de fluxos de trabalho de serviços coordenados, que eventualmente estão associados a ações de objetos. Uma abordagem SOA também permite a reutilização de software e hardware, porque não impõe uma tecnologia específica para a implementação do serviço.

A middleware é um requisito essencial no desenvolvimento de aplicações conscientes. As soluções de middleware propostas permitem a comunicação e o gerenciamento de dados para aplicativos distribuídos, incluindo paradigmas de coordenação e comunicação entre componentes distribuídos. Porém a maioria das soluções não suporta a implantação e a configuração de novos componentes, a reconfiguração dinâmica de componentes ou a privacidade do usuário (HENRICKSEN, INDULSKA, *et al.*, 2005).

3.5. Áreas com aplicações baseadas na IoT

Diversas aplicações baseadas na IoT são desenvolvidas através das potencialidades oferecidas, das quais apenas alguns aplicativos são implantados no momento (GUBBI, BUYYA, *et al*., 2013).

As aplicações estão no topo da arquitetura, exportando todas as funcionalidades do sistema para o usuário final. Através do uso de protocolos de serviço *web* padrão e tecnologias de composição de serviços, as aplicações podem realizar uma perfeita integração entre sistemas distribuídos e aplicativos.

Os efeitos mais evidentes da introdução da IoT serão observados nos campos domésticos e de trabalho. Neste contexto, a domótica, a vida assistida, a saúde eletrônica, o aprendizado aprimorado são apenas alguns exemplos de possíveis cenários de aplicação em que o novo paradigma desempenhará um papel de liderança no futuro próximo.

Nas subseções a seguir, algumas das principais aplicações de exemplo da IoT são brevemente discutidas.

3.5.1. Veículos de transporte

Veículos são equipados com sensores que geram grande quantidade de dados a cada segundo, ao mesmo tempo em que as estradas são equipadas com *tags* RFID, componentes inteligentes, e microcontroladores embutidos.

Plataformas de sensores os quais fornecem informações aos motoristas, que por sua vez enviam dados filtrados dos sensores para a nuvem, como localização do GPS ou condições da estrada, ou para uma rede de veículos autônomos que trocam informações entre si.

Entretanto, a complexidade de controle da distribuição de centenas de milhares de carros tem que ser tomada em conta, por exemplo no caso de catástrofes naturais: os veículos devem ser capazes de coordenar a rota de evacuação da área de risco de maneira segura, rápida e organizada, além de conhecimento a respeito de recursos necessários (ambulâncias, veículos policiais).

Para que isso ocorra, necessita-se de uma comunicação eficiente e segura (a fim de evitar ataques maliciosos) entre si. Este ambiente eficiente de processamento de comunicações e distribuição pode ser fornecido por um novo paradigma de computação especificamente projetado para veículos: a Nuvem veicular (GERLA, et al., 2014).

3.5.2. Assistência médica

A assistência médica ubíqua tendo sido prevista durante as últimas duas décadas. A IoT oferece uma plataforma perfeita para realizar a previsão (realizada durante as últimas duas décadas) da assistência médica ubíqua utilizando-se sensores de área corporal e *backend* da IoT para enviar os dados para servidores.

Em (DOHR, MODRE-OPSRIAN, *et al*., 2010) introduz-se uma abordagem baseada na IoT em ambientes médicos para conseguir uma conectividade global com o

paciente, com sensores e tudo ao seu redor. O objetivo deste recurso é fornecer uma tecnologia consistente, segura e robusta para tornar a IoT uma realidade em ambientes médicos, além de fornecer uma sensibilidade ao contexto para tornar a vida do paciente mais fácil e o processo clínico mais eficaz.

Como exemplo de utilização da IoT em um cenário ambiental de assistência médica, pode-se citar pessoas idosas vivendo em suas casas equipadas com objetos inteligentes, como *smartwatches*, para comunicação entre si e elaborar a construção de uma rede de coisas. O *smartwatch* atua como terminal móvel para a pessoa e é capaz de enviar dados relevantes para um centro de serviço, onde eles são processados. Pessoas ligadas a um grupo de assistência têm acesso aos dados processados e podem interagir diretamente entrando em contato com a pessoa ou interagindo com os objetos inteligentes em torno da pessoa em questão.

