**Internet das Coisas: sua história, conceito e seu potencial de impacto mundial**

Jackson Platiny Soares Leite

[jacksonplatiny@hotmail.com](mailto:jacksonplatiny@hotmail.com). Instituto Federal da Paraíba.

**Resumo**

Internet das Coisas é uma tecnologia que vem ganhando cada vez mais espaço no cotidiano das pessoas e em suas áreas de atuação profissional, isso se dá graças a facilidade que a tecnologia proporciona para a solução de problemas e otimização de tempo de execução de certas atividades, graças a sua tecnologia que funciona em dispositivos que possuem conexão com a Internet. Por meio dessa conexão é possível a coleta de um certo dado, através de sensores presentes nesse dispositivo e posteriormente envio desses dados para análise e processamento por algum sistema interconectado a esse dispositivo via Internet. Essa tecnologia tem o potencial de mudar o mundo, solucionando diversos problemas da atualidade, como problemas na área da saúde, indústria e infraestrutura, assim como também movimentar trilhões de dólares ao redor do mundo, e, portanto, é necessário que medidas sejam tomadas para visar a segurança dessa tecnologia e dos dispositivos que a possuem, o que cada vez mais vem sendo priorizado pelas empresas que desenvolvem dispositivos eletrônicos, onde os investimentos em pesquisas para segurança na área da Internet das Coisas já está na casa dos bilhões de dólares e cada vez crescendo mais. É certo de que o futuro está nessa tecnologia, mas como dito, é necessário muito investimento em segurança para garantir a qualidade dos serviços e sistemas que o utilizarão, que ao que os dados indicam, será concretizado.

**Palavras-chave:** Internet das Coisas; tecnologia; dispositivos; Internet; interconexão.

**Abstract**

*Internet of Things is a technology that has been gaining more and more space in people's daily lives and in their professional areas, thanks to the ease that technology provides for problem solving and optimization of certain activities, thanks to its technology that works on devices that have an Internet connection. Through this connection it is possible to collect a certain data through sensors present in this device and later send this data for analysis and processing by some interconnected system to this device via the Internet. This technology has the potential to change the world, solving many of today's issues, such as health, industry and infrastructure issues, as well as moving trillions of dollars around the world, and therefore action is needed to target the security of this technology and the devices that own it, which is increasingly being prioritized by companies that develop electronic devices, where investments in security research in the Internet of Things is already in the billions of dollars and each growing more and more. It is true that the future lies in this technology, but as said, much security investment is needed to ensure the quality of the services and systems that will use it, which data indicate will be realized.*

**Keywords:** *Internet of Things; technology; devices; Internet; interconnectivity.*

**Introdução**

O termo Internet das Coisas (IdC) vem do inglês *Internet of Things* (*IoT*) e foi cunhado pelo pioneiro tecnológico britânico Kevin Ashton em 1999, enquanto trabalhava em pesquisas relacionadas à identificação via radiofrequência (RFID) e a rede de sensores sem fio (RSSF) no laboratório de Auto-ID do Instituto de Tecnologia de Massachusetts (*MIT*) nos Estados Unidos. A IdC surgiu devido ao avanço de diversas áreas do conhecimento tecnológico, sendo algumas delas, os sistemas embarcados, sensoriamento, microeletrônica e comunicação. O trabalho no laboratório tinha como objetivo desde o início a criação de um sistema global de registros de bens utilizando um sistema de numeração único, que é o código do produto, e foi graças ao trabalho de Kevin Ashton, que enquanto trabalhava na área de RFID desenvolveu um sistema de sensores omnipresentes, que através disso conectava o mundo físico à Internet, e devido a isso que o conceito de IdC foi possível, mesmo que no seu primórdio a ideia era uma conexão máquina a máquina (*M2M*), enquanto atualmente a tecnologia avançou o suficiente para que possa haver uma interação homem a máquina(s). Embora a Internet, as "coisas" (*things*) e a conectividade entre elas sejam os três principais componentes da Internet, o valor acrescentado está no preenchimento das lacunas entre os mundos físico e digital em sistemas que existia até aquele momento. O primeiro dispositivo IdC foi desenvolvido por Simon Hackett e John Romkey em um desafio de uma feira anual de tecnologia da informação organizada pela empresa britânica UBM, e o objetivo dado a eles era conseguir fazer com que uma torradeira pudesse ser ligada e totalmente controlada através da Internet, o que eles conseguiram, ao conectá-la a um computador, o que os transformou na grande atração da feira. Posteriormente foi implementado um guindaste robótico ao protótipo original, cuja função era pegar o pão e adicionar na torradeira, o que possibilitou que absolutamente todo o processo envolvido nesse aparelho, fosse feito de forma automática. Como dito anteriormente, os estudos na área de radiofrequência foram essenciais para a viabilização da IdC, visto que a tecnologia RFID foi a maneira inicialmente encontrada para dar o pontapé inicial nesse conceito, e essa tecnologia se trata de um método de identificação automática, através de sinais de rádio que recupera e armazena dados remotamente através de dispositivos denominados etiquetas RFID, que por sua vez, é basicamente um transponder, que é um pequeno objeto que pode ser colocado nas coisas e é composto de chips de silício e antenas que lhe permitem responder a sinais de rádio enviados de uma base transmissora, assim como também em alguns casos essa etiqueta pode ser não só passiva (apenas responde ao sinal), como também ativa, que por possuir uma bateria, pode responder e transmitir seu próprio sinal.

