UNIVERSIDADE FEDERAL FLUMINENSE

Vitor Pinheiro Figueira

“Internet das Coisas” – Um Estudo sobre Questões de Segurança, Privacidade e Infraestrutura.

Niterói

2016

Vitor Pinheiro Figueira

“Internet das Coisas” – Um Estudo sobre Questões de Segurança, Privacidade e Infraestrutura.

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Orientadora:

Juliana Mendes Nascente Silva Zamith

NITERÓI

2016

Ficha Catalográfica elaborada pela Biblioteca da Escola de Engenharia e Instituto de Computação da UFF

F475 Figueira, Vitor Pinheiro
"Internet das coisas" : um estudo sobre questões de segurança, privacidade e infraestrutura / Vitor Pinheiro Figueira. – Niterói, RJ : [s.n.], 2016.
65 f.

Projeto Final (Tecnólogo em Sistemas de Computação) – Universidade Federal Fluminense, 2016.
Orientadora: Juliana Mendes Nascente e Silva Zamith.

1. Internet das coisas. 2. Segurança da informação. 3. Criptografia. I. Título.

CDD 004.678

Vitor Pinheiro Figueira

“Internet das Coisas” – Um Estudo sobre Questões de Segurança, Privacidade e Infraestrutura.

Trabalho de Conclusão de Curso submetido ao Curso de Tecnologia em Sistemas de Computação da Universidade Federal Fluminense como requisito parcial para obtenção do título de Tecnólogo em Sistemas de Computação.

Niterói, ___ de _____ de 2016.

Banca Examinadora:

_____

Prof[a]. Juliana Mendes Nascente Silva Zamith, DSc. – Orientadora

UFF – Universidade Federal Fluminense

_____

Prof. Marcelo Panaro de Moraes Zamith, DSc. – Avaliador

UFRRJ – Universidade Federal Rural do Rio de Janeiro

Dedico este trabalho a minha família, a minha noiva, aos meus amigos e a todos que me apoiaram até aqui.

AGRADECIMENTOS

A Deus, que sempre iluminou a minha caminhada.

A minha Orientadora Juliana de pelo estímulo, compreensão e paciência que me concedeu durante o curso.

Aos Colegas de curso pelo incentivo e troca de experiências.

A todos os meus familiares e amigos pelo apoio e colaboração.

“O mais competente não discute, domina a sua ciência e cala-se”.
(Voltaire)

RESUMO

O presente trabalho apresenta um estudo sobre algumas questões básicas da nova fase da internet, a internet das coisas. Isto incluiu uma breve introdução da evolução da internet até a chegada da internet das coisas, bem como uma pequena introdução ao conceito. Além disso, este trabalho aborda questões relevantes à segurança da informação e dos dados. Isto inclui uma discussão de contramedidas e apresentação de alguns mecanismos para a proteção da internet das coisas. Este trabalho também discute sobre a privacidade dos indivíduos envolvidos e sobre a grande gama de dados coletados pelos dispositivos da internet das coisas. Concluísse com uma breve análise sobre a infraestrutura da internet das coisas, desafios e obstáculos que retardam o seu desenvolvimento e os principais padrões utilizados nas implementações de internet das coisas.

Palavras-chaves: Internet das Coisas, Criptografia e Privacidade.

ABSTRACT

The present work presents a study on some basic questions of the new phase of the internet, the internet of things. This included a brief introduction of the evolution of the internet until the arrival of the internet of things, as well as a small introduction to the concept. In addition, this paper addresses issues relevant to information and data security. This includes a discussion of countermeasures and presentation of some mechanisms for protecting the internet from things. This paper also discusses the privacy of the individuals involved and the wide range of data collected by the Internet devices of things. Conclude with a brief review of the Internet infrastructure of things, challenges and obstacles that slow it down, and the major standards used in Internet deployments of things.

Key words: Internet of Things, Encryption and Privacy.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

6LoWPAN – IPv6 over Low power Wireless Personal Area Networks
AES – Advanced Encryption Standard
ARP – Address Resolution Protocol
ARPANet – Advanced Research Projects Agency Network
CBC – Cipher Block Chaining
CFB – Cipher Feedback Block
CoAP – Constrained Application Protocol
CTR – Counter
DAG – Directed Acyclic Graph
DES – Data Encryption Standard
DODAG – Destination Oriented DAG
DoS – Denial of Service
DSA – Digital Signature Algorithm
ECB – Electronic Codebook Mode
ECC – Elliptic Curves Cryptography
EEPROM – Electrically-Erasable Programmable Read-Only Memory
FFD – Full Function Device
GPRS – General Packet Radio Services
HMAC – Hash-based Message Authentication Code
HTTP – Hypertext Transfer Protocol
IaaS – Infrastructure as a Service
IAB – Internet Architecture Board
IBM – International Business Machines
IDEA – International Data Encryption Algorithm
IEEE – Institute of Electrical and Electronics Engineers
IETF – Internet Engineering Task Force
IGMP – Internet Group Management Protocol
IoT – Internet of Things
IP – Internet Protocol
IPsec – IP Security Protocol
IPv4 – Internet Protocol version 4

IPv6 – Internet Protocol version 6

LoWPAN – Low power Wireless Personal Area Network

MAC – Message Authentication Code

MIT – Massachusetts Institute of Technology

MQTT – Message Queuing Telemetry Transport

NIST – National Institute of Standards and Technology

OFB – Output Feedback Block

PaaS – Platform as a Service

PGP – Pretty Good Privacy

QoS – Quality of Service

REST – Representational State Transfer

RFD – Reduced Function Device

RFID – Radio Frequency Identification

RPL – Routing Protocol for Low Power and Lossy Networks

SaaS – Software as a Service

S/MIME – Secure/Multipurpose Internet Mail Extensions

TCB – Trusted Computing Base

TCP – Transmission Control Protocol

TLS – Transport Layer Security

UDP – User Datagram Protocol

URI – Uniform Resource Identifier

URL – Uniform Resource Locator

WPAN – Wireless Personal Area Network

WSN – Wireless Sensor Network

SUMÁRIO

1 INTRODUÇÃO

Além de conectar pessoas, a internet está vivenciando uma nova fase, onde não apenas pessoas e seus dispositivos, como computadores, *notebooks*, *smartphones* e *tablets*, estarão conectados, mas qualquer outro equipamento, como eletrodomésticos, carros, máquinas, sensores, atuadores e outros produtos em geral serão capazes de se conectar à internet. Essa nova fase da internet também é conhecida como Internet das Coisas. Segundo Khan et al [1], a Internet das Coisas dispõe conectividade para toda e qualquer pessoa e para toda e qualquer coisa em qualquer tempo e lugar.

A extraordinária potencialidade da Internet das Coisas é o poder que confere a objetos do uso cotidiano ser capazes de coletar, processar, armazenar, transmitir e expor informações. Interligados em uma rede, estes objetos são capacitados para exercer ações de forma independente e gerar dados em quantidade e diversidade exponenciais. Nesse cenário, a informação passa a ser um aspecto do ambiente, e caracteriza-se em novos contornos de comportamento das pessoas no mundo.

1.1 MOTIVAÇÃO

Escolheu-se o tema internet das coisas, pois é uma tecnologia promissora e inovadora. São novas tecnologias que serão aplicadas em produtos do cotidiano e que terão como resultado inúmeros benefícios não somente para pessoas, mas também para corporações, especialmente porque esta tecnologia trará evoluções com relação a infraestrutura, proporcionando total interconectividade entre dispositivos totalmente distintos.

Contudo, verifica-se que o conhecimento sobre esta tecnologia ainda é limitado, quer dizer, poucas pessoas sabem como sucede a integração entre os dispositivos e quais as questões positivas e negativas que resultam desta integração. Dessa forma, esse trabalho busca apresentar uma concepção sobre o que é, como funciona e até onde se supõe que a internet das coisas pode chegar.

1.2 OBJETIVO

O presente estudo tem como objetivo principal trazer um pouco de informação – por se tratar de um assunto muito abrangente – sobre o conceito de internet das coisas que tem por proposição a conexão de objetos do mundo real com a internet. Esse conceito já é amplamente discutido por profissionais da área, mas que para a grande maioria das pessoas ainda é um conceito desconhecido. Esse texto traz ao leitor informações sobre a definição do conceito de internet das coisas, apresenta vantagens e desvantagens da implantação desta tecnologia e discorre sobre questões como segurança, privacidade e infraestrutura.

1.3 ORGANIZAÇÃO DO TRABALHO

O trabalho se organiza como segue. O Capítulo 2 faz uma breve introdução ao conceito de internet das coisas, abordando alguns tópicos, computação em nuvem e modelos de comunicação. O Capítulo 3 entra no tema segurança e apresenta uma discussão sobre possíveis perigos, contramedidas que podem ser tomadas e apresentação de mecanismos que podem ser adotados para proteção. Já o Capítulo 4, debate sobre a privacidade e apresenta algumas questões chave que devem ser evidenciadas no contexto internet das coisas. O Capítulo 5 apresenta desafios e obstáculos de infraestrutura, como a necessidade de implantação do protocolo IPv6, e os principais padrões utilizados nos projetos de implementação da internet das coisas. O Capítulo 6 apresenta a conclusão do trabalho.

2 DEFINIÇÃO DE INTERNET DAS COISAS

Neste capítulo é apresentado um breve histórico da evolução da internet e a definição do conceito de “Internet das Coisas”.

2.1 BREVE HISTÓRICO DA EVOLUÇÃO DA INTERNET

Atualmente o mundo vive uma era tecnológica, onde a internet é incorporada na maioria das práticas cotidianas do ser humano, permeando afazeres e intermediando suas conexões com outros humanos.

A busca do que está à frente sempre aguça o pensamento científico a lançar-se em direção das perspectivas e desafios que o mundo pode enfrentar diante dos próximos anos.

A internet está tão presente no cotidiano, e consequentemente habituamos a usa-la tantas vezes no dia a dia, que deixou de ser necessário um manual para acessar a internet através de um *tablet*, *smartphone* ou computador.

Extremamente útil no dia a dia, a internet dispõe de praticamente todo tipo de serviço e informação, por exemplo: Empresas oferecem serviços, compram e vendem através da internet. Crianças e Jovens jogam online. Cidadãos podem ser relacionar com o Poder Público através dela. Estudantes podem buscar conhecimentos sobre os mais variados assuntos e temas, se comunicarem e trocarem informações, etc.

Criada com o objetivo de ligar grandes universidades e centro de pesquisas, a internet, como é conhecida hoje, nasceu da ARPANet, uma rede experimental financiada pelos militares dos EUA. Era uma rede que servia de interligação entre computadores de médio e grande porte, com o intuito que os pesquisadores em cada universidade compartilhassem as capacidades de processamento dos seus equipamentos. Com o passar dos tempos, cada vez mais computadores foram ligados a esta rede até evoluir para a grande rede mundial que temos nos dias de hoje [2].

No decorrer da evolução foram criadas muitas aplicações para facilitar de alguma forma a interação entre pessoas. Houve grandes avanços da tecnologia, foi criado o e-mail, surgiram os computadores pessoais, a web, o comercio eletrônico, a tecnologia de rede sem fio e de voz sobre IP, os *tablets* e *smartphones* e as diversas redes sociais que existem nos dias de hoje.

No final da década de 80, Mark Weiser et al [3], foi criado o conceito de Computação Ubíqua. Weiser diz que é o computador que se integra a vida das pessoas de modo que elas nem percebam, mas o utilizem. Segundo Weiser a computação ubíqua é definida como:

> *"A computação ubíqua é a terceira onda da computação, que está apenas começando. Primeiro tivemos os mainframes, compartilhados por várias pessoas. Estamos na era da computação pessoal, com pessoas e máquinas estranhando umas às outras. A seguir vem a computação ubíqua, a era da tecnologia calma, quando a tecnologia recua para o plano de fundo de nossas vidas [3]."*

Sempre que a mente humana assimila algo relativamente bem, ela deixa de estar ciente da existência de tal coisa. Segundo Weiser, esse desaparecimento não é resultado dos avanços tecnológicos e sim da própria psicologia humana. Em verdade, ainda hoje, existem muitas pessoas que não estão habituadas a tecnologia, porém, é cada vez mais realidade que a internet é de suma importância no cotidiano dos seres humanos.

2.2 SURGIMENTO E DEFINIÇÃO DO TERMO INTERNET DAS COISAS

Pode-se dividir a história da internet em 3 fases: a primeira é a fase da internet como uma rede de computadores, com o tempo ela evoluiu para sua segunda fase, onde se tornou uma rede de pessoas e comunidades. Atualmente está acontecendo o nascimento da terceira fase, que é chamada fase da Internet das Coisas (do inglês, *Internet of Things* – IoT). Nessa fase a internet não mais

interliga apenas computadores, ela agora passa a interligar vários tipos de objetos e dispositivos inteligentes que irão interagir com as pessoas, tornando o dia a dia mais fácil.