3.5.3. Ambiente inteligente

Existem muitos tipos disponíveis de sistemas de automação residencial projetados e comprados para diferentes fins, sendo que um dos principais problemas na área é que esses diferentes sistemas não são interoperáveis nem interconectados, portanto a automação residencial é uma aplicação extremamente atraente da IoT.

A automação residencial proporciona um futuro ambiente doméstico onde sensores e atuadores integrados são autoconfigurados e podem ser controlados remotamente através da Internet, possibilitando uma variedade de aplicações de monitoramento e controle.

Os sistemas domésticos inteligentes, capazes de monitorar simultaneamente as atividades físicas gerais de um habitante, bem como entidades fisiológicas e ambientais, foram desenvolvidos para observar o bem-estar das pessoas idosas que vivem de forma independente na sua própria casa. Através de sensores espalhados em cada canto do ambiente, os sistemas obtêm todos os valores essenciais nos locais onde são aplicados para obter-se a determinação do bem-estar do indivíduo que vive neste local.

Em (KELLY, SURYADEVARA e MUKHOPADHYAY, 2013), relata-se uma implementação efetiva para a Internet de Coisas usadas para monitorar condições domésticas regulares por meio de um sistema de detecção ubíqua de baixo custo, através de uma arquitetura de rede integrada e de mecanismos de interconexão para medição confiável de parâmetros por sensores inteligentes e transmissão de dados via internet.

A automação residencial é uma aplicação extremamente atraente da Internet das coisas. Ele prevê um futuro ambiente doméstico onde sensores e atuadores integrados são autoconfigurados e podem ser controlados remotamente através da Internet, possibilitando uma variedade de aplicações de monitoramento e controle. Dentro deste contexto, podemos citar a domótica, importante conceito dentro da IoT, que envolve o controle e monitoramento de eletrodomésticos em um sistema unificado.

O significado de domótica está relacionado à instalação de tecnologia em residências, com o objetivo de melhorar a qualidade de vida, aumentar a segurança e viabilizar o uso racional dos recursos para seus habitantes (SGARBI e TONIDANDEL, 2007).

4. Análise comparativa entre as abordagens

As potencialidades oferecidas pelo IoT permitem desenvolver inúmeras aplicações com base nela.

Existem vários domínios de aplicação que são impactados. Nesta seção são apresentados cinco exemplos de aplicações com base em diversos domínios (monitoramento de ambiente, social, assistência médica) e realizada uma análise comparativa dessas aplicações.

As aplicações mencionadas foram selecionadas para serem exemplificadas pois combinam aspectos e tecnologias provenientes de diferentes abordagens, focando em desafios de pesquisa e questões abertas a serem enfrentadas para a realização do IoT no mundo real. O grande número esperado de dispositivos interconectados e a quantidade significativa de dados disponíveis abrem novas oportunidades para criar serviços que trarão benefícios tangíveis para a sociedade, meio ambiente, economia e cidadãos individualmente.

Os indicadores escolhidos foram levantados, segundo uma observação das características comuns descritas nos artigos pesquisados para este trabalho. Abaixo são descritas as variáveis de comparação e o critério utilizado para avaliação adotado em cada uma:

- Quantidade de Dispositivos IoT: baseado na quantidade de dispositivos, tendo a vista a complexidade e a área de atuação da aplicação. Categorizado em Baixa ou Alta quantidade.
- Desempenho: baseado na importância e na efetividade da aplicação. Categorizado em desempenho Satisfatório ou Não satisfatório.
- Custo: Custo geral de implementação da aplicação. Categorizado em Baixo ou Alto custo.
- Segurança: Risco e impacto em relação à probabilidade de eventualidade surgida a partir de falha de segurança. Categorizado em Baixo ou Alto risco.
- Desafios encontrados: Avaliação visto o nível da dificuldade relativa aos impedimentos encontrados durante a implementação da aplicação. Categorizado em Baixa ou Alta dificuldade.

4.1. Implementação da IoT para monitoramento de condições ambientais em casas

A inteligência ambiental responde ao comportamento dos habitantes em casa e fornece-lhes várias instalações. Em geral, o sistema de automação doméstica inteligente consiste em aglomerados de sensores, coletando diferentes tipos de dados, em relação aos residentes e ao consumo de utilidade em casa. Sistemas com capacidades informáticas analisam os dados assimilados para reconhecer as atividades de habitantes ou eventos. Existem vários exemplos de automação doméstica inteligente ou *Smart Home Monitoring*.

