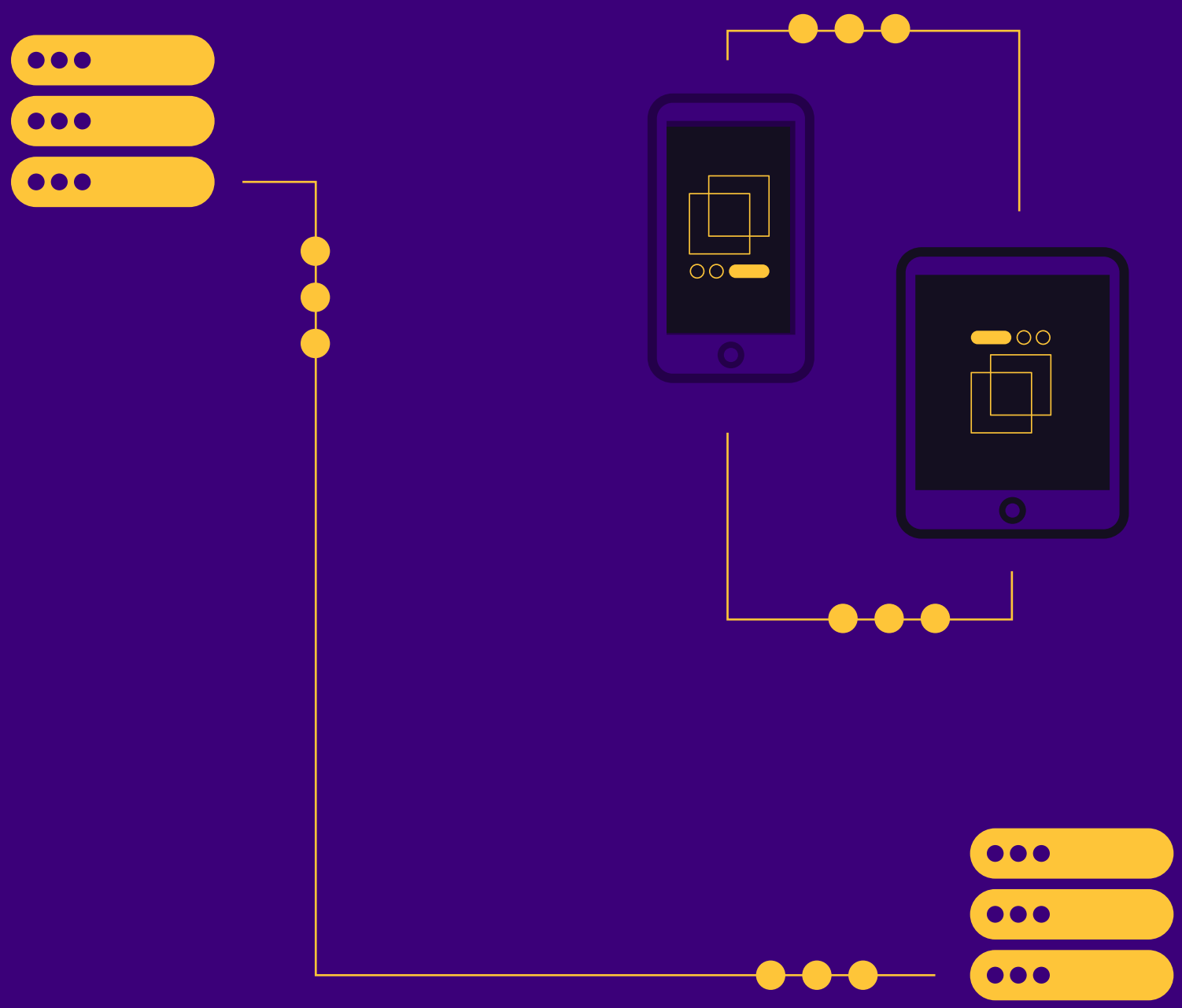
Relatório Técnico:

Desafios da implementação da Portabilidade de Dados em ambientes inteligentes conectados