A origem da IoT tem sido remetida ao *Auto-ID Center* do *Massachusetts Institute of Technology* (MIT) [4], um grupo de desenvolvimento focado em estudos sobre identificação por *Radio Frequency Identification* (RFID). O ponto de vista do grupo estava ligado a compreensão de informações sobre um objeto através de um reconhecimento de radiofrequência, por meio de um endereço de internet ou um registo de banco de dados. Nos dias de hoje, o conceito de objetos inteligentes não se limita apenas ao RFID. Qualquer objeto físico ou digital que pode ser reconhecido, detectado, controlado via internet, além de apresentar a capacidade de se comunicar e interagir com o ambiente pode ser considerado inteligente.

Segundo Atzori et al [5], a Internet das Coisas é um modelo tecnológico em que objetos físicos embarcados da vida cotidiana, estariam conectados por redes sem fio e se comunicariam através da internet, trabalhando em conjunto e formando um sistema que propicia uma comunicação completa entre o mundo digital e o mundo real. A adição e disponibilização deste agregado de tecnologias interconectadas entre si e com outros recursos, transforma estes objetos em dispositivos inteligentes aptos a coletarem novos tipos de dados, e se favorecerem com novos serviços e operações.

A IoT é um tema de grande importância técnica, social e econômica. A cada dia que passa mais e mais objetos estão sendo interligados com a conectividade da internet, tais como bens duráveis, produtos de consumo, componentes industriais, automóveis, sensores e muitos outros objetos.

Hoje já é possível, por exemplo, automatizar uma casa de forma a ser controlada por celular ou *tablet*. Porém, com os avanços tecnológicos, esses dispositivos não serão mais necessários, a própria casa irá reagir a sua presença, controlando-se sozinha e automaticamente respondendo as suas necessidades. Cidades poderão espalhar sensores por todos os cantos para poder medir a temperatura, velocidade do vento, umidade, qualidade do ar, etc. Isso trará medições mais atualizadas e precisas, já que a medição poderá ser dada em tempo real por toda a cidade.

Carros equipados com sensores e internet serão capazes de informar uns aos outros sobre engarrafamentos, ou sobre algum acidente ocorrido na rota em que

este se desloca, assim como, por exemplo, o carro da frente, pode avisar ao carro que vem logo atrás, que irá fazer uma freada brusca. Objetos como relógio e roupas poderão monitorar constantemente a nossa saúde, emitindo alertas quando algo estiver fora do normal. Resumidamente, são inúmeras as possibilidades de uso e aplicações que poderão auxiliar o dia a dia do ser humano.

As evoluções tecnológicas recentes foram responsáveis por possibilitar o nascimento da IoT, por exemplo, redes de sensores sem fio, comunicabilidade móvel e computação ubíqua. Todavia, ainda existem muitos obstáculos a serem vencidos, em especial a criação de aplicações e a alta desigualdade resultante das diferentes tecnologias de *hardware* e *software*, para que a IoT seja impulsionada em larga escala.

2.3 COMPUTAÇÃO EM NUVEM

A IoT pretende interligar quase tudo que faz parte do cotidiano e encolher a distância entre os mundos físico e digital. Todavia essa transformação só será possível com a ajuda da computação em nuvem (do inglês, *Cloud Computing*). A ascensão da computação em nuvem trouxe para IoT um alto ganho de popularidade. Desta forma, pode-se afirmar que a computação em nuvem é uma grande alavanca para estimular os projetos de IoT devido a sua eficácia em proporcionar recursos sob demanda para armazenamento e hospedagem de aplicações criadas para acesso em tempo real de qualquer ambiente.

O conceito de computação em nuvem ainda é bem complexo. Todavia, um dos conceitos existentes refere-se a utilização de memória, dos recursos de armazenamento e da capacidade de processamento de computadores e servidores compartilhados. Estes recursos estão acessíveis e interligados por meio da internet. Todos os dados armazenados podem ser acessados remotamente de qualquer lugar, a qualquer instante, independentemente de plataformas, sem a necessidade de instalação de programas ou armazenamento dos dados [6].

Já para Armbrust et al [7], a computação em nuvem pode ser definida como um agregado de serviços de rede ativados, possibilitando escalabilidade,

qualidade de serviço, infraestrutura acessível de computação de acordo com a demanda e que pode ser acessada de uma forma simples e universal.

Para um melhor entendimento do termo, o NIST et al [8], propõe que a infraestrutura da computação em nuvem possui cinco características dadas como essenciais, são elas: serviço de autoatendimento sob demanda; acesso à internet por meio de banda larga; *pool* de recursos computacionais (memória, rede, armazenamento e processamento); ágil flexibilidade com intenção de prover uma maior escalabilidade de serviços e por último, medição transparente do emprego de serviços/recursos.

Mell e Grance et al [8], discorrem que a computação em nuvem apresenta três modelos de tipo de serviço: software como serviço (SaaS), plataforma como serviço (PaaS) e infraestrutura com serviço (IaaS). Mel e Grance também discorrem que a computação em nuvem pode ser implantada em quatro disposições diferentes: publica, privada, comunitária e híbrida (pública/privada).

Resumidamente, o principal objetivo do modo de comunicação em nuvem é a utilização de aplicações sem a necessidade de acesso a uma rede física. Desta forma, as aplicações passariam a ficar nas “nuvens”, ou seja, na internet. Portanto, caberá ao fornecedor de uma aplicação em nuvem, prover todas as tarefas de armazenamento, escalonamento, backup, manutenção, atualização, etc. O usuário da aplicação não terá necessidade de se preocupar com nenhum destes tópicos, apenas acessar e utilizar.

2.4 MODELOS DE COMUNICAÇÃO

Existentes implementações de objetos IoT revelam modelos de comunicação que podem ser reaplicados por desenvolvedores com a vantagem de reduzir a concepção e o esforço no desenvolvimento de novos projetos. A RFC 7452 et al [9] submetida pelo *Internet Architecture Board* (IAB) e publicada em Março/2015 pelo *Internet Engineering Task Force* (IETF), descreve quatro modelos básicos de comunicação utilizados no ambiente inteligente de dispositivos IoT. A discussão a seguir apresenta estes modelos e evidencia as principais particularidades básicas da arquitetura de cada um deles.

2.4.1 *Device-to-Device* (Dispositivo para Dispositivo)

Nesse modelo de comunicação um dispositivo se conecta e se comunica diretamente com o dispositivo alvo. Esses dispositivos podem se comunicar por diferentes tipos de redes, incluindo redes IP e a Internet e utilizam protocolos de comunicação como o *Bluetooth*, *Z-Wave* e *ZigBee* para estabelecer essa conexão direta. A Figura 1 ilustra a comunicação entre um *smartphone* e uma cafeteira através de uma rede *bluetooth*.

Figura 1: Cenário de Aplicação de *Device-to-Device*

2.4.2 *Device-to-Cloud* (Dispositivo para Nuvem)

Neste modelo, o dispositivo é conectado diretamente com um serviço de nuvem da internet, sem fazer uso de um equipamento intermediário que instaure essa comunicação. Devido a isso, os dispositivos conectados nesse modelo podem transmitir dados diretamente a um servidor de nuvem sem a necessidade de uma infraestrutura própria de rede *Ethernet* ou *Wi-Fi*, por exemplo. Para que este serviço em nuvem possa ser usado por diversos tipos de dispositivos de diferentes fabricantes, é essencial o suporte de protocolos de comunicação padrão e abertos como o CoAP e MQTT. A Figura 2 mostra a comunicação de um automóvel com um serviço em nuvem através de um rádio GPRS embutido.

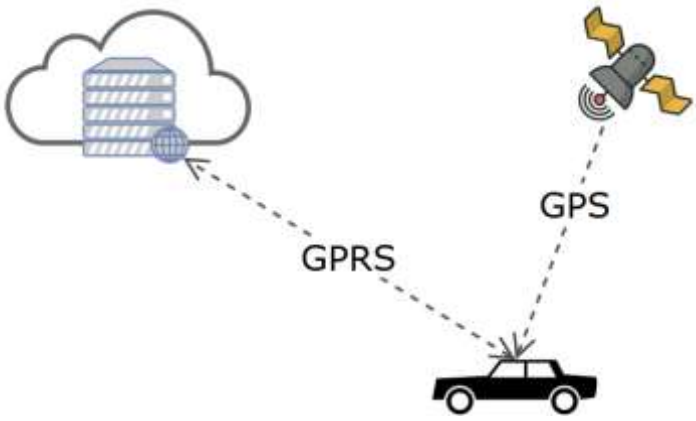

Figura 2: Cenário de Aplicação de *Device-to-Cloud*

2.4.3 *Device-to-Gateway* (Dispositivo para Gateway)

Neste modelo, um dispositivo se conecta a IoT através de um serviço de *Gateway* como um canal para chegar ao serviço de nuvem. Em outras palavras, significa que um software de aplicação que atua num dispositivo de *Gateway* local que tem o papel de atuar como um intermediador entre o dispositivo e o serviço de nuvem, esse *Gateway* também provê funcionalidades como: segurança, dados e protocolos de tradução. A Figura 3 ilustra o uso de uma pulseira para monitorar exercícios físicos do cotidiano, enquanto a Figura 4 mostra uma casa totalmente conectada, onde a comunicação é feita através de um *Gateway*.

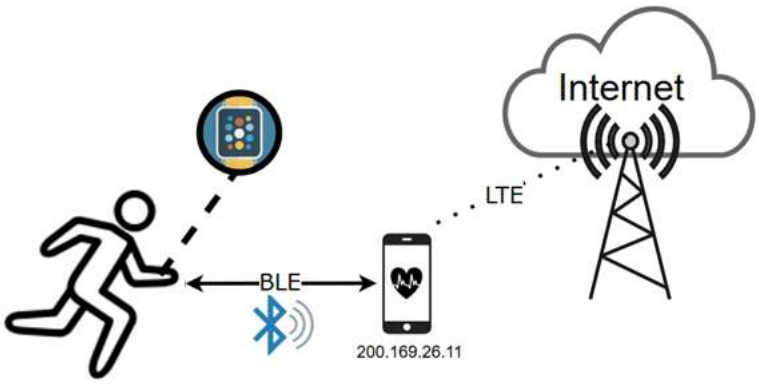

Figura 3: Cenário de Aplicação de *Device-to-(Smartphone)Gateway*

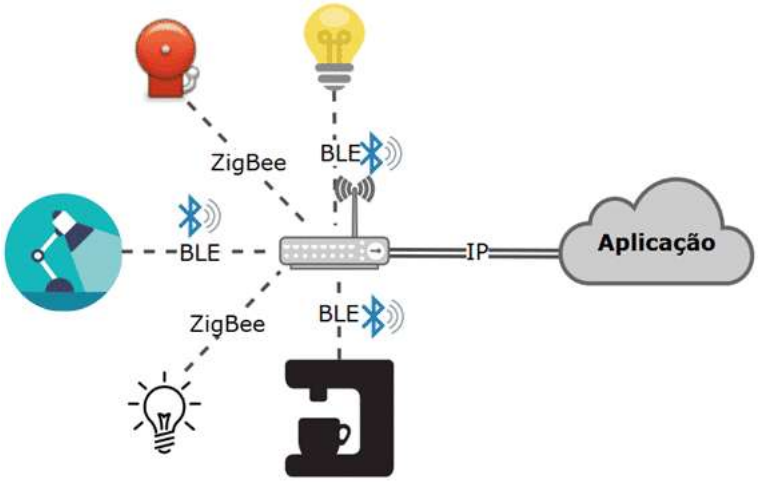

Figura 4: Cenário de Aplicação de *Device-to-(Access Point)Gateway*

2.4.4 *Back-End Data Sharing* (Compartilhamento de Dados Back-End)

A IoT nos possibilita coletar, combinar e analisar uma enorme quantidade de dados exportados de diferentes plataformas e dispositivos. O conceito de *Back-End Data Sharing* torna possível manipular e trazer sentido a estes dados coletados. Esse modelo é uma extensão do modelo *Device-to-Cloud*, e que pode levar a silos de dados onde os dispositivos da IoT fazem *upload* de dados para um único provedor de serviços de aplicativos. A Figura 5 ilustra uma fazenda de servidores conectados onde o Servidor A faz a comunicação com os Servidores B e C para agregar um maior valor aos dados coletados por seus sensores.