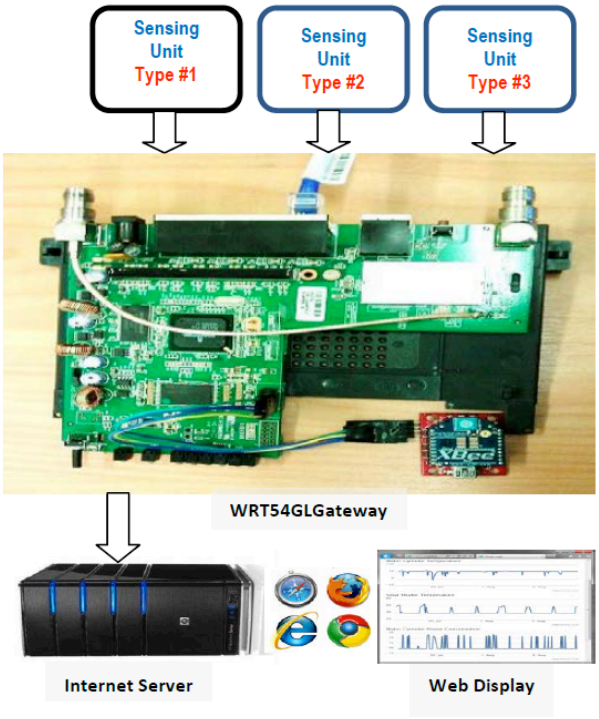

Figura 5. Estrutura geral do sistema conectando diferentes unidades de detecção.

Fonte: (KELLY, SURYADEVARA e MUKHOPADHYAY, 2013)

Em (KELLY, SURYADEVARA e MUKHOPADHYAY, 2013) apresenta-se uma solução efetiva de baixo custo e flexível para monitoramento de condições e gerenciamento de energia em casa. O esquema de automação residencial proposto pode medir parâmetros elétricos e controlar objetos domésticos através de certa distância. A intenção é evitar a utilização de diversos sistemas diferentes para monitoramento da utilização doméstica, portanto o sistema pode ser executado com a ajuda de um laptop ou i-Pad.

Os elementos-chave do sistema WSN integrado com sistema de internet consistem em um dispositivo de sensoriamento inteligente, um *Gateway* IoT e o Servidor de internet. Conforme a Figura 5, é possível visualizar que foram utilizados três diferentes tipos de unidades de detecção para o gerenciamento efetivo de dados nas redes IoT. A unidade de detecção tipo #1 mede os atributos de um sistema de água quente em casa; a unidade de detecção do tipo # 2 mede os parâmetros de corrente e tensão de um aparelho doméstico, indicando a energia consumida e o condicionamento do uso do aparelho; e a unidade de detecção tipo # 3 mede os valores de condicionamento ambiental, como temperatura, intensidade da luz, umidade, etc.

Como a maioria dos domínios da internet ainda operam usando IPv4 e a adoção do IPv6 é baixa, problemas como a disponibilidade de conectividade IPv6 podem ser uma grande preocupação na implementação dos métodos. Apesar disso, a vantagem do sistema desenvolvido é um maior controle sobre o roteamento de pacotes (segurança e personalização) e a capacidade de se adaptar a outras redes de sensores sem fio.

A estabilidade do monitoramento da condição dos aparelhos domésticos da IoT relacionado à interconexão com o WSN e o IPv6, mostra que a tecnologia IoT é

confiável na transformação da intranet de coisas na internet de coisas com utilização de sistema de baixo custo.

4.2. Conectando agricultura à Internet das Coisas através de redes de sensores

Com a ajuda da Internet, da comunicação móvel e das redes de sensores, os agrônomos, independentemente das restrições geográficas, podem fornecer orientações de cultivo oportunas, como o manejo de pragas, doenças e advertências climáticas desastrosas para os agricultores. Através da IoT, os agrônomos terão uma melhor compreensão dos modelos de crescimento das culturas além das melhorias na geração de produtos agrícolas.

