UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
Campus de Marília, São Paulo
Faculdade de Filosofia e Ciências
Programa de Pós-Graduação em Ciência da Informação

VICTOR UBIRACY BORBA

PROPOSTA DE UM MODELO DE REFERÊNCIA PARA INTERNET DAS COISAS: aspectos de segurança e privacidade na coleta de dados

Marília, São Paulo
2018

UNIVERSIDADE ESTADUAL PAULISTA "JÚLIO DE MESQUITA FILHO"
Campus de Marília, São Paulo
Faculdade de Filosofia e Ciências
Programa de Pós-Graduação em Ciência da Informação

VICTOR UBIRACY BORBA

PROPOSTA DE UM MODELO DE REFERÊNCIA PARA INTERNET DAS COISAS: aspectos de segurança e privacidade na coleta de dados

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação da Faculdade de Filosofia e Ciências – Universidade Estadual Paulista "Júlio de Mesquita Filho" – UNESP – campus de Marília, São Paulo, como requisito parcial para a obtenção do título de Mestre em Ciência da Informação.

Linha de Pesquisa: Informação e Tecnologia

Orientador: Prof. Dr. Ricardo César Gonçalves Sant'Ana

Marília, São Paulo
2018

Borba, Victor Ubiracy.
B726p Proposta de um modelo de referência para Internet das coisas: aspectos de segurança e privacidade na coleta de dados / Victor Ubiracy Borba. – Marília, 2018.
80 f. ; 30 cm.

Orientador: Ricardo César Gonçalves Sant'Ana.
Dissertação (Mestrado em Ciência da Informação) – Universidade Estadual Paulista (Unesp), Faculdade de Filosofia e Ciências, 2018.
Bibliografia: f. 81-86

1. Ciência da informação. 2. Tecnologia da informação. 3. Proteção de dados. 4. Internet. I. Título.

CDD 005.73

Ficha catalográfica elaborada por
André Sávio Craveiro Bueno
CRB 8/8211
Unesp – Faculdade de Filosofia e Ciências

VICTOR UBIRACY BORBA

PROPOSTA DE UM MODELO DE REFERÊNCIA PARA INTERNET DAS COISAS: aspectos de segurança e privacidade na coleta de dados

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Informação da Faculdade de Filosofia e Ciências – Universidade Estadual Paulista "Júlio de Mesquita Filho" – UNESP – campus de Marília, São Paulo, como requisito parcial para a obtenção do título de Mestre em Ciência da Informação.

Linha de Pesquisa: Informação e Tecnologia

Orientador: Prof. Dr. Ricardo César Gonçalves Sant'Ana

Prof. Dr. Ricardo César Gonçalves Sant'Ana (Orientador)
Universidade Estadual Paulista - UNESP

Prof. Dr. Mario Mollo Neto
Universidade Estadual Paulista - UNESP

Prof. Dr. Rogério Aparecido Sá Ramalho
Universidade Federal de São Carlos - UFSCAR

Marília, São Paulo
2018

Dedico este trabalho à minha família e todos meus colegas que participaram de alguma forma para a conclusão do meu Mestrado.

AGRADECIMENTOS

Agradeço primeiramente a Deus pela oportunidade e pelas conquistas para chegar até aqui.

A minha família que sempre me incentivou e me fortaleceu durante minha caminhada.

A meus amigos e colegas de trabalho que foram pacientes e prestativos em todos os momentos.

Ao meu orientador prof. Dr. Ricardo César Gonçalves Sant'Ana pela paciência, conhecimento e confiança depositados.

Aos profs. Mario Mollo Neto e Rogério Aparecido Sá Ramalho pelas contribuições que enriqueceram a dissertação.

Ao Grupo de Pesquisa sobre Tecnologias de Acesso a Dados (GPTAD).

Ao projeto de extensão Competências Digitais para a Agricultura Familiar (CoDAF).

Ao Centro de Inovação no Agronegócio (CIAg).

A todos os docentes do Programa de Pós-graduação em Ciência da Informação (PPGCI), de dentro e fora da UNESP, que participaram durante minha formação.

“A mente que se abre a uma nova ideia jamais voltará ao seu tamanho original.”

Albert Einstein

RESUMO

Internet das Coisas (IoT), do termo em inglês “Internet of Things”, é um termo genérico que começou a ser utilizado no final dos anos 90 e início dos anos 2000 para caracterizar objetos conectados à internet, produzindo ou processando dados de forma autônoma em tempo real. IoT é um fenômeno que envolve um contexto diverso e complexo, na qual atuam diversos atores, incluindo a sociedade como um todo. Neste sentido, o objetivo geral deste trabalho é propor um modelo de referência para IoT, considerando aspectos de segurança e privacidade no cenário de IoT. Para tal, a metodologia utilizada neste trabalho foi de pesquisa bibliográfica e de cunho exploratório, utilizando método quantitativo e qualitativo para atingir alguns objetivos específicos. Como resultado, foi proposto um modelo de referência com base em arquiteturas e modelos de referência IoT estudados previamente, na qual são considerados três atores no cenário: os Usuários, o Referenciado e o Detentor, atores estes que são de vital importância para o fluxo informacional presente no cenário de IoT. Outro resultado, foi uma reflexão na qual, durante a coleta, o dispositivo não deveria ter conhecimento sobre o usuário ou entidade requisitante, pois, os usuários fazem uso da Tecnologia IoT através de uma camada de abstração disponibilizada pela Aplicação, bem como os dados devem ser protegidos e anonimizados através das funções presentes na camada de segurança. Além disso, o trabalho traz uma reflexão sobre a responsabilidade dos atores envolvidos com a privacidade dos indivíduos imersos no universo de IoT.

Palavras-chave: Internet das Coisas; IoT; Dados; Segurança; Privacidade; Ciência da Informação.

ABSTRACT

Internet of Things (IoT) is a generic term that has started being used between the end of the 90's and beginning of the 00's to characterize objects that are connected to the internet, producing or processing data in an autonomous way in real time. IoT is a phenomenon that involves a diverse and complex context, consisting of several agents, including the society as a whole. Saying that, the main goal of this work is to propose a reference model for IoT, considering aspects of security and privacy in this scenario. In order to achieve that, the methodology used for this work was bibliographical and exploratory research, but to reach some specific goals, using a quantitative and qualitative research showed necessary. As a result, a reference model was proposed based on architectures and reference models previously studied, in which three agents were included: Users, Referrer and Holder, all of them representing vital importance for the information flow present in the IoT scenario. Another result was a contemplation in which, during the mining phase, the device should not have known about the user or requesting entity, once users make use of the IoT Technology through an abstraction layer made available by the Application; moreover, the data must be protected through the functions present in the security layer. Also, the work brings a contemplation about agent's responsibility in terms of user's privacy in IoT world.

Keywords: Internet of Things; IoT; Data; Safety; Privacy; Information Science.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AAA - *Authentication, Authorization and Accounting* (Autenticação, Autorização e Contabilidade)

ACE - *Authentication and Authorization in Constrained Environments* (Autenticação e autorização em ambientes restritos)

API – *Application Protocol Interface* (Interface de protocolo de aplicação)

ARC – Arquitetura de Referência de Camadas

BPM – *Business Process Model* (Modelo de processo empresarial)

CAPES - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior

CI – Ciência da Informação

CVD – Ciclo de Vida dos Dados

DNS – *Domain Name System* (Sistema de Domínio de Nomes)

EF – Entidade Física

EPC - *Electronic Product Code* (Código de Produto Eletrônico)

EV – Entidade Virtual

IEEE – *Institute of Electrical and Electronics Engineers* (Instituto de Engenheiros Elétricos e Eletrônicos)

IoT – *Internet of Things* (Internet das Coisas)

IoT-A – *Internet of Things – Architecture* (Internet das Coisas - Arquitetura)

IP – *Internet Protocol* (Protocolo de Internet)

IPSec – *IP Security* (Segurança IP)

ISO/OSI – *Open System Interconnection* (Interconexão de sistemas abertos)

ITU – *International Telecommunication Union* (União Internacional de Telecomunicações)

ITU-T – *International Telecommunication Union - Telecommunication Standardization* (União Internacional de Telecomunicações - Padronização de telecomunicações)

KEM - *Key Exchange and Management* (Troca e gerenciamento de chaves)

M2M - M*achine-to-Machine* (Máquina-para-Máquina)

MIT - *Massachusetts Institute of Technology* (Instituto de Tecnologia de Massachusetts)

OAuth – *Authorization Framework* (Estrutura de autorização)

RFID - *Radio-Frequency Identification* (Identificação de rádio frequência)

SO – *Service Organization* (Organização de Serviços)

TCP - *Transmission Control Protocol* (Protocolo de Controle de Transmissão)

TD – *Thing Description* (Descrição da coisa)

TIC – Tecnologias de Comunicação e Informação

TLS - *Transport Layer Security* (Segurança da camada de transporte)

UPC – *Universal Product Code* (Código de Produto Universal)

W3C – *World Wide Web Consortium* (Consórcio *World Wide Web*)

WoT – *Web of Things* (*Web* das Coisas)

WWW – *World Wide Web*

SUMÁRIO

1 Introdução

Imagine o seguinte cenário, você está saindo do trabalho cansado após um dia inteiro de trabalho e enquanto você esteve fora, sua casa fez tudo àquilo que você precisaria fazer após o trabalho, como fazer compras, limpar a casa, equilibrar o clima da casa, alimentar os animais, etc. "Mas como assim a casa fez tudo isso?" Quando fala-se em Internet das Coisas, ou o termo em inglês *Internet of Things* (IoT), imaginamos coisas com internet, como computadores, *smartphones, smart tvs, smart watches*, entre outros dispositivos que possuem internet, no entanto, IoT é mais do que isso, são dispositivos conectados que podem ter ou não interação entre eles.

No cenário descrito anteriormente, imagine que quando você saiu de casa, sua geladeira percebeu que o seu leite acabou e automaticamente enviou uma notificação para você, informando que o leite acabou e com um *link* para você autorizar a compra de um novo leite, imagine que quando você saiu de casa, seu aspirador de pó autônomo fez toda a limpeza de sua casa, quando você saiu do seu trabalho, seu carro mapeou o trajeto e identificou um acidente no percurso, alterando automaticamente seu trajeto, além de informar sua casa que você está a caminho e com isso sua casa irá ligar o ar condicionado para que você entre na sua casa com um clima agradável, enfim, existem infinitas possibilidades quando pensamos em "coisas" conectadas.

Outro exemplo de aplicação de IoT é Centro de Operações da Prefeitura do Rio de Janeiro, na qual dados de sensores, câmeras, chamadas de emergência e redes sociais são combinados e exibidos informações sobre o trânsito, clima em entre outras informações em uma tela de 80m². Todas essas informações auxiliam para que os problemas da cidade sejam tratados e resolvidos o quanto antes.

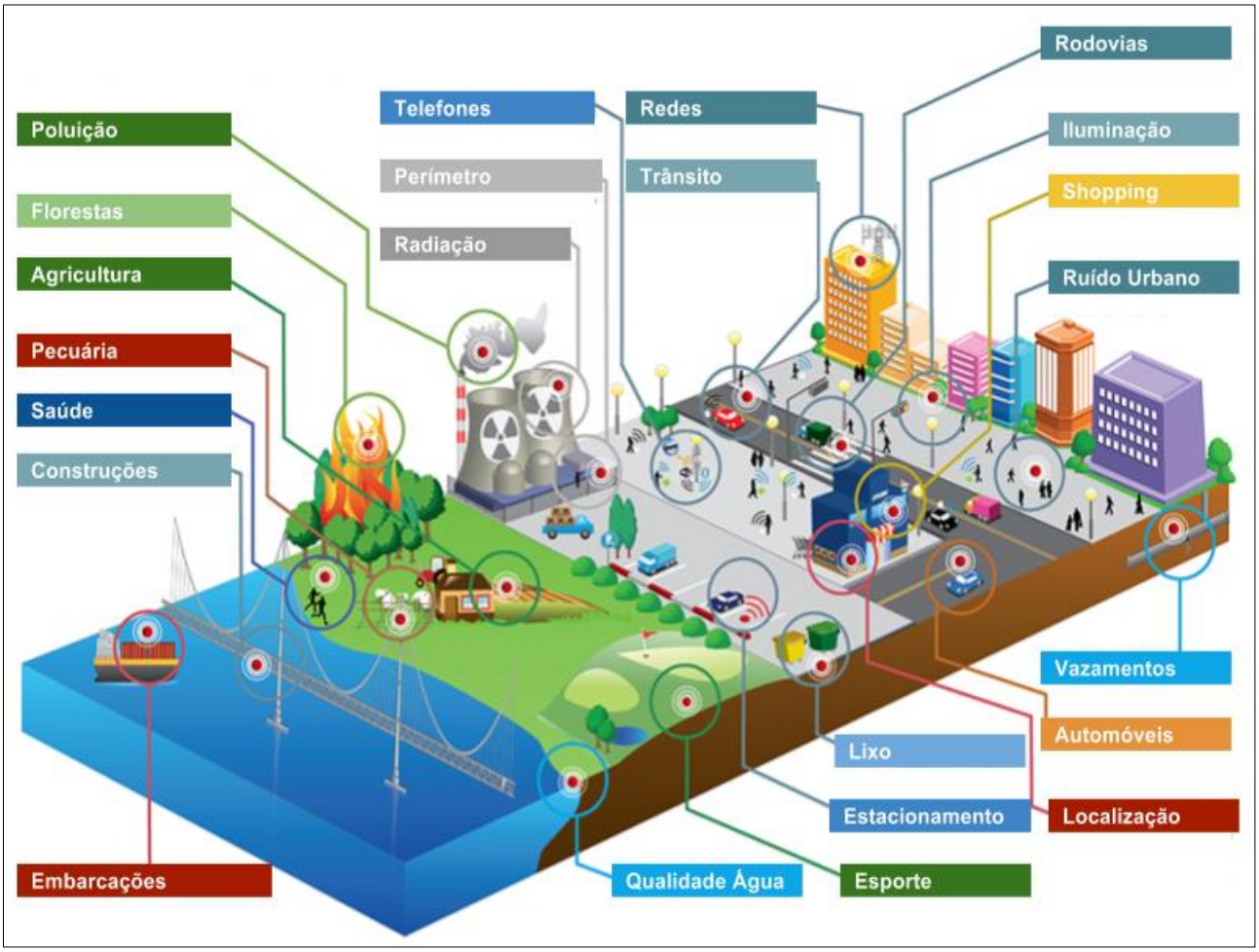
IoT também pode auxiliar no meio educacional, como é o caso de uma escola no interior da Bahia, na qual foram instaladas etiquetas RFID (*Radio-Frequency Identification*) nos uniformes dos alunos, para monitorar a entrada e saída dos alunos. Além disso, no caso de uma falta, entrada ou saída inadequada, o sistema da escola notifica os pais dos alunos através do celular.

Todos estes exemplos combinam diferentes tecnologias e possuem diferentes finalidades, no entanto todos estes exemplos ilustram o que chamamos hoje de IoT. De acordo com Singer (2012), este é um termo genérico, e vem sendo usado de 1999 até hoje para caracterizar objetos que estejam conectados à internet, produzindo ou processando dados de forma autônoma em tempo real.

De acordo com Lacerda e Marques (2015), o potencial de IoT é determinado pela competência de capturar, processar, armazenar, transmitir e apresentar informações, na qual objetos interligados por uma rede são capazes de realizar ações de forma independente, gerando como produto uma grande quantidade e variedade de dados.

A IoT é um fenômeno que envolve um contexto diverso e complexo como pode ser observado na Figura 1, onde existem diversos ambientes conectados e interagindo entre eles, o que pode-se chamar de Mundo Inteligente.

Figura 1 - Cenário hipotético de IoT



Fonte: adaptado pelo autor com base em Libelium (2013).

Neste cenário são apresentados ambientes, fenômenos, e coisas que podem ser observadas e conectadas através de algum tipo de tecnologia, abaixo serão exemplificados alguns dos itens citados na imagem, idealizando uma possível aplicação tecnologia para coletar dados e gerar algum tipo de informação.

Começando da esquerda para a direita, a primeira camada é no mar, ou nas águas, onde é possível identificar embarcações, coletar dados dos navios, dados sobre construções como pontes, para que com os dados coletados seja possível prever acidentes, e, ou, falhas.

Com relação a saúde, é possível coletar informações como batimentos cardíacos, glicemia, contador de passos, entre outros dados para medir a qualidade da saúde do indivíduo.

Além da qualidade da saúde de pessoas, é possível medir também a saúde de animais e de ambientes, como por exemplo florestas, plantações, rebanhos, qualidade do ar, da água entre outros

fatores que podem interferir no meio ambiente, um exemplo de aplicação é a previsão de riscos para queimadas, doenças em animais, poluição do ar pelas indústrias, radiação, etc.

Nas cidades existem diversas outras aplicações de IoT, como por exemplo o uso de *smartphones* para diversas coisas, carros cada vez mais tecnológicos, *shoppings* inteligentes, sistemas de estacionamento, limpeza, identificação de vazamentos na rede abastecimento de água, identificação e auxílio em zonas de trânsito intenso, iluminação inteligente para economia e energia, entre diversas outras aplicações de tecnologias e dispositivos conectados que podem trazer benefícios para a população.

Entretanto, estes dados que são coletados a todo momento e em todos os lugares, nem sempre são coletados com o consentimento dos indivíduos que estão inseridos no ambiente, como é o caso de câmeras de monitoramento, sensores de movimento, dados sensíveis disponíveis nos *smartphones*, como localização, fotos, contatos, entre outros.

Conforme citado anteriormente, IoT é um fenômeno que envolve um contexto diverso e complexo, na qual atuam diversos atores como técnicos, engenheiros, cientistas, filósofos, designers, entre outros, além de diversas áreas de conhecimento, como ciência da computação, agricultura, química, biologia, ciência da informação, eletrônica, etc. Vislumbrando esse fenômeno que une diversas áreas e atores, uma frase chama muita a atenção. “O mundo precisa de pensamento multidisciplinar agora mais do que nunca” (ROMEO, 2014).

É neste cenário que a Ciência da Informação (CI) pode contribuir, pois, segundo Le Coadic (1996), a CI é a ciência que estuda as propriedades gerais da informação (natureza, gênese e efeitos) em meio aos processos e sistemas de construção, comunicação e uso da informação, e de acordo com Hawkins (2001), a CI se preocupa com os processos de geração, distribuição, organização, representação, processamento, comunicação e uso da informação. Ainda nesta mesma linha de raciocínio Saracevic (1995, p. 4) completa que a CI possui uma interdisciplinaridade que foi introduzida pelas diferentes experiências daqueles que procuram soluções para problemas, ainda segundo ele, tais interdisciplinaridades, podem ser mais fortemente percebidas com sua aproximação a Biblioteconomia, Ciência da Computação, a Ciência Cognitiva e a Comunicação.

Ramalho, Vidotti e Fujita (2007, p. 6), afirmam que existe:

> [...] uma tendência de aproximação entre as áreas de Ciência da Informação e Ciência da Computação, principalmente no que tange ao desenvolvimento de novos instrumentos de representação e recuperação de recursos informacionais. (RAMALHO, VIDOTTI e FUJITA, 2007, p. 6)

Dando continuidade a questão da interdisciplinaridade, Sant’Ana (2013, p.2) relata que dentro da CI é importante a “[...] participação de todas as áreas do conhecimento, como por exemplo na elaboração, gestão e manutenção de recursos tecnológicos pela Ciência da Computação [...]”. Assim,

a CI pode ter importante papel na construção de uma base teórica e na definição de caminhos para que as novas tecnologias contribuam para o atendimento das necessidades informacionais, já que cabe a esta ciência o papel de investigar o comportamento da informação, seu fluxo e os meios para o seu acesso (BORKO, 1968; CAPURRO, 2003).

1.1 Problema de pesquisa

Atualmente diversos países trabalham para definir uma arquitetura padrão de comunicação para os dispositivos IoT, em que para cada camada da arquitetura existem protocolos de comunicação diferentes, na qual deveriam ser mantidos os princípios do Ciclo de Vida dos Dados (CVD), em que acredita-se que todos os objetivos que permeiam as fases do CVD proposto por Sant'Ana (2016) deveriam ser estudados e atendidos em dispositivos IoT, tendo em vista que os mesmo lidam com dados e muitas vezes com informações sensíveis que requerem maior atenção.

O problema a ser discutido neste trabalho é com relação aos atores envolvidos no cenário de IoT, bem como a privacidade dos indivíduos inseridos em meios informacionais, onde suas informações são coletadas a todo momento de diversas maneiras através de dispositivos inseridos no fenômeno chamado Internet das Coisas.

No cenário de IoT, existem fragilidades em relação a manutenção da segurança e privacidade dos indivíduos inseridos neste contexto, fato que é agravado pela falta, ou o não uso, de uma arquitetura de referência padrão, na qual alguns atores envolvidos nesse cenário muitas vezes são ignorados.

A reflexão levantada a partir deste cenário motivou a problemática deste estudo, que está baseada na maneira em que as arquiteturas analisadas trabalham a questão da segurança e da privacidade dos dados. Levantando-se então uma questão sobre quais são as responsabilidades de quem trabalha com essas tecnologias com relação à privacidade dos indivíduos imersos no universo de IoT.

1.2 Objetivos

O objetivo geral deste trabalho é propor um modelo de referência para IoT, considerando aspectos de segurança e privacidade no cenário de IoT.

Para tanto, consideram-se os seguintes objetivos específicos:

- Apresentar um panorama histórico sobre IoT, bem como definições e conceitos que circundam a temática;
- Identificar e descrever as principais arquiteturas e modelos de referência de IoT;

- Identificar e descrever os aspectos que envolvem segurança e privacidade em arquiteturas e modelos de referência de IoT;
- Elaborar um modelo de referência com base em arquiteturas e modelos de referência de IoT;
- Associar o objetivo de privacidade na fase de coleta de dados do CVD com os aspectos de segurança e privacidade identificados em arquiteturas e modelos de referência IoT.

1.3 Metodologia

Para cumprir com os objetivos deste trabalho, primeiramente foi realizada uma pesquisa bibliográfica associada à uma metodologia exploratória. A análise exploratória da literatura disponível, permitiu embasamento teórico sobre a temática, bem como vislumbrar um panorama histórico de IoT.

Contribuindo para o panorama histórico, foi realizada uma pesquisa bibliográfica de cunho quantitativo nos periódicos da área de Ciência da Informação classificados pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) com padrão Qualis A1, em que foram usados os termos "*Internet of Things*", "Internet das Coisas" e "IoT" para busca nos periódicos, no entanto, após o início da pesquisa nos periódicos foi identificado que os artigos encontrados com o termo "IoT", eram em repetidos, portanto esse termo foi removido das buscas.

Analisando os trabalhos encontrados durante a pesquisa bibliográfica exploratória, notou-se uma similaridade sobre as arquiteturas e modelos de referência estudados, o que levou a realizar uma pesquisa aprofundada sobre estas arquiteturas e modelos de referência, na qual foram encontrados trabalhos de organizações de padronização como o W3C (World Wide Web Consortium) e o IEEE (Institute of Electrical and Electronics Engineers). Levando em consideração as arquiteturas e modelos de referência encontrados durante a pesquisa, foram identificados os principais para aprofundamento e estudo sobre suas camadas, bem como realizar uma análise qualitativa quanto aos aspectos de segurança e privacidade abordados nos mesmos.

Após isto foi realizada uma pesquisa bibliográfica sobre o Ciclo de Vida dos Dados (CVD) de Sant'Ana (2016), onde levantam-se reflexões acerca da privacidade na coleta de dados, que é o objetivo principal deste trabalho, com isso os aspectos de segurança e privacidade analisados durante a pesquisa e desenvolvimento do trabalho são equiparados e considerados de acordo com a reflexão sobre privacidade na coleta abordada por Sant'Ana (2016).

O estudo realizado permitiu a reflexão sobre um novo modelo de referência para IoT, onde são considerados além da tecnologia, aspectos sociais que fazem parte do cenário onde encontram-se estes dispositivos pertencentes ao fenômeno do IoT, bem como reflexões acerca de segurança e privacidade dos atores envolvidos no cenário.

Em sua maior parte, a metodologia utilizada para este trabalho foi de pesquisa bibliográfica e de cunho exploratório, no entanto para atingir o objetivo específico de associar o objetivo da privacidade da fase de coleta de dados do CVD com os aspectos de segurança e privacidade identificados nas arquiteturas e modelos de referência citados no desenvolvimento do trabalho, foi necessário realizar uma análise qualitativa dos modelos de referência estudados.

1.4 Justificativa

Primeiramente, como justificativa cientifica, tem-se em vista que o objeto de estudo deste trabalho, "*Internet of Things*", é um assunto de grande visibilidade, pois de acordo com o gráfico apresentado pelo Gartner (2015), *"Internet of Things"* está no topo das tendências tecnológicas mundiais dos próximos anos.

Além disso, segundo Evans (2011),

> [..] IoT representa a próxima evolução da Internet, dando um grande salto na capacidade de coletar, analisar e distribuir dados que nós podemos transformar em informações, conhecimento e, por fim, sabedoria. Nesse contexto, a IoT se torna bem importante. (EVANS, 2011, p. 2)

Conforme observado durante a pesquisa, parte da motivação dos trabalhos encontrados, tanto da indústria quanto da academia, relaciona-se à desafios observados por Evans (2011), na qual, está entre eles a padronização de dados, arquiteturas, dispositivos e soluções IoT, em outros casos, a motivação dos trabalhos é uma aplicação específica para um determinado contexto.

Para o autor, fatores como segurança, privacidade e interoperabilidade de dados chamam a atenção neste cenário, pois, de acordo com o site Worldometers (2018), cerca de 40% da população mundial está conectada na Internet, ou seja, boa parte da população mundial está conectada, portanto, qualquer tecnologia que esteja conectada a esta grande rede é de interesse da sociedade.

Neste sentido, o tema deste trabalho está fortemente relacionado com a Ciência da Informação (CI), uma ciência social aplicada, que segundo Le Coadic (1996), é a ciência que estuda as propriedades gerais da informação (natureza, gênese e efeitos) em meio aos processos e sistemas de construção, comunicação e uso da informação.

Tendo em vista que a CI, segundo Le Coadic (1996), estuda processos informacionais, esta Ciência tem importante papel para o IoT, pois em um cenário onde dispositivos que processam dados e informações podem estar conectados e presentes em qualquer lugar, de qualquer forma e a qualquer momento, torna-se necessária a atenção com relação os processos informacionais.

Esta atenção é necessária, pois, de acordo com a previsão da Cisco (2011), atualmente já possuímos mais dispositivos conectados do que pessoas no mundo, este fator indica que a sociedade

está ou em breve estará imersa em um mundo tecnológico e repleto de dispositivos conectados e interagindo entre eles, na qual, atualmente já existem celulares, câmeras, diversos sensores, TVs, roteadores de internet sem fio, estações meteorológicas, relógios, entre outros dispositivos que hoje já possuem conexão e estão disponíveis conectados à grande rede informacional da Internet.