Everton de Matos



SUMÁRIO

1. INTRODUÇÃO

O direto pela portabilidade de dados (*Right to Data Portability* - RTDP) presente na Lei Geral de Proteção de Dados Europeia (*General Data Protection Regulation* - GDPR) trouxe novos desafios para diversas áreas do conhecimento [32]. Tal direito tem como objetivo dar uma maior autonomia ao usuário para com seus dados. Ao passo que a Lei Geral de Proteção de Dados (LGPD) do Brasil tomou forma, com alguns aspectos semelhantes a GDPR [19], a discussão sobre a portabilidade dos dados também veio à tona. Dentre os desafios para a garantia do direto a portabilidade de dados, estão questões ligadas ao lado tecnológico e as características relacionadas aos sistemas computacionais em garantir a portabilidade.

Dentre os desafios técnicos na área tecnológica para prover a portabilidade de dados, destacam-se: garantir a segurança durante todo o processo, e prover interoperabilidade entre as partes [9]. Uma área da computação que vem ganhando destaque nos últimos anos é a Internet das Coisas [4]. Esta área está diretamente relacionada com o provimento de diversos dados relacionados aos usuários que eventualmente serão portados. Além disso, questões de segurança e interoperabilidade são frequentemente discutidas por pesquisadores e indústria da Internet das Coisas, além da relação direta dela com o direto a portabilidade de dados [47].

Durante a última década, o paradigma de computação chamado Internet das Coisas, em inglês *Internet of Things (IoT)*, vem ganhando atenção nas áreas acadêmica e industrial. A Internet das Coisas alcançou novas dimensões no mundo da comunicação e tecnologia da informação por embarcar redes móveis e a capacidade de processar informações dentro de uma grande gama de dispositivos e itens do dia-a-dia da vida das pessoas [3]. A IoT está presente em diferentes domínios de aplicação como por exemplo *healthcare*, agricultura, educação, transporte, trânsito, cidades inteligentes.

O conceito da IoT é a evolução de diversos elementos tecnológicos como sensores, *hardware*, semântica, armazenamento, processamento e comunicação, que quando juntos em um mesmo ambiente, representam o futuro da computação e das comunicações. A IoT tem o objetivo final de criar um mundo melhor para todas as pessoas, onde objetos a nossa volta tenham conhecimento e possam agir de forma autônoma e inteligente sem instruções explícitas [39].

A ideia da IoT é basicamente a presença pervasiva de uma variedade de “coisas”, ou objetos, que são capazes de interagir entre si

e cooperar com seus vizinhos a fim de alcançar objetivos comuns. Isto é feito através de esquemas únicos de endereçamento e meios de comunicação confiáveis através da Internet. São objetos pertencentes da rede da IoT qualquer dispositivo físico que possua a capacidade de conectar-se através da Internet. Muitas vezes, objetos do dia-a-dia que anteriormente não possuíam tal funcionalidade, agora podem permanecer conectados na rede. Alguns exemplos de "coisas" da IoT podem ser: sensores, atuadores, smartphones, tags RFID (*Radio-frequency identification*), dispositivos inteligentes como carros, geladeiras [3].

Para ser considerado um dispositivo IoT, o mesmo deve possuir seis blocos básicos: (i) identificação, (ii) sensores/atuadores, (iii) computação, (iv) comunicação, (v) semântica, e (vi) serviços [10]. A identificação (i) está relacionada ao dispositivo possuir um identificador único na rede, como por exemplo um endereço IP (*Internet Protocol*). Sensores (ii) são utilizados para perceber o ambiente que o dispositivo está inserido (por exemplo, localização, hábitos, preferências, dados climáticos) e atuadores são utilizados para manipular o ambiente ou agir de acordo com os dados sensoreados (por exemplo, alertas, movimentações, ações). A computação (iii) é a unidade de processamento que irá tomar as decisões baseadas nos dados. Executa algoritmos pré-definidos ou adaptativos. A comunicação (iv) é responsável pela troca de informações entre dispositivos e entre os mesmos e a Internet. A semântica (v) está relacionada com dar um sentido de alto nível para os dados, tornar a informação entendível para os usuários finais. Por fim, os serviços (vi) são o último elo da IoT, é através deles que os usuários recebem as informações, ou proveem informações para o ambiente.