Em (MA, ZHOU, *et al*., 2011) é discutido o design da rede de sensores ao conectar a agricultura à IoT, com foco em dois objetivos principais: ajudar os agrônomos a compreender melhor os modelos de crescimento das plantas, fornecendo aos mesmos um novo instrumento para suas observações, por meio das redes de sensores e da Internet; auxiliá-los a realizar as práticas agrícolas de forma mais eficiente, estabelecendo vínculos entre agrônomos, agricultores e culturas.

Arquitetura proposta do sistema consiste em um ambiente direcionado (estufas ou terras agrícolas), onde os nós sensores implantados e os nós de retransmissão formam uma rede multi-hop enraizada em um gateway.De acordo com as tarefas atribuídas pelo gateway, os nós sensores despertam periodicamente para tomar medições ambientais relevantes e enviar os dados diretamente ou através de *multi-hop* para o *gateway*. Dentre as medições está incluso temperatura e umidade relativa do ar, temperatura e umidade do solo, luz ambiente e concentração de CO2. O gateway envia os dados de sensor coletados para o servidor de comunicação, que armazena os dados no banco de dados. O sistema de apoio à decisão (DSS), contendo vários modelos agrícolas, analisa o banco de dados e publica orientações relevantes, como irrigação, manejo de pragas e advertências climáticas desastrosas, para os agricultores via SMS.

Os desafios foram encontrados durante o processo de desenvolvimento do software, pois dependiam do auxílio das obras existentes da comunidade de código aberto. Por este motivo, uma vez que não há garantia de correção para o *software* de fonte aberta, foi preciso realizar alterações no código ou esperar por consertos da comunidade quando há algo de errado. Além disso, as redes de sensores implantadas são notoriamente propensas a falhas e difíceis de depurar mesmo no caso de utilização de *hardware* de ponta e o *software* padronizado e atualizado.

4.3. Visão geral da IoT para pessoas com deficiências

A IoT permite novas formas de comunicação entre pessoas e coisas e entre as próprias coisas, portanto permite oferecer às pessoas com deficiência a assistência o apoio que precisam para alcançar uma boa qualidade de vida que lhes permita participar da vida social e econômica.

Em (DOMINGO, 2011), é fornecida uma visão geral da IoT para pessoas com deficiência, tendo como objetivo analisar como as pessoas com deficiências visuais,

auditivas e físicas podem interagir e se beneficiar do IoT. Para isso, discute-se uma arquitetura proposta a partir de uma perspectiva técnica da IoT, além da apresentação de diferentes cenários de aplicação são considerados para ilustrar a interação dos componentes da IoT, ferramentas poderosas para aumentar a independência e melhorar a participação.

A partir de uma perspectiva técnica, a arquitetura IoT proposta é dividida em três camadas: camada de percepção, a camada de rede e camada de aplicação.

A camada de percepção tem como principal função, identificar objetos e coletar informações conscientes do contexto relativas ao ambiente de pessoas com deficiência. É formado principalmente por sensores e atuadores, estações de monitoramento (como telefone celular, *tablet* PC, smartphones, etc.), nano-nós e *tags* RFID.

A camada de rede consiste em uma rede convergente composta por redes de rede privada com fio / sem fio, internet, sistemas de administração de rede, etc. Sua principal função é transmitir informações obtidas a partir da camada de percepção. As redes sem fio são uma boa opção para estabelecer comunicações no IoT, uma vez que não dependem de uma infraestrutura preexistente, elas requerem configuração mínima e são implantadas rapidamente com baixo custo. Os diferentes meios de transmissão incluem Redes de área local sem fio (WLANs) (IEEE 802.11), *Bluetooth* (IEEE 802.15.1), *ZigBee* (IEEE 802.15.4), *General Packet Radio Service* (GPRS), entre outros.

A camada de aplicação trata-se de um conjunto de soluções inteligentes que aplicam a tecnologia IoT para satisfazer as necessidades dos usuários. Esta camada fornece uma plataforma de suporte de operação, que pode ser acessada por estações de monitoramento e aplicativos. Fornece funcionalidades importantes como autenticação, cobrança, gerenciamento de serviços, aceitação de serviço e roteamento de pacotes.

Como exemplo de cenário de aplicação da IoT para pessoas com deficiência visual, pode-se utilizar o ambiente de compras em um supermercado. As *tags* RFID anexadas aos produtos do supermercado fornecem dados do produto, como nome, descrição, preço, temperatura ou choques durante o transporte. O leitor de etiquetas (bengala com RFID) transmite a sequência de identificação da etiqueta para a estação de monitoramento, que a encaminha para o servidor RFID, onde as informações do produto são retornadas do banco de dados RFID para a estação de monitoramento e são reproduzidas em forma de mensagens de voz.