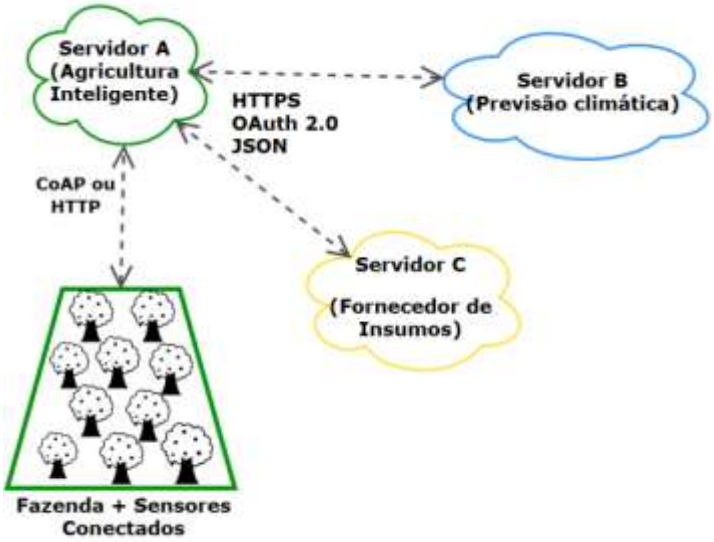

Figura 5: Cenário de Aplicação de *Back-End Data Sharing*

2.5 PERSPECTIVAS DA IOT PARA O MERCADO ATUAL

A IoT conduz boas perspectivas ao mercado atual e atrai inúmeros benefícios para a sociedade, essa ligação de objetos possibilitado pela IoT proporciona um maior controle e compreensão de como os sistemas interagem entre si e consequentemente possibilita uma melhora significativa na qualidade de vida de todos. Com a evolução da internet para o IoT, as empresas vêm mudando a sua maneira de abordar seus ativos, assim como a maneira de monitorar suas operações comerciais e a sua interação com o mercado consumidor.

Graças a IoT surgiram novas formas de gerenciar remotamente equipamentos por artificio de telemetria, captando os dados dos dispositivos em tempo real. Essas novas formas permitem projetar novos modelos operacionais e utilizar de verificação de local e produtos mais inteligentes para relacionar com os clientes. Essa inovação proporcionaria serviços mais completos assim como novos serviços que antes não existiam. Um outro exemplo são as empresas que fabricam equipamentos que estão se beneficiando de sensores integrados que são capazes de prover dados em tempo real sobre seu uso, possíveis falhas que podem ocorrer, local, questões de segurança e consumíveis que serão necessários. Com esses dados sendo obtidos em tempo real haverá uma grande potencialização do tempo

de atividade e proporcionar respostas mais rápidas dos serviços. Esses objetos assim ditos na IoT de um ponto de vista empresarial podem variar muito, tanto em tamanho quanto em complexidade, além disto, podem variar de simples termostatos até veículos pesados totalmente independentes e turbinas.

3 SEGURANÇA NA INTERNET DAS COISAS

Neste capítulo é apresentado um estudo sobre as questões de segurança dos dispositivos na IoT, problemas e soluções que surgiram com essa nova fase.

3.1 INTRODUÇÃO

Essa nova realidade da internet conduzida pela IoT, diminuirá a segurança da internet como um todo. Cada um dos dispositivos IoT pode ser, potencialmente um ponto de vulnerabilidade, onde um código mal intencionado pode ser inserido, afetando a segurança dos sistemas. Com um mundo cada vez mais interconectado, um vírus de software pode afetar a operação de redes integradas de energia elétrica e causar blecautes que afetem a economia de um país inteiro.

Do lado dos servidores, já existem muitos mecanismos para garantir a segurança. Diversos softwares e processos de segurança já foram criados para garantir níveis de segurança adequados. Por outro lado, os sensores e outros dispositivos nas extremidades das redes tendem a ser os pontos de maior fragilidade a quebra de segurança.

É necessário colocar nos dispositivos IoT mecanismos de segurança que indiquem que os sensores estejam funcionando adequadamente e que não estejam contaminados por algum vírus. Além disso, em um mundo cada vez mais móvel, com *smartphones* e *tablets* se multiplicando a cada minuto, mais pontos de acesso, que nem sempre oferecem segurança, são inseridos nas redes de informação.

3.2 PROBLEMAS DE SEGURANÇA

No contexto atual da tecnologia, considerações a respeito de segurança não são nenhuma novidade. As características de novas implementações de IoT apontam novos desafios a segurança. Portanto, é uma prioridade fundamental explorar estes desafios afim de encontrar soluções capazes de garantir a segurança que os produtos e serviços IoT necessitam. Caso tais produtos e serviços não estejam protegidos, eles podem ser usados como potenciais pontos de entrada para ataques cibernéticos e exposição de dados de usuários conectados ao roubo.

Como na IoT todos os dispositivos estão interconectados, um dispositivo que esteja mal protegido e conectado na internet poderá consequentemente afetar toda a segurança e resiliência da internet em um nível global. A implantação em massa de dispositivos IoT e a propriedade de se conectarem automaticamente e por conta própria agravam essa questão.

Na IoT, o usuário necessita confiar na natureza segura dessa massa de dispositivos conectados. Existe uma necessidade absoluta de que seus dispositivos e suas informações estejam devidamente protegidas contra usos indevidos e danos causados por falta de segurança.

É mais útil conceituar a segurança dos dispositivos IoT como um espectro de vulnerabilidade que esses dispositivos estão sujeitos. Esse espectro pode variar entre dispositivos com nenhuma segurança, ou seja, totalmente desprotegidos até dispositivos que possuem inúmeras camadas de segurança, ou seja, altamente protegidos.

A IoT ainda está muito longe de estar segura o suficiente contra os problemas de segurança e ataques da internet atual, muito em parte, devido a particularidades desta tecnologia, tais como:

- Comunicações em IoT podem ser realizadas através de redes sem fio: qualquer indivíduo com mais intenções pode ouvir essas transmissões e se comunicar usando esse mesmo meio;
- É possível acessar os dispositivos fisicamente: os dispositivos IoT podem ser colocados em locais públicos onde estão ao alcance de qualquer indivíduo;

- Muitos dispositivos contam com recursos limitados: a limitação de recursos insere medidas de segurança bem restritas nesses dispositivos.

3.3 DESAFIOS À SEGURANÇA

Conforme mais automóveis, sistemas industriais, dispositivos médicos são conectados a IoT, assim como mais empresas criam modelos de negócios com base na conectividade da IoT, a visibilidade de segurança deve se estender além dos domínios tradicionais. Quanto mais dados são disponibilizados e dispositivos conectados a IoT, maior será a necessidade de desenvolver modelos de segurança capazes de tornar a conectividade IoT confiável.

Dispositivos da IoT diferem dos computadores tradicionais conectados à rede e dos dispositivos tradicionais de maneiras importantes e que desafiam a segurança de diferentes formas:

- Grande quantidade dos dispositivos IoT, tais como sensores e itens de consumo, são criados para ser implantados em uma escala maciça o que difere dos dispositivos tradicionais conectados à internet, isso acarreta que a interligação entre esses dispositivos não tem precedentes;
- Muitas das implantações IoT consistem de conjuntos de dispositivos idênticos ou quase idênticos. Essa igualdade entre dispositivos aumenta o impacto potencial que uma fragilidade única pode acarretar devido ao grande número de dispositivos que possuem as mesmas particularidades;
- Muitos dispositivos IoT são implementados com um tempo de serviço muito superior do que normalmente os equipamentos de alta tecnologia tem associado a eles. Além do que, esses dispositivos podem ser implantados em ambientes e circunstâncias que podem torná-los difíceis ou até impossíveis de serem reconfigurados ou atualizados;

- Muitos dispositivos IoT são criados propositadamente sem capacidades de atualização, devido ao fato de que o processo de atualização é impossível ou dificultoso demais;
- Grande quantidade de dispositivos IoT atuam de forma que o usuário não tem pouca ou nenhuma visão real do funcionamento interno dos dispositivos e das informações que são geradas por eles;
- Alguns desses dispositivos IoT podem ser implantados em locais de fácil aceso, onde medidas de segurança podem ser muito difíceis ou até mesmo impossíveis de ser implantada;
- Dispositivos IoT como sensores ambientais, são projetados para se misturar discretamente no ambiente para o qual foi projetado. Isso pode fazer com que o usuário não tenha percepção da localização dos dispositivos e consequentemente não poder monitorar o status operacional do dispositivo;

Outro desafio à segurança é em relação a sobrecarga adicional de recursos computacionais que ela pode acarretar. A capacidade de poder confiar nas mensagens dos dispositivos não é totalmente privada de desvantagens. Executar as medidas de segurança como por exemplo, código criptográfico adicional usado para garantir que as comunicações sejam feitas de forma confiável, demanda recursos computacionais como:

- **Tempo adicional de CPU**: em vez de executar algum outro pedaço de código a CPU terá que dedicar tempo a execução de primitivas criptográficas;
- **Energia**: o dispositivo deve ser mantido ativo e não em um modo de baixo consumo de energia, portanto, mais energia será usada para operar unidades de CPU durante a execução do algoritmo;
- **Memória RAM**: será consumida mais RAM temporariamente e até mesmo permanente caso o estado de operação assim necessite;
- **Memória Permanente**: O código irá consequentemente aumentar de tamanho caso haja adição de primitivas criptográficas;

Adicionar segurança requer uma escolha apropriada tanto dos dispositivos, como primitivas adotadas para atestar a funcionalidade do dispositivo sem que este seja prejudicado pela adição de segurança. Caso isto não seja feito,

poderá acarretar em impactos negativos como: redução de funcionalidades, demandar exagerada de recursos e insuficiência de cumprir requisitos em tempo real.

3.4 RISCOS E CONTRAMEDIDAS DE SEGURANÇA

Os avanços tecnológicos consequentemente trazem novas oportunidades para ataques de cibercriminosos. Quanto maior é essa quantidade de dispositivos que podem ser acessados, maior é a extensão do dano que podem causar. Como na IoT a variedade de dispositivos é muito grande, é difícil saber como, onde e quando os dados pessoais estão sendo coletados e se o dispositivo está atualizado com as últimas medidas de segurança.

Kalita e Kar et al [10], enumeraram e apresentaram uma descrição sobre 37 possíveis ataques que as redes sem fio (*WSNs*) estão sujeitas e que são transponíveis à IoT, entre esses possíveis ataques estão:

- **Ataques de Negação de Serviço (DoS)**: impedimento ou restrição do uso normal da rede ou administração de dispositivos de rede ou rede sem fio;
- **Ataques *Sybil***: dispositivos maliciosos ilegitimamente que tomam inúmeras identidades.
- ***Wormhole***: encaminhamento de mensagens recebidas em um link de baixa latência e as reproduz em outra parte diferente da rede com o propósito de interrompe o roteamento;
- ***Skinhole* (Buraco Negro)**: transforma um nó comprometido em particularmente atraente de uma perspectiva de roteamento, atraindo todo o trafego para uma área especifica através deste nó;
- **Encaminhamento seletivo**: os nós comprometidos se comportam como buracos negros recusando a encaminhar mensagens e simplesmente descartando-as;
- **Analise de Tráfego**: monitoramento das transmissões vias redes sem fio para o propósito de identificar padrões de comunicação e participantes [11];

- **Espionagem**: um atacante mal-intencionado monitora de forma passiva redes sem fio para coletar dados, incluindo credencias de autenticação;

Ainda hoje não há solução para todos os ataques a que a IoT está sujeita. Os ataques de DoS podem ser mitigados ou evitados em algumas situações especificas, por exemplo, não processar mensagens que sejam originadas de dispositivos que transmitem um número maior do que o limite definido. Entretanto, um indivíduo pode acabar investindo em dispositivos com maiores recursos, e consequentemente com capacidade de gerar mais colisões, ou dispositivos usados exclusivamente para inunda o trafego de uma rede sem fio. Problema esse muito intrínseco quando a meio de transmissões sem fio e que não tem como ser evitado.

Uma medida importante a levar em consideração na segurança é prevenir que adulterações físicas possam ser feitas, visto que elas podem destruir/danificar nós de uma rede para efetivamente permitir reprogramação dos nós, engenharia reversa e aquisição de chaves criptográficas [10]. Em um ambiente onde a importância da segurança supera a importância dos dispositivos, então medidas destrutivas devem ser consideradas quando houver tentativas de adulteração física nesses dispositivos.

Outra contramedida que pode ser usada para reduzir as questões de privacidade dos dados e o número de ataques bem-sucedidos é o uso de mensagens seguras por meio de medidas criptográficas inclusivamente nas camadas de roteamento [10]. Mensagens que forem criptografadas vão garantir que um invasor não possa ler o conteúdo de uma mensagem sem possuir a chave descriptográfica. Já as mensagens que forem autenticadas de forma correta não podem ser falsificadas. Os dispositivos estrangeiros não poderão adulterar identidades quando a autenticação é necessária. Os atacantes que não fazem parte da rede autenticada não podem transmitir mensagens falsas para atrair tráfego.

Outra medida a ser empregada é o projeto de protocolos meticulosos, que contam com políticas de prevenção de ataques além de apenas garantir a comunicação [10]. Estes protocolos também podem permitir que partes confiáveis tenham participação no que diz respeito as decisões de roteamento. Combinando criptografia e protocolos protegidos podem também mitigar a análise de tráfego, garantir que todas as mensagens tenham o mesmo tamanho e a transmissão de mensagens falsas entre os dispositivos.