Este fator chama a atenção com a relação à sociedade, pois de acordo com Evans (2011), com diversos dispositivos conectados, aumenta-se exponencialmente a quantidade de dados na Internet, segundo Evans (2011), "a Internet dobra de tamanho a cada 5,32 anos". Esta informação chama a atenção do autor com relação aos aspectos de segurança e privacidade dos indivíduos que fazem parte deste cenário, pois os dispositivos IoT que coletam dados, muitas vezes estão conectados à Internet.

Existem alguns casos clássicos de invasão de privacidade no cenário de IoT, como é o caso da babá eletrônica que foi invadida através da internet, na qual um indivíduo malicioso invadiu a babá eletrônica de uma criança de 2 anos, onde segundo os pais da criança o indivíduo falava ofensas e palavras obscenas à criança (BBC, 2013).

Isso se dá pelo fato de que muitos destes dispositivos conectados estão vulneráveis na internet, pois além das vulnerabilidades presentes no desenvolvimento dos dispositivos, muitos usuários não configuram corretamente os dispositivos ou muitas vezes deixam senhas e portas padrões de fábrica em seus equipamentos domésticos.

De acordo com Greenberg (2017), estão sendo desenvolvidos robôs (software com alguma inteligência programada que, age por conta própria após executado, parecido com os vírus conhecidos por infectar computadores através das mais variadas formas) que exploram essas vulnerabilidades, segundo ele, no ano passado foi desenvolvido um robô, chamado de Mirai, que causou interrupções generalizadas, atingindo câmeras IP e roteadores conectados à internet, simplesmente explorando suas senhas fracas ou padrão.

Ainda segundo Greenberg (2017), atualmente está circulando um robô muito mais poderoso e com mais ferramentas do que o Mirai, chamado de IoT Troop ou Reaper, na qual utiliza de técnicas reais de *hacking* para invadir dispositivos IoT. A grande diferença entre esses robôs, é que enquanto o Mirai explorava apenas dispositivos com senhas padrão ou senhas fracas, o Reaper está explorando diversas vulnerabilidades e formas de invasão.

No entanto, de acordo com Greenberg (2017), este novo robô ainda não foi utilizado para realizar nenhum ataque generalizado como foi executado com o Mirai, onde os dispositivos infectados foram utilizados para bombardear o provedor de DNS dos principais destinos da internet em outubro do ano passado, prejudicando o tráfego de dados de grandes sistemas como Spotify, Reddit e The New York Times.

E é neste cenário caótico de dispositivos inseguros conectados que está a justificava social e também pessoal do autor para a realização deste trabalho, na qual, após observar a Figura 2 a seguir, nota-se que Mark Zuckerberg, co-fundador da maior rede social da atualidade, o Facebook, também se preocupa com a imagem e o áudio que supostamente possam vir a serem capturadas pelo seu computador.

Figura 2 - Mark Zuckerberg com suposta fita adesiva na *webcam* e no microfone do laptop

Fonte: Estadão (2016).

As setas vermelhas apontam para a câmera e microfone do *laptop* de Mark Zuckerberg, na qual estes recursos do *laptop* estão supostamente bloqueados por uma fita adesiva preta, fato que despertou a curiosidade do mundo e também do autor para o tema abordado neste trabalho.

1.5 Estrutura do trabalho

Esta dissertação foi dividida em seis capítulos, sendo que o primeiro contém uma breve introdução ao tema (capítulo 1), assim como o problema de pesquisa (subcapítulo 1.1), os objetivos (subcapítulo 1.2), a metodologia (subcapítulo 1.3) e a justificativa (subcapítulo 1.4).

No capítulo 2, está presente o referencial teórico do trabalho, já no subcapítulo 2.1, são apresentados assuntos pertinentes à Internet das Coisas, como as definições sobre o assunto (subcapítulo 2.1.1) e perspectiva histórica (subcapítulo 2.1.2).

No capítulo 3, inicialmente é realizada uma introdução à modelos e arquiteturas de referência, já no subcapítulo 3.1, são detalhados os modelos e arquiteturas de referência de IoT, sendo eles, IoT-A (subcapítulo 3.1.1), ITU-T (subcapítulo 3.1.2) e WoT (subcapítulo 3.1.3).

Já no capítulo 4, são explorados os aspectos de segurança e privacidade dos dispositivos IoT, na qual são relatados os requisitos de segurança e privacidade (subcapítulo 4.1), abordagens à segurança e privacidade (subcapítulo 4.2) e privacidade no CVD (subcapítulo 4.3).

Então, o capítulo 5, traz o modelo de referência proposto (subcapítulo 5.1) e considerações do autor sobre segurança e privacidade (subcapítulo 5.2).

Por fim no capítulo 6 são apresentadas as considerações finais do trabalho, que destacam objetivos alcançados, as contribuições do trabalho e as sugestões de trabalhos futuros.

2 Referencial Teórico

A relação, dados, informação e conhecimento, é algo que traz muita discussão e diversos autores defendem diferentes pensamentos a respeito desses conceitos, no entanto para este trabalho seguiremos a linha de pensamento de Santos e Sant'Ana (2002), em que um dado é

> um elemento básico, formado por signo ou conjunto finito de signos que não contém, intrinsecamente, um componente semântico, mas somente elementos sintáticos (SANTOS e SANT'ANA, 2002)

, informação é

> um conjunto finito de dados dotado de semântica e que tem a sua significação ligada ao contexto do agente que a interpreta ou recolhe e de fatores como tempo, forma de transmissão e suporte utilizado (SANTOS e SANT'ANA, 2002)

, e por fim conhecimento é definido como

> um conjunto de informações contextualizadas e dotadas de semânticas inerentes ao agente que o detém, seja a mente humana ou não, e seu conteúdo semântico se dará em função do conjunto de informações que o compõem e de suas ligações com outras unidades de conhecimento, e do processo de contextualização. (SANTOS e SANT'ANA, 2002)

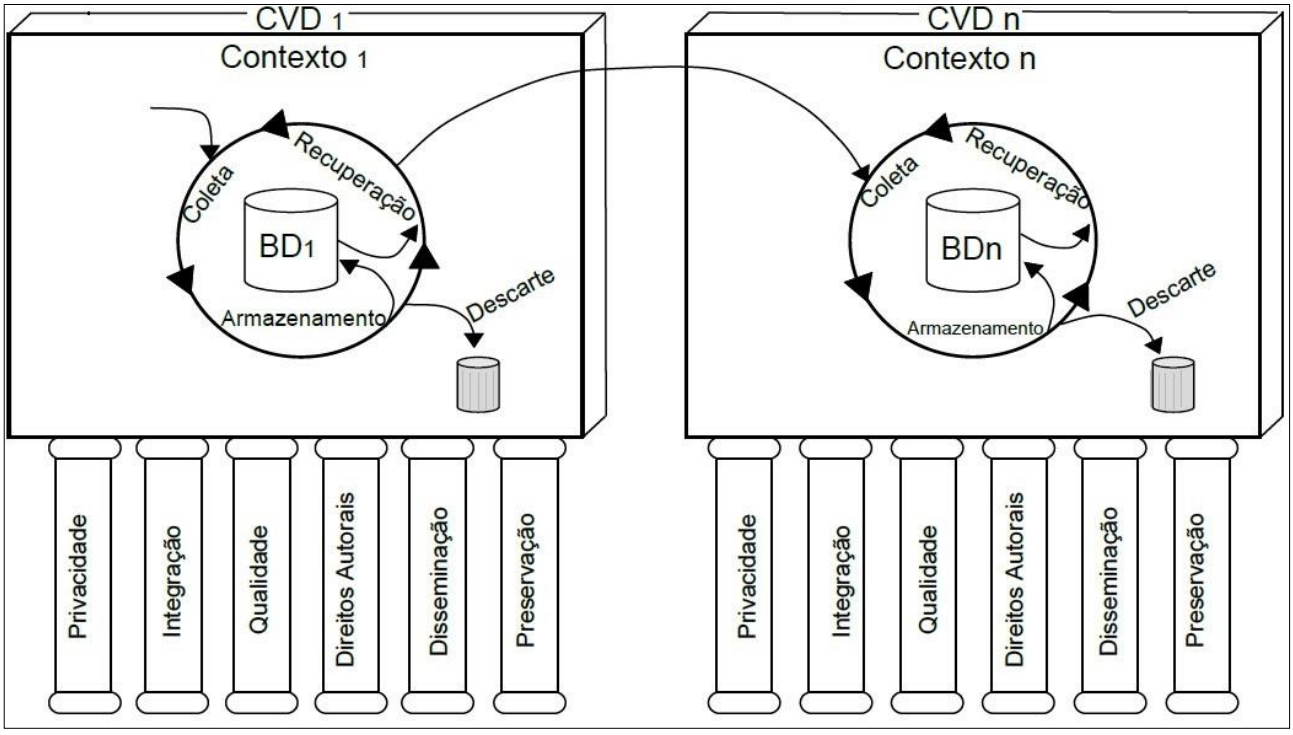
Tendo vislumbrado estes pensamentos e conceitos, passamos para o próximo ponto de interesse que seria o Ciclo de Vida dos Dados (CVD), conceito de Sant'Ana (2016) em que são detalhadas atividades envolvidas no acesso, manutenção e disponibilização dos dados. Este ciclo é composto por quatro fases: Coleta, Armazenamento, Recuperação e Descarte, e vale ressaltar que estas fases são cíclicas, ou seja, a qualquer momento pode-se voltar ao início do ciclo. São elas:

- **Coleta** é a fase que além da ação de coletar dados, é responsável pelo planejamento da maneira como os dados serão coletados, como eles serão filtrados e organizados, além de definir a estrutura, o formato e meios de descrição a serem utilizados.

- **Armazenamento** é a fase responsável pela persistência dos dados em suporte digital ou não, ou seja, por funções como inserção, processamento, transformação, migração, transmissão, etc.
- **Recuperação** é a fase responsável pela consulta e visualização dos dados coletados ou persistidos em algum meio.
- **Descarte** é a fase responsável pela eliminação dos dados, dados armazenados ou não.

Conforme mostra a Figura 3, além das fases do CVD, existem alguns objetivos que permeiam todas as fases, que são: Direitos Autorais, Disseminação, Integração, Qualidade, Preservação e Privacidade. Estes objetivos trazem aspectos relevantes ao CVD e podem ou deveriam ser atendidos em todas as fases do CVD.

Figura 3 - Ciclo de Vida dos Dados



Fonte: Sant'Ana (2016).

Com o constante aumento da demanda informacional e do acesso a dados, de acordo com Sant'Ana (2013) a Ciência da Informação (CI) tem papel fundamental para desempenhar a tarefa de pensar e propor recursos e melhorias no processo informacional, pois a CI, segundo Le Coadic (1996), é a ciência que estuda as propriedades gerais da informação (natureza, gênese e efeitos) em meio aos processos e sistemas de construção, comunicação e uso da informação.

De acordo com Borko (1968), a CI se preocupa com processos como coleta, armazenamento, recuperação e descarte, ele ainda conclui que a CI é uma área derivada de múltiplas disciplinas, destacam-se, a Psicologia e a Ciência da Computação. Ainda nesta mesma linha de raciocínio

Saracevic (1995, p. 4) completa que a CI possui uma interdisciplinaridade que foi introduzida pelas diferentes experiências daqueles que procuram soluções para problemas, ainda segundo ele, tais interdisciplinaridades, podem ser mais fortemente percebidas com sua aproximação a Biblioteconomia, Ciência da Computação, a Ciência Cognitiva e a Comunicação.

Ramalho, Vidotti e Fujita (2007, p. 6), afirmam que existe:

> [...] uma tendência de aproximação entre as áreas de Ciência da Informação e Ciência da Computação, principalmente no que tange ao desenvolvimento de novos instrumentos de representação e recuperação de recursos informacionais. (RAMALHO, VIDOTTI e FUJITA, 2007, p. 6)

Dando continuidade a questão da interdisciplinaridade, Sant'Ana (2013, p.2) relata que dentro da CI é importante a "[...] participação de todas as áreas do conhecimento, como por exemplo na elaboração, gestão e manutenção de recursos tecnológicos pela Ciência da Computação [...]".

Um dos assuntos que possuem grande destaque e discussão dentro da CI é o conceito de "Informação como Coisa" de Buckland (1991), na qual o termo "informação" é também atribuído para objetos, assim como dados para documentos, que são considerados como "informação", porque são relacionados como sendo informativos, tendo a qualidade de conhecimento comunicado ou comunicação, informação, algo informativo. Além disso, essa definição abre novos caminhos a serem explorados através de áreas heterogêneas que podem colaborar para novos estudos associados a CI.

Então nesta linha de raciocínio, em que qualquer "coisa" pode fornecer alguma informação, chegamos ao tema deste trabalho é a "Internet das Coisas", mas primeiramente, o que exatamente significa o termo 'Internet'? Este é o termo que muitas vezes é utilizado como sinônimo de '*Web'*, no entanto, refere-se à infraestrutura global de redes de computadores interconectados, que utiliza o protocolo TCP/IP para a troca de dados, enquanto a '*Web'* ('*World Wide Web*' - WWW) é uma das aplicações que utilizam a Internet como plataforma de comunicação, materializando-se em um espaço de informação (W3C, 2004).

No entanto, Castells (2003) entende a Internet como "a base tecnológica para a forma organizacional da Era da Informação: a rede". De acordo com Lacerda (2015), este fato é evidenciado na atual geração da Internet, em que sistemas estão interligados em diferentes escalas, criando ecossistemas de diversas naturezas, como urbanos, biológicos e materiais.

Na qual entende-se que os dados são a base para a informação estar presente e fluir em todos os lugares, e com isso, chegamos ao conceito de Internet das Coisas, que muitas vezes também é conhecida como 'Internet Ubíqua'.

Internet Ubíqua faz parte de uma linha de raciocínio, despertada na década de 80 pelo pesquisador Mark Weiser, chamada de Computação Ubíqua (*Ubiquitous Computing* ou *Ubicomp*), na

qual Weiser imaginava um futuro em que tecnologias computacionais fariam parte do “tecido da vida cotidiana”. (WEISER, 1991)

Mas antes disso, existe um conceito que por muitos vem sendo esquecido com o passar dos anos, que é o conceito de cibernética, cunhado por Nobert Wiener (1948), na qual define cibernética como estudo dos autocontroles biológicos, mecânicos e elétricos encontrados em sistemas estáveis, na qual autocontroles seria um vislumbre do que hoje chamamos de objetos autônomos. Em 1950, ele ainda conclui que:

> Além da teoria da transmissão de mensagens da engenharia elétrica, há um campo mais vasto que inclui não apenas o estudo da linguagem, mas também o das mensagens como meio de controle das máquinas e da sociedade, o desenvolvimento de máquinas de calcular e outros autômatos que tais, reflexões acerca da psicologia e do sistema nervoso, e uma nova teoria conjetural do método científico. Esta teoria mais vasta das mensagens é uma teoria probabilística, uma parte intrínseca do movimento que deve sua origem à Willard Gibbs [física estatística]. Até recentemente, não havia palavra específica para designar este complexo de ideias e, para abarcar todo o campo com um único termo, vi-me forçado a criar uma. Daí ‘Cibernética’. (WIENER, 1950, p. 15)

Cibernética é um conceito muito importante para o que atualmente chamamos de Internet das Coisas, ou IoT, um termo que está chamando a atenção e crescido muito rapidamente nos últimos anos. Basicamente, segundo Atzori et al. (2010), pode-se dizer que IoT é uma variedade de objetos ou “coisas” do cotidiano conectadas entre si ou em uma rede maior podendo interagir uns com os outros.

Portanto, IoT tem um grande impacto de diversas formas no cotidiano das pessoas, como por exemplo na saúde, ambiente de trabalho, ambiente pessoal, educacional, no trânsito, etc. No entanto, de acordo com Atzori et a. (2010) para as empresas outros segmentos serão afetados, como por exemplo na automação de máquinas ou ambientes, manufatura, logística, gerenciamento de processos e negócios, entre outros.

Segundo Dutra et al. (2016), existe um pano de fundo IoT, que é a utilização de uma infraestrutura, baseada em TIC, para coletar, armazenar, recuperar e descartar dados gerados e utilizados pelos dispositivos e suas funcionalidades. Entretanto, as fases citadas anteriormente por Dutra et al. (2016), fazem parte do CVD, na qual existem diversas preocupações que permeiam todas as fases, e uma delas é a privacidade.

A privacidade, no entanto, é algo que está em constante discussão no que diz respeito ao anonimato, pois de acordo com Affonso e Sant’Ana (2017), o anonimato pode conter um conceito multifacetado, e ser tratado de forma diferente de acordo com o contexto. Como mostra o exemplo citado pelos autores, na qual em uma rede militar o anonimato não é algo desejado ou aceitável, porém em uma sala de bate-papo na *web*, um certo nível de anonimato dos usuários é aceitável.

> Existe uma diferença importante entre a privacidade e o anonimato: sob a condição de privacidade, pode-se ter o conhecimento da identidade de uma pessoa, mas não de um fato pessoal associado a ela, que, nos termos de condição do anonimato, tem-se o conhecimento de um fato pessoal, mas não da identidade da pessoa associada. Neste sentido, a privacidade e o anonimato são faces opostas uma da outra. Enquanto a privacidade, muitas vezes esconde fatos sobre alguém cuja identidade é conhecida, removendo informações e outros bens associados à pessoa de circulação pública, o anonimato, muitas vezes esconde a identidade de alguém sobre quem os fatos são conhecidos, com a finalidade de colocar tais dados em disponibilização (SKOPEK; 2014, p. 1755, tradução de Affonso e Sant'Ana; 2017).

Então, esta questão da privacidade se tornou algo importante no contexto de dados, pois de acordo com Wong et al. (2006), técnicas de preservação da privacidade são necessárias para disponibilização de dados, visando minimizar a possibilidade de identificação de informações sensíveis sobre os indivíduos, humanos ou não.

Segundo Fung et al. (2010) e Vimercati et al. (2012), técnicas como generalização, supressão, permutação e perturbação de dados são as principais operações utilizadas para viabilizar a privacidade e anonimizar dados sensíveis. Nergis (2014) complementa que estes métodos possuem uma característica em comum, que ele utiliza a generalização com forma de manipulação de dados para viabilizar a anonimização. De acordo com Affonso e Sant'Ana (2017), os objetivos destas técnicas, "é essencialmente evitar que a divulgação dos dados de contexto possa ser combinada por um atacante para re-identificar os sujeitos na base de dados".

Entretanto, essas técnicas de anonimização que garantem a privacidade, fazem parte de uma estrutura maior no contexto de IoT, em que para garantir a interoperabilidade dos dados faz-se necessário o uso de um modelo ou arquitetura de referência.

No entanto, quando fala-se de arquitetura ou modelo, o que realmente significa? Apesar das diversas definições encontradas na literatura, a arquitetura ou arquitetura de referência, pode ser compreendida como um desenho abstrato que relaciona conhecimento e experiências sobre a maneira de projetar coisas (sistemas, aplicativos, dispositivos IoT, etc.) em um determinado domínio, contribuindo para fornecer um caminho a seguir para o desenvolvimento de determinada tecnologia. Com isso, as arquiteturas de referência também podem ser utilizadas como uma forma de padronização, ou seja, facilitando e permitindo a interoperabilidade entre tecnologias baseadas na mesma arquitetura. (Muller 2008, Angelov et al. 2009, Nakagawa et al. 2011).

Estes termos, arquitetura de referência e modelo de referência, nos últimos anos estão sendo utilizados sem restrição ou até mesmo como sinônimos. No entanto, existem definições distintas para estes termos, modelo de referência é algo abstrato que representa um conjunto de conceitos e os relacionamentos entre eles com dentro de um domínio específico, sendo, portanto livre de padrões, tecnologias, implementações ou outros detalhes mais técnicos e concretos, geralmente são

representados por desenhos ou quadros, por exemplo, de modelos conceituais, ontologias ou taxonomias (Nakagawa et al., 2014).

Ainda de acordo com Nakagawa et al. (2014), uma arquitetura de referência é construída através de um ou mais modelos de referência, unificando regras de negócio, definições, padrões arquiteturais, estilos, boas práticas de desenvolvimento e até mesmo elementos de *hardware* e/ou *software* necessários à construção de arquiteturas específicas e concretas, que dizem respeito aos sistemas propriamente ditos no domínio em questão.

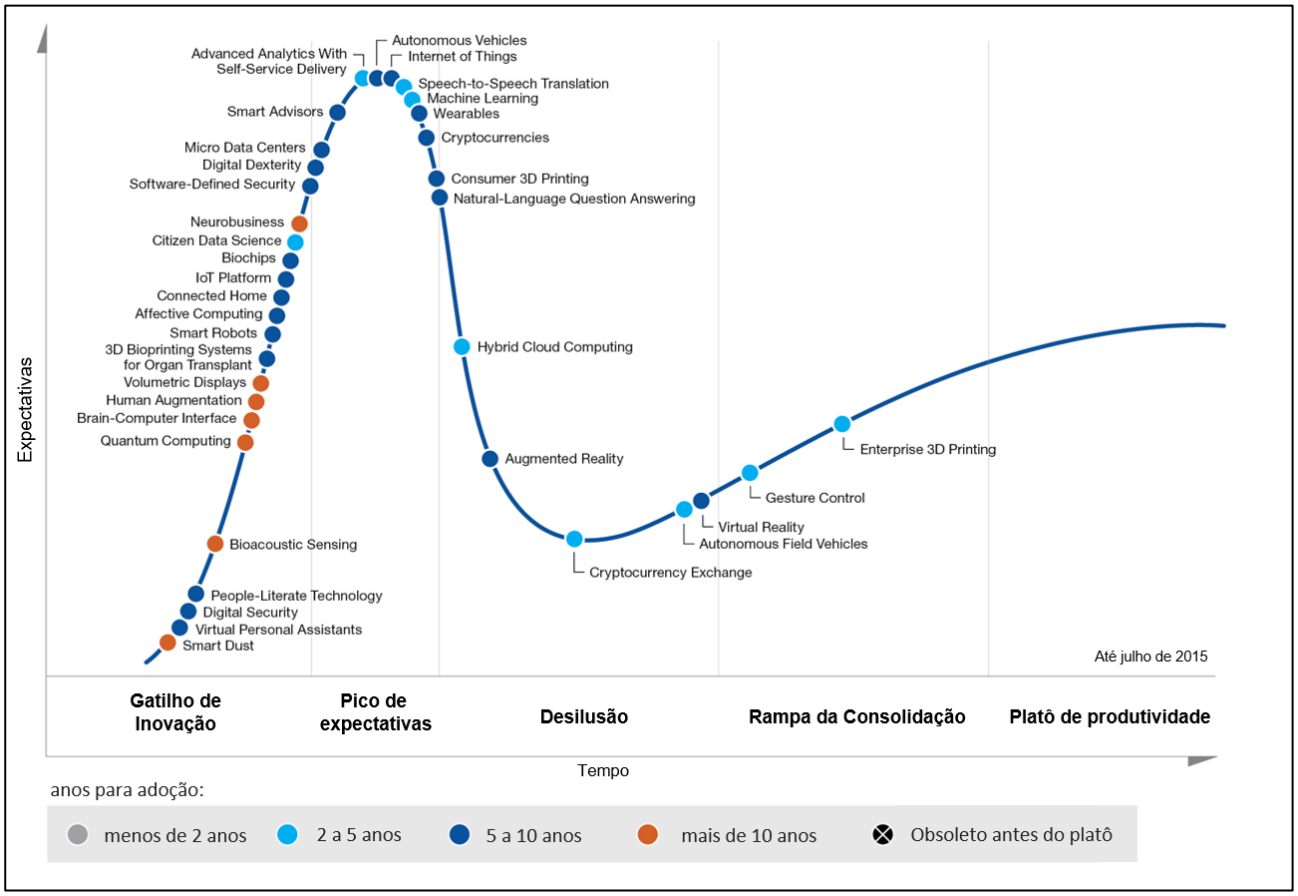
Então, um modelo de referência geralmente é a base utilizada para uma arquitetura de referência, ou que não é algo obrigatório, e a arquitetura de referência, fornece a estrutura e os elementos que deveriam ser utilizados para construir uma arquitetura real de um sistema.

2.1 Internet das Coisas – *Internet of Things* (IoT)

Conforme citado durante a introdução, o termo Internet das Coisas é uma tradução do termo em inglês *Internet of Things* (IoT), este termo, no entanto não faz referência apenas à “Internet”, mas sim a diversas áreas como eletrônica, ciência da computação, ciência da informação, comunicação, entre outras áreas tão importantes quanto a internet.

Observa-se que IoT tem ganhado enfoque no cenário acadêmico e industrial, pois de acordo com o gráfico apresentado pelo Gartner (2015) na Figura 4, IoT levaria de 5 a 10 anos para atingir um grau de maturidade suficiente para que tenha um impacto significativo no mercado. Este capítulo aborda a Internet das Coisas através de uma perspectiva teórica, na qual o conteúdo abordado explora as definições, a perspectiva histórica e a estrutura de IoT mediante ao uso de dados e comunicação.

Figura 4 - Gráfico de Expectativas do Gartner



Fonte: Gartner (2015), tradução do autor.

Em suma, de acordo com Santos et al. (2016) Internet das Coisas é uma extensão da Internet atual, expandindo a internet aos dispositivos físicos, objetos utilizados no dia-a-dia, na qual a abstração de conteúdo é elevado a outro patamar, em que com o passar dos anos o foco da coleta de dados e informações foi sendo alterado, no início da internet, apenas eram apresentados dados e informações, pouco tempo depois os usuário estavam compartilhando conteúdo, e a partir deste ponto tornou-se necessário entender melhor o usuário sendo necessário coletar dados sobre os mesmos.

Entretanto quando chegamos nos dias de hoje, além de todos os dados coletados sobre o usuário, tornou-se necessário expandir estas informações, coletando dados de objetos do dia-a-dia (quaisquer que sejam) que se conectem à internet.

A internet viabilizou diversos avanços na tecnologia nas últimas décadas, ainda segundo Santos et al. (2016), através desta rede mundial de computadores já é possível controlar objetos remotamente, bem como programá-los ou deixá-los disponíveis como provedores de serviços. Porém com esta expansão da internet, surgem novos desafios e grandes oportunidades tanto para a comunidade acadêmica quanto para as indústrias, tanto em assuntos técnicos quanto sociais.

2.1.1 Definição

Apesar da breve introdução ao conceito feita durante o capítulo anterior, este subcapítulo surge para trazer diversos pensamentos e conceitos desenvolvidos ao longo dos anos sobre este assunto complexo e dinâmico, na qual é conhecido por diversos termos e ideias diferentes. Esta ideia de objetos conectados, trocando informações em uma grande rede mundial, é bastante ampla e torna possível que diversas tecnologias e aplicações diferentes possam ser denominadas de Internet das Coisas.

Conforme dito no primeiro parágrafo, existem termos parecidos com IoT, bem como tecnologias que hoje atendem pelo nome de Internet das Coisas, no entanto, durante muitos anos, outros trabalhos e tecnologias travam este assunto com outros nomes. A organização europeia The Internet of Things Council*,* traz através de Kranenburg et al. (2011, p.2), que durante os anos 80, diversos projetos sobre este assunto já eram desenvolvidos, porém eram conhecidos por nomes diferentes como *ambient intelligence, calm computing, ubicomp* ou *ubiquitous computing*, e *pervasive computing*.