Um desafio fundamental encontrado é a personalização para pessoas com deficiência, pois a IoT deve ser adaptada às suas circunstâncias particulares. A padronização também é um desafio muito importante, pois torna-se necessário criar padrões aceitos globalmente para evitar problemas de interoperabilidade.

4.4. A Internet das coisas na Assistência à Autonomia Domiciliar

A Assistência à Autonomia Domiciliar (AAL - *Ambient Assisted Living*) abrange sistemas técnicos que buscam apoiar pessoas idosas e pessoas com necessidades especiais em sua rotina diária, para aumentar a segurança em seu estilo de vida e em seu ambiente doméstico.

Para permitir maior segurança e bem-estar na casa, a casa precisa se tornar inteligente com a ajuda de itens inteligentes, que é o princípio da Inteligência Ambiental.

Em (DOHR, MODRE-OPSRIAN, *et al*., 2010) é apresentado o desenvolvimento de uma tecnologia que possui o objetivo de coletar e encaminhar os dados necessários para pessoas cronicamente doentes e pessoas idosas para monitorar o estado de saúde e a adesão à terapia, a KIT. *Keep In Touch* (KIT) usa objetos inteligentes e tecnologias (NFC - *Near Field Communication* e RFID - *Radio Frequency Identification*) para facilitar os processos de telemonitoramento.

A comunicação pessoal entre pessoas idosas, seu ambiente e grupos relevantes de cuidadores é um aspecto importante na AAL. Através da combinação de KIT e dos serviços de assistência médica, um paradigma central da AAL pode ser realizado através da IoT, capazes de processar dados relevantes e estabelecer canais de comunicação entre pessoas idosas e seu ambiente e diferentes grupos de cuidadores (médicos, parentes, provedores de cuidados móveis) possibilitando os idosos de viverem em suas casas com objetos inteligentes, logo casas inteligentes, comunicando-se com o mundo exterior.

O uso da tecnologia RFID e NFC, através da criação de uma aplicação com alta usabilidade e manipulação intuitiva, soluciona os problemas de usabilidade e conformidade terapêutica em sistemas de monitoramento de telefonia. Porém, o fator econômico de implementar a AAL através da IoT deve ser levado em conta, com o aumento associado dos custos de cuidados de saúde.

4.5. Aplicação de Internet das coisas da Comunidade inteligente

As casas inteligentes avançam para o futuro ambiente doméstico onde os sensores e atuadores incorporados são autoconfigurados e podem ser controlados remotamente através da Internet, possibilitando uma variedade de aplicativos de monitoramento e controle.

Em (LI, LU, *et al*., 2011) apresenta-se o conceito de casa inteligente de uma forma adicional, criando-se assim a noção de comunidade inteligente. A comunidade inteligente, é uma aplicação de internet de coisas que se refere a uma classe paradigmática de casas inteligentes em rede.

Define-se uma arquitetura da comunidade inteligente e descreve-se o modo de utilização de redes seguras e robustas entre casas individuais. Pode ser visto como um sistema cibernético, em que as casas são sensores virtualmente multifuncionais com necessidades individuais, monitorando continuamente vários aspectos do ambiente da comunidade e, quando necessário, o feedback físico automático ou controlado por humanos é incorporado para melhorar a segurança da comunidade, a segurança do lar, a qualidade da saúde e as habilidades de resposta em uma emergência. Uma comunidade inteligente é uma rede multi-instalações de casas inteligentes que estão interligadas através de frequências de rádio seguindo padrões de comunicação sem fio, como Wi-Fi (IEEE 802.11) e a terceira geração (3G) de telefonia móvel.

A plataforma da comunidade inteligente pode suportar muitas aplicações, uma das principais a Vigília de vizinhança (*Neighborhood Watch*), que melhoram a

segurança da comunidade, segurança doméstica e habilidades de resposta de emergência.

Vigílias de vizinhança são programas implementados como uma função de uma associação comunitária, envolvendo um grupo de residentes dedicados à prevenção do crime e do vandalismo dentro de um bairro. O ambiente da comunidade inteligente fornece uma plataforma perfeita para implementar vigília de vizinhança sem vigias autônomos, economizando recursos humanos e aumentando a eficácia.