A grande quantidade de dados que trafegam em sistemas desenvolvidos para IoT exige serviços de segurança capazes de garantir a proteção dos dados em toda a extensão do sistema [42]. Soluções de IoT usualmente trafegam e gerenciam informações sensíveis dos usuários, além de possuir diversos dispositivos finais, aumentando a suscetibilidade a ataques. A área de segurança é uma das mais pesquisadas para soluções IoT. Gartner [22] informa que os gastos a nível mundial com segurança para IoT chegarão na marca de $3.1 bilhões de dólares em 2021. Tais investimentos apenas comprovam a necessidade de pesquisas e desenvolvimento relacionados com a área de segurança para IoT.

Um possível cenário de aplicação da IoT pode ser definido como uma casa inteligente, com diversos dispositivos conectados como *smartphone*, *smartwatch*, lâmpadas inteligentes, termostato automático, entre outros. Todos estes dispositivos terão informações dos moradores da casa, como preferências de uso e rotinas

pré- programadas. Estas informações serão processadas por *softwares*, ou sistemas, que dispararão as atuações necessárias sobre o ambiente, como alterar configurações de climatização, iluminação, mídias, entre outros. Neste cenário, como aconteceria a portabilidade dos dados se o usuário decidir alternar entre sistemas para um serviço que melhor lhe atender?

Na maioria dos casos, os dados dos dispositivos IoT são armazenados individualmente pelos sistemas, não disponibilizando acesso para comunicação entre sistemas ou entidades fora do domínio de aplicação restrito [31]. A interoperabilidade destes dados é um requisito essencial para a implantação da IoT, pois este requisito possibilita que diferentes entidades possam "entender" os dados de um determinado domínio de aplicação, ou entre diferentes domínios. Além disso, a interoperabilidade de dados é considerada um desafio no desenvolvimento de soluções para IoT [14].

O objetivo do presente relatório técnico é apresentar o desafio da portabilidade de dados na perspectiva da área de Internet das Coisas, envolvendo questões de interoperabilidade e segurança. A Seção 2 apresenta conceitos relacionados a portabilidade, responsabilidade e ambientes inteligentes, os quais fazem parte da IoT. A Seção 3 apresenta uma visão técnica sobre os principais pontos da portabilidade de dados. Por fim, a Seção 4 apresenta os desafios para o desenvolvimento da portabilidade tendo em vista ambientes IoT e as conclusões do presente relatório.

2. PORTABILIDADE, RESPONSABILIDADE E AMBIENTES INTELIGENTES CONECTADOS

A presente Seção tem como objetivo detalhar as definições refentes a Portabilidade, Responsabilidade e Ambientes Inteligentes Conectados. A Subseção 2.1 apresenta definições sobre os temas de Portabilidade e Responsabilidade, além de sua relação com as tecnologias da informação. A Subseção 2.2 apresenta definições sobre Ambientes Inteligentes Conectados, mais especificamente, ambientes de Internet das Coisas, além dos cenários nestes ambientes em que pode haver a necessidade de portabilidade de dados.

2.1. PORTABILIDADE E RESPONSABILIDADE

Nos últimos anos, o debate em torno da portabilidade dos dados de usuários vem ganhando forma. Leis vem sendo criadas, em diversos países, no intuito de garantir que o usuário de um determinado serviço online possa portar seus dados pessoais para um outro serviço. Esta abordagem justifica-se no objetivo de dar uma maior liberdade de escolha para o usuário, tornando possível a escolha pelo serviço de melhor custo-benefício e diminuindo a complexidade ao trocar o prestador de serviço online [18].

Existem diversas questões com discussões em aberto com relação a portabilidade de dados. Dentre estes pontos estão questões de ordem técnica na aplicação da portabilidade por parte dos serviços digitais. Os principais pontos de discussão envolvem desde quais métodos que devem ser implementados tecnologicamente para garantir a portabilidade até a definição se dados de terceiros, relacionados com o solicitante da portabilidade, devem ser portados [9].