Ainda de acordo com Kranenburg et al. (2011, p.4), algumas variações de entendimento existem em função de limites nacionais, pois segundo eles, enquanto na Europa e na China o termo IoT é bem aceito, nos Estados Unidos as referências mais frequentes são *smart objects*, *smart grid* e *cloud computing*.

Estes e outros termos são criados quando existe uma certa intersecção entre objetos do cotidiano e a tecnologia, Greenfield (2006) conclui que a computação está migrando para nossa vida cotidiana, na qual a interação entre humanos e computadores será reconstruída, em que serão oferecidas informações sobre clima, localização, e até mesmo informações sobre as próprias pessoas. Este tipo de informação pode ser considerada como informação ubíqua ou '*everyware'*, pois se manifesta em diversos lugares e contextos, de forma variada, afetando o cotidiano dos indivíduos estando eles conscientes sobre isso ou não.

Greenfield (2006) diferencia alguns conceitos parecidos, que muitas vezes são usados com o mesmo significado, porém possuem conceitos e ideias diferentes:

- **computação ubíqua** é a integração de processos informacionais em ambientes do cotidiano, provendo serviços, informação e comunicação em ambientes comuns do cotidiano das pessoas;
- **computação física** é a maneira como as pessoas têm acesso à computação, por meio de objetos e não através de ambiente virtuais ou computadores tradicionais;
- **computação pervasiva** se refere à forma como essa nova tecnologia prevalece atualmente;

- **inteligência ambiental** é a inclusão de dispositivos computacionais em espaços construídos pelo homem, tornando esses dispositivos parte do ambiente;
- **Internet das Coisas** é o mundo em que objetos físicos são digitalmente identificáveis e estão relacionados entre eles.

No entanto diversos outros autores definem IoT de modo mais completo e claro, como por exemplo uma definição técnica proposta pelo "*Strategic Research Agenda*" da *"*Cluster of European Research Projects on the Internet of Things*"* (CERP-IoT) de 2009 que define a IoT como:

> infraestrutura de rede global dinâmica com capacidades de autoconfiguração baseadas em protocolos de comunicação padrão e interoperáveis onde "coisas" físicas e virtuais têm identidades, atributos físicos e personalidades virtuais e usam interfaces inteligentes e são integradas de forma transparente na rede de informações. No IoT, espera-se que as "coisas" se tornem participantes ativos em negócios, informações e processos sociais, onde eles são capazes de interagir e se comunicar entre si e com o meio ambiente, trocando dados e informações "percebidas" sobre o meio ambiente, enquanto reagem de forma autônoma a os eventos do "mundo real / físico" e influenciá-lo executando processos que desencadeiam ações e criam serviços com ou sem intervenção humana direta. As interfaces na forma de serviços facilitam as interações com essas "coisas inteligentes" pela Internet, consultam e alteram seu estado e qualquer informação associada a eles, levando em consideração problemas de segurança e privacidade. (CERP IoT, 2009, p. 6, tradução do autor)

Outra grande organização é o W3C (World Wide Web Consortium), que foi fundado por ninguém menos que Tim Berners-Lee, e é a principal organização de padronização da *Web*, também tem sua definição sobre IoT, na qual definem que IoT é uma rede de objetos conectados à Internet, que permite a conectividade e interação entre objetos, dados e pessoas, através de tecnologias que tornam possível o acesso à esta rede por qualquer pessoa, de qualquer lugar e a qualquer momento, através de qualquer dispositivo do cotidiano, como relógios, automóveis, celular, roupas, etc. (W3C, 2010).

Tecnologicamente falando, IoT é

> [...] uma infraestrutura dinâmica global com capacidades de autoconfiguração, baseada em protocolos de comunicação padronizados e interoperáveis, onde 'coisas' virtuais e físicas possuem identidades, atributos físicos e personalidades virtuais, usam interfaces inteligentes e estão integradas de maneira transparente à Rede de informações (IERC, 2012).

Sobre os termos *smart object* (Objetos Inteligentes) ou *smart things* (Coisas Inteligentes) citados anteriormente, Norman (2009) traz um esclarecimento interessante, na qual ele diz que "objetos não são inteligentes, apenas processam informações". Este pensamento encaixa-se perfeitamente para dispositivos IoT, sendo que tais dispositivos inseridos nos mais diversos contextos não possuem nenhum tipo de inteligência artificial, mas sim sensores e outras tecnologias utilizadas para coletar dados.

Tendo isso em vista o assunto de sensores, observa-se que outras instituições como o IEEE (Institute of Electrical and Electronics Engineers) também descrevem o conceito de Internet das Coisas. Em um relatório especial sobre Internet de Coisas, o IEEE descreveu IoT como: "Uma rede de itens - cada uma incorporada a sensores - que estão conectados a Internet."(IEEE, 2014).

Por fim, com intuito de definir de forma clara e objetiva, McEwen e Cassimally (2013) propõem a seguinte composição para definir a Internet das Coisas:

objeto físico + controladores, sensores e atuadores + Internet = IoT

Com todas essas definições foi concluído que IoT é um assunto que está longe de ser esgotado, pois existem diversas frentes de pesquisa e organizações interessadas neste assunto, devido à grande quantidade de dispositivos eletrônicos processados existentes atualmente, na qual, segundo MCCULLOUGH (2004), a Intel informou que mais de 95% dos dispositivos que contêm microchips já não se apresentam aos usuários na forma de computadores. Este relato foi em 2004, o que de acordo com o crescimento exponencial da tecnologia nos últimos anos esse número deve ser ainda maior atualmente.

Como o assunto está longe de ser esgotado, deve-se ter a consciência de que este tema também não foi criado a poucos anos, existem diversos autores que tratavam sobre este assunto à algumas décadas atrás. No próximo item deste trabalho é apresentada uma perspectiva histórica sobre este assunto.

2.1.2 Perspectiva histórica

O artigo *The Computer of 21st Century* de Mark Weiser, publicado em setembro de 1991 na *Scientific American* (WEISER, 1991), é um marco na pesquisa sobre a Internet das Coisas. De acordo com Singer (2012), este texto é considerado como o primeiro texto publicado sobre o tema de computação ubíqua e o mesmo é citado em boa parte da literatura sobre IoT.

No entanto, o termo "*Internet of Things*" foi cunhado em 1999 pelo pesquisador Kevin Ashton, pesquisador e co-fundador do Auto-ID Center do Massachusetts Institute of Technology (MIT). Entretanto, o termo IoT só aparece escrito em 2001 no livro branco de Brock, também pesquisador do Auto-ID Center (BROCK, 2001). Ashton (2009) afirmou que originalmente a ideia de IoT previa a conexão de todos os objetos físicos à Internet, capturando informações através de RFID e outras tecnologias de sensoriamento, permitindo observar, analisar, identificar e compreender o mundo sem depender do tempo e da disposição das pessoas.

Outra vertente para o nascimento do termo é através de Neil Gershenfeld, na época diretor do consórcio de pesquisa "*Things that Think*" do MIT Media Lab, que publicou o livro "*When Things Start to Think*" em 1999. No livro ele traz o seguinte trecho,

> Mais do que procurar fazer computadores ubíquos, devemos tentar fazê-los discretos [...] A promessa real de conectar computadores é libertar as pessoas, incorporando meios para resolver problemas nas coisas ao nosso redor (GERSHENFELD, 1999)

, além disso, Singer (2012) relata que no livro, Gershenfeld descreve experiências de computação vestível, experimentos com nanotecnologia e preocupações relacionadas às emoções e direitos civis em uma realidade em que objetos processam informação.

No ano seguinte, ano 2000, a LG lança o primeiro eletrodoméstico conectado à internet, uma geladeira, o produto deveria fazer conjunto com uma série de outros dispositivos da mesma marca, todos conectados à internet e gerenciados através de um sistema proprietário da LG.

Após o ano 2000, o conceito de IoT começa a ganhar visibilidade e cada vez mais são produzidos objetos com a ideia de uma rede de objetos conectados trocando dados. Em 2003 projetos como "*Cooltown"*, "*Internet0*", e "*Disappearing Computer Initiative*" implementaram algumas ideias para fortalecer e popularizar o IoT. Em 2004 G. Lawton traz o termo M2M (*machine-to-machine*), um conceito de comunicação entre coisas ou máquinas, este termo é muito importante dentro do cenário de IoT, pois aparece em diversas literaturas e padrões de implementação.

Ainda em setembro de 2004, a *Scientific American* lança o termo de casas inteligentes, na qual sensores interligados e outras tecnologias permitam que tudo seja conectado à casa, isso foi descrito em um artigo assinado por Neil Gershenfeld e outros pesquisadores do MIT Media Lab. Em 2005, o termo IoT apareceu pela primeira vez no New York Times, o que alavancou as pesquisas e interesses no assunto, chamando a atenção do governo e de grandes instituições.

Conforme dito no parágrafo anterior, a partir de 2005, a discussão sobre assuntos relacionados a IoT foi pulverizada e começou a ganhar a atenção dos governos, e a chamar a atenção para questões relacionadas à privacidade e segurança de dados. Foi em 2005 que o IoT tornou-se assunto do International Telecommunication Union (ITU), uma agência das Nações Unidas com foco em tecnologias da informação e da comunicação.

Este grupo declarou que o IoT é o "próximo passo das tecnologias '*always on*' [...] que prometem um mundo de dispositivos interconectados em rede" (ITU, 2005, p. 1), assim como a internet móvel e outras vertentes fizeram sucesso, este assunto pretende mudar a maneira como enxergamos o mundo atualmente.

Em 2005 também foi o ano do lançamento do Nabaztag, um objeto muito parecido com o que conhecemos hoje como Google Home e Amazon Alexa, este objeto tinha a forma de um coelho e era conectado Internet, podendo ser programado para informar a previsão do tempo, ler *e-mails* ou notícias, entre outras aplicações. Ainda em 2005 foi criado o Arduino, uma placa com um micro controlador de baixo custo, que é usado para implementação e prototipação de diversos projetos de eletrônica e dispositivos IoT.

Adam Greenfield lançou seu livro "*Everyware*" em 2006, em que traz seus anseios e preocupações acerca dos objetos conectados. Greenfield além de trazer a definição de *everyware*, ele discute sobre o potencial das tecnologias ubíquas para o bem-estar das pessoas e também chama a atenção para os perigos relacionados à vigilância e privacidade.

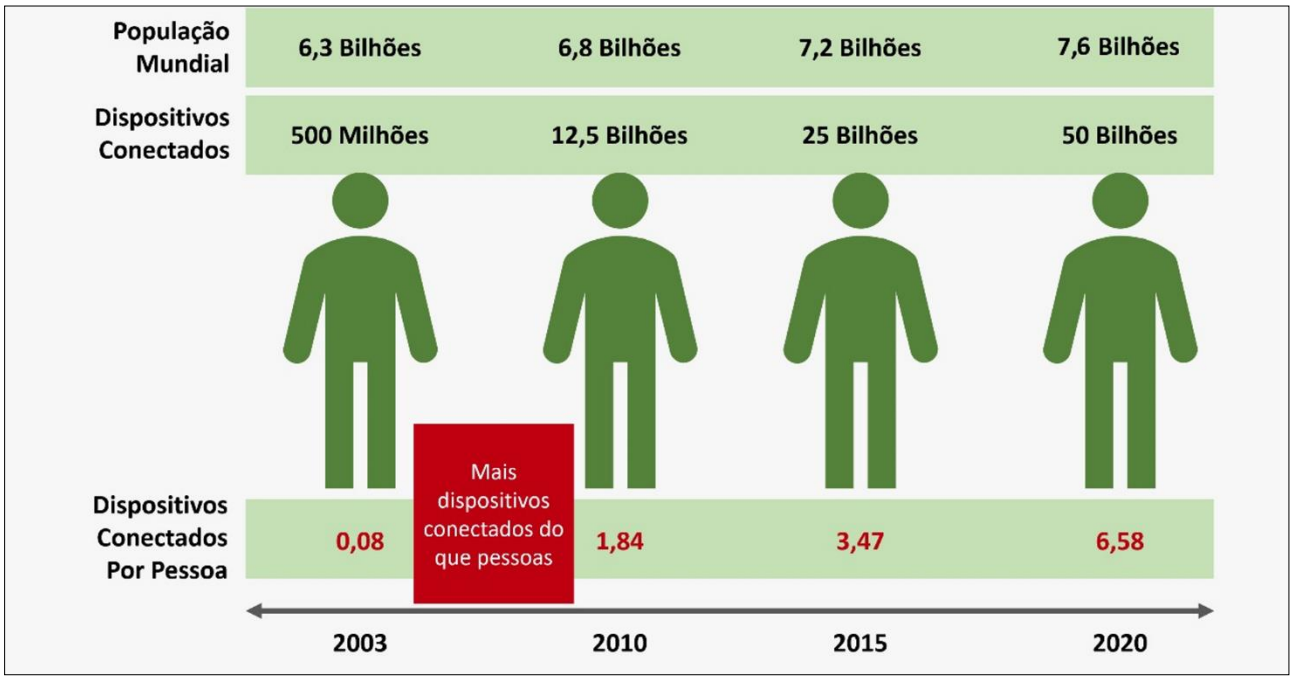
Assim como os livros "*Shaping Things*" e "*Everyware*", em 2008 foi publicado outro título muito importante para a temática, o livro "*The Internet of Things*" de Rob Van Kranenburg, que fala sobre objetos que produzem informação. De acordo com Singer (2012), este livro traz conceitos de ambientes humanos que processam informação de forma autônoma através de dispositivos conectados e ainda as preocupações do autor sobre as vigilâncias que as coisas conectadas podem exercer e a necessidade de se apropriar dessa tecnologia.

Em 2008 foi criado a IPSO Alliance, uma aliança entre empresas para promover o uso do *Internet Protocol* (IP) em redes de "objetos inteligentes" e possibilitar a Internet das Coisas, a aliança possui mais de 50 empresas associadas, incluindo Google, Cisco, SAP, Bosch, Ericsson, Intel e Fujitsu.

Ainda em 2008, aconteceu a primeira conferência sobre IoT, a *Internet of Things Conference* em Zurique na Suíça, este evento ainda teve suas discussões compiladas em um livro que foi publicado no mesmo ano sob a organização de Christian Floerkemeier, Marc Langheinrich, Elgar Fleisch, Friedemann Mattern e Sanjay E. Sarma. A segunda edição foi realizada dois anos depois, em 2010 na cidade de Tóquio e a terceira edição aconteceu em 2012 na cidade de Wuxi na China.

Entre os anos de 2008 e 2009, de acordo com a previsão da Cisco (2011) a quantidade de máquinas, objetos ou coisas conectadas seria maior que número de pessoas. Em 2020 de acordo com a mesma fonte, existirá uma imensa quantidade de dispositivos conectados, cerca de 50 bilhões de objetos conectados para 7,6 bilhões de pessoas, como observa-se na Figura 5.

Figura 5 - Previsão de crescimento dos objetos conectados



Fonte: Cisco (2011), tradução do autor.

Em 2009, um ano após a conferência internacional, aconteceu em Salvador o primeiro evento sobre IoT no Brasil, chamado de 1º Congresso de Tecnologia, Sistemas e Serviços com RFID, o evento foi organizado pelo CIMATEC SENAI e pela Saint Paul Etiquetas Inteligentes (fabricante de etiquetas RFID). No entanto, em sua segunda edição seu nome foi alterado e o evento passou a ser chamado de Congresso Brasileiro de Internet das Coisas e RFID, a segunda edição ocorreu dois anos após a primeira edição e foi em Búzios no ano de 2011.

Então em 2010 começam a ser levantadas preocupações com relação a interoperabilidade, pois de acordo com o modelo da Cisco (2011), em 2010 a quantidade de dispositivos já era quase o dobro da quantidade de pessoas e com a diversidade de novas tecnologias, começou-se em meio às empresas e governos uma discussão sobre a criação de padrões internacionais que possibilitem a existência de uma rede autônoma de objetos conectados, como os padrões ITU-T, IoT-A, WoT, etc.

Em 2012, a União Europeia criou um evento na qual os cidadãos tivessem a oportunidade de destacar seus anseios e inseguranças sobre a IoT, o evento aconteceu em Londres e foi chamado de "1ª *Open IoT Assembly*". Como resultado das discussões e conclusões levantadas durante o evento foi criado um documento com princípios de transparência e bom uso das informações na IoT.

Em 2012 também foi criado o famoso "*Google Glass*", um óculo com um *display* óptico embutido, que exibe informações coletadas sem fio, de acordo com a especificação do usuário. O produto somente foi vendido ao público em 2014, e fez muito sucesso em seu lançamento, gerando muitas discussões acerca de assuntos como privacidade, mas logo o produto foi descontinuado pela

Google e as discussões sobre este produto esfriaram, mas até hoje existem muitas discussões sobre privacidade não somente deste tipo de dispositivos, mas de todos os dispositivos conectados e coletam dados dos usuários direta ou indiretamente.

2014 foi considerado pelo *Venture Beat* como o ano do IoT, e de 2014 para frente foram criados os mais diversos produtos inseridos no contexto de IoT, no entanto nos últimos anos, nota-se um esforço acerca da segurança e privacidade dos dispositivos IoT.

Em 2015 foi lançada a primeira edição do guia de cibersegurança desenvolvido pela AT&T (empresa de telecomunicações americana), e em 2016 a segunda edição. Atualmente o guia está na quinta edição e traz discussões e melhores práticas de segurança de dados em diversos contextos, desde a *web* até *smartphones* e dispositivos IoT.

Com o passar dos anos, as tecnologias que inicialmente foram desenvolvidas para aplicações industriais e de logística, passaram a criar o conceito que hoje é conhecido como Internet das Coisas e se estendeu das indústrias para objetos do cotidiano, como eletrodomésticos, roupas, etc., bem como trazendo preocupações sobre privacidade e até mesmo debates públicos sobre segurança e transparência.

Por fim, os eventos descritos neste trabalho não esgotam a história acerca do tema Internet das Coisas, apenas elenca alguns dos mais importantes acontecimentos e produtos criados ao decorrer dos anos, outros autores também trazem uma linha do tempo sobre este assunto, como é o caso de Lacerda (2015), que em sua tese elabora uma linha do tempo com os principais acontecimentos sobre IoT, abaixo será apresentada a linha do tempo atualizada com base nos eventos listados por Lacerda (2015).

Tabela 1 - Linha do tempo sobre Internet das Coisas

Ano	**Fato ou Pessoa**	**Descrição**
1832	Baron Schilling	Telégrafo eletromagnético
1833	Carl Friedrich Gauss and Wilhelm Weber	Código para se comunicar a uma distância de 1200 m
1844	Samuel Morse	Mensagem telegráfica em código Morse.
1926	Nikola Tesla	“Quando a tecnologia sem fio estiver perfeitamente aplicada, a Terra inteira será transformada em um enorme cérebro, todas as coisas serão como partículas de um todo real e rítmico... e os instrumentos que utilizaremos para fazer isso serão incrivelmente mais simples em comparação com o presente telefone. Um homem será capaz de transportar um no bolso do colete” (*Colliers Magazine*).
1948	Norbert Wiener	lançou seu livro “Cibernética”

Ano	Fato ou Pessoa	Descrição
1949	Norman Joseph Woodland	Código de barras linear.
1950	Norbert Wiener	lançou seu livro “Cibernética e sociedade: o uso humano de seres humanos”
1950	Alan Turing	“...é melhor equipar a máquina com os melhores órgãos dos sentidos que o dinheiro possa comprar, e depois ensiná-la a entender e a falar inglês. Este processo poderia seguir o ensino normal de uma criança”.
1961	Edward Thorp Claude Shannon	Testado em *Las Vegas* o primeiro computador vestível, um dispositivo do tamanho de uma caixa de cigarros, usado no sapato para prever roletas. O protótipo foi feito em 1955.
1964	Marshall McLuhan	“...através de meios elétricos, criamos uma dinâmica pela qual todas as tecnologias anteriores - incluindo cidades - serão traduzidas em sistemas de informação” (*Understanding Media*).
1965	Gordon Moore (*Intel*)	Antecipou que a quantidade de transistores em um circuito integrado comercialmente viável dobraria a cada 18 meses, mantendo o custo de fabricação - Lei de Moore.
1966	Karl Steinbuch	Em poucas décadas, computadores estarão entrelaçados em quase todos os produtos industriais.
1967	Hubert Upton	Computador analógico vestível com visor em óculos para ajudar a leitura labial.
1969	Arpanet	Primeira mensagem enviada via rede pelo projeto *Advanced Research Project Agency Network* (Arpanet) do U.S. *Departament of Defense*.
1973	Mario Cardullo	Patente da etiqueta de radiofrequência RFID passiva, de leitura escrita.
1974	TCP/IP	Primeira especificação do conjunto de protocolos de comunicação em rede TCP/IP (Transmission Control Protocol/Internet Protocol) pela Universidade de Stanford e University College of London.
1974	*Universal Product Code* (UPC)	Simbologia de código de barras, utilizada pela primeira vez para compras de supermercado.
1984	*Domain Name System* (DNS)	Foi criado o DNS (*Domain Name System*) - “Sistema de gerenciamento de nomes hierárquico e distribuído para computadores, serviços ou qualquer recurso conectado à Internet ou em uma rede privada”. 1980s *Carnegie-Mellon Computer Science Department*, Membros da CMU instalaram micro chaves na máquina da Coca-Cola e as conectaram ao computador departamental para que eles pudessem ver em seus terminais quantas garrafas restavam e se estavam frias ou não.

Ano	Fato ou Pessoa	Descrição
1989	Tim Berners-Lee	Criou a *World Wide Web*. No ano seguinte, com a ajuda de Robert Cailliau e um jovem estudante do CERN, implementou a primeira comunicação bem sucedida entre um cliente HTTP e o servidor através da internet.
1990	John Romkey	Primeiro artefato de Internet, uma torradeira que pode ser ligada e desligada pela rede.
1990	Olivetti	Sistema de identificação ativa com sinais infravermelhos para comunicar a localização de uma pessoa.
1991	Mark Weiser	Artigo na *Scientific American* sobre computação ubíqua. "O futuro tecnológico será caracterizado pela computação, não por computadores".
1993	Quentin Stafford Fraser and Paul Jardetzky	Cafeteira *Trojan Room* desenvolvida na Universidade de Cambridge, foi usada para monitorar os níveis de café, pelo envio de imagem atualizada 3x por minuto
1994	Steve Mann	*WearCam*, a primeira versão comercial da câmera sem fio, considerada o primeiro exemplo de registro do cotidiano.
1994	Mik Lamming Mike Flynn (Xerox EuroPARC)	*Forget-Me-Not*, dispositivo vestível sem fio com armazenamento de informações.
1994	B.N. Schilit M.M. Theimer	Primeira ocorrência do termo '*context-aware*' na literatura - "*Disseminating active map information to mobile hosts*" *Network*, Vol.8, Issue 5.
1995	Amazon e Echobay (Ebay)	A Internet torna-se comercial.
1995	Nicholas Negroponte Neil Gershenfeld (MIT)	Artigo "*Wearable Computing*", publicado na *Wired*. "Para *hardware* e *software* confortavelmente segui-lo por aí, devem fundir-se em *softwear* ... A diferença de tempo entre as ideias malucas e produtos entregues está encolhendo tão rapidamente que é agora [...] cerca de uma semana"
1997	Paul Saffo	Artigo publicado em *Ten-Year Forecast: "Sensors: The Next Wave of Infotech Innovation*".
1997	*Carnegie-Mellon*, MIT e *Georgia Tech*	Organizaram o primeiro IEEE *International Symposium on Wearable Computers*, em Cambridge, MA.
1998	Scott Brave Andrew Dahley Hiroshi Ishii (MIT)	Projeto *inTouch* - telefone tangível para comunicação tátil de longa distância.
1998	Mark Weiser	Fonte de água que altera o fluxo e o volume em função do mercado de ações.
1999	Sanjay Sarma David Brock Kevin Ashton	Ajudaram a desenvolver o *Electronic Product Code* (EPC), sistema de identificação baseado em RFID com a finalidade de substituir o código de barras (UPC). Transformaram a identificação por radiofrequência (RFID) em uma tecnologia de rede, ligando objetos à Internet através de etiquetas RFID.

Ano	Fato ou Pessoa	Descrição
1999	Kevin Ashton (Auto-IDCenter, MIT)	Cunhou o termo "*Internet of Things*" como o título de uma apresentação na *Procter & Gamble*.
1999	Neil Gershenfeld (MIT *Media Lab*)	Publicou o livro "*When Things Start to Think*" Mais do que procurar fazer computadores ubíquos, devemos tentar fazê-los discretos [...] A promessa real de conectar computadores é libertar as pessoas, incorporando meios para resolver problemas nas coisas ao nosso redor.
2000	LG	*Internet Digital* DIOS - o primeiro refrigerador ligado à Internet.
2001	Neil Gershenfeld (MIT *Media Lab*)	Fundou o *Center for Bits and Atoms* no MIT.
2001	BROCK	Primeira vez que o termo IoT aparece escrito, foi no livro branco de Brock, também pesquisador do Auto-ID Center
2002	David Rose e outros (MIT *Media Lab*)	*The Ambient Orb*, monitora a bolsa de valores, portfólios pessoais, clima e outras fontes de dados e muda de cor com base em parâmetros dinâmicos.
2003	Projetos como *Cooltown*, *Internet0*, e *Disappearing Computer Initiative*	Buscaram implementar algumas ideias e popularizar a IoT.
2003	Bernard Traversat e outros	Project JXTA-C: *Enabling a Web of Things*, publicado em HICSS '03 *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*. Projeto de código aberto, que especificou um conjunto de protocolos padrão para computação ad hoc, pervasiva e P2P que serviriam como base para a *web* das coisas.
2003	*BigBelly Solar*	Lixeira inteligente recarregada pelo sol, que comunica seu estado pela Internet.
2004	Bruce Sterling	Propôs o conceito de "*Spime*", objeto localizado em determinado espaço e tempo, que têm sua história registrada. "No futuro, a vida de um objeto começa em uma tela gráfica. Nasce digital. Suas especificações de *design* irão acompanhá-lo ao longo de sua vida. É inseparável do modelo digital original, que governa o mundo material".
2004	G. Lawton	M2M: em "*Machine-to- machine technology gears up for growth*" publicado em *Computer*: Há muito mais máquinas – definidas como coisas com propriedades mecânicas, elétricas ou eletrônicas – no mundo do que pessoas. E um número crescente de máquinas está em rede... M2M é baseada na ideia de que a máquina tem mais valor quando está em rede e que a rede se torna mais valiosa quanto mais máquinas estão conectadas".