Já contra os ataques de *Wormhole* podem ser utilizadas medidas como abordagens de nível superior e abordagens de comportamento para ajudar a detectar esses ataques identificando os nós replicados nos diferentes locais da rede [10]. Protocolos de roteamento devem ser planejados meticulosamente de forma que possam vencer este tipo de ataque. Constatar esse tipo de ataque não é uma tarefa tão simples, pois os dispositivos podem funcionar perfeitamente no ponto de vista da rede, mais estar envolvido à espera de um gatilho ou condição de disparo ou com a comunicação com um dispositivo fora da percepção da rede.

3.5 MECANISMOS DE SEGURANÇA PARA IOT

Dizer que um sistema ou dispositivo está protegido, pode ser uma afirmação totalmente incerta, pois a segurança, como muitas outras propriedades relacionadas é uma condição muita delicada, que só pode ser alcançada por completo através de uma análise de todas as situações e cenários de riscos possíveis a um determinado sistema ou dispositivo.

Referências à expressão Base de Computação Confiável (do inglês – *Trusted Computing Base* – TCB) podem ser rastreadas até o ano de 1979 [12], onde são apresentados mecanismos de controle de acesso para sistemas operacionais, correspondendo apenas a mecanismos de *hardware* e *software*. Todavia, recentemente [13] já considera-se *firmware* a esses mecanismos de controle.

Para aplicar a definição de Computação confiável à IoT, deve-se considerar a proteção também da interação entre seus componentes que podem estar fisicamente separados e que se comunicam por intermédio de um meio compartilhado. Tal proteção pode ser feita através da utilização de criptografia, o que ajuda a fornecer um número de propriedades adicionais a segurança IoT [14]:

- Autenticação: é a verificação de onde se origina uma mensagem. As mensagens são originadas de uma fonte conhecida e não de uma parte externa que não se sabe a procedência;
- Autorização [15]: é a verificação dos privilégios de acesso. Criptografia em geral não fornece mecanismos de autorização,

porém, a autenticação é essencial para implementação de mecanismos de autorização que podem ser fornecidos através dela;

- Confidencialidade dos dados: o conteúdo de mensagens é oculto na rede, e pode ser vista apenas pelo remetente e destinatário;
- Integridade: garantir que as comunicações não sofreram adulteração durante o trânsito. Se aplica a todas as situações em que as mensagens, ao chegar ao seu destino, se desviam do conteúdo original;
- Não repudio: incapacidade de um remetente de mensagem última, negar de envia-la.

Conforme dito anteriormente, oferecer segurança as comunicações entre os dispositivos IoT requer uma sobrecarga adicional. Para minimizar essa sobrecarga seria desejável algoritmos que fossem mais rápidos, de baixa memoria, criptograficamente robustos que executam de forma análoga aos algoritmos de arquiteturas homogêneas. Todavia, não é compatível com o mundo real onde:

- Algoritmos criptograficamente mais fortes são frequentemente considerados algoritmos com baixo rendimento. Esses algoritmos fortes utilizam muitos recursos e realizam um grande número de operações. Com esse grande número de operações, estes se tornam lentos em dispositivos que não possuem uma alta capacidade de processamento;
- Uma dada implementação pode favorecer o tempo de execução em vez da memória (como nos casos de: uso de tabelas de pesquisas, multiplicação de loops, etc.). Nem sempre haverá um tempo de troca definida entre ambos;
- O desempenho de um código exato pode oscilar de acordo com as características da arquitetura como número e tamanho dos registros da CPU ou instruções especificas.

Mecanismos de segurança não são mais do que políticas de segurança. Este fato leva à conclusão que uma determinada técnica criptográfica poder ser considerada ótima em um cenário e péssima em outro ou vice-versa, vai depender basicamente do nível de segurança requerido pela política de segurança empregada. Múltiplos métodos devem ser levados em consideração quando se discute a forma de empregar a segurança. Desvantagens de um cenário podem não

aparecer assim em outro e as vantagens de outro podem ser irrelevantes. Somente os requisitos de segurança podem definir o nível de segurança adequado a um cenário, incluindo o nível de segurança das comunicações.

Além da definição do nível de criptografia adequado a um cenário, é necessário identificar quais exatamente serão as propriedades que deverão ser analisadas nesse cenário. A importância da privacidade das informações em muitas, senão na maioria das situações, implica que não existe nenhum ponto negativo em aplicar técnicas criptográficas. Aplicar medidas de segurança criptográficas efetivamente reforçam as propriedades de segurança.

3.5.1 Cifras de Chaves Simétricas

Cifras de chaves simétricas são as que utilizam a mesma chave simétrica para poder executar a criptografia e a descriptografia, respectivamente, de texto puro e de texto cifrado. Nesse sistema de Cifras é imprescindível que os integrantes tenham o conhecimento das chaves simétricas, por ventura, uma só chave secreta. Essa chave corresponde a um segredo compartilhado entre os integrantes para ser estabelecer uma ligação confidencial. Essa exigência de que todas as partes tenham acesso a essa mesma chave secreta pode ser considerada a principal desvantagem se comparada à criptografia de chave assimétrica, que se utiliza de duas chaves, uma pública e outra privada.

A criptografia de chaves simétricas, bem como todas as demais técnicas de criptografia, tem como objetivo neutralizar os ataques de espionagem, proporcionando assim a privacidade dos dados. Garantindo que o segredo é comum apenas entre as partes. Isso irá resultar em que somente as partes pretendidas terão meios de interpretar essas informações.

Algoritmos de chave simétrica podem ser divididos em dois tipos: Cifras por Blocos e Cifras por Fluxos ou Contínuas.

3.5.1.1 Cifras de Chaves Simétricas por Blocos

Algoritmos de cifras de bloco operam através de agrupamentos de *bytes* (blocos) de tamanho fixo, mapeando em blocos de tamanho n-*bytes* de texto simples em blocos de n-*bytes* de texto cifrado. Esse mapeamento entre esse texto simples e o texto criptografado é determinado por uma chave secreta K. Essa situação é ilustrada na Figura 6.

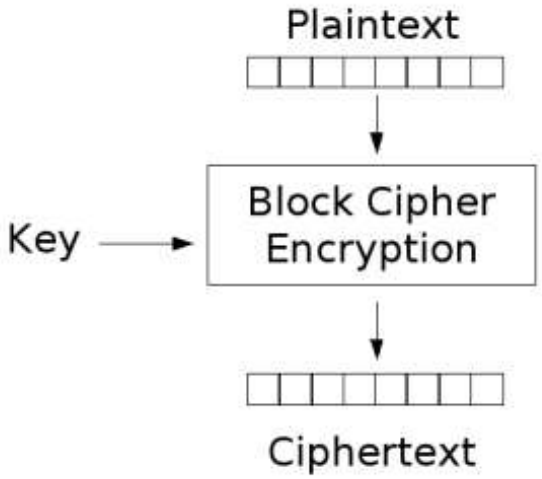

Figura 6: Esquema de operação de cifras por bloco

Cifras em bloco são melhores para criptografar dados estáticos, onde já se sabe antecipadamente o tamanho e se podem dividir em blocos de M bits. Um possível problema com cifras em bloco é o fato da existência de blocos repetitivos que acabam por criar um padrão. Para evitar o reconhecimento de padrões repetitivos usa-se os *feedbacks modes* [16]:

- *Electronic Code Book* (EBC): a mensagem é dividida em blocos de tamanho adequado, onde cada bloco é cifrado separadamente e os blocos cifrados são concatenados na mesma ordem. Essa técnica não é recomendada no contexto da IoT, pois além do risco de criptoanálise, ela permite ataques de repetição;
- *Cipher Block Chaining* (CBC): nesse modo é feita uma operação de ou exclusivo (*xor*) do bloco de texto simples com o texto cifrado anteriormente, e então ocorre a codificação. Para a inicialização

desta técnica é usado um vetor de inicialização, já que não vai existir texto cifrado para o bloco inicial;

- *Cipher Feedback Block* (CFB): nesta técnica cada bloco de texto cifrado anteriormente é codificado, e o resultado é disposto com o bloco de texto simples através do operador *xor* para o bloco de cifra atual;
- *Output Feedback Block* (OFB): esse modo é similar ao CFB, diferencia-se apenas no fato que agora a quantidade de *xor* com cada bloco de texto simples é gerado de forma independente do bloco de texto simples ou de texto cifrado;
- *Counter* (CTR): esse modo começa com um valor de contrato ctr, onde cada i-ésimo bloco de cifra é um *xor* com o fluxo de chaves resultante de ctr + i.

3.5.1.2 Cifras de Chaves Simétricas por Fluxo

Cifras de fluxo também são conhecidas como Cifras em cadeia, atuam em unidades menores, geralmente bits, o que faz delas bem mais rápidas. Elas geram uma sequência de bits que será usada como chave, conhecida como *keystream*, a partir de uma chave inicial. A encriptação [16] de texto simples geralmente ocorre através de operações *xor* com a *keystream*. A representação do comportamento de cifras por fluxo é mostrada na Figura 7.

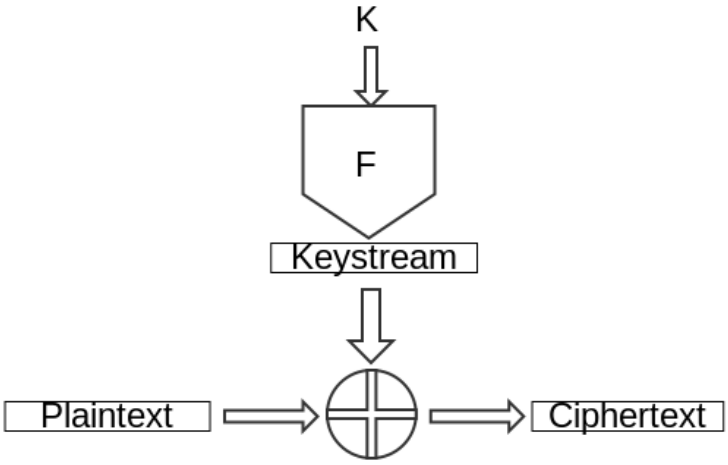

Figura 7: Esquema de operação de cifras por fluxo

É importante salientar que para a mesma chave e texto simples, sem um estado anterior, o texto cifrado resultante será o mesmo. Se o estado interno de uma cifragem de fluxo pode ser reiniciado várias vezes, é uma boa prática combinar a chave com um vetor de inicialização, para assim pode evitar ataques de repetição.

A Tabela 1 apresenta alguns dos principais algoritmos utilizados na criptografia de chave assimétrica.

Tabela 1: Principais Algoritmos de Criptografia de Chave Simétrica [17].

Algoritmo	**Bits**	**Definição**
AES	128	O *Advanced Encryption Standard* (AES) é um algoritmo de cifra por bloco. É um dos algoritmos mais comuns para criptografia de chave privada desde 2006, sendo sucessor do algoritmo DES. O AES possui um tamanho de blocos fixo de 128 e chaves de tamanho 128, 192 e 256 bits. Ele é rápido, de fácil execução e utiliza pouca memória.
DES	56	O *Data Encryption Standard* (DES) foi o algoritmo de chave privada mais difundido até a normalização do AES. Criado pela IBM em 1997, permiti cerca de 72 quadrilhões de combinações. Todavia, seu tamanho de chave (56 bits) é considerado pequeno.
3DES	112 ou 128	O 3DES é uma simples mudança do DES. Utilizando o em três ciframentos consecutivos, sendo capaz de usar

		versões com duas e três chaves diferentes. É muito lento para ser considerado padrão, contudo, é muito seguro.
IDEA	128	O *International Data Encryption Algorithm* (IDEA) é construído seguindo as mesmas normas gerais do DES. Na maioria dos microprocessadores, a execução por software do IDEA é mais veloz do que por DES. É muito utilizado no mercado financeiro e no PGP, programa para criptografia de e-mail particular mais difundido no mundo.
Blowfish	32 a 448	Criado por Bruce Schneier, fornece a seleção entre maior segurança ou desempenho por meio de chaves de tamanho variável. Schneier o complementou no Twofish.
Twofish	128	O Twofish é um dos poucos algoritmos envolvidos no OpenPGP. O Twofish utiliza cifras de bloco de 128 bits, operando com chaves de tamanho variável, podendo ser de 128, 192 e 256 bits. Executa 16 interações durante a criptografia, sendo um algoritmo bastante rápido.
RC2	8 a 1024	Criado por Ron Rivest, é empregado no protocolo S/MIME, direcionado a criptografia de e-mail corporativo. Possui chave de tamanho variável. Rivest também desenvolveu os algoritmos RC4, RC5 e RC6.
CAST	128	O CAST é um algoritmo de cifragem por bloco. Foi criado em 1996 por Carlisle Adams e Stafford Tavares. O CAST-128 é um algoritmo de Feistel, com 12 a 16 iterações da etapa fundamental, tamanho de blocos de 64 bits e chaves de tamanho variável entre 40 a 128 bits, com adições de 8 bits. As 16 interações são utilizadas quando a chave varia em valores maiores que 80 bits.

3.5.2 Códigos de Autenticação de Mensagens

Simplesmente criptografar mensagens, no entanto, não prova que a mensagem não foi alterada (sem verificação de integridade) e não prova que a mensagem foi originada na fonte pretendida (sem não-repúdio). A fim de fornecer a privacidade de dados, a integridade da mensagem e/ou não-repúdio, a criptografia deve ser combinada com técnicas criptográficas adicionais.