**Conexão e funcionamento do dispositivo**

Para entender bem o conceito e o funcionamento de um dispositivo IdC, é preciso tomar conhecimento de que para algo estar conectado à Internet, é preciso que esse algo tenha um espaço único para si reservado na rede, um endereço virtual que seja apenas daquele objeto, para que ele possa receber, enviar e compartilhar dados pela Internet, e esse endereço é chamado de *Internet Protocol*, ou como é mais conhecido, endereço IP. Nos primórdios da internet, por volta de 1983, a versão do IP vigente era o IPv4 (*Internet Protocol version 4*), e partindo direto ao ponto, essa versão fornecia endereços de apenas 32 bits, o que significa dizer que o espaço de endereçamento que existia na rede naquela época, era de 2³² endereços, que resulta em aproximadamente 4,3 bilhões de endereços IP, onde desse total, haviam aproximadamente 18 milhões de endereços reservados para redes privadas e 270 milhões reservados para *multicast* (tipo de conexão para vários destinatários ao mesmo tempo). Com o surgimento da IdC, cada vez mais dispositivos estariam sendo conectados à Internet, e para isso tudo o que eles precisavam era de um endereço de IP único para si, porém os endereços disponíveis estavam se esgotando cada vez mais rápido, devido ao crescimento exponencial desses dispositivos. Em 2012 foi oficializado o IPv6, que, resumidamente, diferente do IPv4, fornece endereços de 128 bits, ou seja, 2^128, o que resulta em cerca de 340 undecilhões (3,4x10^38) de endereços únicos disponíveis, acabando assim com a preocupação quanto ao esgotamento de endereços livres por um longo tempo. Quanto ao funcionamento propriamente dito do dispositivo IdC, em primeiro lugar, para ligar os objetos e aparelhos do cotidiano a grandes bases de dados, e consequentemente as redes à rede das redes, à Internet, é necessário um sistema eficiente de identificação. Só desta forma se torna possível interligar e arquivar os dados próprios de cada coisa. O RFID, citado anteriormente, é um exemplo de sistema que possibilita isso, muito embora existam diversos outros, como por exemplo o *Bluetooth*, o *Wifi* e o *NFC* (*Near-field Communication*), que é a comunicação de campo próximo. Em segundo lugar, a base de dados se beneficiará da capacidade do dispositivo de identificar mudanças na qualidade física das coisas, recorrendo a métodos sensoriais. A inteligência tecnológica inerente de cada dispositivo aumentará a capacidade de a rede devolver a informação processada para diferentes pontos. Os avanços na área da nanotecnologia implicam que cada vez mais objetos pequenos poderão ser capazes de interagir e de se conectar a uma rede, e a combinação desses elementos é o que viabiliza cada vez mais a Internet das Coisas, que é a interligação de objetos reais do cotidiano, de um modo sensorial e inteligente.