As casas individuais são equipadas com câmeras de vigilância, que monitoram continuamente o entorno de suas casas, incluindo não apenas as imediações das casas, mas também os segmentos de rua mais próximos, além de sensores com faixa de detecção limitada. A rede comunitária é, portanto, uma rede de sensores sem fio que cobre a região geográfica da comunidade. As casas detectam eventos suspeitos e decidem se um evento detectado é uma ameaça à segurança. Caso necessário, informam outros membros da comunidade ou entram em contato com o *call center*.

São encontrados alguns desafios em relação à aplicação, como no caso da vigília de vizinhança, onde os algoritmos de rastreamento de destino existentes não são projetados para ambientes de comunidades inteligentes, onde o movimento de um alvo é restrito nas ruas da comunidade.

Com dados de eventos coletados pelo algoritmo de rastreamento usado, é preciso classificar o evento como normal ou suspeito. Esta classificação envolve definir padrões de mobilidade suspeitos e comparar um padrão de mobilidade de evento detectado com os padrões maliciosos definidos para tentar encontrar uma correspondência. Portanto necessita-se de algum algoritmo de correspondência compatível com o contexto inteligente para evitar ou minimizar falsos positivos e falsos negativos.

4.6. Análise comparativa

De acordo com as abordagens exemplificadas, foram levantados todos os indicadores de cada critério estabelecido (Dispositivos IoT, Desempenho, Custo, Segurança, Desafios encontrados e Exemplo de Aplicações) resultando na tabela 1 comparativa abaixo:

Tabela 1. Tabela de análise comparativa entre as aplicações abordadas

	1	2	3	4	5
Quantidade de Dispositivos IoT	Alta	Baixa	Baixa	Baixa	Baixa
Desempenho	Satisfatório	Satisfatório	Satisfatório	Satisfatório	Satisfatório
Custo	Baixo	Baixo	Baixo	Baixo	Baixo
Segurança	Alta	Alta	Baixa	Baixo	Alta
Desafios encontrados	Alto	Baixo	Baixo	Alto	Baixo
Exemplo de Aplicações	Vigília de vizinhança (Neighborhood Watch)	Terapia de diabetes em AAL (JARA, ZAMORA e	Supermercado, ambiente escolar	Rastreamento de animais; Produção e alimentação	Design de casas inteligentes

Legenda:
(1) Comunidade inteligente
(2) Assistência à Autonomia Domiciliar
(3) IoT para pessoas com deficiências
(4) IoT na agricultura
(5) Condições ambientais domiciliares

Conforme análise realizada, nota-se uma constante em alguns aspectos como os dispositivos utilizados, a questão do custo e a questão de segurança.

As "coisas" ou objetos inteligentes são participantes ativos nos processos de interação e comunicação, entre si e com o meio ambiente, trocando dados e informações detectadas. Os dispositivos utilizados possuem sensor ou atuador, onde podem funcionar juntos, formando por exemplo, uma rede de sensores sem fio (WSN). Neste contexto, os componentes chave da IoT serão o RFID, NFC e Sensores de rede.

Aliado a isto, com exceção, por exemplo, de outros fatores como em (DOHR, MODRE-OPSRIAN, *et al*., 2010) onde o custo está relacionado aos cuidados com a saúde, o desenvolvimento de nó de sensores inteligentes é de baixo custo, habilitando os dispositivos a serem conectados facilmente para que a informação correspondente possa ser acessada globalmente.

Geralmente os problemas relacionados à segurança são os mesmos, pois à medida que mais e mais objetos se tornam passíveis de serem encontrados com maior facilidade através do IoT, visto que os dispositivos IoT normalmente são wireless e podem estar localizados em locais públicos, as ameaças à privacidade pessoal se tornam mais graves. A comunicação sem fio na Internet de hoje é tipicamente mais segura através da criptografia, portanto vista como a chave para garantir a segurança da informação na IoT. No entanto, muitos dispositivos IoT não são atualmente suficientemente poderosos para suportar essa criptografia robusta. Além da criptografia, o gerenciamento de identidade é um componente importante de qualquer modelo de segurança e os identificadores exclusivos são essenciais para dispositivos IoT.