Ano	Fato ou Pessoa	Descrição
2004	*Scientific American*	Lança o termo de casas inteligentes, onde sensores interligados e outras tecnologias permitam que tudo seja conectado à casa, isso foi descrito em um artigo assinado por Neil Gershenfeld
2005	UN's *International Telecommunications Union* – ITU	Publicou seu primeiro relatório dobre a IoT: "Uma nova dimensão foi adicionada ao mundo das TICs: a conectividade a qualquer tempo, em qualquer lugar e para qualquer pessoa passa a ser agora conectividade em qualquer coisa. Conexões irão multiplicar-se e criar uma dinâmica rede de redes totalmente nova – uma Internet das Coisas".
2005	*Interaction Design Institute Ivrea* (IDII) em Ivrea, Italy	Criaram o Arduino - placa microcontroladora de baixo custo e fácil uso - para o desenvolvimento de projetos interativos, com grande impacto na computação física (MCEWEN; CASSIMALLY, 2013).
2005	Rafi Haladjian Olivier Mével (*Violet*)	Nabaztag (agora parte da Aldebaran Robotics) - pequeno coelho com WiFi, alerta sobre o mercado de ações, notícias, alarme, *feeds* RSS, e conecta-se com outros coelhos. "Se você pode até conectar coelhos, você pode conectar qualquer coisa".
2006	Adam Greenfield	Lançou seu livro "*Everyware"*, onde traz seus anseios e preocupações acerca dos objetos conectados. Greenfield além de trazer a definição de *everyware*, ele discute sobre o potencial das tecnologias ubíquas para o bem-estar das pessoas e também chama a atenção para os perigos relacionados à vigilância e privacidade.
2008	IPSO *Alliance*	Aliança entre empresas para promover o uso do *Internet Protocol* (IP) em redes de objetos inteligentes e possibilitar a Internet das Coisas. A aliança agora possui mais de 50 empresas associadas, incluindo Bosch, Cisco, Ericsson, Intel, SAP, Sun, Google e Fujitsu.
2008	*White space*	A Federal Communications Commission (FCC) aprovou regras para permitir que transmissores de rádio sem licença para operar no espectro de transmissão de televisão utilizassem o 'espaço em branco' (*white space*), que não está sendo utilizado por serviços licenciados, para a banda larga sem fio.
2008	Christian Floerkemeier, Marc Langheinrich, Elgar Fleisch, Friedemann Mattern e Sanjay E. Sarma.	Foram os responsáveis pela primeira conferência sobre IoT a *Internet of Things Conference* em Zurique na Suíça, este evento ainda teve suas discussões compiladas no livro "*Internet of Things*" (2008) que foi publicado no mesmo ano sob a organização dos mesmos.

Ano	Fato ou Pessoa	Descrição
2008 - 2009	Internet das Coisas	A Internet das Coisas surge entre 2008 e 2009 no momento em que o número de coisas ou objetos conectados à Internet ultrapassou o de pessoas (Cisco, 2011).
2009	Ashton	O autor afirmou que originalmente a ideia de IoT previa a conexão de todos os objetos físicos à Internet, capturando informações através de RFID e outras tecnologias de sensoriamento, permitindo observar, analisar, identificar e compreender o mundo sem depender do tempo e da disposição das pessoas.
2009	CIMATEC SENAI e pela Saint Paul Etiquetas Inteligentes (fabricante de etiquetas RFID).	Aconteceu em Salvador o primeiro evento sobre IoT no Brasil, chamado de 1º Congresso de Tecnologia, Sistemas e Serviços com RFID.
2010	*ZigBee Alliance IPv6 Forum*	Parceria estratégica com a IPSO para acelerar a adoção de rede IP para objetos inteligentes.
2010	*Bluetooth 4.0*	Lançamento da tecnologia de *Bluetooth* 4.0 ou *Bluetooth Low Energy*
2011	Arduino e outras plataformas de *hardware*	Tornaram-se maduras e possibilitaram a utilização da Internet das Coisas por pessoas comuns (no estilo faça você mesmo').
2011	Nest Labs	Termostato *Nest Learning*, que usa algoritmos de sensores, aprendizagem de máquina e computação em nuvem para compreender os comportamentos do proprietário da casa e preferências, para ajustar a temperatura.
2011	ICT-FP7 *Work Programme*, IoT-A e *Digital Future Directives*	Europa mostra seu contínuo interesse e apoio aos assuntos relacionados com a IoT por meio de iniciativas como o Programa de Trabalho ICT-FP7, a arquitetura IoT-A e o subsídio do governo do Reino Unido (R$ 5 milhões).
2011	China	Continua a financiar e apoiar a pesquisa de desenvolvimento no campo da IoT em instituições como Instituto Xangai e a Academia Chinesa de Ciências.
2012	IPV6 – lançamento público	O novo protocolo de endereços de IP de 128 bits. "Poderíamos atribuir um endereço IPV6 para cada átomo na superfície da terra, e ainda teríamos endereços suficientes para fazer mais 100 Terras" (Steven Leibson, 2008).
2012	IoT-GSI *Global Standards*	Iniciativa de padronização que promove uma abordagem unificada para o desenvolvimento de padrões técnicos que viabilizem a Internet das Coisas em uma escala global.

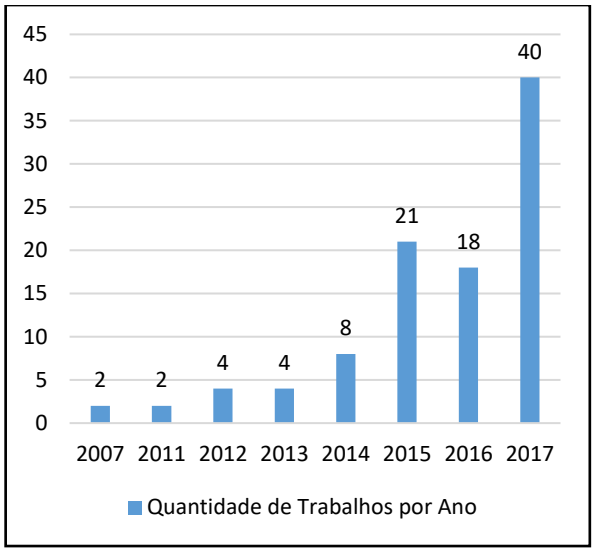
Ano	Fato ou Pessoa	Descrição
2012	Google Protótipo do Google *Glass*	óculos com um *display* óptico embutido, que exibe informações coletadas sem fio, de acordo com a especificação do usuário. Passou a ser vendido ao público em 2014.
2012	*Proteus Digital Health*	Recebe autorização da FDA para lançar dispositivo médico ingerível sem fio que comunica os sinais vitais do paciente por meio de um sistema sobre a pele, que então envia informações a um telefone celular.
2013	AllSeen Alliance e Open Interconnect Consortium	Iniciativas de alianças entre empresas de tecnologia com a Qualcomm, para desenvolver estrutura aberta que possibilite a difusão da Internet das Coisas. A Intel e outras empresas criaram um consórcio concorrente, chamado Open Interconnect Consortium.
2014	*Venture Beat*	2014 é considerado “o ano da Internet das Coisas”.
2015	AT&T	AT&T lança a primeira edição do guia de cibersegurança
2015	Windows 10 IoT Core	Microsoft lança uma nova versão do seu novo sistema operacional voltada para Internet das Coisas
2016	Brasil	BNDES realiza chamada pública para contratar uma consultoria para realizar um plano nacional de Internet das Coisas
2016	Bluetooth 5	Lançamento da nova tecnologia Bluetooth 5, possui um alcance 4 vezes maior, o dobro de velocidade e permite múltiplas conexões
2017	Brasil	Brasil inicia o projeto “Internet das Coisas: um plano de ação para o Brasil”

Fonte: adaptado de Lacerda (2015).

Após observar esta linha do tempo e toda a perspectiva histórica de IoT, foi realizada pelo autor uma pesquisa nos periódicos da área de CI, classificados pela CAPES com Qualis A1, com os termos “*Internet of Things*” e “Internet das Coisas”, afim de identificar o interesse da CI sobre a temática, na qual foi confirmado, através da quantidade de artigos encontrados, que existe um crescente interesse por este assunto no decorrer dos anos, como pode-se observar na Tabela 2.

Tabela 2 - Pesquisa do "*Internet of Things*" e "Internet das Coisas"

Ano	Quantidade de Trabalhos
2007	2
2011	2
2012	4
2013	4
2014	8
2015	21
2016	18
2017	40
Total	105



Fonte: elaborado pelo autor.

Após conhecer um pouco da história sobre o tema, no próximo capítulo, serão apresentados os principais padrões desenvolvidos nos últimos anos, estes padrões são descritos através de uma arquitetura de camadas, conhecida como arquitetura de referência, portanto antes de apresentar os padrões torna-se necessário esclarecer o que é uma arquitetura de referência, como pode-se observar no próximo item deste trabalho.

3 Modelos e Arquiteturas de referência

Com o intuito de conectar bilhões de objetos à Internet torna-se necessária uma arquitetura ou um modelo para padronizar a estrutura de comunicação desses dispositivos. Atualmente encontra-se uma grande variedade de propostas de arquiteturas sofisticadas, na qual baseiam-se nas necessidades da academia e da indústria (Al-Fuqaha et al., 2015).

No entanto, quando fala-se de arquitetura ou modelo, o que realmente significa? Apesar das diversas definições encontradas na literatura, a arquitetura ou arquitetura de referência, pode ser compreendida como um desenho abstrato que relaciona conhecimento e experiências sobre a maneira de projetar coisas (sistemas, aplicativos, dispositivos IoT, etc.) em um determinado domínio, contribuindo para fornecer um caminho a seguir para o desenvolvimento de determinada tecnologia. Com isso, as arquiteturas de referência também podem ser utilizadas como uma forma de padronização, ou seja, facilitando e permitindo a interoperabilidade entre tecnologias baseadas na mesma arquitetura. (Muller 2008, Angelov et al. 2009, Nakagawa et al. 2011).

Estes termos, arquitetura de referência e modelo de referência, nos últimos anos estão sendo utilizados sem restrição ou até mesmo como sinônimos. No entanto, existem definições distintas para estes termos, modelo de referência é algo abstrato que representa um conjunto de conceitos e os

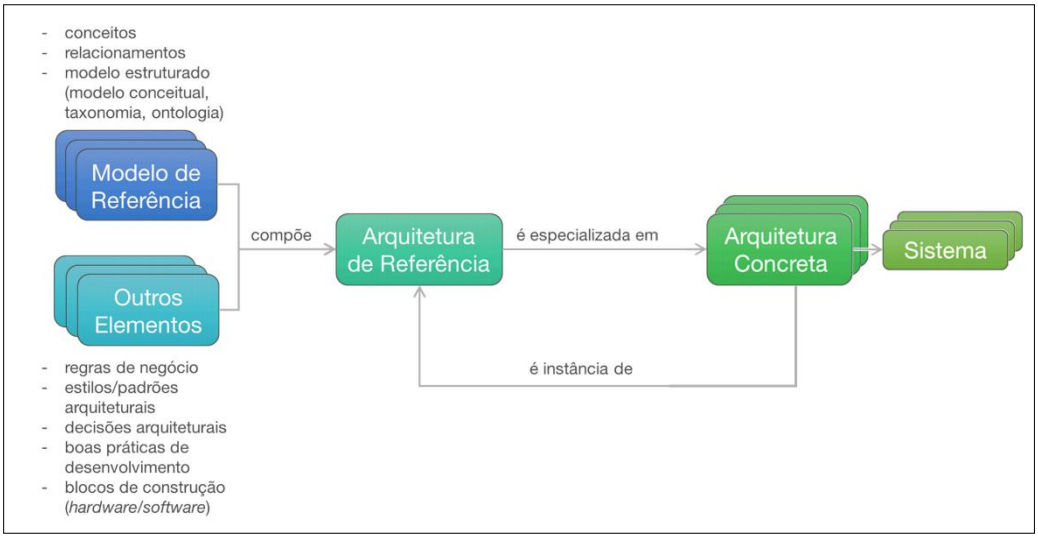
relacionamentos entre eles com dentro de um domínio específico, sendo, portanto livre de padrões, tecnologias, implementações ou outros detalhes mais técnicos e concretos, geralmente são representados por desenhos ou quadros, por exemplo, de modelos conceituais, ontologias ou taxonomias (Nakagawa et al., 2014).

Ainda de acordo com Nakagawa et al. (2014), uma arquitetura de referência é construída através de um ou mais modelos de referência, unificando regras de negócio, definições, padrões arquiteturais, estilos, boas práticas de desenvolvimento e até mesmo elementos de *hardware* e/ou *software* necessários à construção de arquiteturas específicas e concretas, que dizem respeito aos sistemas propriamente ditos no domínio em questão.

Então, um modelo de referência geralmente é a base utilizada para uma arquitetura de referência, ou que não é algo obrigatório, e a arquitetura de referência, fornece a estrutura e os elementos que deveriam ser utilizados para construir uma arquitetura de real de um sistema.

A Figura 6 ilustra esses relacionamentos entre modelos de referência, arquiteturas de referência e arquiteturas concretas, vale ressaltar que, apesar de ser desejável que arquiteturas de referência sejam construídas com base no vocabulário que os modelos de referência possuem, essa não é uma condição mandatória.

Figura 6 - Relacionamentos entre modelos de referência, arquiteturas de referência e arquiteturas concretas.



Fonte: Pires et al. (2015).

Pode-se dizer que o Sistema é o nível mais concreto de um projeto, e o Modelo de Referência é o nível mais abstrato, ou seja, na Arquitetura de Referência o Modelo de Referência é refinado, tornando-se menos abstrato e mais próximo do contexto do projeto. Já na Arquitetura Concreta, a Arquitetura de Referência, que foi refinada do Modelo de Referência, é especializada para que atenda

todos os requisitos do projeto, ou seja, deixa de ser uma arquitetura abstrata e passa a ser uma arquitetura concreta.

No próximo capítulo serão descritas as arquiteturas de referência de IoT estudadas durante o desenvolvimento deste trabalho, delimitando-se o escopo às principais e mais citadas na literatura.

3.1 Arquiteturas de Referência IoT

A fim de padronizar este segmento, a criação de uma arquitetura de referência ou um modelo de referência é muito importante para que no futuro estes dispositivos que denominam-se IoT possam estar realmente conectados uns com os outros, ou seja, que a interoperabilidade seja algo real e não utópico. Então todo o tempo gasto para padronizar e criar uma arquitetura de referência não são em vão, pois estas arquiteturas criam um caminho, um exemplo para ser seguido no desenvolvimento de tecnologias IoT, fator este que atualmente é cada vez mais importante devido a exponencial crescimento deste segmento.

No entanto, considerando a heterogeneidade de soluções que nasceram no IoT, a falta de padronização é algo frequente, o que muitas vezes permite a integração somente de dispositivos da mesma marca ou no mesmo fabricante, que é o detentor da tecnologia. Por fim, estes assuntos com relação a interoperabilidade podem ser resolvidos ou ao menos melhorados projetando-se arquiteturas de tecnologias IoT que sejam fundamentadas em uma arquitetura de referência.

De acordo com Khan et al. (2012), existem diversos modelos e arquiteturas de referência para IoT, cada grupo ou empresa descreve o seu, o que muitas vezes causa conflitos de ideias e torna a tarefa de padronização mais complexa, segundo este autor, existem algumas camadas que formam um modelo básico de arquitetura de referência como apresentado na Figura 7.

Figura 7 - Arquitetura de referência básica para IoT

Fonte: elaborado pelo autor com base em Khan et al. (2012).

A primeira camada é a de dispositivos, ou objetos inteligentes que pode ser considerada uma camada de coleta, representando os objetos físicos, que através de sensores ou outro tipo de tecnologia coletam e em alguns casos processam dados. Já na camada de Rede, é onde estão concentradas as tecnologias utilizadas para comunicação, bem como toda a questão de gerenciamento e distribuição de mensagens, ou seja, é uma camada onde o tráfego de dados é abstraído.

Por fim, a Camada de Aplicação é responsável por tornar os recursos disponíveis para serem usados, seja por um outro dispositivo ou um sistema informacional, por exemplo, existem dispositivos que podem ser conectados nos carros e disponibilizam dados além do que é apresentado no painel para o motorista, a interface que se comunica com a rede e mostra as informações processadas, faz parte da camada de aplicação.

No entanto, estão camadas são muito genéricas e não abrangem toda a complexidade presente no cenário de IoT, sendo necessário criar arquiteturas mais específicas. Com a crescente importância do tema, e a imaturidade das arquiteturas de referência de IoT, que são muito recentes tanto no meio acadêmico quanto na indústria, existem diversas iniciativas de padronização, tanto privadas quanto governamentais.

Embora existam diversas organizações que trabalham no desenvolvimento e no processo de padronização de IoT, nem todas elas possuem uma arquitetura definida, ou seja, ainda estão em processo de aprendizagem ou aprimoramento do tema, como é o caso do IEEE *(Institute of Electrical and Electronics Engineers*), OASIS (*Organization for the Advancement of Structured Information Standards*), NIST (*National Institute of Standards and Technology*), IETF (*Internet Engineering Task Force*) e o ETSI (*European Telecommunications Standards Institute*), que possuem algum artigos e documentos contendo seus estudos e contribuições para a temática.

Então, para este trabalho, o estudo foi focado em 3 arquiteturas de referências que foram construídas nos últimos anos, são elas: a IoT-A (*Internet of Things Architecture*), um projeto de padronização da União Européia (IoT-A, 2013), a ITU-T, é um projeto de padronização do Reino Unido, mais especificamente da ITU (*International Telecommunication Union*) (ITU-T, 2012), e por fim o WoT (*Web of Things*), projeto de padronização do World Wide Web Consortium (W3C) (W3C, 2017b), apresentadas nas seções 3.1.1, 3.1.2 e 3.1.3 na sua respectiva ordem.

De acordo com os autores dessas arquiteturas, elas ainda estão em desenvolvimento e podem ser atualizadas com o decorrer dos anos. A escolha destas arquiteturas para este trabalho foi fundamentada pelo fato de as mesmas estarem presentes em grande parte dos trabalhos estudados durante a pesquisa bibliográfica, bem como, são propostas pelos principais órgãos de padronização mundial nesse setor.

3.1.1 IoT-A (*Internet of Things – Architecture*)

Esta seção descreve a arquitetura de referência IoT-A (2013) proposta pela *Lighthouse* da União Européia (UE), bem como as funções propostas para as camadas.

Lighthouse é um projeto realizado pela UE, em que de setembro de 2014 a agosto de 2017, um consórcio de sete parceiros (Espanha, Noruega, Grécia, França, Chipre e Áustria) países com diversos pesquisadores e conhecimento em diferentes áreas, foram responsáveis pela implementação do projeto.

Este projeto surgiu, pois, os países europeus estavam prevendo uma escassez de mão-de-obra, podendo prejudicar o crescimento econômico da UE, então criaram um projeto para garantir orientação e aprendizagem, aumentando a empregabilidade em todos os Estados membros. Muitos países europeus criaram pontos de acesso público que integram diferentes serviços de aprendizagem, tais como validação de aprendizagem prévia e orientação profissional, e oferecem programas de aprendizado adaptados a alunos individuais.

IoT-A é um projeto dessa *Lighthouse* da UE com o objetivo de estudo e padronização da Internet das Coisas, o projeto foi concluído em 2013, após de mais de 3 anos de trabalho. Durante esse período foram desenvolvidos uma série de conceitos e tecnologias que são utilizadas em diversos países ao redor do mundo.

Em particular, para este trabalho foram pesquisados os fundamentos de IoT no que diz respeito a uma "Arquitetura de Referência" para projetos IoT. Este padrão permite que qualquer projeto de IoT tenha uma base, ou seja, tenha uma referência sobre qual estrutura seguir bem como tecnologias entre outras definições que são abordadas na IoT-A. O objetivo técnico do IoT-A é criar os fundamentos da arquitetura de Internet das Coisas, na qual permite uma integração das tecnologias IoT heterogêneas em uma arquitetura coerente e sua utilização em outros sistemas da Internet do Futuro.

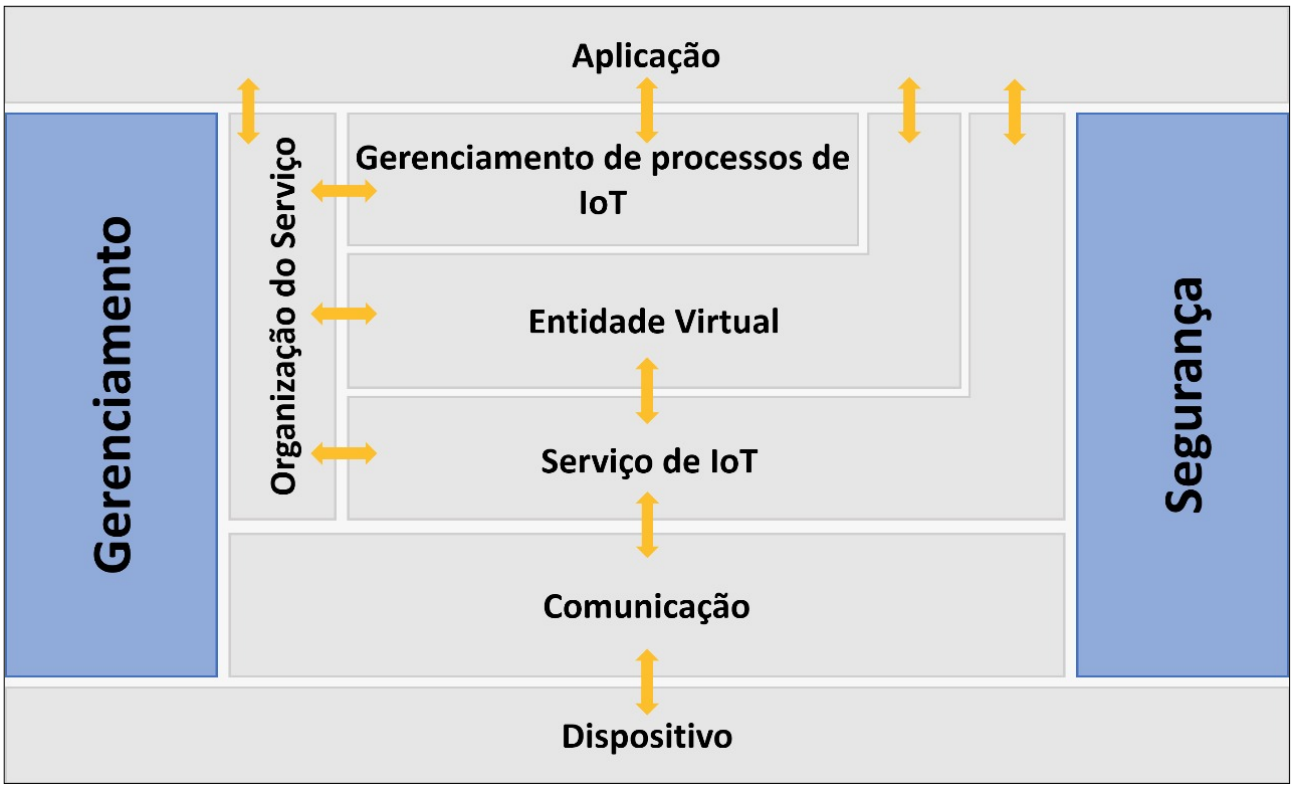
Este projeto disponibiliza diversos documentos que foram criados durante o desenvolvimento das tecnologias e definição dos padrões criados, sendo que estes estão divididos em sete grupos de documentos, o primeiro refere-se ao estado da arte e a arquitetura de referência, o segundo grupo refere-se à integração de serviços de IoT ao mundo real, o terceiro grupo refere-se ao detalhamento técnico da comunicação dos dispositivos, o quarto grupo traz o detalhamento sobre infraestrutura, os grupos 5 e 6 trazem definições e processos para o desenvolvimento de tecnologias IoT, e por fim o grupo 7 reúne casos de uso e validações de implementações de tecnologias IoT.

No entanto como este trabalho possui foco na arquitetura de referência e mais especificamente na camada de segurança, foi utilizada a última versão da arquitetura, presente no documento D1.5, que possui a versão 3.0 da arquitetura de referência.

A arquitetura de referência está descrita em três modelos (IoT-A, 2013, p.47), o Modelo de Domínio, Modelo de Informação e Modelo Funcional, no entanto as camadas da arquitetura de referência estão definidas dentro do Modelo Funcional que será descrito a seguir. A arquitetura funcional deste padrão de IoT é representada na Figura 8, na qual "Aplicações", "Entidade Virtual", "Serviço IoT" e "Dispositivo" são os elementos principais desta arquitetura, porém, no que diz respeito à diversidade de tecnologias de comunicação que o modelo precisará suportar exige a necessidade de um grupo funcional de "Comunicação", bem como sobre a possibilidade de criar serviços e aplicativos no topo do IoT que são cobertos pelos grupos funcionais "Gerenciamento de processos de IoT" e "Organização de serviços".

No entanto somente estes grupos não seriam suficientes para cobrir todas as necessidades do modelo, então para atender a preocupação sobre segurança e privacidade do IoT, foi identificada a necessidade de um grupo funcional transversal de "Segurança", bem como o grupo funcional transversal "Gerenciamento", que é necessário para promover a gestão e interação entre os diferentes grupos de funcionalidades.

Figura 8 - Modelo Funcional IoT-A



Fonte: IoT-A (2013, p.69), tradução do autor.

Este modelo funcional contém sete grupos de funcionalidades horizontais (Dispositivo, Comunicação, Serviços de IoT, Entidade Virtual, Gerenciamento de processos de IoT, Organização de Serviço e Aplicação) complementados por dois grupos de funcionalidades verticais

(Gerenciamento e Segurança). Esses grupos verticais disponibilizam funcionalidades que são utilizadas por cada um dos grupos horizontais, ou seja, as tecnologias e regras que estão contidas nos grupos verticais não só serão aplicadas aos próprios grupos, mas também aplicam-se aos grupos horizontais. Por exemplo, se algum destes grupos funcionais tivesse uma funcionalidade que não passa pelas regras de segurança, seria possível um acesso não autorizado à determinada função.

Em seguida, serão descritas as relações entre os grupos funcionais de acordo com a tradução realizada pelo autor deste trabalho. De acordo com a Figura 8, os fluxos de comunicação são descritos por setas bidirecionais, no entanto os grupos funcionais verticais não possuem uma relação explícita com os demais grupos.

Os grupos funcionais de Aplicação e Dispositivo não são descritos no texto original pois suas propriedades são muito genéricas e segundo o IoT-A não agregaria valor algum descrevendo essas relações dentro do modelo.

- **Gerenciamento de processos de IoT**

O grupo de Gerenciamento de Processos de IoT, abreviado como BPM (*Business Process Management*), refere-se à integração de sistemas tradicionais de gerenciamento de processos com a arquitetura de IoT-A. O objetivo deste grupo é fornecer além de conceitos, *interfaces* funcionais, necessárias para facilitar o uso comercial de dispositivos conectados no mundo IoT, de modo que as empresas possam efetivamente utilizar os subsistemas IoT aderindo aos padrões comuns e às melhores práticas, evitando assim despesas desnecessárias e outros custos de soluções isoladas e proprietárias.

No projeto IoT-A, este grupo funcional é descrito detalhadamente no segundo grupo de documentos disponível no site oficial, grupo de lida com a integração de serviços para o mundo real e para uma internet do futuro. No entanto podemos dizer que este grupo traz extensões ao padrão da indústria que incluem aspectos específicos de processos ao IoT, como a confiabilidade ou a responsabilidade dos dados dos sensores, fornecendo informações sobre entidades virtuais ou as capacidades de processamento necessários dos dispositivos que hospedam determinados recursos relevantes para o mundo real.