**Aplicabilidades**

Os dispositivos IdC ou dispositivos *IoT* já estão presentes no dia a dia de muitas pessoas e já são utilizados em diversas áreas e a tendência é que cada vez mais aparelhos sejam agregados a tecnologia IdC para sanar problemas atuais. Na área da saúde por exemplo, a tecnologia IdC já é utilizada para transporte e armazenamento de vacinas. Segundo dados da Organização Mundial da Saúde (OMS), 1,5 milhões de crianças morrem anualmente por doenças que poderiam ser facilmente evitadas através de vacinas, e uma das causas associadas a esse problema era a falta de sistemas seguros de armazenamento e transporte de vacinas, visto que eles precisariam de uma ótima refrigeração e controle para preservar a integridade e qualidade das vacinas. O sistema chamado *Vaccine Smart Fridge*, funciona através de sensores que se encontram na própria geladeira portátil, conectados com uma plataforma *IoT*, que monitoram em tempo real o estado das vacinas, assim como a quantidade atualizada. Assim, os profissionais podem levá-las para qualquer lugar, com a garantia de que mais pessoas poderão ser vacinadas sem prejuízo. Outra aplicação ainda na área da saúde, é a utilização de *IoT* para o monitoramento em tempo real da evolução dos sintomas da doença *Parkinson* em pacientes. Este é o Projeto *Blue Sky*, fruto de uma parceria entre a empresa IBM e a companhia farmacêutica Pfizer. Por se tratar de uma doença degenerativa, crônica, neurológica e progressiva, é necessário monitorar se os pacientes estão respondendo positivamente ao tratamento, que é realizado através de remédios que buscam aumentar a qualidade de vida do paciente e retardar a degeneração, já que a doença ainda não possui cura. Já na área industrial, essa tecnologia já é utilizada na fabricação de veículos automotivos, possibilitando que eles forneçam ao seu dono informações acerca do veículo e do estado de seus componentes, motor, freios, *airbags*, travas, entre outros, em tempo real, mas não é só isso pois como o próprio veículo dispõe de diversos aparelhos *IoT* acoplados nele que adicionam funcionalidades como GPS, espelhamento de tela com aparelhos celulares, reconhecimento facial, dentre outras, as funcionalidades crescem ainda mais, por exemplo, com o reconhecimento facial, é possível identificar se o veículo foi furtado, e nesse caso, acionar as travas do veículo imediatamente, assim como emitir a localização do veículo para o dono e as autoridades locais, ou então em caso de acidentes, emitir sinal de emergência para que possa ser feito o socorro o mais rápido possível. Outro exemplo ainda na área industrial é a utilização de sistemas de IdC para otimizar o processo de fabricação de algo, atuando desde a matéria prima até o produto final. Esses sistemas podem ser divididos em subsistemas, onde cada um será responsável por alguma etapa ao longo de todo o processo de transformação do produto, agindo, por exemplo, no controle e qualidade do produto que chega, no tempo que o produto leva para sair da fábrica e através dessa informação controlar o maquinário para retardar, congelar ou acelerar o processo de produção a depender também dos dados gerados sobre os números de unidades no estoque, entre outras possibilidades. Indo para a área de geração de energia, o Brasil já conta por exemplo com IdC sendo aplicado para reduzir os custos da manutenção preditiva de parques eólicos no Ceará graças a sensores de pressão de temperatura instalados em cada turbina, possibilitando assim que seja possível saber antecipadamente se algum equipamento da turbina está se desgastando além do esperado. A ideia é que a tecnologia contribua para redução de 25% a 30% dos custos de manutenção e no aumento de até 10% na produtividade dos parques, o projeto é fruto de uma parceria da empresa IBM com a cearense Energo. Como ilustrado, a tecnologia IdC está presente em diversas áreas do conhecimento humano e de diferentes maneiras, e claro, não restrita apenas as apresentadas anteriormente.