Questões de responsabilidade também estão sendo discutidas no que diz respeito a portabilidade dos dados [25]. O serviço digital possui responsabilidade sobre os dados de seus usuários, portanto infere-se que o serviço também pode possuir responsabilidade no processo de portabilidade, garantindo que os dados sejam exportados de maneira segura para estes serem importados em outro serviço. A responsabilidade de garantir a segurança e privacidade dos dados deve ser portada para o serviço de destino juntamente com os mesmos [9], garantindo assim que o usuário não fique desassistido na questão de segurança e privacidade.

Com o crescimento em número de usuários de ambientes inteligentes conectados através da Internet, a quantidade de dados também aumentou [22]. Embora inicialmente definida como um conceito legislativo, a portabilidade de dados possui diversos requisitos técnicos, o que torna extremamente necessário o entendimento sobre os ambientes conectados modernos e suas peculiaridades no que diz respeito ao cumprimento do direito à portabilidade de dados.

2.2. AMBIENTES INTELIGENTES CONECTADOS

Ambientes inteligentes conectados, como por exemplo ambientes de aplicação de tecnologias de Internet das Coisas (*Internet of Things* — IoT) possuem uma grande quantidade de dispositivos e usuários. A Ericsson estima que cerca de 25 bilhões de dispositivos estejam conectados através da Internet até 2025 [20]. Podemos imaginar que boa parte destes dispositivos estará gerando diferentes tipos de dados,

relacionados aos usuários ou ao ambiente em que o mesmo estará inserido. Portanto, a quantidade de dados gerados em ambientes de Internet das Coisas beira o inimaginável. Para tanto, é possível imaginar que a portabilidade destes dados também é um ponto importante de discussão nesta área.

O conceito geral da IoT gira em torno da evolução de diversos elementos tecnológicos como sensores, *hardware*, semântica, armazenamento, processamento e comunicação, que quando juntos em um mesmo ambiente, representam o futuro da computação e das comunicações. A IoT tem o objetivo final de criar um mundo melhor para todas as pessoas, onde objetos a nossa volta tenham conhecimento e agem de forma autônoma e inteligente sem instruções explícitas [39]. Neste contexto, podemos ver que o serviço de vários setores, tais como: transportes, cidades inteligentes, saúde, governo, educação, varejo, logística, agricultura, automação, manufatura industrial e negócios/gerenciamento de processos etc., já estão sendo beneficiados pela Internet das Coisas e suas diferentes implementações [37].

Ambientes da IoT são geralmente implementados baseando-se em uma arquitetura padrão que consiste de várias camadas: a camada de aquisição de dados até a camada de aplicação. A seguir, são apresentadas as funcionalidades das principais camadas da IoT [4]:

- **Camada de aplicação:** Esta camada é responsável por disponibilizar vários serviços para diferentes usuários/aplicações de ambientes da IoT. As aplicações podem ser de diferentes domínios, como por exemplo indústria, fábricas, logística, meio ambiente, segurança pública, *healthcare*, cidades inteligentes. É a camada que o usuário final terá acesso, com objetivo de consumir os serviços providos pela solução ou sistema de IoT em que o mesmo possui autorização para acesso.
- **Camada Middleware:** Esta camada age como uma interface entre a camada de *hardware* e a camada de aplicação. É responsável por funções críticas como por exemplo o gerenciamento de dispositivos e informação, e também cuida de problemas como filtragem de dados, agregação de dados, análise semântica, controle de acesso, e descoberta de informação.
- **Camada de gateway de acesso:** A primeira fase de tratamento de dados acontece nesta camada. É nela que é feito o roteamento de mensagens via Internet, e também realiza comunicação *corss-platform* se necessário.
- **Camada de dispositivos:** Esta camada de *hardware* consiste de redes de sensores, sistemas embarcados, *tags* e *readers RFID*, ou outro dispositivo da IoT. Estas entidades são as fontes de dados implantadas em ambientes da IoT. Muitos destes elementos de hardware proveem identificação e armazenamento de dados, coleta de dados (redes de sensores), processamento de dados (processadores embarcados), comunicação, e controle. Além disso, dispositivos IoT também podem atuar sobre o ambiente,

a fim de realizar uma ação física quando necessário, como por exemplo alertas sonoros, visuais, ou realizar movimentações.