Códigos de autenticação de mensagens (MACs) são pedaços de informação que resultam de uma operação sobre uma determinada mensagem e uma chave secreta com a finalidade de certificar condições de integridade e autenticidade das informações. O objetivo de um MAC é atestar que uma mensagem não sofreu nenhuma adulteração, todavia, somente os elementos que possuem conhecimento dessa chave secreta serão capazes de fazer tal verificação.

Uma característica importante de um bom MAC é que mínimas alterações no texto simples original, devem ser evidenciadas em mudanças significativas de MAC. Outra importante característica é que um MAC deve ser capaz de resistir a uma falsificação existencial. Mesmo que um indivíduo malicioso tenha conhecimento da chave usada no processo capaz de gerar MACs para determinados textos simples, ele ainda assim não seria capaz de extrair a chave secreta [18]. Números de pares capturados de textos simples não deve ser capaz de fornecer induções sobre a chave usada. Existem várias estratégias para dar origem aos MACs, abrangendo [18]:

- Usando cifra na técnica CBC: como dito anteriormente, esta técnica utiliza do bloco anterior para fazer a criptografia, as mudanças nos blocos são propagadas até que o último bloco seja usado como MAC para verificar a correção da mensagem;
- Operando funções pseudoaleatórias (MAC *XOR*) [19]: operando com essa função, o estado interno será inicializado pela chave secreta. A mensagem então é dividida em blocos e processada por esta função, gerando um conjunto de blocos de chave corrente. De modo estes blocos executam um *xor* para obter o MAC.
- Função de resumo Hash: construído com base em uma chave compartilhada e uma mensagem, um resumo Hash é gerado. Uma

função Hash traz benéficos como [20]: resistência ao descobrimento do texto original, resistência ao descobrimento de um segundo texto com o mesmo Hash e não permitir a recuperação da chave e adulteração de novas mensagens;

3.5.2.1 HMAC

O código de autenticação de mensagens baseado na função Hash (HMAC), é digno de um lugar singular ao longo das técnicas baseadas em Hash para gerar MACS devido ao fato de que ele é usado amplamente, incluído tanto no IPsec quanto no TLS.

Uma vez que o cálculo de um Hash normalmente requer mais instruções (e, consequentemente, mais tempo) do que executar operações *xor* entre a chave e o preenchimento (e aqueles que podem ser pre-computados), o desempenho do HMAC pode ser comparado com o desempenho da função Hash subjacente, sendo o desempenho tão variado quanto no possível universo de funções Hash.

De forma análoga as vantagens que as cifras simétricas proporcionam, os MACs são ótimas escolhas para dispositivos altamente restritos. A criptografia de chave simétrica é geralmente, mais rápida do que a assimétrica e pode ser inserida num número maior de dispositivos IoT. MACs devem ser sempre usados em dispositivos restritos, em contrapartida exige integridade ou autenticação dos dados.

3.5.3 Criptografia de Chave Assimétrica

Também conhecida como Criptografia de chave pública, não se baseia na existência de uma chave compartilhada como na simétrica. Em vez disso, se utiliza de duas chaves distintas e matematicamente relacionadas: uma chave pública que é livremente distribuída e uma chave privada (secreta) que deve ser mantida em sigilo por seu dono. Mensagens codificadas com a chave pública só podem ser decodificadas através da chave privada correspondente. Os dados enviados de um

dispositivo para outro podem usar a chave pública do dispositivo para criptografar os dados com a garantia de que apenas o dispositivo destino (que possuir a chave privada correspondente) será capaz de decodifica-los.

Como a chave pública é de conhecimento de todos, inclusive de espiões, não é possível ter certeza de que uma mensagem se originou de uma fonte válida. Para resolver esse problema, o remetente da mensagem deve criar (por exemplo) um resumo Hash para a mensagem e, logo depois, criptografa-lo com sua própria chave privada. Desta forma, tanto a autenticidade quanto a integridade da mensagem seriam asseguradas. A origem da mensagem poderia ser identificada exatamente, fornecendo a propriedade de não-repúdio. Essa técnica é chamada de assinatura digital.

As assinaturas digitais não passam de pedaços de informação que, além de garantir a integridade de uma grande parte da informação, permitem o reconhecimento da entidade que a produziu. Ela baseia-se no fato de que apenas o dono conhece a chave privada e que, se ela foi usada para codificar uma informação, então apenas seu dono poderia ter feito isto. A verificação da assinatura é feita com o uso da chave pública, pois se o texto foi codificado com a chave privada, somente a chave pública correspondente pode decodificá-lo. Como as chaves assimétricas tem uma baixa eficiência, a codificação pode ser feita sobre o Hash e não sobre o conteúdo em si, pois é mais rápido codificar o Hash (que possui tamanho fixo e reduzido) do que a informação toda.

A Tabela 2 apresenta, resumidamente, algumas das principais diferenças entre a criptografia de chave simétrica e a criptografia de chave assimétrica.

Tabela 2: Tabela Comparativa entre Chave Simétrica e Assimétrica [17].

Criptografia de Chave Simétrica	**Criptografia de Chave Assimétrica**
Processo de cifragem é rápido	Processo de cifragem é lento
Processo de administração e partilhamento das chaves é complexo	Processo de administração e partilhamento das chaves é simples
Não fornece Assinatura Digital	Fornece Assinatura Digital

Como especificado mais acima, a segurança da técnica de criptografia de chave assimétrica só é válida quando o conhecimento da chave privada se dá

apenas pela entidade adequada. Portanto é essencial garantir que a chave privada não pode ser proveniente da chave pública no tempo polinomial utilizando um tamanho de chave adequado e algoritmos que sejam baseados em: fatorização de números inteiros, logaritmos discretos e curvas elípticas. A Tabela 3 apresenta alguns dos principais algoritmos de criptografia de chave assimétrica.

Tabela 3: Principais Algoritmos de Criptografia de Chave Assimétrica [17].

Algoritmo	**Definição**
RSA	Desenvolvido por Ron Rivest, Adi Shamir e Len Adleman, RSA é um algoritmo assimétrico criado em 1977 no MIT. É o algoritmo de chave pública mais usado no mundo atualmente. É uma das mais bem sucedidas formas de criptografias chave assimétrica conhecidas até o presente momento. Utiliza números primos na cifragem. O princípio por trás do RSA consiste na simplicidade de multiplicar dois números primos para obter um terceiro número, mais extremamente difícil retomar os dois primos a partir do terceiro número. Isso é popularmente denominado como fatoração. A segurança do RSA se fundamenta na complexidade de fatorar números grandes. Desta forma, a fatoração reflete um limite superior do tempo essencial para quebra o algoritmo.
ElGamal	O ElGamal é um algoritmo de chave pública para administração de chaves. Sua matemática é diferente do RSA, mas também é um sistema equivalente. Envolve domínio matemático de grandes quantidades numéricas. O ElGamal consegue sua segurança através da complexidade de calcular logaritmos discretos em um corpo finito, o que é bastante comum com o problema da fatoração.
Diffie-Hellman	Esse algoritmo é baseado no problema do logaritmo discreto. É a técnica criptográfica de chave pública mais antiga ainda em uso. A concepção de chave pública foi integrada a esse algoritmo somente em 1976, contudo, ele não permite ciframentos e assinatura digital. Esse algoritmo foi desenvolvido para permitir que dois indivíduos entrassem em acordo ao partilharem

	privacidades tal como uma chave, ainda que eles apenas permutem mensagens de maneira pública.
Curvas Elípticas	Definido abaixo no Capitulo 3.5.3.1

3.5.3.1 Criptografia de Curva Elíptica

A criptografia de chave assimétrica expressa uma inconveniência que é ser várias ordens de grandeza mais lenta se comparada a técnica de chave simétrica [21]. Em chaves simétricas a chave cresce linearmente com a velocidade de processamento, já em chaves assimétricas, o mesmo não ocorre, ou seja, se não considerarmos técnicas baseadas em curvas elípticas (ECC). Algoritmos de curvas elípticas são descritos como ideais para aplicações embutidas, devido a diminuição de requisitos de velocidade de processamento e memória se comparado as técnicas de fatoração de inteiros e logaritmos discretos. Enquanto essas técnicas tem uma complexidade sub-exponencial, a ECC é totalmente considerada exponencial [22]. Relações entre tamanho de chaves (em bits) podem ser evidenciadas na Tabela 4.

Tabela 4: Tamanhos de chaves para fornecer segurança em diferentes técnicas [23].

Chave simétrica	**ECC**	**RSA/DH/DSA**
80	163	1024
128	283	3072
192	483	7680
256	571	15360

ECC é uma escolha de fato quando se considera o uso de técnicas assimétricas para proteger dispositivos restritos. As execuções necessitam de menos memória e funcionam muito mais rapidamente (e com a diferença aumentando à medida que aumenta o tamanho da chave) [24]. No entanto, ela é mais lenta do que muitas técnicas de chave simétricas disponíveis. Porém, isso não quer dizer que a criptografia de chave pública deve ser descartada, simplesmente deve se considerar as vantagens e desvantagens ao decidir entre os dois.

A criptografia de chave assimétrica pode ser usada, por exemplo, para distribuição de chaves (e posteriormente usar algoritmos simétricos) para prevenir o uso excessivo de chaves e assim resolver o problema de distribuição de chaves. Vale notar que mesmo no mundo de computadores, sempre que ocorre transmissão de dados periódica e esporádica, o uso exclusivo de métodos assimétricos não é nada comum. Em dispositivos IoT restritos ou mesmos poderosos (porém, com muito menos recursos do que um computador normal) não há razões para que isso aconteça, a menos que o não-repudio seja uma imposição.

3.5.4 Criptografia e Encaminhamento

A comunicação entre dispositivos pode ser realizada de duas formas: realizada diretamente entre um dispositivo e um *gateway* (ou simplesmente entre dois dispositivos) ou ser realizada através do uso de outros nós no caminho de roteamento da rede. Conforme elucidado previamente, apenas criptografia não é o bastante para eliminar as ameaças, também é necessário um projeto cuidadoso de protocolos. Valido que qualquer protocolo projetado com intuitos de segurança, assim como o encaminhamento dos mesmos, só irão considerar mensagens que que a fonte possa ser autenticada.

Todos os dispositivos que fazem parte do processo de roteamento, devem estar preparados com medidas para fazer a validação das mensagens que recebem. As mensagens que não são validadas nesse processo, são imediatamente descartadas. Na prática, isso quer dizer que usando criptografia simétrica pelo menos um segredo compartilhado será usado e na criptografia assimétrica um par de chaves pública/privada por dispositivo. Não teria fundamento ter uma chave privada comum entre dispositivos, uma vez que eles não seriam considerados privados.

Duas situações podem ser concebidas entre uma única chave simétrica conhecida por todos os dispositivos e uma chave/par única para cada nó no caminho de roteamento. A primeira tem a desvantagem de permitir o sucesso em comprometer um único nó e a obtenção de sua chave secreta é igual a obtenção da

chave secreta usadas por todos os nós restantes no caminho de roteamento. Já a segunda leva a um cenário particularizado entre criptografia simétrica e assimétrica:

- No caso de uso de criptografia simétrica, se houver existência de uma única chave compartilhada entre pares, apenas o próximo salto no caminho do roteamento será capaz de analisar a autenticidade das mensagens, logo, seria necessário criar uma nova marca de autenticação a cada salto. Isso introduz um atraso maior do que simplesmente verificar a autenticidade da mensagem;
- Já usando a criptografia assimétrica, todos os nós do caminho podem analisar a autenticidade das mensagens, uma vez que, para essa verificação apenas a chave pública é necessária. Entretanto, isso implica na utilização de mais recursos de memória, pois cada dispositivo gerencia outros dispositivos com chaves públicas.

Empregar o roteamento seguro em qualquer cenário é uma tarefa bastante difícil e não poder ser abordado de forma trivial. Os endereços de roteamento devem ser adequados as políticas de segurança e ao cenário em questão, determinado a gravidade de comprometimento que a estrutura de roteamento está sujeita.

4 PRIVACIDADE NO CONTEXTO DA INTERNET DAS COISAS

Neste capítulo é apresentado um estudo sobre as questões de privacidade referentes a grande quantidade de dados disponíveis pela IoT.

4.1 INTRODUÇÃO

Além da segurança, a privacidade merece muita atenção, pois a IoT é capaz de disponibilizar uma coleta variada de dados e informações, para diversos

fins, no cotidiano das pessoas e das organizações, seja em ambientes de usuários privados ou em ambientes de usuários de negócios. A coleta autônoma dos dados e das informações das pessoas torna a privacidade uma das principais preocupações morais em relação à IoT. A discursão sobre os limites da privacidade na internet já é atualmente uma pauta importante e sua importância só tende a aumentar.