**Barreiras e dificuldades de sua implantação**

Como apresentado anteriormente, esses dispositivos necessitam de uma conexão com a internet para que seja possível a transmissão dos dados coletados e gerados por eles, e infelizmente, a internet não é acessível, seja do ponto de vista financeiro ou geográfico, para todo mundo com a mesma qualidade de serviço e velocidade, e essa dificuldade de acesso é uma das razões de ainda não existir, por exemplo, uma cidade que fosse inteiramente conectada, as chamadas *Smart Cities*, que seriam cidades onde cada aspecto de sua infraestrutura (iluminação pública, tempo de abertura entre sinais de transito, irrigação pública, entre outros) seriam administrados através de dispositivos IdC que estariam gerando dados a todo momento para serem trabalhados. Outra grande barreira é justamente a questão da transmissão dos dados coletados, que é imensa e geralmente precisariam ser transmitidos rapidamente para o sistema que os analisaria. Uma possível solução no momento para essa questão, é a tecnologia 5G, que já está em desenvolvimento e por prometer frequências maiores que a atual 4G, pode ser a solução para o problema da quantia de dados transmitida por segundo, mas apesar de toda a questão de distribuição de internet e envio de dados coletados, esses ainda não são a maior barreira encontrada. A barreira principal quanto a implantação de IdC é a questão da segurança, de como criar maneiras de proteger e garantir que os dados que estão sendo gerados não serão usados, utilizando o exemplo das *Smart Cities*, para no lugar de economizar com iluminação pública, causar um apagão na cidade, ou ainda no exemplo dos sinais de transito, gerar inúmeros acidentes de transito. Alguns desses dispositivos de IdC são voltadas para uso comercial, ou seja, para uso cotidiano das pessoas, e alguns desses dispositivos possuem definidos por padrão de fábrica um usuário e uma senha, que ao adquirir o produto, o usuário final pode e deveria modificar para garantir uma melhor segurança de seus aparelhos. Um dos principais problemas quanto a segurança desses dispositivos é justamente a questão da falta de informação ou cuidado do usuário final quanto a sua segurança digital, visto que esses aparelhos podem ser facilmente hackeados, uma vez que uma pessoa mal-intencionada só precisa descobrir o padrão do fabricante e sair “testando” até conseguir ter acesso aos dispositivos que não tiveram suas informações modificadas. Um exemplo disso aconteceu em 2016 nos Estados Unidos onde hackers, justamente ao utilizar de dispositivos IdC que não tiveram seus dados de usuário modificados após a compra, os usaram para arquitetar e gerar um ataque *DDoS*, que pode ser entendido como um tipo de ataque hacker onde uma quantidade massiva de dados ou solicitação de algum serviço de rede é realizado para alguma plataforma ou servidor, que nisso acaba por sobrecarregar ele com tantas solicitações sendo recebidas num curto espaço de tempo e ocasiona a queda dessas plataformas ou servidores, e as vezes até vazamento de dados presente neles, que na maioria dos casos é o objetivo principal desse tipo de ataque. Segundo pesquisas da Gartner, foi descoberto que 20% das empresas de tecnologia observaram um ataque baseado em *IoT* nos últimos três anos, e devido a isso essas empresas vem investindo cada vez mais em pesquisa para segurança de dispositivos *IoT*, e a estimativa é que em 2021 já sejam investidos mais de US$3,1 bilhões. As principais despesas são testes de invasão, avaliação de segurança de sistemas e o uso de ferramentas e serviços para melhorar a gestão de ativos.

**Conclusão e considerações Finais**

Após análise de bibliografia pesquisada sobre Internet das Coisas, é possível afirmar que a tecnologia é muito bem-vinda para ser aplicada em diversas áreas do conhecimento, porém é necessário que aja cada vez mais investimentos para a segurança de dispositivos dotados da tecnologia, e uma possível medida para melhorar a segurança, seria buscar entender melhor as implicações da conectividade de rede de externalização, mas não só isso, como também uma maior demanda por regulamentação da tecnologia, visto o potencial dela de fomentar diversas áreas. Outra medida que já é adotada quanto a segurança dos dispositivos é que cada vez mais ao desenvolver esses dispositivos IdC, eles sejam pensados desde sua base com uma preocupação maior com a sua segurança, o que é chamado de “*Security by Design”*, ou em português, Design de segurança, que desse modo reduz bastante os riscos que o produto final possa ter. A tendência é que cada vez mais os países e as empresas invistam nessa área, já que segundo apontam pesquisas, o mercado tem potencial de gerar entre US$3,9 e 11,1 trilhões anuais desde que bem implantado e devidamente seguro, garantindo a privacidade de seus usuários e seus dados. A tendência é que cada vez mais essa tecnologia se torne aplicável e faça parte do dia a dia de todos, unificando inúmeras coisas em diversos sistemas interconectados.

**Referências**

ALECRIM, Emerson. O que é Internet das Coisas (Internet of Things)?. Info Wester, março de 2016. Disponível em: <https://www.infowester.com/iot.php>. Acessado em: 4/11/2019.

CHUI, Michael; MANYIKA, James. By 2025, Internet of things applications could have $11 trillion impact. Revista Fortune, julho de 2015. Disponível em: <https://www.mckinsey.com/mgi/overview/in-the-news/by-2025-internet-of-things-applications-could-have-11-trillion-impact>. Acessado em: 8/11/2019.