A Figura 2.1 representa a disposição das diferentes camadas na arquitetura padrão IoT: *Cloud*, *Fog* e *Edge*. A base da pirâmide é composta pelos dispositivos responsáveis pela coleta dos dados. *Edge*, ou *Edge Computing*, diz respeito às tecnologias que possibilitam que a computação seja executada na borda da rede, tirando o massivo processamento da nuvem — *Cloud Computing* — e colocando este processamento embarcado nos dispositivos da IoT. Assim diminuindo problemas relacionados a latência da rede, descentralizando o processamento, e aumentando a escalabilidade. A adoção de *Edge Computing* se popularizou pelo constante aumento de poder de processamento computacional de dispositivos finais implantados em ambientes IoT.

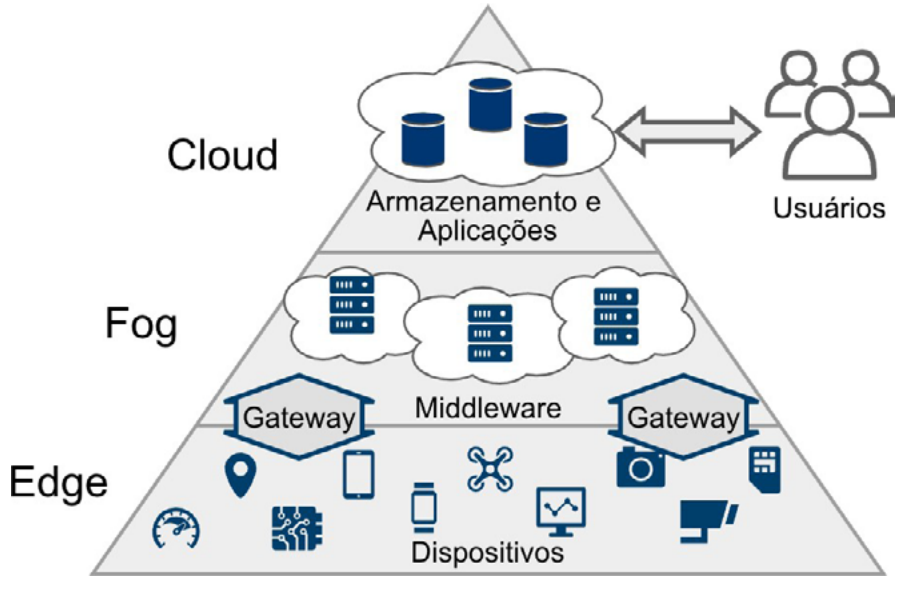


Figura 2.1 Diferentes camadas presentes em ambientes IoT.

A parte intermediária da pirâmide (veja Figura 2.1) é responsável pelos dispositivos que processam e (ou) manipulam os dados, definda como camada *Middleware*. Esta camada é interligada com os dispositivos via Gateway de comunicação. O conceito de Fog, ou *Fog Computing* — Computação de Neblina, foi introduzido pela *Cisco Systems* em 2012, e em sua definição inicial foi considerada como uma "*extensão do paradigma da computação em nuvem que fornece serviços de computação, armazenamento e rede entre dispositivos físicos e servidores de nuvem tradicionais*" [38]. Portanto, *Fog Computing* não canibaliza a computação em nuvem, mas complementa: a arquitetura de *Fog* facilita a criação de uma infraestrutura hierárquica, onde a análise das informações de um determinado domínio de aplicação é realizada localmente, e a coordenação e análise global são realizados na nuvem [38].

A ponta da pirâmide (veja Figura 2.1) representa a nuvem (*Cloud*), onde os dados podem ser armazenados. O paradigma *Cloud Computing* ou Computação em Nuvem, é o resultado da evolução e adoção de tecnologias e paradigmas computacionais consolidados [39]. A Computação em Nuvem torna possível que diferentes dados sejam acessados de diferentes pontos geográficos, sem a necessidade de uma proximidade física do ponto de partida dos mesmos [5]. Por ser uma espécie de subconjunto da *Cloud*, a camada de *Fog* também compartilha destas características, porém em menor escala quanto a quantidade de dados que podem ser armazenados e processados em tempo real.