Neste sentido as aplicações que interagem com o BPM têm uma comunicação transparente e protegida com as de camadas mais baixas do modelo funcional, o que reduz consideravelmente os custos de integração e contribui para uma maior adoção de sistemas IoT baseados no padrão IoT-A.

Uma importante característica deste grupo de gerenciamento de processos de IoT é a sua proximidade com sistemas empresariais, no que diz respeito a objetos e processos de negócios

combinados com o mundo do IoT. É neste grupo que todas as regras de negócio são definidas, ou seja, é aqui que são definidas as regras para os usuários, conforme descrito abaixo exemplos de regras:

- Permissão: o que pode ser feito? Por exemplo, um sistema de ventilação auto regulável pode ser iniciado por um sistema de controle central;
- Proibição: o que não deve ser feito? Por exemplo, o sistema de ventilação pode não ser desligado totalmente se a temperatura externa estiver acima de um valor pré-definido e se os humanos estiverem presentes no prédio;
- Obrigações: o sistema de controle central precisa economizar parâmetros ambientais registrados para cada sala em todo o edifício (temperatura, umidade, configurações de ventilação). Tais registros podem, por exemplo, ser exigidos pelas leis nacionais de saúde ocupacional.

Segundo os idealizadores da arquitetura, no que diz respeito à realização prática do gerenciamento de processos, essas diferentes políticas entrarão em jogo quando os respectivos processos de negócios forem modelados.

Além disso, o BPM está fortemente relacionado ao grupo de Organização de Serviços, tradução de *Service Organization* (SO) e resumindo, ele atua como uma camada de fachada para aplicativos que precisam integrar um sistema IoT compatível com IoT-A. As aplicações utilizam as ferramentas e as interfaces disponibilizadas pelo grupo ao mesmo tempo que faz uso das funcionalidades relacionadas com dispositivo sem a necessidade de lidar com as complexidades de um serviço IoT completo.

Então entende-se que o BPM fornece interfaces menos complexas para a arquitetura de IoT-A que as interfaces contidas no grupo funcional Entidade Virtual e no grupo SO que fazem parte de um nível de abstração menor e mais detalhado, portanto possuem uma interface mais complexa para operar projetos de IoT dentro dos padrões IoT-A. Portanto entende-se que o grupo BPM tem uma dependência do grupo SO, pois ele depende do serviço de organização para mapear as definições do processo abstrato das demais camadas para invocações de serviços mais concretas.

Resumidamente este grupo é o que muitas vezes se comunica com a Aplicação e essa por sua vez com o usuário, ou seja, este grupo facilita a camada de comunicação das aplicações com os outros grupos inseridos na arquitetura de referência, garantindo assim a padronização de requisições da aplicação, bem como de respostas para a aplicação.

- **Organização de serviços**

O grupo de Organização de Serviço, é responsável pela principal comunicação entre os grupos, pois este grupo é o responsável por orquestrar e compor os demais grupos funcionais em diversas camadas de abstração. Esse grupo possui três funções principais: Composição de Serviço, Orquestração de Serviço, e Coreografia de Serviço.

Composição de Serviço, é responsável por determinar serviços compostos por serviços IoT bem como outros serviços derivados de uma funcionalidade estendida, através de suporte à composição de serviços flexíveis e do aumento da qualidade da informação.

Orquestração de Serviço é responsável coordenar serviços de IoT de modo a atender as requisições dos usuários ou de outros grupos funcionais da arquitetura, caso necessário, esta função cria recursos temporário para armazenar resultados da Composição de Serviço.

Coreografia de Serviço é responsável por ser o mediador, aquele que trata a comunicação entre serviços. Quando um serviço está disponível, o mediador garante que um cliente ou requisitante encontre o serviço, e mesmo quando o serviço não está disponível este mediador notifica o requisitante quando o serviço estiver disponível.

Com essas três funções principais, conclui-se que este grupo funcional tem a finalidade de organizar as requisições feitas aos pelos outros grupos, bem como tornar essa tarefa mais simples para os demais grupos, ou seja, o nível de abstração na comunicação dos demais grupos é maior, pois eles não precisam se comunicar diretamente com os Serviços de IoT ou diretamente com os dispositivos.

- **Entidade Virtual**

No meio digital as Entidade Físicas (EF) são representadas por Entidades Virtuais (EV), no IoT, uma EV é associada apenas a uma EF, ou seja, é associada a EF que ela representa, no entanto, a mesma EF pode ser associada à diversas EV, mas esse tipo de abordagem não é muito comum.

A EV contém funções para interagir com os Serviços IoT, bem como funcionalidades para descobrir e procurar serviços que podem fornecer informações sobre EVs ou que permitem a interação com EVs. Ou seja, é de responsabilidade da EV fornecer o contexto para os Serviços IoT, na qual somente o dado retornado de um sensor pode parecer uma informação inútil caso não esteja associada a uma EV.

Então, EVs representam um determinado conjunto de propriedades de uma EF, ou seja, os dados das características de uma EF são fornecidos através de parâmetros digitais pelo Serviço IoT imediatamente após a leitura na EF, de contrapartida, funcionalidades da EF podem ser alteradas através da EV, ou seja, tudo que for feito na EV reflete na EF e tudo da EF reflete na EV.

- **Serviço IoT**

O grupo Serviço IoT contém os serviços de Internet das Coisas bem como funcionalidades para descoberta, busca e resolução de nomes dos serviços IoT, basicamente é composto por dois componentes, o componente de Serviços e o componente de Resolução de Serviço.

O componente de Serviços torna um recurso acessível para outras partes da arquitetura IoT, ou seja, pode ser usado para entregar ou recuperar dados dos recursos, controlar e configurar dispositivos. Além disso essas funções do Serviço IoT podem ser executadas de forma síncrona no caso de respostas de requisições, ou assincronamente, para notificações ou leituras previamente realizadas por um serviço.

O componente Resolução de Serviço basicamente disponibiliza as funções de descoberta, busca, resolução e gerenciamento de Serviços IoT, sendo a descoberta uma função utilizada na procura de um serviço sem conhecimento prévio, ou seja, é realizado por um identificador de serviço, a busca ou pesquisa, permite que o usuário acesse a descrição do serviço com o conhecimento prévio do identificador do serviço, a resolução é responsável por definir os identificadores do serviço, reduzindo a quantidade de informações para a comunicação, e por fim, o gerenciamento é responsável por inserir, alterar e excluir a descrição dos serviços.

Em linhas gerais este grupo funcional é responsável por relacionar a requisição de serviços com suas respectivas funções, ou seja, é responsável por direcionar e controlar o fluxo da comunicação, resolvendo nomes e devolvendo informações sobre os dispositivos.

- **Comunicação**

O grupo de Comunicação abstrai a diversidade dos esquemas de comunicação dos diversos dispositivos pertencentes a um sistema IoT, fornecendo uma interface comum para os demais grupos se comunicarem com os dispositivos. Este grupo fornece uma interface de comunicação em um nível de abstração mais alto, tornando simples o instanciamento e gerenciamento do fluxo informacional.

No grupo de Comunicação, são levados em consideração os seguintes aspectos: a partir das camadas superiores do modelo ISO/OSI, considera-se a representação de dados, informações de caminho de ponta a ponta, problemas de endereçamento, gerenciamento de rede e recursos específicos do dispositivo.

Este grupo ainda pode ser personalizado de acordo com os diferentes requisitos definidos no projeto IoT seguindo essa arquitetura. Por exemplo, com relação a integridade e a segurança podem ser explorados esquemas de assinatura e criptografia em várias camadas do modelo ISO/OSI, sobre a confiabilidade, ela pode ser alcançada por meio de reconhecimento da camada de *link* ou dos

esquemas de correção de erros ponto a ponto nas camadas superiores, a qualidade do serviço é alcançada através de técnicas de gerenciamento de filas, e por fim, a comunicação é realizada através da tradução de protocolos e de troca de contexto descritas para os dispositivos

O grupo de Comunicação possui três componentes principais, a Salto-a-Salto (*Hop-to-Hop*), que é a primeira camada de abstração, e está diretamente relacionada com a comunicação dos dispositivos físicos, permitindo o uso e a configuração de qualquer tecnologia da camada de enlace, transmitindo *frames* ou quadros da rede e dos dispositivos para este componente.

Rede, é o componente responsável pela comunicação entre redes através de identificadores (IDs) e localizadores (endereçamento), transmitindo pacotes das funções Salto-a-Salto e Fim-a-Fim para o próprio componente de rede. Além disso, este componente faz o roteamento, permitindo relacionar endereços de redes de diferentes tecnologias, através da tradução dos protocolos de rede.

Por fim o componente Fim-a-Fim (*End-to-End*) é responsável por toda a abstração de comunicação final, que envolve algumas características importantes, como confiabilidade, transporte, tradução e *proxies/gateways*. Esse componente faz a transmissão das mensagens entre o grupo Serviço IoT e o componente de Rede do grupo de Comunicação, para isso esse componente conta com *proxy* de mensagem, tradução de protocolos, *cache* e credenciais de segurança.

Para todos os componentes são observados os seguintes critérios com relação a transmissão de pacotes e quadros: confiabilidade, integridade, criptografia, endereçamento e controle de acesso, bem como a qualidade, observada na capacidade de gerenciar filas e configurar o tamanho e prioridades das filas de entrada e saída de pacotes.

- **Gestão**

O grupo de Gestão provê todas as funcionalidades que são necessárias para gerir um sistema IoT, esse grupo surge na necessidade de suprir alguns objetivos como redução de custos (energéticos ou financeiros), atender problemas inesperados, manipulação de falhas e flexibilidade.

Esse grupo gerencia a associação e as informações de acompanhamento de uma determinada entidade no sistema IoT, sendo que essa entidade pode ser um componente funciona dentro de um grupo, uma Entidade Virtual, um Serviço IoT, uma Aplicação, um Dispositivo. Para gerir todas essas informações e todos os demais grupos, esse grupo conta com cinco componentes: Configuração; Falha; Membro; Relatório; Estado.

  - Configuração é responsável por realizar a configuração inicial do sistema, como por exemplo coletar, rastrear alterações e armazenar as configurações dos demais componentes e dispositivos presentes no sistema.

- Falha é responsável por identificar, notificar, isolar, corrigir e registrar todas as falhas que ocorrerem no sistema de IoT.
- Membro é responsável pela gestão dos membros pertencentes ao sistema IoT, bem como pelas informações relevantes de qualquer entidade ou grupo do sistema.
- Relatório é responsável por tratar as informações recuperadas de todos os componentes dos grupos, possibilitando a construção de relatórios em geral.
- Estado é responsável por monitorar e fornecer os estados do sistema IoT. Além da informação sobre o estado atual de uma entidade ou grupo do sistema, este componente permite recuperar o estado do sistema através de um histórico e até mesmo prever o estado por um determinado tempo.

Este grupo é um dos principais integrantes da arquitetura IoT, pois, ele é o responsável por todo o gerenciamento do sistema dentro da arquitetura, pois ele permeia todas as camadas da arquitetura de referência.

- **Segurança**

O grupo Segurança é responsável por garantir a segurança e a privacidade dos sistemas compatíveis com IoT-A. Esse grupo é responsável pelo registro inicial de um cliente no sistema de forma segura, garantindo que somente clientes legítimos e já registrados possam acessar os serviços fornecidos pelo sistema IoT.

Ele também é responsável por proteger os parâmetros privados dos usuários, ou seja, garantindo o anonimato (fazendo com que a identidade do usuário permaneça confidencial quando ele acessa um recurso ou um serviço dentro da arquitetura) e "*unlinkability*" ou em português “não linkável” (garantir que o usuário não seja encontrado e que um possível invasor não seja capaz de estabelecer vínculos com o usuário), no entanto essas garantias de privacidade dependem do gerenciamento de identidade que for ajustado durante a implementação da arquitetura de referência.

Este grupo também é responsável por uma interação confiável e legítima entre pares que estão autorizados para interagir uns com os outros, que através de funções presentes dentro do grupo de Segurança, garantem a autorização, bem como validam o quanto determinado usuário ou cliente é confiável, utilizando um modelo de reputação.

Autenticação, Autorização, Confiança e Reputação, Gerenciamento de Identidade, e Troca de Chaves e Gerenciamento

Por fim, o grupo de Segurança permite comunicações seguras entre diversos nós gerenciando o estabelecimento de integridade e características de confidencialidade entre duas entidades que podem possuir ou não conhecimento inicial entre si.

3.1.2 ITU-T (*International Telecommunication Union - Telecommunication Standardization*)

Esta seção descreve o modelo de referência ITU-T (2012) proposto pela International Telecommunication Union (ITU), bem como suas funções propostas para as camadas.

ITU é a agência especializada em TIC (tecnologias da informação e comunicação) da ONU (Organização das Nações Unidas), com o intuito de padronizar e regulamentar ondas de rádio e telecomunicações internacionais. A ITU tem o objetivo de conectar todas as pessoas do mundo, independente de onde vivam ou de sua condição de vida, eles defendem o direito fundamental de todos para a comunicação.

Dentro do ITU existem grupos de estudo e um deles é o ITU-T, responsável pela padronização e normalização dos serviços de TIC, e um desses projetos de padronização é sobre IoT, e o projeto ficou conhecido pelo nome do grupo, ITU-T.

De acordo com a ITU-T (2012,p.2), a IoT é uma

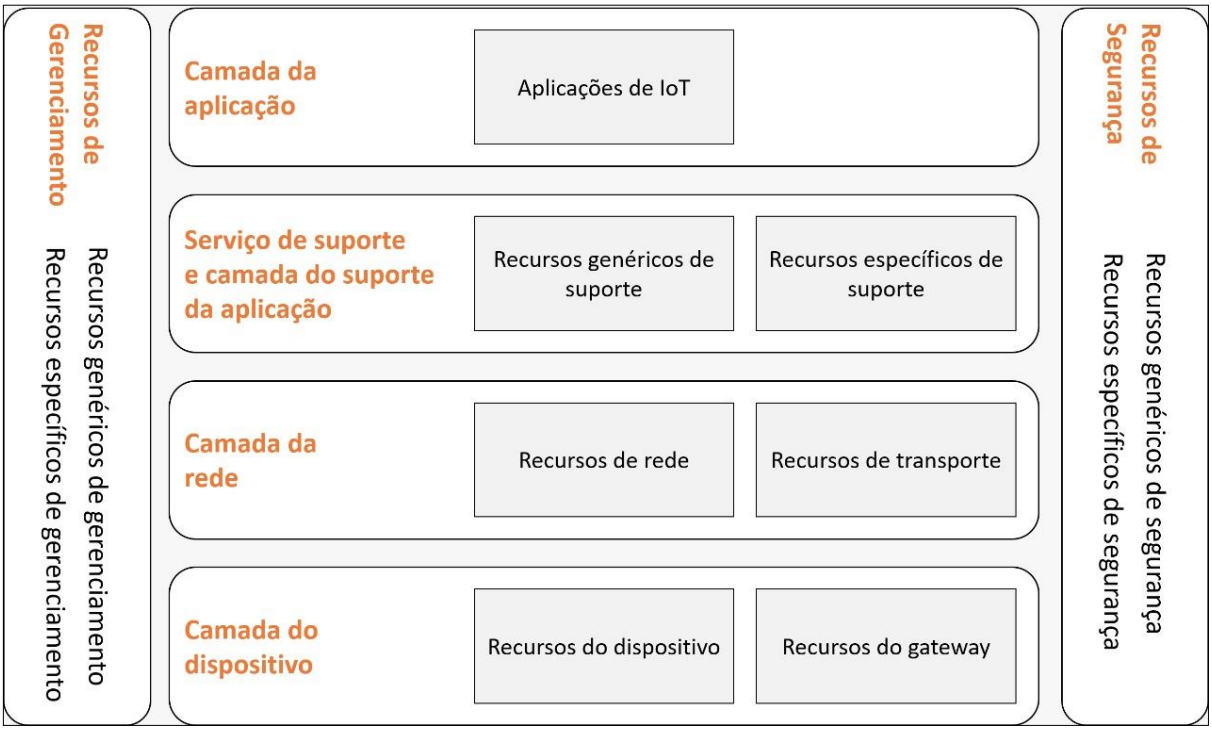
> [...] uma infra-estrutura global para a sociedade da informação, permitindo serviços avançados interligando (físicos e virtuais) coisas baseadas em Tecnologias de Comunicação e Informação (TIC) interoperáveis existentes e em constante evolução. (ITU-T, 2012, p.2)

A seguir é descrito o modelo de referência ITU-T, desenvolvido pelo ITU, com o intuito de padronizar a comunicação de dispositivos inseridos no universo de objetos conectados chamado IoT.

- **Modelo de referência ITU-T**

A Figura 9 mostra o modelo de referência IoT proposto pelo ITU, em que é composto por quatro camadas horizontais e duas camadas verticais na qual suas funções atendem todas as quatro camadas horizontais.

Figura 9 - Modelo de referência ITU-T



Fonte: ITU-T (2012), traduzido pelo autor.

- **Camada de aplicação**

Esta é a primeira camada, ela é responsável pela integração com os aplicativos ou sistemas IoT, disponibilizando uma camada de abstração mais alta, simples para ser utilizado pelos sistemas, facilitando a interoperabilidade dos aplicativos e sistemas.

- **Serviço de suporte e camada de suporte da aplicação**

Esta camada é responsável por fornecer os recursos necessários para as aplicações IoT, estes recursos consistem em diferentes tipos de funcionalidades, desde as mais básicas como coleta e armazenamento de dados, como atém mesmo funcionalidades mais específicas e customizadas da aplicação.

A camada de serviço de suporte e suporte a aplicação possui dois grupos de funcionalidades, funcionalidade de Recursos genéricos de suporte, responsável pelos recursos genéricos de suporte, como recursos comuns que podem ser usados por diferentes Aplicações IoT, por exemplo processamento e armazenamento de dados, e funcionalidade de Recursos Específicos de Suporte, que

é responsável pelos recursos de suporte mais específicos e particulares do sistemas IoT, consistem em agrupamentos de requisitos e podem ser criados mais de um grupo de Recursos Específicos de Suporte para diferentes tipos de aplicação ou sistema IoT.

- **Camada de rede**

Esta camada é responsável pela comunicação, ou seja, é responsável por interpretar e traduzir as mensagens enviadas e solicitadas, esta é uma das camadas mais importantes do modelo, pois é através dela que todos os dados transitam, portanto requer grande atenção com relação aos princípios de segurança.

Esta camada possui duas funcionalidades, a primeira é referente aos Recursos de rede, responsável por fornecer funções de controle de conectividade de rede, como acesso, transporte, gerenciamento móvel, autenticação, autorização e contabilidade (*Authentication, Authorization and Accounting* - AAA), e a funcionalidade de Recursos de transporte, responsável pelo fornecimento de conectividade para o transporte do serviço IoT e informações de dados específicos da aplicação, bem como o transporte de informações de controle e gerenciamento relacionadas ao IoT.

- **Camada do dispositivo**

A camada dos dispositivos é responsável pelas entidades físicas, ou seja, os próprios objetos conectados, que podem ser diversas coisas, desde sensores de temperatura até câmeras e muito mais. Esta camada possui dois grupos funcionais distintos:

  - Recursos do dispositivo é responsável mas não estão limitados à: Interação direta com a rede de comunicação, coletando e carregando informações diretamente (sem usar recurso de *gateway*) para a rede de comunicação e pode receber diretamente informações (por exemplo, comandos) da rede de comunicação; Interação indireta com a rede de comunicação, quando os próprios dispositivos são capazes de coletar e fazer o *upload* de informações diretamente para a rede de comunicação, ou seja, através de recursos de *gateway*; Rede *Ad-hoc*, quando os dispositivos podem ser capazes de construir redes de forma *Ad-hoc* em alguns cenários que precisam de escalabilidade aumentada e implantação rápida; e por fim, “*Sleeping*” e “*Waking-up*”, quando os recursos do dispositivo podem suportar mecanismos de "dormir" e "acordar" para economizar energia.
  - Recursos de *gateway* são responsáveis, mas não estão limitados à: Suporte a várias interfaces, quando na camada de dispositivo, os recursos de *gateway* suportam

dispositivos conectados através de diferentes tipos de tecnologias com fio ou sem fio; Conversão de protocolo, quando as comunicações na camada do dispositivo usam diferentes protocolos de camada de dispositivo e quando comunicações envolvendo camada de dispositivo e camada de rede usam protocolos diferentes.

- **Recursos de gerenciamento**

Os Recursos de gerenciamento ou camada de gerenciamento, é responsável por gerir as demais camadas, levando em consideração o gerenciamento de falhas, configurações, contabilidade, desempenho e segurança. Esta camada está dividida em dois grupos de funcionalidades, recursos genéricos de gerenciamento e recursos de gerenciamento específicos.

Os recursos genéricos de gerenciamento são: gerenciamento de dispositivos, como ativação remota de dispositivos e desativação, diagnóstico, atualização de *firmware* e/ou atualização de *software*, gerenciamento de *status* de funcionamento do dispositivo; gestão de topologia de rede local; gerenciamento de tráfego e congestionamento, como a detecção de condições de transbordamento de rede e a implementação de reserva de recursos para fluxos de dados críticos e/ou críticos para a vida.

As capacidades específicas de gerenciamento estão intimamente associadas aos requisitos específicos da aplicação, por exemplo, requisitos de monitoramento da linha de transmissão de energia da rede inteligente.

- **Recursos de segurança**

Os recursos de segurança ou camada de segurança é responsável pelo critérios e padrões de segurança de todas as camadas, no entanto não são definidos no documento apresentado pelo ITU. Existem dois grupos de funcionalidades de segurança de capacidades de segurança, recursos genéricos de segurança e recursos de segurança específicos.

As capacidades genéricas de segurança são independentes dos aplicativos e atuam: na camada de aplicação com autorização, autenticação, confidencialidade de dados do aplicativo e proteção de integridade, proteção de privacidade, auditoria de segurança e antivírus; na camada de rede com autorização, autenticação, uso de dados e confidencialidade de dados de sinalização e proteção de integridade de sinalização; na camada do dispositivo com autenticação, autorização, validação de integridade do dispositivo, controle de acesso, confidencialidade de dados e proteção de integridade.

Os recursos de segurança específicos estão intimamente associados aos requisitos específicos da aplicação, por exemplo, requisitos de segurança para pagamento móvel.

3.1.3 WoT (*Web of Things*)

O início da "*Web of Things*" (WoT) foi em 2010, em um *Workshop* Internacional anual sobre a *Web* das Coisas, com o objetivo de melhorar a interoperabilidade e a usabilidade na Internet das coisas (IoT). Vislumbrando o crescente interesse sobre o tema IoT, em 2015 o W3C criou um grupo de interesse para estudar e identificar tecnologias para uma recomendação de padronização. (W3C, 2017b)

O World Wide Web Consortium (W3C) é uma comunidade internacional com 458 membros, na qual membros, funcionários e usuários públicos trabalham em conjunto para desenvolver padrões da *Web*. A organização é dirigida pelo inventor da *Web* Tim Berners-Lee e CEO Jeffrey Jaffe, a missão do W3C é encaminhar a *Web* para todo o seu potencial. (W3C, 2017a)

O W3C foi fundado por Tim Berners-Lee em 1994, com o intuito de levar a *Web* para o uso máximo do seu potencial, através do desenvolvimento de protocolos e fóruns abertos, a evolução da *Web* aconteceu muito rapidamente nos últimos anos, na qual sistemas desenvolvidos seguindo esses padrões podem ser acessados no mundo todo, independente do meio ou da tecnologia utilizada.

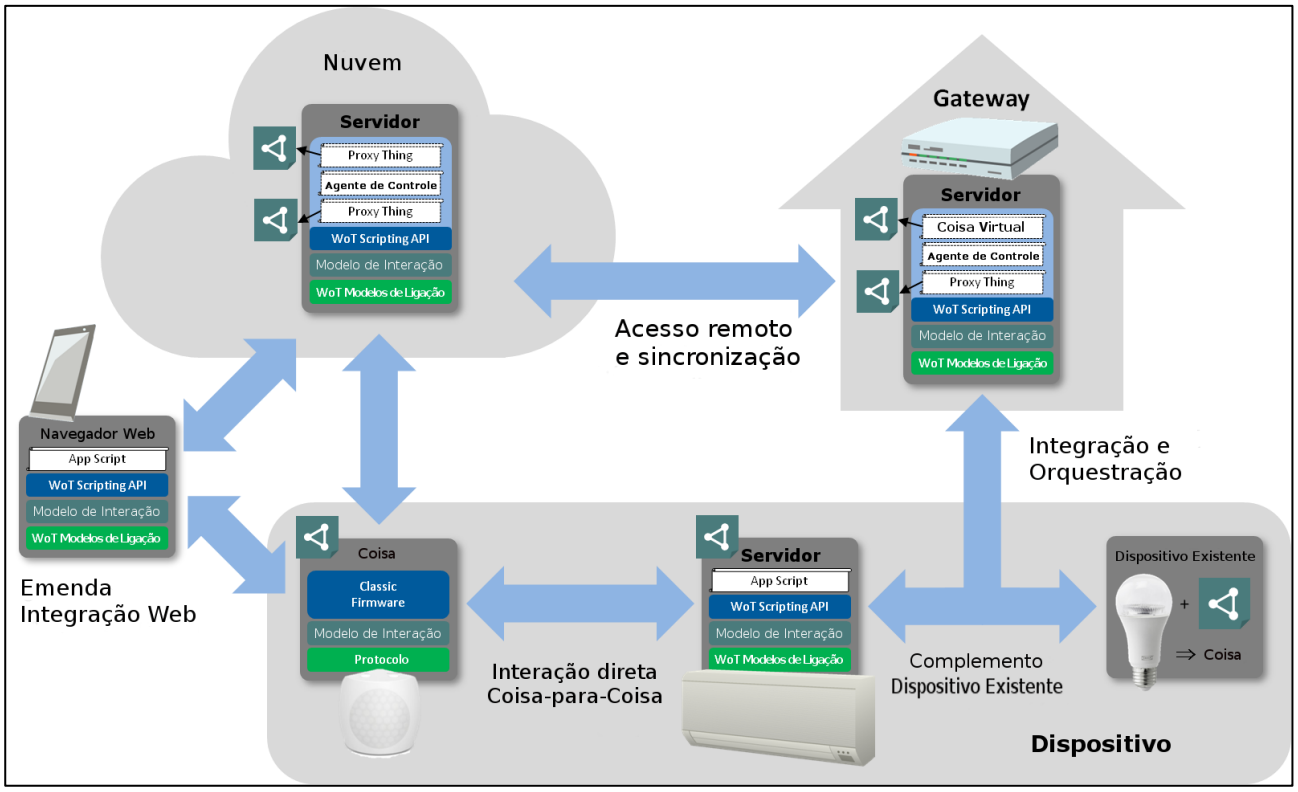
A WoT tem o objetivo de garantir a interoperabilidade em plataformas IoT e domínios de aplicativos e sistemas que fazem uso dessas tecnologias. Através da arquitetura de referência, o W3C fornece mecanismos para descrever formalmente as interfaces IoT permitindo que os dispositivos e serviços IoT se comuniquem entre si, independentemente da implementação e os protocolos de rede utilizados, além de fornecer uma forma padronizada de desenvolver soluções IoT.