Época Negócios. Veja como os carros ficaram mais inteligentes. Época Negócios, janeiro de 2018. Disponível em: <https://epocanegocios.globo.com/Publicidade/Embratel-IOT/noticia/2018/01/veja-como-os-carros-ficaram-mais-inteligentes.html>. Acessado em: 11/11/2019.

EVANS, Dave. *Internet de las cosas - Cómo la próxima evolución de Internet lo cambia todo*. *Cisco Internet Business Solutions Group* (IBSG), 2011. Disponível em: <http://www.cisco.com/web/LA/soluciones/executive/assets/pdf/internet-of-things-iot-ibsg.pdf>. Acessado em: 10/11/2019.

FEARN, Nicholas. *IoT smart fridge revolutionising vaccine care*. *Internet of Business*, agosto de 2016. Disponível em: <https://internetofbusiness.com/iot-smart-fridge-vaccine-care/>. Acessado em: 9/11/2019.

FERREIRA, Alexandre. Considerações para a segurança de dispositivos IoT. Arcon, março de 2019. Disponível em: <https://www.arcon.com.br/blog/consideracoes-para-a-seguranca-de-dispositivos-iot>. Acessado em: 11/11/2019.

GERSHENFELD, Neil (et al). “*The Internet of Things*”. *Scientific American*, outubro de 2004. disponível em: <http://cba.mit.edu/docs/papers/04.10.i0.pdf>. Acessado em: 9/11/2019.

GOGONI, Ronaldo. O que é Internet das Coisas?. Technoblog, 2018. Disponível em: <https://tecnoblog.net/263907/o-que-e-internet-das-coisas/>. Acessado em: 4/11/2019.

GOODIN, Dan. *Record-breaking DDoS reportedly delivered by >145k hacked câmeras. ArsTECHNICA,* setembro de 2016. Disponível em: <https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/>. Acessado em: 9/11/2019.

HSC Brasil. Segurança para IoT: quais os desafios e seus impactos em segurança. HSC Brasil, dezembro de 2018. Disponível em: <https://www.hscbrasil.com.br/seguranca-em-iot/>. Acessado em: 12/11/2019.

*IBM Research Editorial Staff. Monitoring Parkinson’s disease with sensors and analytics to improve clinical trials*. IBM, abril de 2017. Disponível em: <https://www.ibm.com/blogs/research/2017/04/monitoring-parkinsons-disease/>. Acessado em: 9/11/2019.

JIMÉNEZ, Javier. Usando a integração de sistemas para otimizar o processo de fabricação. Revista AECweb, agosto de 2018. Disponível em: <https://www.aecweb.com.br/cont/a/usando-a-integracao-de-sistemas-para-otimizar-o-processo-de-fabricacao_17726>. Acessado em: 12/11/2019.

MAGRANI, Eduardo. A Internet das Coisas. 1 ed. Rio de Janeiro: Editora FGV, 2018.

MILLMAN, Rene. *Connected cars report: 125 million vehicles by 2022, 5G coming*. *Internet of Business*, abril de 2018. Disponível em: <https://internetofbusiness.com/worldwide-connected-car-market-to-top-125-million-by-2022/>. Acessado em: 12/11/2019.

O’CONNOR, Mary. Armazenamento de remédios ganha inteligência. RFID Journal Brasil, agosto de 2016. Disponível em: <https://brasil.rfidjournal.com/noticias/vision?14797/>. Acessado em: 9/11/2019.

Sumus. Investimentos Em Segurança IoT Pode Chegar A 1.5 Bilhões De Dólares. Sumus, 2018. Disponível em: <https://www.sumus.com.br/publicacoes/investimento-seguranca-iot/>. Acessado em: 12/11/2019.

VILLARINO, Julia. Internet das Coisas: Um Desenho do Futuro. Blog Proof, novembro de 2016. Disponível em: <https://www.proof.com.br/blog/internet-das-coisas/>. Acessado em: 4/11/19.

Internet das Coisas e seus desafios de segurança, Proof, novembro de 2016. Disponível em: <https://www.proof.com.br/blog/iot-internet-das-coisas/>. Acessado em: 4/11/2019.

ZAMBARDA, Pedro. ‘Internet das Coisas’: entenda o conceito e o que muda com a tecnologia. Technotudo, agosto de 2014. Disponível em: <https://www.techtudo.com.br/noticias/noticia/2014/08/internet-das-coisas-entenda-o-conceito-e-o-que-muda-com-tecnologia.html>. Acessado em: 4/11/19.