Existem diversos desafios a serem superados em sistemas de IoT [31]. Mesmo com

os avanços em questão de arquitetura, alguns pontos são alvo de pesquisas e discussões em tempos atuais, como por exemplo: segurança das informações, gerência de dados, e interoperabilidade [14]. A portabilidade de dados é uma área presente nos três desafios previamente citados. Os dados que serão portados de ambientes IoT, devem ser transportados em canais de comunicação seguro, para que seja possível garantir a privacidade e integridade dos mesmos.

Com a grande quantidade de dados gerenciados por sistemas presentes em ambientes IoT, por muitas vezes, será necessária a portabilidade dos mesmos para diferentes instâncias de camadas de *Fog*, *Cloud*, ou até mesmo em nível de dispositivos, na camada *Edge*. Os ambientes IoT podem possuir dispositivos de hardware e sistemas de software com características diferentes entre si. É comum que elementos de diferentes fabricantes não compartilhem do mesmo formato de apresentação de dados, cadência de transmissão de dados, e até no que diz respeito aos protocolos de comunicação envolvidos. Portanto, é essencial o provimento de interoperabilidade entre estes diferentes contextos em ambientes IoT. Tal desafio vai de encontro com a portabilidade de dados, uma vez que a implementação de tal direito deve garantir o transporte das informações independente de questões técnicas específicas.

A fim de elucidar os desafios e possíveis soluções para a garantia da portabilidade de dados em ambientes de IoT, é necessária uma discussão sobre os principais pontos que envolvem tal direito, porém com a visão técnica das aplicações de ambientes inteligentes conectados, como a IoT. A seguir, na Seção 3, tais pontos são apresentados e detalhados.

3. VISÃO TÉCNICA DAS CINCO QUESTÕES SOBRE PORTABILIDADE E RESPONSABILIDADE

Além dos conceitos gerais apresentados na Seção 2, é importante discutir do ponto de vista técnico, como a portabilidade de dados será realizada em ambientes inteligentes conectados, como por exemplo sistemas de Internet das Coisas. A presente Seção tem como objetivo discutir as cinco principais questões quanto ao direito da portabilidade de dados levando em consideração sistemas de Internet das Coisas. As próximas Subseções detalham cada uma das cinco questões detalhadas no *White Paper* intitulado "*Data Portability and Privacy* ", o qual foi publicado pelo *Facebook* [18].

3.1. O QUE É "PORTABILIDADE DE DADOS"?

Portabilidade de dados é a possibilidade de copiar e transferir os próprios dados pessoais inseridos em um determinado serviço para outro. Experiências prévias com portabilidade foram amplamente difundidas na área da telefonia [30]. Porém, através das leis de proteção de dados, a portabilidade também ficou relacionada com os dados dos usuários em serviços digitais, como por exemplo o campo das mídias sociais [17]. Um dos objetivos gerais da portabilidade de dados é dar uma maior autonomia ao usuários sobre os seus dados. Desta maneira, tornando possível que o usuário decida qual é o serviço online que lhe oferece o melhor custo-benefício. O prestador de serviço online deve oferecer maneiras para que o usuário consiga realizar a portabilidade de seus dados, tornando assim possível o carregamento destes dados em um outro serviço [7].

Em ambientes de Internet das Coisas, os diversos dispositivos e usuários presentes na rede possuem a possibilidade de gerar novos dados. Estes dados podem ser sensoreados do meio ambiente, ou criados a partir de hábitos de uso de uma determinada ferramenta ou sistema [4]. Embora algumas soluções para ambientes IoT apenas realizam o repasse dos dados, interligando o usuário final à um dispositivo, muitas delas detém os dados por um certo período de tempo [3]. A portabilidade de dados nestes cenários está em concatenar os dados dos usuários e permitir que o usuário possa migrar seus dados entre diferentes plataformas.