Em questão de desempenho, o conceito central é que os objetos do cotidiano podem ser equipados com recursos de identificação, detecção, rede e processamento que lhes permitam se comunicar uns com os outros e com outros dispositivos e serviços pela Internet para conseguir alguns objetivos úteis. Nesse sentido, planejamento e design é

um processo social contínuo, no qual o desempenho de cada item foi relatado e comparado com os outros.

As potencialidades oferecidas pelo IoT permitem desenvolver inúmeras aplicações baseadas nela, das quais apenas alguns aplicativos são implantados no momento. O domínio das áreas de aplicação para o IoT é limitado apenas pela imaginação neste ponto. No futuro, haverá aplicações inteligentes para lares e escritórios inteligentes, sistemas de transporte mais inteligentes, hospitais mais inteligentes, empresas e fábricas mais inteligentes.

5. Conclusão e Sugestões para trabalhos futuros

A proliferação de dispositivos com capacidades de comunicação está aproximando a visão de uma Internet de Coisas, onde as funções de detecção e atuação se misturam perfeitamente ao fundo e novas capacidades são possíveis graças ao acesso de novas fontes de informação. A IoT é uma tecnologia emergente ideal para influenciar este domínio, fornecendo novos dados em evolução e os recursos computacionais necessários para a criação de aplicativos revolucionários. Baseando-se em tecnologias existentes, tais como RFID e WSN, juntamente com padrões e protocolos para suportar a comunicação máquina-máquina.

Neste artigo são apresentadas as mais relevantes áreas de tecnologia que possibilitam a utilização da IoT e algumas de suas aplicações. Além de apresentados cinco exemplos de aplicações com base em diversos domínios (monitoramento de ambiente, social, assistência médica) e realizada uma análise comparativa dessas aplicações.

Tendo em vista as tecnologias de última geração de hoje, obtém-se uma indicação clara de como a IoT será implementado em um nível universal nos próximos anos. Também temos uma indicação dos aspectos importantes que precisam ser mais estudados e desenvolvidos para fazer uma implantação em larga escala de IoT uma realidade. Embora as tecnologias atuais tornam o conceito IoT viável, não se encaixam bem com os requisitos de escalabilidade e eficiência que enfrentarão. Acredita-se que nos próximos anos, abordar tais questões será um poderoso motor de busca para pesquisas em redes e comunicação.

A IoT tem a promessa de melhorar a vida das pessoas através da automação. As possibilidades oferecidas pela IoT podem economizar tempo e dinheiro para pessoas e organizações, além de ajudar a melhorar a tomada de decisões e os resultados em uma ampla gama de áreas de aplicação. Com os avanços na tecnologia, espera-se que a disponibilidade de internet esteja em todos os lugares e online em todos os momentos. O desenvolvimento de nós de sensores inteligentes de baixo custo permitiu dispositivos a serem conectados facilmente e permite que a informação correspondente possa ser acessada globalmente.

Diversos foram os desafios encontrados na IoT. Desfios éticos, tecnológicos, de segurança e privacidade.

Uma das às preocupações levantadas é de que as pessoas podem ter vivendo em um futuro ambiente conectado, pois a privacidade torna-se um desafio fundamental. As

arquiteturas tecnológicas que preservam o respeito da privacidade devem ser desenvolvidas e usadas como base para qualquer desenvolvimento futuro.

O domínio tecnológico da IoT abrange vários desenvolvimentos. Devido a isso, é bastante difícil estabelecer limites a fim de determinar claramente quais tecnologias estão dentro do seu alcance.

A questão de ter-se segurança suficiente em dispositivos com capacidades limitadas ainda não foi resolvida de forma convincente.

Resta-se saber se a IoT deve ou não ser uma tecnologia duradoura, seja caso falhe em materializar-se ou se será apenas um trampolim para outro paradigma.

Como possíveis trabalhos futuros, há uma necessidade emergente de se obter maior flexibilidade para se adaptar às mudanças de requisitos e desenvolvimentos tecnológicos para aplicações para IoT. O seu desenvolvimento pode ser acelerado, por exemplo, através da disponibilidade de software de código aberto e compartilhamento de soluções aos demais pesquisadores da área.