Algo a ser discutido em um contexto teórico é a privacidade dos usuários das tecnologias IoT, diante de sua legalidade, explorando possíveis soluções neste cenário ainda em construção. Chabridon et al [25] compreende a privacidade como uma questão essencial que pode enquadrar a implantação da visão IoT seja para os usuários privados ou para organizações.

Chabridon e Weber et al [26], destacam que a privacidade é fundamental para o controle deste novo ambiente complexo. A troca de dados frequente e oculta entre as coisas e as pessoas, e entre as coisas e outras coisas, acontecerá de maneira que os donos e criadores desses dados não sejam caracterizados. A própria grandeza e propensão das novas tecnologias vai ampliar este problema.

4.2 DIREITOS FUNDAMENTAIS DE EXPRESSÃO

Manifestações de pensamento na internet, assim como em qualquer outro ambiente difusor, por exemplo, televisão, jornais ou de forma presencial, encontram sua base no direito à liberdade de expressão. Constantemente o direito de um indivíduo vai colidir diretamente com o direito de outros indivíduos à dignidade, à particularidade e à privacidade. Isso demanda que o tradutor faça uso de uma técnica de ponderação para buscar uma solução adequada ao caso concreto.

Na internet, esses declarados direitos do indivíduo ganham particularidades que trazem princípios diferentes para a ponderação do tradutor, não exatamente pelo conteúdo em si, e sim pela maneira como são desempenhados esses direitos. Isso porque toda informação que é inserida na internet, caso não seja mais tarde deletada, fica permanentemente gravada. Esta informação atinge potencialmente milhões de indivíduos e se tornara de fácil acesso a qualquer um que venha a pesquisar. Assim sendo, uma dada solução a uma situação pode sofrer

uma variação dependendo do ambiente escolhido para seu exercício, podendo ser severa com quem abusa em um ambiente, e em outros, podendo ser mais suave.

O respeito pelos direitos e expectativas de privacidade são fundamentais para a construção da confiança na internet, bem como influenciar a capacidade dos indivíduos se comunicarem de maneira significativa. Esses direitos são, em muitas vezes, agregados em análise de dados morais, o que faz elevar a importância em se manter o respeito às expectativas de um indivíduo e o uso justo de seus dados [27]. A IoT pode incitar as expectativas tradicionais de privacidade.

4.3 PRINCIPIOS DE PRIVACIDADE NA INTERNET DAS COISAS

A privacidade é um direito fundamental presente na Declaração Universal dos Direitos Humanos e na Constituição da República de 1988. Privacidade relaciona-se com tudo a que um indivíduo não tem a intenção de que seja conhecido pelo público, exclusivamente a aqueles que fazem parte da sua esfera de contato pessoal. É uma expressão que sugere um elevado número de conceitos e ideias. Pode também ser associada com a percepção de um indivíduo que controla o acesso a suas informações particulares. Weber et al [28] identificam três áreas associadas à privacidade, sendo elas:

- O espaço físico, que pode ser caracterizado como uma proteção contra objetos malquistos ou sinais, nesta acepção o termo privacidade está mais relacionado a segurança da infraestrutura;
- O poder de tomada de decisão em associação ao fluxo de dados com a intenção de proteger a liberdade de um indivíduo a fazer as próprias escolhas em relação aos seus dados;
- O controle de um indivíduo sobre o processamento da informação compreendendo a aquisição, exposição e aplicação das informações pessoais;

No atual mundo da comunicação e informação, não é mais plausível preservar a privacidade através do isolamento da informação. Nas circunstâncias de um ambiente inteligente IoT, as aplicações se transfiguram de fácil usabilidade e as informações são dispostas muitas vezes de maneira invisíveis. Sendo assim, a

privacidade é geralmente concebida pelos usuários como uma promessa de se situar em um estado de proteção. Seguindo a essa linha de pensamento, Marx e Murky et al [29] caracterizaram quatro níveis de privacidade percebível pelas pessoas, e que definem a maneira como estas enxergam as violações de privacidade. Estes níveis são identificados como fronteiras e são descritos abaixo:

- A fronteira natural que impede a presença, sentimentos e/ou emoções não sendo reparados através de um dos sentidos humanos. Portas, paredes, roupas, cartas seladas, telefone e e-mail representam fronteiras naturais para observação;
- A fronteira da sociedade que envolve expectativas que as pessoas com certos papéis sociais como médicos, advogados, engenheiros e outros profissionais não irão divulgar informações sigilosas a eles fornecidas pelas pessoas envolvidas;
- A fronteira espacial ou temporal que faz a separação da informação dos vários períodos ou particularidades da vida da pessoa;
- A fronteira dos efeitos efêmeros ou transitórios que se fundamenta na ideia de que a interação e a comunicação são efêmeras e transitórias como ações que se espera, sendo facilmente esquecidas em um curto período de tempo;

Na grande rede de dispositivos conectados pela IoT, é correto entender que parte desses dispositivos são projetados para a coleta de dados no ambiente em que está inserido, e nessa coleta, regularmente são incluídos dados relacionados a pessoas. Esses dados coletados podem fornecer benefícios tanto ao proprietário do dispositivo quanto ao fabricante ou fornecedor do mesmo.

Combinações complacentes de fluxos de dados IoT também podem afetar a privacidade. Uma imagem digital mais invasiva de um indivíduo pode ser alcançada através da combinação e correlação de dados individuais coletados do mesmo, quando comparado a um fluxo de dados IoT individual sem essa combinação. Este efeito pode ser especialmente importante em relação aos dispositivos IoT, pois muitos produzem dados extras como data, hora, informações de localização, o que consequentemente adiciona mais particularidades sobre o usuário.

Há situações em que o usuário também pode não saber que um determinado dispositivo IoT está coletando dados sobre ele e partilhando com outros

indivíduos. Um indivíduo pode estar na presença de um dispositivo desse tipo, sem saber que sua conversa ou atividade está sendo monitorada e seus dados coletados. Esses recursos podem possibilitar benefícios a um indivíduo que sabe da existência desse dispositivo. Todavia, para aqueles que não sabem da existência desse dispositivo e não tem influência em como a informação coletada vai ser usada, grandes problemas de privacidade podem surgir para este indivíduo.

Independente se o usuário está ciente e permite a coleta e análise de seus dados, estas condições enfatizam o valor desses fluxos de dados particularizados para empresas e organizações que buscam sempre coletar e capitalizar informações provenientes de dispositivos IoT. A procura por estas informações relata os desafios legais e constantes que que vão de encontro as leis de proteção e privacidade de dados.

Esses problemas de privacidade apresentados acima são indispensáveis para debater porque eles têm consequências sobre os direitos básicos e sobre a capacidade coletiva dos indivíduos confiarem na internet. Indivíduos reconhecem que sua privacidade é intimamente preciosa, e tem perspectivas sobre quais informações podem ser coletadas e como outras partes processam esses dados.

Esse discernimento de privacidade é verídico para as informações coletadas pelos dispositivos IoT. Contudo, estes mesmos dispositivos podem influenciar negativamente a capacidade do usuário para expressar e estabelecer propensões de privacidade. Se os usuários perdem confiança na internet, devido ao fato de que suas propensões de privacidade não estejam sendo satisfeitas na IoT, então consequentemente os usuários podem deixar de usar a internet.

4.4 A PRIVACIDADE E A INTERNET DAS COISAS

A privacidade pode ser caracterizada como uma das principais preocupações éticas que usuários têm em relação à IoT. Segundo Miorandi et al [30], essa preocupação pode consequentemente impor limites à implementação da visão IoT. A administração deste novo ambiente complexo e a transação de dados invisíveis entre as coisas e as pessoas e entre as coisas e outras coisas, deve acontece de forma anônima, sem a consciência dos donos e criadores desses

dados. A grande massa de dispositivos IoT assim como as inúmeras capacidades que as novas tecnologias possuem vão aumentar ainda mais esse problema. Processar as informações coletadas por todos os dispositivos conectados que compõem o ambiente IoT é uma tarefa chave para desenvolver essa nova realidade [25].

Nenhuma definição que a privacidade possa assumir é capaz de atender a todos os aspectos que são compreendidos por ela. Todavia, existem várias formas de privacidade que propõem uma taxonomia. Essa taxonomia de privacidade representa uma perspectiva das atividades que podem conduzir a sua violação. São elas [31]:

- Coleta de informação que envolve atividades de violação de privacidade no momento da coleta de dados sobre um indivíduo ou grupo de indivíduos. Cobranças forçadas ou interrogatórias podem levar a uma violação de privacidade, mesmo que esses dados tenham sido coletados com o consentimento do indivíduo.
- O processamento da informação que envolve atividades prejudiciais à privacidade a partir do processo de armazenamento, manipulação e utilização dos dados sobre indivíduos.
- A disseminação da informação que envolve atividades de divulgação, exposição e disseminação de informações sobre indivíduos. Quando realizadas pode incorrer no estrapolamento da confidencialidade.
- Por último a invasão que envolve atividades de invasão à privacidade de indivíduos. Pode ocorrer através de acesso intrusivo e através de interferências decisórias;

Embora esta taxonomia almeja ser utilizada como um meio para a proteção legal, ela também é capaz de ser produtiva para as tecnologias [32]. Provedores de tecnologias devem examinar se algum software ou tecnologia pode contribuir para o aumento das chances de tal problema ocorrer, e trabalhar no desenvolvimento de soluções para amenizar essas chances.

Cuidados com a privacidade são atenuados pela maneira como a IoT expande a sua efetividade e o alcance da vigilância e rastreamento. A forma que estes dispositivos são utilizados em conjunto com suas características redirecionam a discussão sobre as questões inerentes a privacidade na IoT. Dispositivos IoT

acabam alterando a maneira de como as informações pessoais são coletadas, processadas, utilizadas e conservadas.

O habitual paradigma de privacidade online onde usuários podem afirmar suas propensões de privacidade interagindo diretamente com as informações que são apresentadas em um computador ou tela de celular, selecionando por exemplo uma opção “Aceito” ou “Concordo”, não é comumente válida na IoT. Constantemente dispositivos IoT não apresentam telas de configuração de privacidade ao usuário. Em muitas destas configurações IoT, os usuários não sabem ou não tem nenhum tipo de controle em como os seus dados pessoais são coletados ou processados. Isso consequentemente cria um abismo entre as perspectivas de privacidade do usuário e a conduta dos dispositivos IoT na hora da coleta dos dados.

Na hipótese de que um instrumento eficaz possa ser concebido para permitir a um usuário expressar a autorização de suas escolhas de privacidade aos dispositivos IoT, esse instrumento precisara atender a grande quantidade de dispositivos IoT que um mesmo usuário pode controlar. Um usuário não irá interagir diretamente com cada dispositivo IoT que encontrar ao longo do dia para expor suas escolhas de privacidade. Ao contrário, os instrumentos de interface de privacidade precisam se adaptar ao tamanho do problema IoT, e ainda devem ser amplos e funcionais ao ponto de vista do usuário.

A IoT pode ameaçar as pretensões de privacidade que um indivíduo tem em situações comuns. Entretanto, existem normas sociais e expectativas de privacidade que se diferenciam em espaços públicos e privados. Entretanto, os dispositivos IoT desafiam essas normas e expectativas. Por exemplo, expectativas de privacidade de um indivíduo em espaços considerados públicos, estão sendo desafiados pelo aumento do monitoramento nesses espaços.

Uma análise aplicada a dados pessoais apresenta um grande risco de invasão de privacidade. Este risco é aumentado na IoT devido a maior proporção e intimidade na coleta destes dados pessoais. Os dispositivos IoT podem fazer a coleta dessas informações sobre os indivíduos, sem que anteriormente seja criado um grau de especificidade e penetração. O refinamento da tecnologia IoT pode consequentemente criar situações em que o indivíduo seja exposto a danos físicos, criminais, financeiros ou de reputação.

A grande maioria dos dispositivos IoT podem ser encontrados em muitos lugares e tem uma familiaridade e um envolvimento social com o ambiente. Eles podem criar uma falsa impressão de segurança e instigar os indivíduos a divulgarem informações pessoais sem total percepção das consequências que essa divulgação pode lhe trazer.

Como a IoT é capaz de desafiar as noções de privacidade habituais, existem muitas questões que devem ser reavaliadas nos modelos de privacidade online no contexto da IoT. Dados pessoais tem um alto valor pessoal e comercial e as fontes e coletores podem enxergar esse valor de forma diferente. Ambas as partes podem ter interesses genuínos que podem ser conflitantes. Estes interesses devem ser expressos de forma que atente a regras que sejam justas tanto para as fontes quanto para os coletores.

Políticas e práticas de privacidade devem ser disponibilizadas e facilmente compreendidas no contexto da IoT. Devem existir maneiras alternativas ao modelo tradicional em que os usuários podem afirmar suas propensões de privacidade interagindo com um computador ou celular e que nem sempre pode ser possível a um dispositivo IoT. Normas e expectativas de privacidade que quase sempre estão intimas ao contexto social e cultural do indivíduo, podem variar de um determinado grupo ou nação para outro. Muitos cenários em que são implantados dispositivos IoT, cruzam fronteiras sociais e culturais. Isso terá um peso importante no desenvolvimento de modelos de proteção à privacidade aplicáveis a IoT.