- **Blocos de Construção WoT**

A criação desses blocos de construção é derivada de um estudo de caso de uso de dispositivos IoT em diferentes cenários, como *Smart Home, Smart Factory e Smart Car*, além de diversas formas de comunicação, como Dispositivos Controlados e comunicação *Thing-to-Thing* (Coisa-para-Coisa). Após estudar estes cenários foram levantados requisitos que deveriam ser atendidos por estes Blocos de Construção WoT, que são, Flexibilidade, Compatibilidade, e Segurança e Privacidade.

Com isso foi construído a Arquitetura Abstrata da WoT apresentada na Figura 10, na qual resume os casos estudados e os requisitos funcionais em blocos de construção WoT que serão a base para aplicações e sistemas IoT. Esses blocos se resumem em três níveis, nível do dispositivo, nível do *gateway* e nível da nuvem.

Figura 10 - Arquitetura Abstrata da WoT



Fonte: W3C (2017b), tradução do autor.

Essa figura traz os blocos conceituais dentro dos três níveis citados no parágrafo anterior, os blocos Coisa, Servidor e Navegador *Web* serão descritos com mais detalhes a seguir. No entanto, para compreender a comunicação entre esses blocos, primeiramente é necessário compreender a comunicação entre os níveis, por exemplo, como o dispositivo se comunica com a nuvem.

Um dispositivo pode estar conectado a um Servidor dentro de um ambiente local (nível do dispositivo) ou dentro de um *Gateway* (responsável pela integração e orquestração), o Servidor presente no nível local, na nuvem e no *Gateway* são praticamente iguais, com diferença no *Script* de Aplicação, pois em cada local o *script* é diferente, possuindo regras e comportamentos próprios de acordo com o nível em que Servidor está.

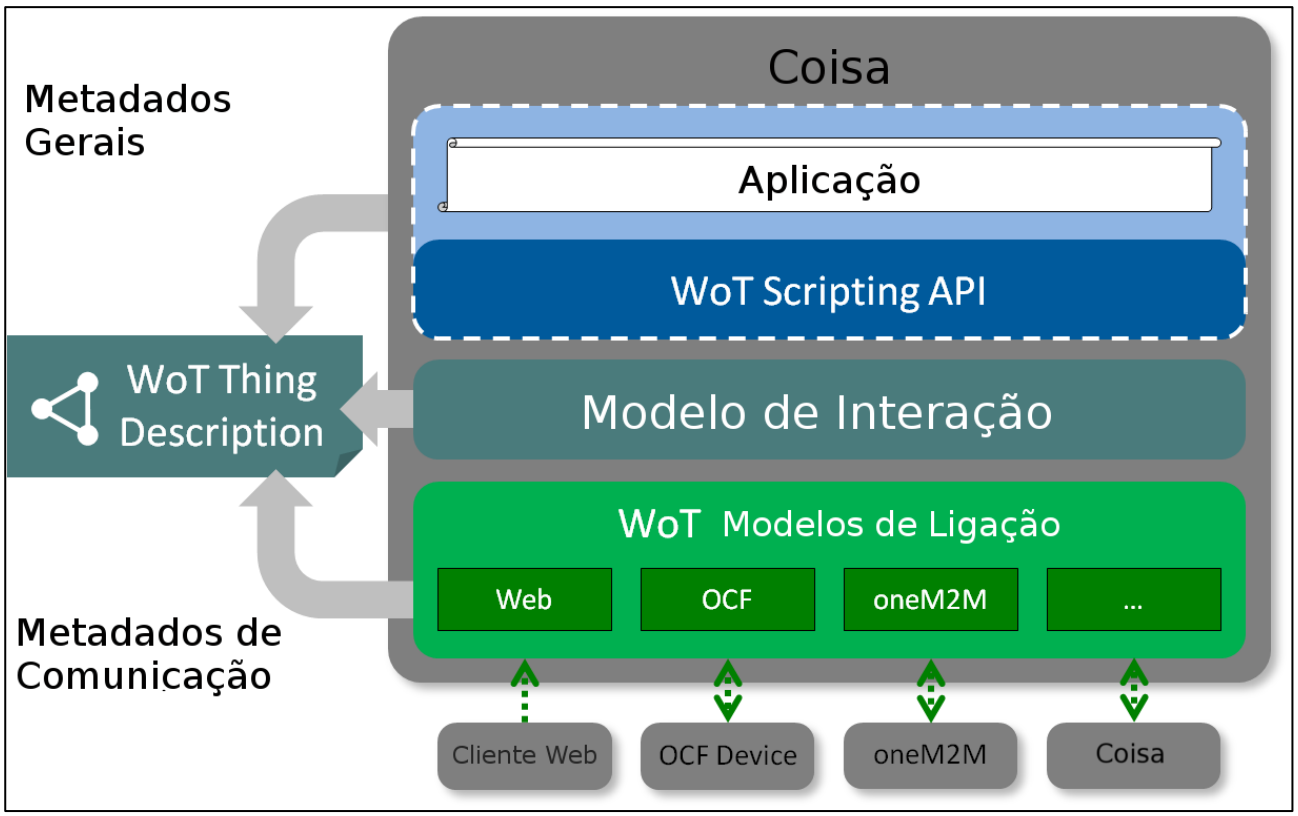
A Coisa presente dentro do nível do dispositivo é uma representação virtual do dispositivo, contendo todos os atributos, informações e protocolos necessários para a comunicação dos outros níveis com o Servidor local.

Fora do nível do dispositivo, temos o Gateway, que como informado seve para a orquestração e comunicação com o dispositivo, a Nuvem, que funciona como um servidor ou atuador global, e o Navegador Web, que funciona como uma ponte para do nível do dispositivo para Nuvem, através de uma aplicação.

- ***WoT Thing Architecture* - Arquitetura de Coisa**

De acordo com o W3C (2017b), Coisa é uma "abstração de uma entidade física ou virtual que precisa ser representada nas aplicações IoT". Esta entidade representada pode tanto ser algo físico, por exemplo, dispositivos eletrônicos e sensores, como algo lógico, por exemplo a localização de uma sala ou a cotação de uma moeda. A Figura 11 mostra com mais detalhes a arquitetura conceitual de uma Coisa, bem como a descrição de alguns itens dessa arquitetura.

Figura 11 - Arquitetura Conceitual de uma Coisa da WoT



Fonte: W3C (2017b), tradução do autor.

Esses blocos chamados de Coisa, podem fornecer uma API (*Application Protocol Interface*) padrão para interação baseada em interface WoT, essa API é formada por um grande conjunto de APIs da *Web*. Essa interface externa é diferente da comunicação interna chamada de "WoT *Scripting* API", pois esta camada de comunicação interna é opcional e pode variar de acordo com a aplicação ou sistema IoT.

No entanto não é obrigatório que essa Coisa forneça a interface WoT, por exemplo a Coisa pode conter apenas os metadados obrigatórios (WoT *Thing Description* - TD) informando sua descrição, o que para todas as Coisas é obrigatório informar na descrição que aquele objeto é uma "Coisa".

A Figura 11 mostra o padrão definido para “Coisas” no modelo WoT, na qual toda Coisa possui uma aplicação disponível com atributos e informações para serem consultados através de um Servidor, seja ele Local, Web ou na Nuvem.

- **WoT *Thing Description* (TD)**

Os TDs são dados estruturados que fornecem metadados gerais de uma Coisa, assim como metadados sobre as interações, modelo de dados, comunicação e mecanismos de segurança de uma Coisa, na qual, utilizam metadados específicos do domínio a qual pertence. No entanto, os vocabulários específicos do domínio estão fora do controle de padronização do W3C.

O TD facilita a interoperabilidade, pois com ele é possível fazer uma comunicação máquina-máquina, bem como desenvolvedores recuperarem dados necessários para acessar o dispositivo IoT.

- ***WoT Binding Templates* - Modelos de Ligação**

Um dos grandes desafios é permitir a interação do WoT com vasta quantidade de plataformas diferentes de IoT, e vale lembrar que muitas plataformas de dispositivos IoT não seguem nenhum padrão ou arquitetura de referência para o desenvolvimento, o que é um agravante quando fala-se de interoperabilidade. Para dispositivos IoT existe uma grande variedade de protocolos de comunicação, tendo em vista que para cada contexto é usado um protocolo diferente.

O WoT trata essa questão da variedade de plataformas incluindo metadados de comunicação, que explicam como interagir com as diferentes plataformas.

- ***WoT Scripting API***

O WoT *Scripting* API é um bloco de construção opcional que facilita o desenvolvimento de aplicações IoT, pois, permite criar um sistema de tempo de execução para as aplicações IoT, algo semelhante a um navegador da *Web*, visando melhorar a produtividade e reduzir os custos de integração.

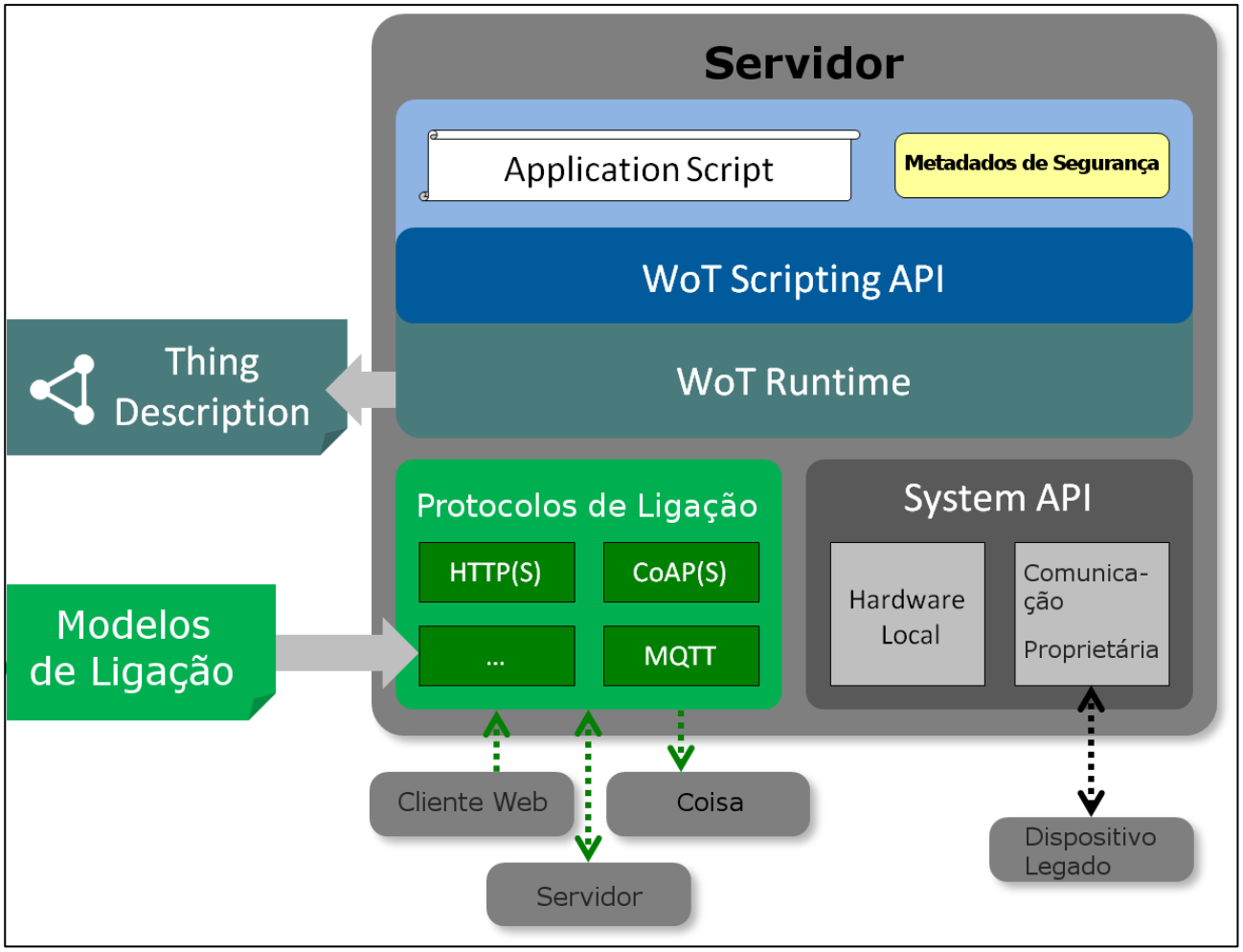
Além disso, essas APIs padronizadas permitem a portabilidade de uma maneira facilitada, pois são baseadas na abstração da Coisa e no TD, possuindo ainda três sub-APIs: a API WoT *Objects*, como ponto de entrada da API para descobrir, consumir e expor Coisas; a API *ConsumedThing Interface*, que funciona como um cliente, consumindo coisas através da rede ou localmente (por exemplo, *hardware* fisicamente conectado); e, por fim, a API *ExposedThing Interface*, que funciona como uma API de Servidor, utilizada para configurar e expor Coisas na rede.

- **WoT *Servient Architecture* - Arquitetura de Servidor**

O bloco chamado de Servidor é um bloco capaz de implementar blocos de Coisas, ou seja, um Servidor pode hospedar, expor e/ou consumir Coisas. Então, desta maneira os Servidores podem desempenhar as funções do Servidor e de Coisa.

A Figura 12 mostra detalhes da implementação do bloco do Servidor, bem como abaixo da figura serão detalhados alguns itens dessa arquitetura conceitual.

Figura 12 - Arquitetura Conceitual de um Servidor da WoT



Fonte: W3C (2017b), tradução do autor.

- ***Application Script***

Aplicações executadas em um Servidor geralmente são implementados através de *scripts*, por isso o nome "*Application Script*", os quais devem ser fornecidos juntamente com metadados de segurança, para definir o ambiente de execução, bem como a maneira com que os *scripts* devem ser isolados. Os metadados de segurança também precisam incluir material de chave ou certificados para autenticar as coisas que o *script* pode expor.

A camada WoT *Scripting* API é opcional na construção de bloco, podem existir implementações de Servidor em que as aplicações são nativas, neste caso, tanto a camada WoT *Scripting* API e a WoT *Runtime* não fazem parte do bloco.

- **WoT *Scripting* API**

Essa é a camada de API padrão de *scripts* WoT na qual é feito o contrato entre aplicativos e o sistema em tempo de execução do Servidor, que é chamado de WoT *Runtime*. A camada WoT *Scripting* API é equivalente a qualquer API da plataforma, portanto, deve haver mecanismos de segurança para evitar o acesso malicioso ao sistema.

- **WoT *Runtime***

O WoT *Runtime* é usado para interagir com a camada *Protocol Bindings* (protocolos de ligação) para acessar Coisas externas, ele também se comunica com a API do sistema para acessar informações locais e protocolos de comunicação proprietários da aplicação.

Hardware e dispositivos locais por trás dos protocolos de comunicação proprietários também podem ser representados como Coisas em tempo de execução, ou seja, eles também são acessados através da API do sistema.

O WoT *Runtime* também tem a função de gerar descrição para a Coisa, baseado nos metadados do "Servidor", metadados da aplicação e protocolos de ligação disponíveis.

- ***Protocol Bindings* - Protocolos de Ligação**

Os Protocolos de Ligação são implementações dos Modelos de Ligação descritos no bloco da Coisa. Eles são responsáveis por produzir mensagens e interagir com as Coisas na rede, baseado nas informações descritas no TD. Geralmente os Servidores possuem diversos protocolos de ligação, para garantir a comunicação e interação com diferente plataforma IoT.

Em diversos casos, em que os protocolos padrão são usados, as pilhas de protocolos genéricos são usadas para produzir mensagens específicas da plataforma, entretanto, em alguns casos, na qual nenhum aspecto pode ser compartilhado, o protocolo de ligação é comparado a um *driver* específico de uma plataforma específica, na qual somente é possível gerar mensagens para aquele protocolo específico.

- ***System* API**

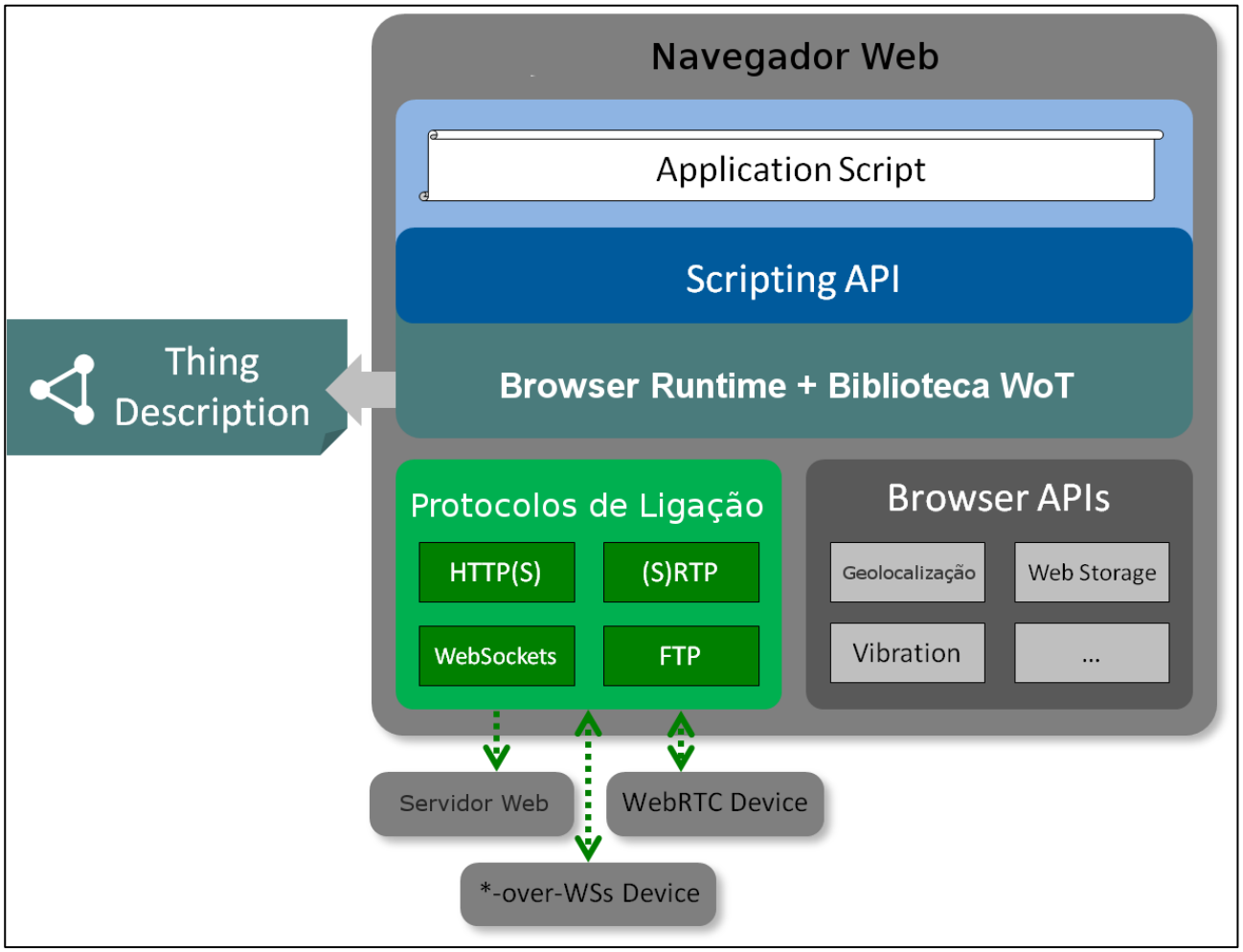
Uma Coisa pode acessar informações de um dispositivo físico ou serviços locais, como armazenamento e configurações locais, através de APIs proprietárias ou outros meios locais, e de acordo com o W3C (2017b), esse bloqueio está fora do alcance da padronização da WoT.

Não necessariamente um dispositivo precisa estar fisicamente ligado a um Servidor, ele pode estar externo ao Servidor, porém conectado através de protocolos proprietários. Nesse caso, WoT *Runtime* implementado pode acessar dispositivos com tais protocolos através das APIs proprietárias.

- **WoT no navegador da *Web***

De acordo com o autor do WoT, esta abstração do WoT no Navegador *Web* ainda é um esboço inicial e mais informações serão adicionados conforme o andamento da pesquisa. A Figura 13 representa de forma mais detalhada as camadas presentes na arquitetura conceitual de um Navegador Web.

Figura 13 - Arquitetura Conceitual de um Navegador Web da WoT



Fonte: W3C (2017b), tradução do autor.

As camadas deste bloco são muito parecidas com as camadas do bloco de Servidor, no entanto possui algumas diferenças, por exemplo, no Navegador da *Web* a aplicação é isolada em guias, usando a mesma política da origem, o que faz com que, nessa camada sejam dispensados os metadados de segurança. Ainda os *scripts* da aplicação fazem parte de uma página da *Web* e podem fornecer a visualização e interação do usuário.

A camada *Scripting* API precisa ser adicionada por uma biblioteca WoT, devendo ser carregada juntamente com os *scripts* do aplicativo pela página da *Web*. Junto com a biblioteca, são implementados os tratamentos e descrições do TD, bem como uma lista de códigos para usar as APIs do navegador. Ainda assim, outras características do WoT *Runtime* são fornecidas pelo sistema em tempo de execução através do *JavaScript* do navegador.

Outra característica marcante desse bloco do Navegador *Web* é que os protocolos de ligação são limitados aos protocolos implementados pelos navegadores da *Web*, mas as outras APIs do navegador são compatíveis à API do sistema dos Servidores e podem permitir o acesso às informações locais.

Concluídos os estudos sobre as três arquiteturas, IoT-A, ITU-T e WoT, nota-se a importância de ressaltar as questões de segurança e privacidade citadas nas mesmas, portanto, o próximo capítulo tem o intuito de explanar estes princípios relatados na documentação das arquiteturas estudadas.

4 Segurança e Privacidade

Após estudar e compreender as arquiteturas de referência para IoT, notou-se que algumas delas ainda são muito superficiais com relação às questões de privacidade e segurança, o que encaminhou para um capítulo de apresentação sobre este assunto.

Como seções deste capítulo serão apresentadas as premissas e requisitos de segurança e privacidade propostas pelas organizações e grupos de pesquisa estudados, bem como expor as soluções apresentadas pelas mesmas, além de trazer as questões de privacidade do CVD de Sant'Ana (2016).

4.1 Requisitos de Segurança e Privacidade

A WoT do W3C traz algumas premissas com relação a segurança e privacidade, e possui uma frente exclusiva de estudo, na qual as considerações apresentadas no documento da WoT ainda podem ser atualizadas e/ou reorganizadas.

A arquitetura funcional da WoT deve permitir o uso das melhores práticas em segurança e privacidade disponíveis na *Web* e nos dispositivos móveis. A WoT deve suportar ao menos o modelo de segurança e privacidade do sistema a qual está conectada. No entanto a segurança e a tolerância de risco desses sistemas podem variar e com isso os mecanismos de segurança do dispositivo WoT também pode variar.

Quando fala-se de segurança e privacidade, refere-se a coisas diferentes, na qual segurança quer dizer que o sistema deve preservar sua integridade e funcionalidades mesmo quando está sujeito a ataques, já privacidade, significa que o sistema deve preservar a confidencialidade das informações

pessoalmente identificáveis. Em linhas gerais a WoT não garante a segurança e a privacidade, no entanto ela deve suportar as melhores práticas disponíveis para assegurar estes princípios.

De acordo com o WoT, a segurança e a privacidade são especialmente importantes no domínio IoT, pois os dispositivos IoT precisam operar de forma autônoma e, em muitos casos, têm acesso a dados pessoais e/ou podem controlar os sistemas críticos de segurança, outro fator importante é proteger os sistemas IoT para que eles não possam ser usados para lançar ataques em outros sistemas informáticos.

O ITU-T, também faz algumas recomendações, no caso eles criaram uma lista de requisitos, na qual existem três itens referentes a segurança e privacidade, um deles chama Segurança, o outro Proteção de privacidade e por fim um chamado de Serviços relacionados com o corpo humano.

Em Segurança eles informam que no IoT, cada "coisa" está conectada, portanto estão sujeitas a ameaças de segurança, por exemplo ameaças de confidencialidade, autenticidade e integridade de dados e serviços, e esta situação é agravada devido à variedade de dispositivos e políticas de segurança existentes no contexto de IoT.

Para proteção de privacidade, eles ressaltam que muitas "coisas" tem seus proprietários e usuários, e os dados coletados pelas "coisas" podem conter informações privadas sobre seus proprietários ou usuários. O IoT deve oferecer suporte para a proteção da privacidade durante a transmissão, agregação, armazenamento, mineração e processamento dos dados, além disso, essa proteção não pode bloquear a autenticação da fonte dos dados.

Por fim, os serviços relacionados com o corpo humano devem ser altamente seguros e cada país possui leis diferentes com relação a este tipo de serviço, pois eles estão relacionados a captura, comunicação e processamento de dados relacionados a características humanas e comportamento dinâmico com ou sem intervenção humana.

No padrão IoT-A não foi citado nada com relação à requisitos de segurança e privacidade, no entanto esta arquitetura é a mais detalhada com relação à estes princípios. A seguir serão apresentadas as soluções dos três padrões com relação à segurança e privacidade.

4.2 Abordagens à Segurança e Privacidade

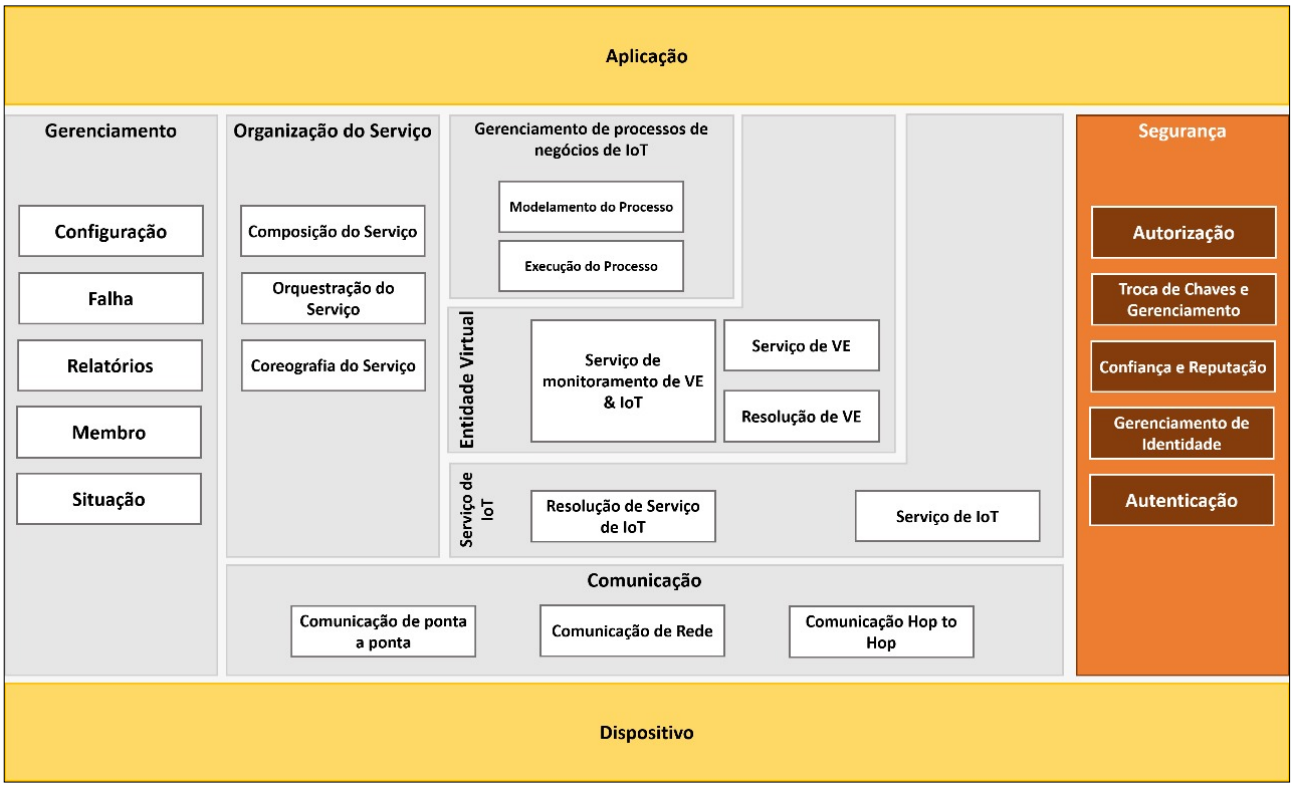
Assim como no subcapítulo anterior foram apresentados os requisitos e premissas de segurança e privacidade, neste subcapítulo são apresentadas as abordagens realizadas pelas arquiteturas com relação a estes tópicos.