Devido ao seu caráter inovador e que, de certa forma, implementa soluções tecnológicas que interfere na vida pessoal de um indivíduo, a IoT, sobre alguns aspectos, tais como privacidade, controle domésticos e etc, necessita de se ter e pesquisar as questões relacionadas jurídicas e legais, além de governança que irão regular a IoT.

Uma pesquisa importante sobre a IoT seria investigar como os sistemas de informação que trabalham com dados IoT superam a complexidade inerente e o volume de dados para fornecer suporte de decisão útil. Além disso, há áreas de aplicativos não atendidas da IoT, como por exemplo, área militar, que seria viável a pesquisa de como ela poderia atender, usando de sua contextura atual e seus prognósticos futuros.

Além disso, pode-se estabelecer possíveis modelos de negócios da IoT que direcionarão negócios globais, além de se aplicar novas tecnologias já em processo de testes, tais como sensores inteligentes (bioquímicos), Nanotecnologia e novos materiais.

Esforços de pesquisa significativos no IoT são realizados, principalmente a partir da perspectiva orientada a coisas. No entanto, o lado social do IoT, ainda foi pouco explorado.

6. Referências

AGARWAL, T. **RFID – A Basic Introduction & Simple Application**. Elprocus. Disponivel em: <https://www.elprocus.com/rfid-basic-introduction-simple-application/>.

AKYILDIZ, I. et al. **Wireless sensor networks**: a survey, 09 Janeiro 2002.

ASHTON, K. **That 'Internet of Things' Thing**. RFID Journal, 22 Junho 2009. Disponivel em: <http://www.rfidjournal.com/articles/view?4986>.

ATZORI, L.; IERA, A.; MORABITO, G. **The Internet of Things**: A survey, 15 Outubro 2010.

BANDYOPADHYAY, D.; SEN, J. **Internet of Things - Applications and Challenges in Technology and Standardization**, 09 Abril 2011.

CHASE, J. **The evolution of the internet of things.** Texas Instruments, 2013.

DARNELL, L. **The Internet of Things:** A Look at Real-World Use Cases and Concerns. [S.l.]: Desconhecido, 2015.

DEORAS, S. **First ever IoT device**- "The Internet Toaster". IoT India Magazine, 05 Agosto 2016. Disponivel em: <http://iotindiamag.com/2016/08/first-ever-iot-device-the-internet-toaster/>.

DOHR, A. et al. **The Internet of Things for Ambient Assisted Living**, 14 Abril 2010.

DOMINGO, M. C. **An overview of the Internet of Things for people with disabilities**, 29 Outubro 2011.

FERREIRA, H. G. C.; DIAS CANEDO, E.; DE SOUSA, R. T. **IoT Architecture to Enable Intercommunication Through REST API and UPnP Using IP; ZigBee and Arduino**, 25 Novembro 2013

GERLA, M. et al. Internet of vehicles: **From intelligent grid to autonomous cars and vehicular clouds**, 24 Abril 2014.

GUBBI, J. et al. **Internet of Things (IoT)**: A Vision, Architectural Elements, and Future Directions, 24 Fevereiro 2013.

HENRICKSEN, K. et al. **Middleware for distributed context-aware systems**, 31 Outubro 2005.

JUELS, A. **RFID Security and Privacy**: A Research Survey, 28 Setembro 2005.

KELLY, S. D. T.; SURYADEVARA, N. K.; MUKHOPADHYAY, S. C. **Towards the Implementation of IoT for Environmental Condition Monitoring in Homes**, 16 Maio 2013.

LI, X. et al. **Smart community**: an internet of things application, 10 Novembro 2011.

LIOW, W. Q. **Riding the Waves of Internet of Things**. [S.l.]: [s.n.], 2017.

MA, J. et al. **Connecting Agriculture to the Internet of Things through Sensor Networks**, 22 Outubro 2011.

MAKSIMOVIć, M. et al. **Raspberry Pi as Internet of things hardware: performances and constraints**, Junho 2014.

SGARBI, J. A.; TONIDANDEL, F. Domótica Inteligente: Automação Residencial baseada em Comportamento, 2007.

VERMESAN, O. et al. **Internet of Things Strategic Research Roadmap**, 15 Setembro 2009.

WANT, R. **An Introduction to RFID Technology**, 13 Fevereiro 2006.

ZCORUM. **The Internet of things explained**. [S.l.]: Marsha Hemmerich, 2016.