Outra importante prática é conciliar requisitos de funcionalidade e privacidade nas diferentes fases de desenvolvimento e operação de um produto IoT. Fabricantes devem aspirar que seus produtos e práticas de respeito à privacidade tragam satisfação, confiança e fidelidade por parte dos usuários. Devesse sempre proteger os dados recolhidos pelos dispositivos IoT que parecem não ser pessoais no momento da coleta, pois estes podem eventualmente ser tornarem dados de natureza pessoal.

A IoT cria desafios únicos à privacidade. Desafios que não estão dispostos nas questões de privacidade de dados que existem atualmente. Portanto, é necessário desenvolver políticas e práticas para atender as escolhas de privacidade individuais de cada indivíduo em uma ampla visão de expectativas, ao mesmo tempo em que possibilita inovações no campo tecnológico da IoT.

5 INFRAESTRUTURA, A INTERNET EM PROCESSO DE TRANSIÇÃO

Neste capítulo é apresentado um estudo sobre as questões de infraestrutura que surgirão com a implantação da tecnologia IoT.

5.1 INTRODUÇÃO

A IoT torna possível uma vasta quantidade de aplicações. Muitos equipamentos e dispositivos do cotidiano do cotidiano estão (ou estarão) conectados à internet, como geladeiras, óculos, relógios, carros, elevadores, etc. Entretanto, essa tecnologia gera uma grande demanda de recursos de comunicação e consequentemente precisa de uma boa infraestrutura.

Com toda a usabilidade proporcionada pela IoT, aparecem inúmeros projetos para unificar a IoT envolvendo a indústria, entidades acadêmicas e de pesquisa e órgão reguladores e de padronização de todo o mundo. Contundo, ainda que várias empresas desenvolvam diferentes tipos de protocolos, todos estes utilizarão a internet como rede de comunicação para conduzir as várias informações que esses dispositivos irão gerar.

5.2 DESAFIOS E OBSTÁCULOS DA INTERNET DAS COISAS

Vários obstáculos tem o poder de retardar o desenvolvimento da IoT. Entre eles, os três maiores são: a implantação do IPv6, a alimentação dos sensores e um acordo entre padrões. Estes três tópicos são discutidos abaixo:

5.2.1 Implantação do IPv6

Os protocolos IP e TCP (Transmission Control Protocol) são os principais dentre todo o conjunto de protocolos que direcionam o funcionamento da internet. Um protocolo IP é uma combinação numérica que estabelece conexões entre computadores. O IP é responsável pelo roteamento e encaminhamento das informações a serem enviadas em uma rede [32]. Todavia, não possui nenhuma responsabilidade em manter a integridade dos dados enviados.

IPv4 significa *Internet Protocol version* 4 e permite que computadores, *smartphones*, *tablets* ou outros aparelhos se conectem à internet. Cada aparelho que estiver *online* receberá um código único, que o possibilitará de enviar e receber dados de outros que estiverem conectados. O protocolo IPv4 possui um endereço na internet com um comprimento de 32 bits possibilitando cerca de 4 bilhões de endereçamentos possíveis. Estes endereços são descritos em notação decimal onde cada *byte* é separado por um ponto, por exemplo, 292.174.227.227.

A cada dia novos tipos de serviços surgem na internet e com o IPv4 será impossível atribuir endereços IP a todos esses serviços e dispositivos. A única solução para o continuo crescimento da internet é o uso do protocolo IP na versão 6 ou IPv6 (*Internet Protocol version* 6). O protocolo IPv6 possui um endereço na internet de 128 bits, além da introdução de uma notação hexadecimal com 8 palavras e de 16 bits cada, por exemplo: 2016:7b:b070:cde0: 6497:4001:7777:7ab1. Além disso, o IPv6 facilita o gerenciamento de redes devido a recursos de autoconfiguração e oferece recursos de segurança aprimorados [33]. A Tabela 5 apresenta algumas das principais diferenças entre os protocolos IPv4 e IPv6.

Tabela 5: Diferença entre os protocolos IPv4 e IPv6 [34]

IPv4	**IPv6**
Endereço de 32 bits (*4 bytes*) de comprimento	Endereço de 128 bits (*16 bytes*) de comprimento
IPSec é opcional e deve ser suportado externamente	O suporte IPSec não é opcional
Cabeçalho não identifica o fluxo de	Cabeçalho contém campo de etiqueta de

pacotes para a manipulação de QoS por roteadores	fluxo, que identifica o fluxo de pacotes para o tratamento de QoS por roteador
Processo de fragmentação realizada pelo roteador	A fragmentação deixa de ser realizada pelos roteadores e passa a ser processada pelos *host*s emissores
O cabeçalho inclui os campos de opção	Todos os campos de opção foram mudados para dentro do campo *extension header*
O protocolo ARP utiliza requisitos do tipo Broadcast.	O ARP foi abandonado, sendo substituídos pelas mensagens *Neibhbor Discovery*
O IMGP (*Internet Group Management Protocol*) é utilizado para gerir relações locais de sub-redes	O IGMP foi substituído por mensagens *Multicast Listener Discovery*
Os Endereços de *Broadcast* são utilizados para enviar tráfego para todos os *hosts* de uma rede	Deixa de existir o endereço de *Broadcast*, para utilizar endereços *Multicast*
O endereço tem de ser configurado manualmente	Adição de funcionalidades de autoconfiguração
Suporta pacotes de 576 bytes, passiveis de serem fragmentados	Suporta pacotes de 1280 bytes, sem fragmentação

Atualmente o IPv6 ainda não está sendo largamente usado na internet e o esgotamento do IPv4 já é uma realidade. Existe a necessidade de implantação do IPv6, pois a internet não para de evoluir, e novos usuários acabam ainda necessitando de protocolos IPv4, mas sem endereços IPv4 livres para atendê-los. Desta forma, novas técnicas auxiliares acabam sendo desenvolvidas para permitir a conexão desses usuários e a transição para o IPv6, tão essencial para o desenvolvimento da IoT, acaba acontecendo de forma lenta.

5.2.2 Alimentação dos Sensores

Um dos dispositivos obrigatórios para emprego na camada de percepção da infraestrutura para IoT é o sensor, ou comumente conhecido como nó de sensor, elemento minúsculo e autônomo que é o encarregado pela captura e comunicação dos dados físicos do ambiente [35].

Um sensor é fundamentalmente um dispositivo eletrônico, leve e pequeno, que tem capacidade de processamento, com reduzida memória, equipado com memória flash ou EEPROM, de sistema operacional simples e pequeno, com uma frágil unidade de transmissão/recepção, bateria ou item de captação de energia, e alternativamente, um modulo de locomoção [36].

Uma WSN (*Wireless Sensor Network*) é uma rede de sensores sem fio composta por uma grande quantidade de sensores dispersos em um ambiente físico, sem apoio de qualquer infraestrutura física sólida. A dispersão destes sensores no ambiente pode depender dos requisitos da aplicação e do espaço delimitado de interesse. A disposição dos sensores no ambiente, fixos ou móveis, influencia diretamente no protocolo de roteamento dos sensores e consequentemente no consumo de energia [36].

Kurami et al [37], afirma que alguns obstáculos ainda necessitam ser superados, entre os quais, tem destaque a segurança e a privacidade das informações, pois elas podem influenciar consideravelmente no aumento de consumo e sobrecarga de processamento em um WSN.

Desta forma, para que a IoT seja capaz de atingir todo o seu potencial, os sensores precisam ser autossustentáveis. Seria um trabalho extremamente difícil e de alto custo trocar baterias de bilhões de dispositivos espalhados por todo o mundo ou até mesmo no espaço. O que é necessário para solucionar este problema são sensores equipados para gerar eletricidade a partir de elementos ambientais, como vibrações, luz solar e fluxo de ar [38].

5.2.3 Interoperabilidade

Na internet tradicional, a interoperabilidade é o valor mais primordial. O requisito preliminar da conectividade com a internet é que os sistemas “conectados” possam se comunicar utilizando um mesmo “sistema” de protocolos e codificações. A interoperabilidade é tão fundamental no ramo da computação e da internet, que os primeiros *Workshops* para fornecedores de equipamentos de internet eram chamados de “*Interops*” [39].

Em um ambiente inteiramente interoperável, todo dispositivo IoT seria apto a se conectar com qualquer outro dispositivo ou sistema para transferência de informações. Entretanto, a interoperabilidade entre dispositivos é muito mais complexa. Uma interoperabilidade entre sistemas e dispositivos IoT acontece em critérios diversos em camadas distintas dentro da pilha de protocolos de comunicação entre os dispositivos. Além disto, a interoperabilidade total em todas as particularidades de um produto nem sempre é desejável, necessária ou viável. E caso esta interoperabilidade total for proposta artificialmente, poderia acarretar em influências negativas ao investimento e a inovação tecnológica.

A adoção e padronização de protocolos que especializam particularidades de comunicação, incorporando onde é ideal ter padrões, é um dos pontos principais em discursões sobre a interoperabilidade na IoT. A interoperabilidade dos dispositivos IoT, caso ocorra de maneira bem definida e eficiente, pode impulsionar a inovação e possibilitar produtividade aos fabricantes de dispositivos IoT. Além do mais, a implementação das regras já existentes e o desenvolvimento de novos padrões livres, ajudam a diminuir barreiras e simplifica novos modelos de negócio.

Interoperabilidade, padrões, protocolos e convenções são uma dificuldade primordial no desenvolvimento e adesão prematura de dispositivos IoT. Numa última análise, o desafio de desenvolver e utilizar padrões de interoperabilidade é primordial para o debate da inovação, concorrência e definição de serviços pelos usuários [40].

Embora haja atualmente grandes progressos nas áreas de normas técnicas, ainda não é o suficiente, em especial nas áreas que envolvem segurança, privacidade, arquitetura e comunicações. A IEEE é umas das organizações que

trabalham para resolver esses desafios assegurando, por exemplo, que pacotes IPv6 possam ser roteados em diferentes tipos de redes.

É importante salientar que embora existem obstáculos e desafios, eles não são insuperáveis. Considerando as vantagens da IoT, esses impasses podem ser solucionados. É apenas uma demanda de tempo.

5.3 PRINCIPAIS TECNOLOGIAS UTILIZADAS

Este Capítulo vai abordar o conhecimento básico à implementação e desenvolvimento da tecnologia IoT. Para tal fim, algumas das principais tecnologias utilizadas no desenvolvimento dos projetos mais comuns da IoT serão discutidas. Vale lembrar que outra tecnologia fundamental para o desenvolvimento da IoT é a computação em nuvem, que foi discutida no Capitulo 2.3.

5.3.1 Padrão IEEE 802.15.4

Redes pessoais estão vigentes em nosso cotidiano. As redes de computadores ligadas à internet, estruturas de telefonia estão presentes em várias casas atualmente. Entretanto, cada umas destas redes pessoais estão isoladas com uma infraestrutura própria. É necessária uma estruturação em uma rede sem fio de área pessoal (*Personal Area Networks* – PAN) para que essas aplicações possam utilizar uma mesma rede e se conectar à internet. O padrão conhecido como IEEE 802.15.4 é um dos padrões definidos para estas redes [41].

O padrão IEEE 802.15.4 caracteriza a camada física e realiza o controle de acesso para as redes sem fio pessoais (*Wireless Personal Area Network* – WPAN) de baixa propagação, também conhecidas como LoWPAN (*Low power Wireless Personal Area Networks*). Ele pretende disponibilizar os princípios fundamentais para as camadas inferiores do tipo PAN e LoWPAN. Uma extensa fração destes dispositivos são portáveis ou moveis com amplitude pequena de

bateria e atuam em áreas de operação próximas a 10 metros. Segundo Callaway et al [42], este padrão estabelece uma taxa de transmissão máxima de 250 Kbps.

O padrão IEEE 802.15.4 possui dois padrões de dispositivos, um com implementação completa (*Full Function Device* – FFD) e outro com funções reduzidas (*Reduced Function Device* – RFD). O FFD é preparado para estruturar uma PAN, fazendo a comunicação com qualquer dispositivo da rede. Como o FFD implementa um protocolo completo, é capaz de operar em qualquer topologia de rede. Já o RFD possui uma implementação simplificada, não sendo capaz de estruturar uma PAN. Ele é restringido a ser nós folha em uma topologia de rede mais complexa [42].

5.3.2 Protocolo 6LoWPAN

6LowPAN é um acrônimo para *IPv6 over Low power Wireless Personal Area Network*. O 6LowPAN permiti que pacotes IPv6 sejam transmitidos sobre redes sem fio pessoais com limitações de potência e restrições de taxa de transmissão, como as definidas pelo padrão IEEE 802.15.4 [43]. Segundo Vasseur, et al [44] está integração é a chave para uma nova realidade de aplicações, uma vez que o 6LowPAN permiti o uso do IPv6 em dispositivos restritos a baixos consumos de energia e de banda de internet.