- **IoT-A**

Na arquitetura de referência do IoT-A abordada no capítulo anterior as camadas são chamadas de grupos funcionais, e o grupo Segurança é composto por cinco componentes: Autorização, Troca

de Chaves e Gerenciamento, Confiança e Reputação, Gerenciamento de Identidade e Autenticação, observado na Figura 14.

Figura 14 - Detalhamento do grupo funcional de segurança.



Fonte: IoT-A (2013, p.107), tradução do autor.

O componente Autorização é responsável por gerenciar políticas e executar decisões de controle de acesso com base em políticas de controle de acesso. Essas decisões de controle de acesso podem ser chamadas sempre que o acesso a um recurso restrito é solicitado (ex.: requisição de acesso pelo componente Resolução de Serviço do grupo Serviços IoT). Esse componente possui duas funcionalidades, primeiro determinar se uma determinada ação é autorizada ou não, e em segundo, a função de gerenciar as políticas de acesso, inclusão, alteração e exclusão de políticas de acesso.

O componente de Troca de Chaves e Gerenciamento - *Key Exchange and Management* (KEM) é responsável por garantir comunicações seguras entre dois ou mais pares que utilizam a arquitetura IoT-A e não possuem conhecimento inicial ou cuja interoperabilidade não é garantida, garantindo integridade e confidencialidade. Este componente possui duas funções, distribuir chaves de forma segura entre dois nós e registrar capacidade de segurança em um nó ou *gateway* que deseja se registrar na rede para estabelecer uma conexão segura.

O componente de Confiança e Reputação é responsável por coletar as pontuações de reputação dos usuários e calcular os níveis de confiança do serviço, este componente basicamente possui duas funcionalidades, solicitar informações de reputação, executada quando uma entidade solicita

informações sobre a reputação de outra entidade, e fornecer informações sobre reputação, invocada em uma entidade para fornecer informações sobre reputação de outra entidade, como por exemplo pontuação e data.

O componente de Gerenciamento de Identidade é responsável pelas questões de privacidade, emitindo e gerenciando pseudônimos e informações aleatórias para que informações confiáveis possam operar anonimamente. Este componente possui apenas uma função, a de criar uma identidade fictícia junto com as devidas credenciais de segurança relacionadas para que os usuários possam usar durante a autenticação.

O componente Autenticação é responsável pela autenticação de usuários e serviços, verificando as credenciais fornecidas por um usuário e, se válido, ele retorna uma afirmação como resultado. No entanto, para um novo nó, são estabelecidos contextos seguros entre esse nó e as entidades em seu ambiente local. Este componente também possui duas funcionalidades, autenticar o usuário baseado nas credenciais fornecidas e verificar se as informações fornecidas por um determinado usuário são válidas ou não.

- **ITU-T**

No ITU-T as únicas recomendações quanto a segurança e privacidade são as mesmas que estão descritas no capítulo anterior, na qual, estão definidos dois tipos de capacidades de segurança, recursos genéricos de segurança e recursos de segurança específicos. As capacidades genéricas de segurança são independentes dos aplicativos e incluem:

  - na camada de aplicação: autorização, autenticação, confidencialidade de dados do aplicativo e proteção de integridade, proteção de privacidade, auditoria de segurança e antivírus;
  - na camada de rede: autorização, autenticação, uso de dados e confidencialidade de dados de sinalização e proteção de integridade de sinalização;
  - na camada do dispositivo: autenticação, autorização, validação de integridade do dispositivo, controle de acesso, confidencialidade de dados e proteção de integridade.

Para os recursos de segurança específicos estão intimamente associados aos requisitos específicos da aplicação, por exemplo, requisitos de segurança para pagamento móvel.

- **WoT**

A WoT não define explicitamente como são implementadas as funcionalidades de segurança e privacidade em seus modelos de blocos, no entanto em alguns momentos é citado que a segurança

pode ser aplicada em diferentes locais da comunicação e, portanto, cabe sua implementação em qualquer camada, e ainda eles citam que para WoT são consideradas as melhores práticas de segurança e privacidade na *Web*. Exemplos de tecnologia que podem ser utilizadas para garantir segurança e privacidade são TLS (*Transport Layer Security*), IPSec (IP *Security*), OAuth (*Authorization Framework*) e ACE (*Authentication and Authorization in Constrained Environments*).

Entretanto, traz considerações de segurança e privacidade que ainda estão em discussão e desenvolvimento, na qual devido à complexidade do assunto, eles consideram produzir um documento separado contendo uma discussão detalhada de considerações de segurança e privacidade, incluindo uma análise de risco, modelo de ameaça, mitigações recomendadas e referências apropriadas às melhores práticas.

Dentre as considerações de segurança, eles informam que a segurança é um problema transversal que precisa ser levado em consideração em todos os blocos de construção do WoT, e a WoT não define ou cria novos mecanismos de segurança, no entanto fornece diretrizes para aplicar as melhores práticas de segurança da *Web*, segurança de IoT e segurança de informações para considerações gerais de *software* e *hardware*.

Eles ainda recomendam que o TD (*Thing Description*) seja usado em conjunto com mecanismos de proteção de integridade e políticas de controle de acesso, na qual os usuários devem garantir que nenhuma informação confidencial seja incluída nos próprios TDs.

Bem como os modelos de ligação (WoT *Binding Templates*) devem garantir com que os mecanismos de segurança empregados pela plataforma IoT sejam aplicados corretamente nos blocos subjacentes. Ainda assim, as implementações de APIs devem possuir mecanismos para evitar o acesso malicioso ao sistema e isolar os *scripts* que tem acesso aos Servidores.

4.3 Privacidade no Ciclo de Vida dos Dados (CVD)

Conforme apresentado durante o referencial teórico, o Ciclo de Vida dos Dados (CVD) de Sant'Ana (2016) possui quatro fases: Coleta, Armazenamento, Recuperação e Descarte, e vale ressaltar que estas fases são cíclicas, ou seja, a qualquer momento pode-se voltar ao início do ciclo. São elas: Coleta, Armazenamento, Recuperação e Descarte.

No entanto, Sant'Ana (2016) detalha os objetivos que permeiam as camadas do CVD, então, como o escopo deste trabalho está delimitado na privacidade da coleta, somente este aspecto será avaliado, na qual o autor destaca que é

> necessário identificar, nas fontes utilizadas, aspectos que possam configurar quebra de privacidade de pessoas ou instituições relacionadas aos dados que estão sendo coletados o que poderia resultar em um passivo futuro a partir da base de dados obtida, comprometendo as próximas fases do ciclo de vida. (SANT'ANA, 2016, p.125)

Entre as reflexões realizadas por este autor, a principal questão que surge com relação à privacidade na coleta é “A coleta destes dados não proporciona risco de privacidade para os indivíduos ou entidades referenciadas por eles?” (SANT’ANA, 2016, p.119)

Terminados os estudos sobre as três arquiteturas, IoT-A, ITU-T e WoT no capítulo 3, bem como as questões de segurança e privacidade abordadas pelas mesmas neste capítulo, o próximo capítulo contém uma síntese feita pelo autor, na qual, baseado no estudo realizado previamente, o autor propõe um modelo de referência para IoT, em que, além de avaliar as questões sobre a privacidade e a segurança das informações no cenário de IoT, delimita os atores envolvidos e discute sobre suas responsabilidades no cenário IoT.

5 Proposta do Modelo de referência IoT

As arquiteturas de referência estudadas anteriormente serviram como base para fazer uma síntese e encontrar uma forma de compreender cada um dos itens envolvidos no cenário de IoT, no entanto existem alguns pontos que as arquiteturas estudadas não detalham ou não citam no cenário.

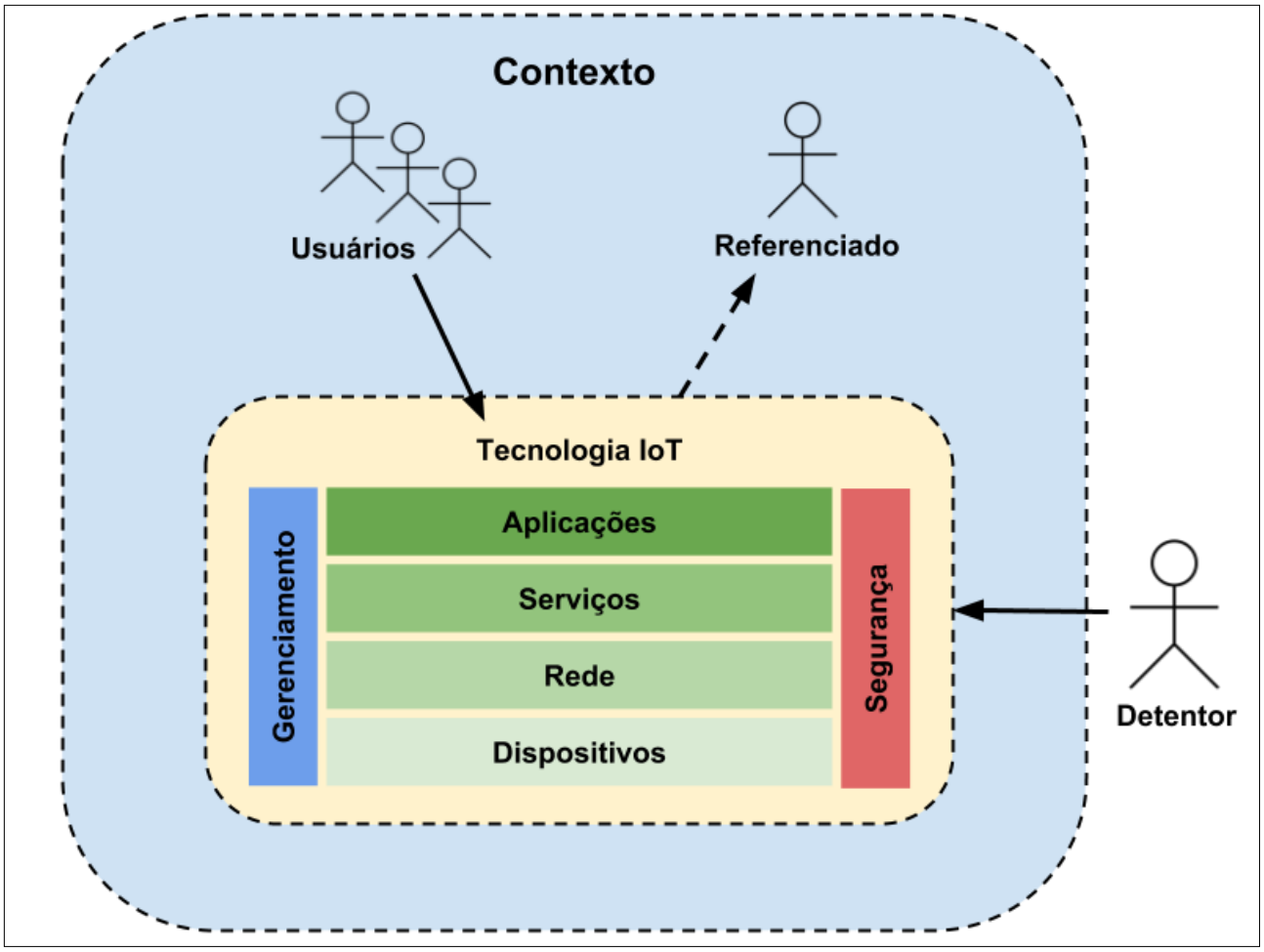
Com base em modelos e arquiteturas estudados, nota-se que existem dois atores, presentes no cenário de diversas tecnologias, que são ignorados ou não recebem a devida atenção, são o “Referenciado” e o “Detentor”, atores que serão explicados um pouco mais adiante no subcapítulo 5.1.

Estes atores são de vital importância para o ciclo de dados e informações contidas no cenário informacional, pois, estão nas extremidades do modelo de referência, ou seja, seus deveres e responsabilidades transpassam sobre o modelo, chegando ao usuário e na sociedade como um todo.

5.1 Modelo proposto

Conforme citado na introdução do capítulo, com base em modelos e arquiteturas de referência IoT estudados, foi construído um modelo de referência de IoT com os seguintes grupos no cenário de IoT: Contexto; Tecnologia IoT; Usuários; Referenciado; Detentor. Estes grupos estão relacionados conforme observa-se na Figura 15.

Figura 15 - Modelo de referência de IoT proposto



Fonte: elaborado pelo autor.

Inspirado pelas arquiteturas estudadas, IoT-A, ITU-T e WoT, entendeu-se como necessário fazer um novo desenho sintetizando as ideias e somando com as reflexões do próprio autor deste trabalho, em que vislumbra-se um cenário na qual determinada solução ou tecnologia baseada nos princípios de IoT está inserida em um determinado Contexto, onde existem os Usuários (humanos ou não) que irão usufruir da tecnologia, o Referenciado (humano ou não) que é o "alvo" de determinada tecnologia, podendo este, ser até mesmo o próprio Usuário, em um cenário que a tecnologia coleta dados do próprio Usuário, neste caso o Usuário é o Referenciado, e a própria Tecnologia IoT, que é composta das camadas horizontais de Aplicação, Serviços, Rede, Dispositivos, e as camadas verticais de Gerenciamento e de Segurança que abrangem as quatro camadas horizontais.

Além disso, em uma camada externa ao contexto, existe o Detentor da tecnologia, sendo este governamental, do setor privado ou até mesmo uma solução particular de uma pessoa física. O detentor, tem ou deveria ter o papel moral de responsável pelos dados coletados e tratados pele Tecnologia IoT desenvolvida por ele, ou seja, o Detentor, é o ator que deve proporcionar segurança e

privacidade para os Usuários e para os Referenciados dentro e fora do contexto em que a sua tecnologia está inserida.

Vale ressaltar o fluxo desenhado na Figura 15, em que o Detentor com a seta até a Tecnologia tem posse da mesma, portanto tem posse dos dados que trafegam pela mesma, os Usuário com seta transpassando a extremidade da Tecnologia, faz uso da mesma, ou seja, tem acesso às camadas de Aplicações disponibilizadas pela Tecnologia, já o Referenciado, com seta tracejada saindo da Tecnologia, é o "alvo" da coleta de dados, e muitas vezes pode ser insciente desta coleta, como ocorre com câmeras de segurança e outros tipos de dispositivos que coletam informações pessoais sem o conhecimento e muito menos o consentimento do Referenciado.

Para esclarecer este modelo de referência, cada um dos itens será descrito mais detalhadamente abaixo:

- **Contexto**

O contexto nada mais é do que o ambiente na qual o Usuário, a Tecnologia IoT e o Referenciado estão inseridos. Este ambiente pode ser um ambiente físico ou virtual, em que no caso de ambientes físicos podemos citar ambiente públicos, privados, de uso comum ou particular de pessoas ou objetos como carros, robôs, animais, etc., no entanto para ambientes virtuais, podemos citar sites, jogos de realidade aumentada, redes sociais, entre outros ambientes na qual pessoas ou objetos podem estar inseridos.

O contexto é a base para esta arquitetura, pois através do contexto delimita-se o cenário em que a tecnologia estará inserida, bem como as variáveis que poderão ser coletadas, ou seja, não pode-se por exemplo coletar dados de radiação solar dentro de um ambiente fechado.

Além disso o contexto está diretamente relacionado com o Referenciado, pois o mesmo faz parte do contexto, ou seja, é o objeto ou pessoa "alvo" da coleta de dados do Dispositivo pertencente à Tecnologia IoT, dados estes que serão utilizados ou apenas visualizados pelos Usuários.

- **Usuários**

Os Usuários são os atores que deveriam ser os atores finais dentro do Contexto, atores estes que visualizam ou utilizam a representação dos dados feita pela Tecnologia IoT. Entretanto, como muitas vezes os Usuários não são os Detentores da tecnologia, ou seja, a Tecnologia não foi desenvolvida pelo Usuário, os dados coletados podem não ter como destino final a visualização e uso do Usuário, mas sim do Detentor da tecnologia.

No entanto usuários não são apenas humanos, podem também ser objetos ou sistemas informacionais, que utilizam os dados fornecidos pela Tecnologia IoT, como é o caso de *smart houses*

por exemplo, que utilizam dados de dispositivos para executar determinada ação como controle de iluminação, temperatura, umidade, etc.

Em um outro cenário, pode-se vislumbrar os Usuários que são os próprios Referenciados, ou seja, o próprio usuário é o "alvo" da coleta, e isso não prende-se apenas em humanos coletando dados sobre eles mesmos em sistemas inteligentes de saúde por exemplo, mas também à objetos e sistemas que podem medir e fazer uso de suas informações para tomar determinada decisão, como seria o caso de um semáforo inteligente por exemplo, que de acordo com o fluxo de veículos e ligado a uma rede inteligente de semáforos, poderia ajustar seu próprio intervalo para fazer com que o transito transcorra de maneira mais fluida.

Vale ressaltar que os Usuários possuem grande responsabilidade nos quesitos de segurança da Tecnologia, pois devem se atentar às recomendações de segurança do Detentor da tecnologia. Além disso, existem recomendações com relação à proteção através de senhas, como por exemplo, definir senhas com alto grau de complexidade e trocá-las periodicamente para evitar possíveis quebra de senha por um atacante externo, não compartilhar senhas com outras pessoas, não utilizar senhas padrão como "123456" ou "admin", entre outras dicas que são importantes para manter a segurança da Tecnologia utilizada.

- **Referenciado**

O Referenciado por sua vez, conforme dito anteriormente é o "alvo" da coleta de dados e pode tanto ser um humano, como um objeto, ambiente ou sistema informacional. Quando fala-se de Segurança, dentro das camadas da ARC, refere-se à segurança destes dados coletados, não somente à segurança, mas também à privacidade, integridade, confiabilidade, características dos dados que devem ser preservadas visando não expor dados sensíveis do Referenciado.

Este ator, muitas vezes, quando ele não é o próprio Usuário, não tem conhecimento prévio de que suas informações estão sendo coletadas, ou seja, o Referenciado é um "alvo" inconsciente, ou insciente, de uma coleta de dados, tornando suas informações vulneráveis dentro de um sistema informacional encapsulado em um dispositivo IoT.

Quando o Referenciado é o próprio Usuário, essa questão de "alvo" inconsciente é menos frequente, mas ainda pode ocorrer, pois diversos usuários sequer leem os termos de uso de qualquer que seja a Tecnologia, concordando muitas vezes que suas informações sejam coletadas e usados pelo detentor da tecnologia, como é o caso de aplicativos como Waze, Google *Maps*, assistentes virtuais como a Siri, Cortana, Alexa, que coletam dados do Usuário para benefício mutuo, ou seja, o usuário faz uso da tecnologia a seu favor e o detentor recebe o histórico de uso, os dados coletados e/ou inseridos pelo usuário.

- **Detentor**

Com relação ao detentor da Tecnologia IoT, este pode ser uma empresa governamental, do setor privado ou até mesmo uma pessoa física que tenha desenvolvido determinada tecnologia IoT. No entanto, o papel do detentor é vital neste cenário, pois ele é o responsável por garantir que todos os princípios da ARC sejam atendidos, bem como preservar os dados e identidade do Referenciado.

Além disso, o Detentor é responsável pela tecnologia desenvolvida, bem como os dados coletados e/ou processados pela tecnologia IoT, ou seja, todos os dados e informações que trafegam pela tecnologia desenvolvida pelo Detentor é de sua responsabilidade e o mesmo deve garantir que os princípios de segurança e privacidade sejam atendidos, pois, caso ocorra um ataque e sua tecnologia seja invadida, os dados e informações devem estar anonimizados e protegidos para que a identidade e outras informações sigilosas do Usuário e do Referenciado sejam preservadas.

Outro fator importante, relacionado ao Detentor da tecnologia, é o uso dos dados e informações coletados pelos dispositivos IoT, se o Detentor faz uso destes dados e informações que pertencem aos Usuários e/ou Referenciados, isso deve ser informado e o Usuário deve autorizar esse uso, tornando essa ação de coleta e uso dos dados consciente para o Usuário.

- **Tecnologia IoT**

A Tecnologia IoT é o corpo principal do modelo de referência, é nela que todas as regras estão definidas, ou seja, é na Tecnologia IoT que está configurado quais variáveis irão ser coletadas daquele Contexto, quem será o Referenciado, qual a periodicidade da coleta, entre outros parâmetros que podem ser definidos de acordo com a solução ou tecnologia implementada pelo Detentor.

No entanto, no que diz respeito à implementação, existem algumas recomendações com relação a padronização, que no futuro facilitaria a interoperabilidade de dados. De acordo com os padrões estudados a padronização é feita seguindo uma Arquitetura de Referência de Camadas (ARC) como observa-se na Figura 16, em que estão presentes as camadas horizontais de Aplicação, Serviço, Rede e Dispositivos, e ainda duas camadas verticais, Gerenciamento e Segurança, camadas essas que estão relacionadas com todas as camadas horizontais.

Figura 16 - Arquitetura de referência proposta para a Tecnologia IoT

Fonte: elaborado pelo autor.

Os usuários fazem uso da Tecnologia IoT através de uma camada de abstração disponibilizada pela Aplicação, ou seja, o usuário não tem ou pelo menos não deveria ter acesso direto às camadas inferiores da ARC. Segue abaixo uma breve descrição das camadas da ARC:

- **Aplicações**

A camada de aplicação é a camada responsável por abstrair as informações disponibilizadas pelas camadas abaixo, no entanto para esta camada é importante que os aspectos de segurança e privacidade sejam mantidos, pois esta é a porta de entrada para invasores, portanto é um dos pontos mais vulneráveis da arquitetura. Além disso, essa camada é responsável por facilitar a interoperabilidade das aplicações ou sistemas IoT.

- **Serviços**

A camada de serviços é responsável por realizar as funções designadas pela camada de aplicação, bem como o monitoramento dos eventos, processamento e armazenamento de dados coletados de sensores e outros dispositivos. Esta camada ainda pode se comunicar com outras aplicações de outros dispositivos IoT, através da camada inferior na qual as requisições são endereçadas e traduzidas.

- **Rede**

É a camada responsável pelo transporte e comunicação das camadas superiores com os dispositivos e outras aplicações IoT. Esta camada integra os diferentes dispositivos na rede e faz a comunicação dos Serviços com os Dispositivos.

- **Dispositivos**

Dispositivos são a camada de percepção, ou a camada que gera dados para alimentar as aplicações. Esses dispositivos podem ser físicos como sensores, celulares, etc., ou lógicos, como valores de moedas, horários de máquina, entre outras informações que não tem origem de uma leitura do meio físico.

- **Gerenciamento**

É responsável pelo orquestramento das camadas, bem como realizar o acompanhamento de falhas e outras complicações que podem ocorrer nas outras camadas.

- **Segurança**

É responsável por garantir a implementação de aspectos de segurança e privacidade em todas as camadas da arquitetura de referência. Nesta camada, que transpassa as camadas horizontais da arquitetura, estão presentes funções como Autenticação, Autorização, Confiança e Reputação, Gerenciamento de Identidade e Troca de Chaves por exemplo. A maneira como são implementadas e quais serão as funções implementadas, são de responsabilidade do desenvolvedor ou Detentor da Tecnologia.

Então, como resultado, no subcapítulo a seguir pretende-se expor os aspectos de segurança e privacidade relacionados a camada de Segurança da arquitetura proposta na Tecnologia IoT, bem como relacionar aos atores do modelo sugerido pelo autor no início do capítulo, refletindo sobre a questão sobre privacidade na coleta de dados.

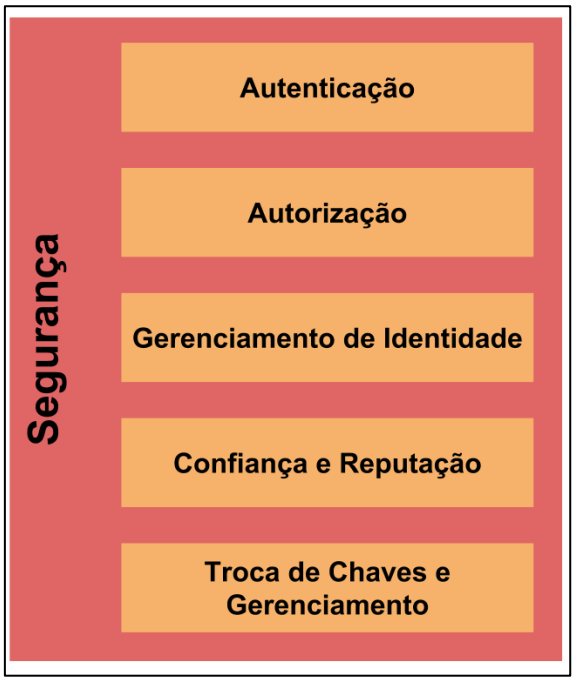
5.2 Segurança e Privacidade no Modelo Proposto

No início do capítulo, foi sugerido pelo autor um modelo de referência de IoT, na qual possui os seguintes grupos inseridos no cenário IoT: Contexto, Tecnologia IoT, Usuários, Referenciado e Detentor. Estes itens envolvidos estão relacionados conforme observa-se na Figura 15.

No entanto a descrição de segurança está um tanto quanto vaga, pois está descrito que a camada de Segurança é responsável por garantir a implementação dos aspectos de segurança e privacidade em todas as camadas da arquitetura de referência.

Durante o estudo realizado neste trabalho o autor considera como relevantes as funções de segurança descritas na arquitetura IoT-A, na qual são consideradas as funções de: Autenticação, Autorização, Confiança e Reputação, Gerenciamento de Identidade, e Troca de Chaves e Gerenciamento, como pode ser observado na Figura 17

Figura 17 - Funções da Camada de Segurança de IoT



Fonte: elaborado pelo autor com base em IoT-A (2013).

Tendo em vista que a camada de segurança permeia todas as demais camadas, acredita-se que para cada função, existem tecnologias que permitam a implementação das mesmas em todas as camadas da arquitetura de referência. No entanto, nem todas as funções são necessárias nas camadas, ou seja, não é obrigatório o uso de todas essas funções em todas as camadas, assim como funções podem e devem ser usadas paralelamente garantindo um maior nível de segurança.

Como o foco do trabalho não é descrever tecnologias, mas sim conceitos e funções para futuras implementações no cenário de IoT, segue abaixo uma breve descrição das funções citadas na Figura 17:

- **Autenticação**: é responsável por validar as credenciais do usuário ou cliente requisitante, validando se todos os atributos definidos na implementação são atendidos pela credencial do requisitante.
- **Autorização**: é responsável pelo controle de acesso de usuários ou clientes a determinadas funcionalidades ou camadas da tecnologia IoT, bem como as políticas de acesso de cada usuário ou cliente (leitura, inserção, alteração ou exclusão);
- **Confiança e Reputação**: é responsável por calcular a reputação de determinado usuário ou serviço baseado nos pontos de reputação e *feedback* de outras entidades;
- **Gerenciamento de Identidade**: é responsável por atribuir apelidos ou pseudônimos às entidades, garantindo que dados e informações trafeguem anonimamente;

- **Troca de Chaves e Gerenciamento**: é responsável pela distribuição de chaves de forma segura, ou seja, é responsável por garantir uma comunicação segura entre pares ou nós de chaves conhecidas.

Nota-se que as funções citadas anteriormente dizem respeito somente a dois atores, os Usuário e o Detentor, na qual, estes atores possuem algumas responsabilidades para garantir com que as funções de segurança descritas anteriormente sejam eficazes para proteger os dados e informações presentes no cenário e disponibilizadas pela Tecnologia IoT.

Cabe ao Detentor a responsabilidade de implementar todas as funções necessárias para garantir a segurança e a privacidade dos Usuários e do Referenciado a qual os dados são coletados, bem como orientar e alertar os mesmos sobre os riscos caso a Tecnologia seja invadida ou exposta à um invasor malicioso.

Para os Usuários, cabe a responsabilidade de seguir as orientações disponibilizadas pelo Detentor da Tecnologia, bem como seguir boas práticas de segurança da informação presentes em sistemas informacionais, como utilizar senhas longas e com alto nível de complexidades de caracteres, trocar sua senha periodicamente, não compartilhar senha com outros usuários, entre outras práticas que são importantes para sua segurança.

No entanto, apesar de estas funções fazerem referência somente as responsabilidades dos Usuários e do Detentor, é implícito que as mesmas existem para proteger os dados e informações presentes na Tecnologia, ou seja, para proteger os dados coletados do Referenciado, ciente ou insciente da coleta.

O Referenciado por sua vez, deve atentar-se e tomar conhecimento sobre a coleta de dados que é realizada pela Tecnologia, pois muitas vezes, a coleta é notificada ao Referenciado, porém o mesmo ignora o texto e simplesmente concorda com a coleta.

Este fato pode ser exemplificado e é muito frequente no cotidiano dos usuários de *smartphones*, na qual utilizando um aplicativo, o Usuário concorda com os termos de uso do mesmo, sem ler ou tomar conhecimento de quais dados o aplicativo está coletando ou utilizando de seu *smartphone*, então, este Usuário passa a ser o Referenciado naquele contexto, e seus dados são coletados com sua autorização, porém sem o seu conhecimento devido ao concordar com os termos de uso sem ler o mesmo.

Outro exemplo interessante são as câmeras de vídeo, que muitas vezes são instaladas em locais estratégicos e os Referenciados não possuem conhecimento que estão sendo monitorados, ou seja, são inscientes naquele cenário, e dados como comportamento, expressão facial, calor do corpo no caso de câmeras termais, estrutura corporal, entre outros dados que podem ser extraídos através dos

diferentes tipos de câmeras existentes, são coletados e utilizados por sistemas computacionais sem que os Referenciados tenham conhecimento ou consentimento sobre os dados coletados.

Nesse sentido, conforme proposto, pretende-se refletir sobre o assunto com base na seguinte questão: “A coleta destes dados não proporciona risco de privacidade para os indivíduos ou entidades referenciadas por eles?” (SANT’ANA, 2016, p.119)

Conforme observa-se na Figura 15, o Referenciado é o “alvo” da coleta de dados, sendo ele humano ou não, no entanto, não são somente informações do Referenciado que trafegam dentro da tecnologia IoT, pois os Usuários também fornecem informações, ou credenciais, para que seja permitido o acesso, ou seja, além de proteger os dados coletados pelos Dispositivos, é necessário proteger os dados fornecidos pelos usuários.

A responsabilidade de proteger estes dados é designada ao Detentor da Tecnologia IoT, portanto, cabe a ele o desenvolvimento das funções necessárias para garantir a privacidade e segurança dos dados tanto dos objetos referenciados quanto dos usuários ou clientes que fazem uso da tecnologia, bem como instruir e informar o Usuário sobre as melhores práticas de segurança para que a Tecnologia que está sendo usada não seja invadida por Usuários maliciosos.

Além disso, é de suma importância que caso ocorra uma invasão, ou quebra de segurança, os dados e informações estejam anonimizados, ou seja, o Detentor da tecnologia deve implementar funções de segurança para não permitir com que seja possível construir uma ligação do dado ou informação capturado com o seu respectivo dono.

Considerando a questão, durante a coleta, o dispositivo não deveria ter conhecimento sobre o usuário ou entidade requisitante, pois, conforme descrito no capítulo anterior, os usuários fazem uso da Tecnologia IoT através de uma camada de abstração disponibilizada pela Aplicação, ou seja, o usuário não tem ou pelo menos não deveria ter acesso direto às camadas inferiores da ARC, bem como os dados devem ser protegidos através das funções presentes na camada de segurança da ARC.

6 Considerações Finais

Como considerações finais, este trabalho teve um resultado satisfatório com relação aos objetivos propostos, tendo em vista que ao longo do trabalho os objetivos específicos foram sendo atendidos, desde o panorama histórico, a criação do modelo de referência e a associação dos aspectos de privacidade de IoT com o CVD.

Com relação a busca por padrões de IoT, nota-se um grande déficit de iniciativas nacionais de padronização IoT, apesar de recentemente o governo brasileiro financiar uma pesquisa através do BNDES (Banco Nacional do Desenvolvimento), na qual será construído um Plano Nacional da Internet das Coisas, em que estão sendo pesquisadas todas as ações de outros países ao redor do

mundo, visando compreender este cenário caótico que é o da Internet das Coisas para assim criar diretrizes sobre desenvolvimento, padronização e segurança dos dispositivos conectados pertencentes a este cenário.

Sobre os padrões analisados, observa-se que os padrões mais avançados em termos de padronização e diretrizes de desenvolvimento são os projetos IoT-A da União Europeia e o projeto WoT do W3C, pois estes dois padrões apresentam diretrizes mais detalhadas sobre o processo de desenvolvimento bem como uma descrição clara sobre o cenário onde estão inseridos.

Com base nos padrões estudados e visando atingir o objetivo geral do trabalho, foi proposto um modelo de referência na qual são adicionados três atores no cenário, os Usuários, o Referenciado e o Detentor, atores estes que são de vital importância para o fluxo informacional presente no cenário de IoT, e se faz de grande relevância que tenha-se conhecimento destes papéis dentro do cenário, bem como suas responsabilidades descritas no desenvolvimento do trabalho.

Sobre as responsabilidades dos atores citados no modelo de referência proposto, chama-se a atenção para a responsabilidade social dos mesmos, pois, por se tratar de dispositivos IoT, que estão presentes no cotidiano das pessoas, é de interesse da sociedade tomar conhecimento sobre seus dados, bem como como estes dados estão sendo coletados por estes dispositivos dentro de nossas casas, na rua, em nosso ambiente de trabalho, etc.

O Detentor da tecnologia é fator chave desta pesquisa, pois este é o responsável pela segurança e privacidade dos dados que trafegam através do dispositivo desenvolvido por ele, no entanto, muitas vezes o Detentor da tecnologia não se responsabiliza por uma invasão ou perda de dados de sua tecnologia, causando desconforto e até mesmo danos morais e financeiros para os Usuários e ou Referenciados.

Relacionando os aspectos de segurança e privacidade presentes nos modelos de referência de IoT com o objetivo de privacidade na fase da coleta do CVD, é feita uma reflexão acerca da seguinte pergunta: “A coleta destes dados não proporciona risco de privacidade para os indivíduos ou entidades referenciadas por eles?” (SANT’ANA, 2016, p.119)

Na qual, durante a coleta, o dispositivo não deveria ter conhecimento sobre o usuário ou entidade requisitante, pois, conforme descrito no capítulo anterior, os usuários fazem uso da Tecnologia IoT através de uma camada de abstração disponibilizada pela Aplicação, ou seja, o usuário não tem ou pelo menos não deveria ter acesso direto a camadas inferiores da ARC, bem como os dados devem ser protegidos e anonimizados através das funções presentes na camada de segurança da ARC.

No entanto, este trabalho possui um viés social, chamando a atenção sobre as responsabilidades dos atores presentes no cenário e não um viés técnico sobre a implementação das funções de segurança citadas na arquitetura de referência, o que abre a possibilidade para trabalhos futuros de construir diretrizes sobre quando e onde utilizar as funções de segurança e privacidade citadas no trabalho, afim de melhor orientar possíveis implementações utilizando este modelo de referência, no entanto, por tratar-se de um trabalho conceitual, não é foco do trabalho, nem de trabalhos futuros impor ferramentas ou métodos de desenvolvimento para aplicações IoT.

As reflexões abordadas durante o desenvolvimento deste trabalho, chamam a atenção para trabalhos futuros em diferentes áreas, como por exemplo Ciência da Computação, Segurança da Informação e Ciência da Informação, em que podem ser desenvolvidos novos conceitos e estudos que tendem a contribuir para o cenário de IoT, tendo em vista que esta é uma temática ampla e recente, que ainda demanda muita pesquisa para um aprofundamento em suas vertentes como por exemplo segurança e privacidade de dados.

Conclui-se que por tratar-se de um tema amplo, IoT demanda muitas pesquisas no futuro e a Ciência da Informação pode contribuir com essa temática de diferentes formas relacionadas à informação e à sociedade, trazendo um viés conceitual e aplicado, fazendo uma ponte da tecnologia com a sociedade, levantando preocupações sobre os dados e informações coletados por estes dispositivos a todo momento e em qualquer lugar, bem como discussões sobre a consciência dessa coleta de dados na sociedade.

Referências

AFFONSO, E. P.; SANT'ANA, R. C. G. PRESERVAÇÃO DA PRIVACIDADE NO ACESSO A DADOS POR MEIO DO MODELO K-ANONIMATO. **Ponto de Acesso**, v. 11, n. 1, p. 20-41, 2017. Disponível em: <https://rigs.ufba.br/index.php/revistaici/article/view/13754>. Acesso em: 10 out. 2017.

AL-FUQAHA, A., GUIZANI, M., MOHAMMADI, M., ALEDHARI, M., and AYYASH, M. Internet of things: A survey on enabling technologies, protocols, and applications. Communications Surveys & Tutorials, 2015 - IEEE, 17(4):2347–2376.

ANGELOV, S., GREFEN, P., GREEFHORST, D. (2009) "A classification of software reference architectures: Analyzing their success and effectiveness". Proceedings of the 2009 Joint Working IEEE/IFIP Conference on Software Architecture & European Conference on Software Architecture. USA, IEEE, pp. 141-150.

ASHTON, K. That 'Internet of Things' thing. Publicano no **RFID Journal**, 2009. Disponível em: <http://www.rfidjournal.com/article/view/4986>. Acesso em: 13 jul. 2017.

ATZORI, L; IERA, A; MORABITO, G. The Internet of Things: A survey. **Computer Networks**, [s.l.], v. 54, n. 15, p.2787-2805, out. 2010. Elsevier BV. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1389128610001568?via%3Dihub>. Acesso em: 15 set. 2017.

BBC. Hacker invade babá eletrônica e grita palavrões para criança de 2 anos. 2013. Disponível em: <http://www.bbc.com/portuguese/noticias/2013/08/130813_babaeletronica_hacer_pai>. Acesso em: 01 out. 2017.

BORKO, H. Information Science: What is it? American Documentation, v.19, n.1, p.3-5, Jan. 1968.

BROCK, L. The Electronic Product Code (EPC) – A naming Scheme for Physical Objects. 2001. Disponível em: <http://autoid.mit.edu/whitepapers/MIT-AUTOID-WH-002.PDF>. Acesso em: 5 jul. 2017.

BUCKLAND, M.K. Information as thing. **Journal of the American Society for Information Science (1986-1998)**, v. 42, n. 5, p. 351, 1991. Disponível em: <https://search.proquest.com/openview/47f25783aa7caf6dbafdddfca1b8ce97/1?pq-origsite=gscholar&cbl=41136>. Acesso em: 5 jul. 2016.

CAPURRO, R. Epistemologia e Ciência da Informação. In: **V ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO**, Belo Horizonte, 10 de novembro de 2003. Disponível em: <http://www.capurro.de/enancib_p.htm>. Acesso em: 10 ago. 2017.

CASTELLS, M. A Galáxia da Internet: reflexões sobre a Internet, negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

CERP IoT - INTERNET OF THINGS EUROPEAN RESEARCH CLUSTER. Internet of Things: Strategic Reserach Roadmap, 2009. <http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf>. Acesso em: 5 jul. 2017.

CISCO. Internet of Things, 2011. Disponível em: <http://www.slideshare.net/CiscoIBSG/internet-of-things-8470978>. Acesso em: 30 jun. 2011.

DUTRA, M. L.; SANT'ANA, R. C. G.; MACEDO, D. D. J. Sublimação de dados: dos objetos físicos às nuvens. In: **ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO**, 17., 2016, Salvador. Anais… Salvador: UFBA, 2016. Disponível em: <http://www.ufpb.br/evento/lti/ocs/index.php/enancib2016/enancib2016/paper/viewFile/3906/256>. Acesso em: 20 set. 2017.

ESTADÃO. Por que Mark Zuckerberg usa fita adesiva na câmera do notebook?. 2016. Disponível em: <http://link.estadao.com.br/noticias/cultura-digital,por-que-mark-zuckerberg-usa-fita-adesiva-na-webcam-do-notebook,10000061108>. Acesso em: 21 out. 2017.

EVANS, D. A Internet das Coisas. **San José: Cisco IBSG**, 2011. Disponível em: <https://www.cisco.com/c/dam/global/pt_br/assets/executives/pdf/internet_of_things_iot_ibsg_0411final.pdf>. Acesso em: 26 jan. 2018.

FUNG, B. C. M.; WANG, K.; FU, A.W.; YU, P. S. Introduction to Privacy-Preserving Data Publishing. Concepts and Techniques. Chapman &Hall/CRC – Data Mining and Knowledge Discovery Series, 2010.

GARTNER, I. Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor. **STAMFORD, Conn.**, 2015. Disponível em: <http://www.gartner.com/newsroom/id/3114217>. Acesso em: 20 ago. 2017.

GERSHENFELD, N. When things Start to Think. Henry Holt and Company: Nova Iorque, 1999.

GREENBERG, A. THE REAPER IOT BOTNET HAS ALREADY INFECTED A MILLION NETWORKS. **Wired**. 2017. Disponível em: <https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/?mbid=nl_102117_daily_list1_p2>. Acesso em: 21 out. 2017.

GREENFIELD, A. Everyware: the Dawning Age of Ubiquitous Computing. San Francisco: **New Riders Publishing**, 2006.

HAWKINS, D.T. Information science abstracts: tracking the literature of information science. Part 1: definition and map. **Journal of the American Society for Information Science and Technology**, v. 52, p. 44-54. 2001. Disponível em: <http://web.simmons.edu/~benoit/infosci/hawkins.pdf>. Acesso em: 13 jul. 2016.

IEEE, The Institute, "Special Report: The Internet of Things.". 2014. Disponível em: <http://theinstitute.ieee.org/static/special-report-the-internet-of-things>. Acesso em: 7 ago. 2017.

IERC. European Research Cluster on the Internet of Things. 2012. Disponível em: <http://www.internet-of-things-research.eu/>. Acesso em: 3 set. 2017.

IoT-A. Internet of Things – Architecture IoT-A, Deliverable D1.5 – Final architectural reference model for the IoT v3.0. 2013. Disponível em: <http://www.meet-iot.eu/deliverables-IOTA/D1_5.pdf>. Acesso em: 10 jun. 2017.

ITU-T. ITU-T Y.2060: Overview of the Internet of things. Jun. 2012. Disponível em: <http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559>. Acesso em: 20 jul. 2017.

ITU - INTERNATIONAL TELECOMMUNICATION UNION. ITU Internet Reports 2005: The Internet of Things. Geneva, 2005. Disponível em: <http://www.itu.int/osg/spu/publications/internetofthings/>. Acesso em: 05 jul. 2017.

KHAN, R., KHAN, S. U., ZAHEER, R., and KHAN, S. (2012). Future internet: the internet of things architecture, possible applications and key challenges. In **Frontiers of Information Technology** (FIT), 2012 10th International Conference on, pages 257–260. IEEE. Disponível em: <http://pure.qub.ac.uk/portal/files/81384964/PID2566391.pdf>. Acesso em: 12 ago. 2017.

KRANENBURG, R.; ANZELMO, E.; BASSI, A.; CAPRIO, D.; DODSON, S.; RATTO, M. The Internet of Things. **1st Berlin Symposium on the Internet and Society**. Outubro de 2011. Disponível em: <http://xindanwei.com/wp-content/uploads/2012/06/The-Internet-of-Things.pdf>. Acesso em: 26 mar. 2017.

LACERDA, F. Arquitetura da Informação Pervasiva: projetos de ecossistemas de informação na Internet das Coisas. Brasília: **Universidade de Brasília**, 2015. 226 fl. Tese de Doutorado. Disponível em: <http://repositorio.unb.br/handle/10482/19646>. Acesso em: 25 mar. 2017.

LACERDA, F.; LIMA-MARQUES, M. Da necessidade de princípios de Arquitetura da Informação para a Internet das Coisas. **Perspect. ciênc. inf.**, Belo Horizonte, v. 20, n. 2, p. 158-171, June 2015 . Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1413-99362015000200158&lng=en&nrm=iso>. Acesso em: 31 ago. 2017.

LE COADIC, Y. F. A Ciência da Informação. tradução de Maria Yêda FS de Filgueiras Gomes. **Brasília: Briquet de Lemos**, 1996. Perspectivas em Ciência da Informação, v. 1, n. 2, 1996.

LEIBSON, S. IPV6: How Many IP Addresses Can Dance on the Head of a Pin?. **EDN Network**, March 28, 2008. Disponível em: < https://www.edn.com/electronics-blogs/other/4306822/IPV6-How-Many-IP-Addresses-Can-Dance-on-the-Head-of-a-Pin- >. Acesso em: 05 jan. 2018.

LIBELIUM. Libelium Smart Word. 2013. Disponível em: <http://www.libelium.com/resources/top_50_iot_sensor_applications_ranking/#show_infographic>. Acesso em: 15 jun. 2017.

MCCULLOUGH, M. Digital ground: architecture, pervasive computing, and environmental knowing. **Cambridge: MIT Press**, 2004.

MCEWEN, A.; CASSIMALLY, H. Designing the Internet of Things. **Chichester**: Wiley, 2013.

MULLER, G. A reference architecture primer. Whitepaper, **Embedded Systems Institute**, The Netherlands.2008.

NAKAGAWA, E. Y., ANTONINO, P. O., BECKER, M. (2011) “Reference architecture and product line architecture: A subtle but critical difference”. In: Crnkovic, I., Gruhn, V., Book, M., eds. **Proceedings of the 5th European Conference on Software Architecture**. Lecture Notes in Computer Science, vol. 6903. Germany, Springer Berlin Heidelberg, pp. 207-211.

NAKAGAWA, E. Y., OQUENDO, F., MALDONADO, J. C. (2014) “Reference architectures”. In: Oussalah, M. C., ed. **Software Architecture 1**. United Kingdom, ISTE Ltd / John Wiley & Sons, Inc., pp. 55-82.

NERGIZ, M. E.; GÖK, M. Z. Hybrid K-Anonymity. **Computers & Security** 44 (2014) 51- 63. Elsevier, 2014.

NORMAN, D. The design of future things. **New York: Basic Books**, 2009.

PIRES, P. F., DELICATO, F. C., BATISTA, T., BARROS, T., CAVALCANTE, E., & PITANGA, M. Plataformas para a Internet das Coisas. **Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos**. 2015. Disponível em: <http://sbrc2015.ufes.br/wp-content/uploads/Ch3.pdf>. Acesso em: 14 ago. 2017.

RAMALHO, R.A.S., VIDOTTI, S.A.B.G., FUJITA, M.S.L. Web semântica: uma investigação sob o olhar da Ciência da Informação. **Datagramazero** (Rio de Janeiro), v. 8, p. 4, 2007. Disponível em: <http://basessibi.c3sl.ufpr.br/brapci/_repositorio/2010/01/pdf_7557383cd1_0007573.pdf>. Acesso em: 18 jul. 2016.

ROMEO, S. Promoting Multidisciplinary Thinking for Leading the Era of Wearable Technologies. **Creative, Digital & Design: Knowledge Transfer Network of Innovate UK Network**. Fev 2014. Disponível em: <https://connect.innovateuk.org/web/creativektn/article-view/-/blogs/promoting-multidisciplinary-thinking-for-leading-the-era-of-wearable-technologies>. Acesso em: 10 jul. 2017.

SANT’ANA, R. C. G. Ciclo de Vida dos Dados e o papel da Ciência da Informação. In: XIV ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO - ENANCIB, 2013, Florianópolis. **Anais do XIV Encontro Nacional de Pesquisa em Ciência da Informação - ENANCIB**. Rio de Janeiro: ANCIB, 2013. Disponível em: <http://enancib2013.ufsc.br/index.php/enancib2013/XIVenancib/paper/viewFile/284/319>. Acesso em: 10 jul. 2016.

SANT’ANA, R. C. G. Ciclo de vida dos dados: uma perspectiva a partir da ciência da informação. **Informação & Informação**, [S.l.], v. 21, n. 2, p. 116–142, dez. 2016. ISSN 1981-8920. Disponível em: <http://www.uel.br/revistas/uel/index.php/informacao/article/view/27940/20124>. Acesso em: 16 fev. 2017.

SANTOS, B. P.; SILVA, L.A.M; CELES, C.S.F.S; NETO, J.B.B; PERES, B.S; VIEIRA, M.A.M; VIEIRA, L.F.M; GOUSSEVSKAIA, O.N.; LOUREIRO, A.A.F. Internet das coisas: da teoria a prática. **Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuıdos**, 2016. Disponível em: <http://homepages.dcc.ufmg.br/~bruno.ps/wp-content/uploads/2016/05/minicurso-sbrc-2016.pdf>. Acesso em: 20 ago. 2017.

SANTOS, P. L. A. da C.; SANT'ANA, R. C. G. Transferência da Informação: análise para valoração de unidades de conhecimento. **DataGramaZero**, v. 3, n. 2, abr., 2002. Disponível em: <https://www.researchgate.net/publication/316859684_Transferencia_da_Informacao_analise_para_valoracao_de_unidades_de_conhecimento_Tranference_of_Information_analysis_for_valuing_units_of_knowledge>. Acesso em: 6 mar. 2017.

SARACEVIC, T. Interdisciplinary nature of information science. **Ciência da informação**, v. 24, n. 1, p. 36-41, 1995. Disponível em: <http://www.brapci.ufpr.br/brapci/_repositorio/2010/03/pdf_dd085d2c4b_0008887.pdf>. Acesso em: 12 jul. 2016.

SINGER, T. Tudo conectado: conceitos e representações da internet das coisas. **Simpósio em tecnologias digitais e sociabilidade**, v. 10, 2012. Disponivel em: <http://www.simsocial2012.ufba.br/modulos/submissao/Upload/44965.pdf>. Acesso em: 21 ago. 2017.

SKOPEK, J. M. Anonymity, the Production of Goods, and Institutional Design. 82 Fordham L. Rev. 1751, 2014. Disponível em: <http://ir.lawnet.fordham.edu/flr/vol82/iss4/4>. Acesso: 15 out. 2017.

THE INTERNET OF THINGS. **First International Conference**, IOT 2008, Zurich, Switzerland, March 26-28, 2008, Proceedings. Editors: Floerkemeier, C., Langheinrich, M., Fleisch, E., Mattern, F., Sarma, S.E. Disponível em: <http://www.springer.com/gp/book/9783540787303?referer=www.springeronline.com>. Acesso em: 05 jan. 2018.

VIMERCATI, S. C. FORESTI, S.; LIVRAGA, G.; SAMARATI, P. Data Privacy: Definicitions and Techiniques. **International Journal of Uncertainty**, Fuzziness and Knowledge-Based Systems Vol. 20, No. 6 (2012) 793–817 World Scientific Publishing Company, 2012.

W3C. Architecture of the World Wide Web, Volume One. 15 dez. 2004. Disponível em: <http://www.w3.org/TR/webarch/>. Acesso em: 1 ago. 2017.

W3C. Ubiquitous Web Domain. 20 jul. 2010. Disponível em: <http://www.w3.org/UbiWeb/>. Acesso em: 1 ago. 2017.

W3C. About W3C. **W3C**, 2017a. Disponível em: <https://www.w3.org/Consortium/>. Acesso em: 30 ago. 2017

____. Web of Things (WoT) Architecture. **W3C**, 2017b. Disponível em: <https://w3c.github.io/wot-architecture/>. Acesso em: 1 ago. 2017.

WEISER, M. The Computer for the 21st Century. **Scientific American**, v. 265, n. 3, p. 94–104, 1991. Disponível em: <http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html>. Acesso em: 3 ago. 2017.

WIENER, N. Cybernetics, or control and communication in the animal and the machine. **The MIT Press**, Cambridge, Masssachusetts. 1a. edição: 1948. 2ª edição revista e aumentada: 1961. Disponível em: <http://uberty.org/wp-content/uploads/2015/07/Norbert_Wiener_Cybernetics.pdf>. Acesso em: 10 out. 2017.

WIENER, N. The human use of human beings: cybernetics and society. **Houghton Mifflin, Boston**. 1a. edição: 1950. 2ª edição revista e alterada: 1954. Disponível em: <https://archive.org/stream/NorbertWienerHumanUseOfHumanBeings/NorbertWienerHuman_use_of_human_beings_djvu.txt>. Acesso em: 10 out. 2017.

WONG, R. C.; LI, J.; FU, A. W.; WANG, K. (α, k)-Anonymity: An Enhanced K-Anonymity Model for Privacy-Preserving Data Publishing. KDD'06, August 20–23, 2006, Philadelphia, Pennsylvania, USA, 2006.

WORLDOMETERS. 2018. Disponível em: <http://www.worldometers.info/>. Acessado em: 26 jan. 2018.