Ko et al [45] afirma que é essencial preservar uma pilha IPv6 poderosa que opere em redes remotas de recursos restritos. Desta forma, uma camada 6LowPAN é um requisito primordial para a infraestrutura de uma rede de sensores. Hui & Thubert et al [46] ainda reiteram que é primordial um encolhimento dos cabeçalhos do IPv6 para que haja uma administração adequada dos recursos remotos.

O 6LoWPAN é fundamentado em tecnologia IP que já é extensivamente disseminada, com isso ele pode usufruir das ferramentas de diagnóstico e gerenciamento de redes IP que existem atualmente. São facilmente conectados a outras redes IP sem o auxílio de tradutores ou proxies, utilizando desta forma toda a estrutura já desenvolvida para as redes IP. O desenvolvimento deste protocolo já pode ser classificado uma tecnologia IoT.

5.3.3 Protocolo RPL

O RPL (*Routing Protocol for Low power and Lossy Networks*) é um protocolo para roteamento em redes de com perdas e baixo consumo de energia. Seu objetivo é prover um roteamento eficaz de caminhos para três padrões de tráfego: ponto-a-ponto, ponto a multiponto e multiponto a multiponto [47].

Redes com baixo consumo de energia e perdas são constituídas por uma ampla quantia de nós restritos. Esses nós restritos possuem links frágeis e instáveis que geralmente sustentam baixas taxas de transferência de dados e que os padrões de tráfego nem sempre são ponto-a-ponto [48].

O RPL constrói suas rotas e topologia em intervalos aleatórios. A topologia é a base de funcionamento do protocolo RPL, que usa a topologia como um Grafo Acíclico Direcionado (*Directed Acyclic Graph* – DAG) para criação de um ou mais destinos orientados (*Destination Oriented DAGs* – DODAGs), que por sua vez podem estar relacionados a uma ou mais instancias de RPL [47].

5.3.4 Protocolo CoAP

O CoAP (*Constrained Application Protocol*) é um protocolo de transferências web especializado para uso em redes restritas tipicamente comuns na IoT. O CoAP suporta um modelo cliente/servidor baseado numa arquitetura REST, onde os recursos são gerenciados no servidor e são diferenciados por uma URI universal. Transações CoAP fazem uso de quatro tipos diferentes de mensagens: CON (*confirmable*), NON (*non-confirmable*), ACK (*Acknowledgment*) e RST (*reset*). Clientes do CoAP manipulam recursos usando os métodos GET, PUT, POST e DELETE. Ele também fornece suporte construído com a descoberta de recursos como parte do protocolo [49].

CoAP possibilita o uso de cache e de uma forma simples de *proxy* com suporte a transações, suporte a URLs e suporte a transmissões UDP. Ele implementa uma camada de aplicação leve, que conta com pequenos tamanhos de mensagens, gerenciamento eficiente e sobrecarga leves, ideias para dispositivos de

baixa potência e pouca memória. O CoAP tem alguns de seus métodos semelhantes a métodos HTTP [49].

6 CONCLUSÕES E TRABALHOS FUTUROS

Chegando a final do trabalho e fazendo uma análise de cada assunto abordado, pode-se dizer que a Internet das Coisas está revolucionando não somente a internet, como também a vivência das pessoas e a sua interação com os objetos presentes no cotidiano. A cada dia a Internet das Coisas se populariza ainda mais entre desenvolvedores, profissionais de TI, usuários finais, pequenas e medias empresas, com a intenção de viabilizar negócios e abrir campos para desenvolvimento de novos produtos e novas áreas de interesse. Conclui-se ainda que há uma série de desafios tecnológicos e informacionais que devem ser estudados e ajustados para possibilitar um funcionamento adequado da Internet das Coisas.

A internet das coisas já tem apresentado inúmeros projetos importantes. Sua tecnologia vem buscando soluções que sustentam um enorme potencial de desenvolvimento. Dentro deste contexto, diversas pesquisas vem sendo desenvolvidas e fortalecendo vertentes, dando origem a um vasto ambiente de favoráveis resultados para a transformação da informação em rede. Portanto, a internet das coisas é uma tecnologia que desponta para impactar e revolucionar o mundo.

REFERÊNCIAS BIBLIOGRÁFICAS

1. Khan, R.; Khan, S. U.; Zahher, R.; Khan, S., “Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges”. 10th International Conference on Frontiers of Information Technology (FIT), pp. 257-260, 2012.
2. Leiner, B. M.; Cerf, G. V.; Clark, D. D.; Kahn, E. R.; Kleinrock, L.; Lynch, C. D.; Postel, J.; Roberts, G. L.; Wolff, S. S. “The past and future history of the Internet”. Communications of the ACM, 40 (2): pp. 102-108, 1997.
3. Weiser, M., “The Computer for the 21st Century”. SIGMOBILE Mob. Comput. Comun. Rev., New York, NY, USA, v. 3, pp. 3-11, 1999.
4. ITU-T. Overview of the Internet of Things. SERIES Y: Global Information Infrastructure, Internet Protocol Aspects and Next Generation Networks - Frameworks and functional architecture models, ITU-T REc.Y.2060, 2012.
5. Atzori, L.; Iera, A.; Morabito, G. “The internet of things: A survey”. Computer Networks, v. 54, no. 15, pp. 2787-2805, 2010.
6. Buyya, R.; Yeo, C. S.; Venugopal, S.; Broberg, J.; Brandic, I. “Cloud computing and emerging it platforms: Vision, hype and reality for delivering computing as the 5th utility”. Future Generation Computer Systems, 2009.
7. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A. D.; Katz, R. H.; Konwinski, A.; Lee, G.; Patterson, D. A.; Rabkin, A.; Stoica, I.; Zaharia, M. “Above the clouds: A berkeley view of cloud computing”. Technical report, EECS Department, University of California, Berkeley, 2009.
8. Mell, P.; Grance, T., “The NIST definition of cloud computing”. NIST – National Institute of Standards and Technology, 2009.
9. Tschofenig, H., et al, “Architectural Considerations in Smart Object Networking”. Tech. no. RFC 7452. Internet Architecture Board, Mar. 2015. Web. https://www.rfc-editor.org/rfc/rfc7452.txt
10. Kalita, H. K; Kar, A. “Wireless sensor network security analysis”, International Journal of Next-Generation Networks, vol. 1, no. 1, pp. 87-115, 2009.
11. Walters, J. P.; Liang, Z.; Shi, W.; Chaudhary, V., “Wireless sensor network security: a survey,” in book chapter of security”, in Distributed, Grid, and Pervasive Computing, Yang Xiao (Eds, CRC Press), 2007.

12. Nibaldi, G. H., “Specification of a Trusted Computing Base (TCB)”, MITRE CORP BEDFORD MA, Tech. Rep., Nov. 1979.
13. NASA, NASA automated information security handbook, 2410.9A, Jun. 1993.
14. Delfs, H.; Knebl, H., “Introduction to Cryptography: Principles and Applications”, 2nd ed., ser. Information Security and Cryptography. Springer, pp. 01-03, 2007.
15. D’Agostino, S. A.; Engberg, D.; Sinko, A., “The roles of authentication, authorization & cryptography in expanding security industry technology”, Security Industry Association (SIA), Tech. Rep., Dec. 2005.
16. Zúquete, A., “Segurança em Redes Informáticas”, 3rd ed. FCA, pp. 38-60, 2010.
17. Oliveira, R. R., “Criptografia tradicional simétrica de chave privada e criptografia assimétrica de chave pública: análise das vantagens e desvantagens”. Nitéroi: Trabalho de pós-graduação Criptografia e Segurança em Redes da UFF, 2006.
18. Black, J. J. R., “Message authentication codes”, PhD thesis, University of California, Davis, pp. 19-28, 2000.
19. Zúquete, A., “Segurança em Redes de Informáticas”, 3rd ed. FCA, pp. 65-67, 2010.
20. Bellare, M.; Guérin, R.; Rogaway, P., “XOR MACs: new methods for message authentication using finite pseudorandom functions”, in Advances in Cryptology — CRYPT0’ 95, pp. 15-28, 1995.
21. Wollinger, T.; Guajardo, J.; C. Paar, C., “Cryptography in embedded systems: an overview”, in Proceedings of the Embedded World 2003 Exhibition and Conference, pp. 735-744, 2003.
22. Vanstone, S., “Next generation security for wireless: elliptic curve cryptography”, Computers & Security, vol. 22, no. 5, pp. 412-415, 2003.
23. Gupta, V.; Gupta, S.; Chang, S.; Stebila, D., “Performance analysis of elliptic curve cryptography for SSL”, in Wise 02 Proceedings of the 1st ACM workshop on Wireless security, pp. 87-94, 2002.
24. Gura, N.; Patel, A.; Wander, A.; Eberle, H.; Shantz, S. C., “Comparing elliptic curve cryptography and RSA on 8-bit CPUs”, in Cryptographic Hardware and Embedded Systems – CHES 2004, pp. 119-132, 2004.

25. Chabridon, S., “A survey on addressing privacy together with quality of context for context management in the Internet of Things”. Annals of telecommunications-annales des telecommunications, v.69, no. 1-2, pp. 47-62, 2014.
26. Weber, R. H., “Internet of Things – New security and privacy challenges”. Computer Law & Security Review, vol. 26, no. 1, pp. 23-30, 2010.
27. Wilton, R., Position Paper: Four Ethical Issues in Online Trust, CREDS. Issue brief no. CREDS-PP-2.0, Internet Society, 2014.
28. Weber, R. H.; Weber, R., Internet of Things. New York: Springer, 2010.
29. Marx, G.; Murky, T., “Conceptual Waters: The public and the private”. Ethics and Information technology, vol. 3, pp. 157-169, 2001.
30. Miorandi, D., Internet of Things: Vision, applications and research challenges. Ad Hoc Networks, vol. 10, no. 7, pp. 1497-1516, 2012.
31. Solove, D. J., A taxonomy of privacy. University of Pennsylvania law review, pp. 477-564, 2006.
32. Braden, R., “Requirements for Internet Hosts – Communication Layers”. RFC1122, 1989;
33. Deering, S.; Hinden, R., “Internet Protocol, Version 6 (IPv6) Specification”. RFC2460, 1998;
34. TECHSUTRAM, “Differences IPv4 Vs IPv6”. Disponível em: . Acessado em: 16 de Dezembro de 2016.
35. Chaqfeh, M.; Mohamed, N., “Challenges in middleware solutions for the internet of things”. In. Collaboration Technologies and Systems (CTS), International Conference on. IEEE, pp. 21-26, 2012.
36. Dwivedi, A. K.; Vyas, O. P., “Wireless Sensor Network: At a Glance”. INTECH Open Access Publisher, 2011.
37. Kurami, P.; Kumar, M.; Rishi, R., “Study of Security in Wireless Sensor Networks”. Proceedings of International Journal of Computer Science and Technology, vol. 1, no. 5, pp. 347-354, 2010.
38. Shwe, Y. W.; Liang, Y. C., “Smart Dust Sensor Network with Piezoelectric Energy Harvesting”. ICITA, 2009.
39. “A History of Internet: 1988”. Web log post. Computer Information, 12 Aug. 2010. Disponível em: , Acessado em: 16 de Dezembro de 2016.

40. Internet Society, “The Open Internet: What it is and how to avoid mistaking it for something else”. September 2014.
41. Tanenbaum, A. S.; Vincent, P. H.; “Computer Networks: AND Computer Systems Design and Architecture”. 1st International Edition, 2004.
42. Callaway, E.; Gorday, P.; Hester, L.; Gutierrez, J. A.; Naeve, M.; Heile, B.; Bahl, V., “Home networking with IEEE 802.15.4: a developing standard for low-rate wireless personal area networks”. Communications Magazine, pp. 70-77, 2002.
43. Shelby, Z.; Bormann, C., “6LoWPAN: The Wireless embedded Internet”. Wiley, vol. 43, 2011.
44. Vasseur, J. P.; Kim, E.; Kaspar, D., “Request for Comments 6568: Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)”, Inc. Cisco Systems, pp. 4-5, 2012.
45. Ko, J.; Dawson-Haggerty, S.; Gnawali, O.; Culler, D.; Terzis, A., “Evaluating the Performance of RPL and 6LoWPAN in TinyOs”. In Workshop on Extending the Internet Low Power and Lossy Networks (IP + SN), pp. 2-5, 2011.
46. Hui, J.; Thubert, P., “Compression Format for IPv6 Datagrams in 6LoWPAN Networks. Internet Draft, IETF, pp. 6-7, 2011.
47. Winter, T.; Thubert, P., RPL Author team. “RPL: IPv6 Routing Protocol for Low power and Lossy Networks”. IETF, pp. 8-17, 2010.
48. Martocci, M. J.; De Mil, P.; Riou, N.; Vemeylen, W., “Building Automation Routing Requirements in Low-Power and Lossy Networks”. IETF, pp. 4-5, 2010.
49. Shelby, Z.; Frank, B.; Sturek, D., “Constrained Application Protocol (CoAP)”. Internet Draft, pp. 1-11, 2010.