Muitas vezes, plataformas na nuvem (*Cloud Computing*) como por exemplo *Google Cloud*, *Amazon AWS*, *Microsoft Azure*, entre outras, são utilizadas para armazenar dados de sistemas IoT. Podemos tomar como exemplo uma determinada solução desenvolvida para uma indústria inteligente, em que os dados relacionados à produção de um determinado produto são armazenados em uma plataforma de nuvem [1]. Estes dados podem indicar um padrão de interações para os dias de produção, quantidade de produtos produzidos por determinado período de tempo, perfil de funcionários acessando determinada área, entre outras situações. Para este cenário específico, a portabilidade de dados se daria pelo fato de remover todos os dados de uma plataforma de nuvem e realizar o *upload* em uma outra plataforma semelhante, ou até mesmo em uma plataforma de nuvem própria da empresa. Tais operações serão relativamente simples se a plataforma de nuvem estiver apenas armazenado os dados para futuras consultas. Deste modo, os dados são encarados como um "pacote" pela plataforma de nuvem, em que ela não precisa ter conhecimento da finalidade de cado dado.

Existem também plataformas de nuvem em ambientes IoT que podem realizar algum tipo de processamento com os dados e entregar novos serviços de "alto nível" para os usuários [11, 31]. Um exemplo de cenário hipotético pode ser visto como uma plataforma que mede a poluição de uma cidade. Para medir a poluição, a plataforma precisará dos dados do nível de poluição da água, do solo, do ar e utilizará regras de negócio pré-definidas, ou ajustáveis, para informar o nível geral de poluição da cidade ao usuário final, através das três médias de poluição providas. Em casos como este, as regras de negócio, responsáveis pelo processamento, também entrariam na definição de portabilidade de dados, uma vez que somente com os dados e sem as regras não seria possível de inferir a informação do nível de poluição da cidade.

3.2. QUAIS DADOS DEVEM SER PORTADOS?

O conceito de dados "fornecidos" pelo usuário é um dos mais utilizados no debate que define quais os dados devem ser portados de um usuário em questão. Este conceito, primeiramente, abrange os dados que intencionalmente foram inseridos pelo usuário no serviço online utilizado por ele. Porém, o conceito também pode abranger dados que não foram fornecidos intencionalmente, com por exemplo preferências inferidas por um determinado comportamento do usuário. Ao realizar buscas por um determinado produto, entende-se que o usuário possa ter interesse em produtos semelhantes [9]. Existe a preocupação de que o usuário não tenha prejuízo ao portar seus dados. Se os dados inferidos pelo comportamento, ou até mesmo os dados que representam a reputação do usuário em um serviço não forem portados juntamente com todos os dados do mesmo, o usuário poderá não receber todos os benefícios da portabilidade de seus dados para um outro serviço [23].

Na área de Internet das Coisas, existe um senso comum de que dispositivos de ambientes IoT geram uma grande quantidade de dados, e estes dados só serão úteis se pudermos analisar, interpretar e entendê-los de forma adequada [31]. Este entendimento pode envolver a utilidade dos dados à possibilidade de portabilidade dos mesmos, em que deve ser possível a transmissão entre diferentes entidades do ambiente.

Dispositivos IoT, como por exemplo, celulares, carros, geladeiras, e sensores em geral, são exemplos de fontes de dados gerados em ambientes IoT. Estes dados caracterizam uma situação, e muitas vezes são dinâmicos[1], alterando sua situação ao passar do tempo [3]. Muitas vezes estes dados são sensíveis, demonstrando informações pessoais, como por exemplo localização atual, padrão de movimentação, dados médicos, entre outros. Os dados gerados por dispositivos IoT devem ser portados, pois em alguns casos o usuário pode desejar uma mudança no prestador de serviços que pode operar tais dados. Diferentes prestadores de serviços poderão analisas estes dados e apresentá-los de maneira diferente para os usuários.

Uma outra categoria de dados que devem ser portados está relacionada aos dados gerados de maneira indireta pelos sistemas de ambientes IoT [14]. Alguns dispositivos podem gerar dados chamados de “baixo nível”, já que não demonstram uma informação sensível à primeira vista. Porém, através de processos como agregação com outros dados ou até mesmo um raciocínio baseado em regras, tais dados podem ganhar um sentido de “alto nível”, ou seja, entendível pelo usuário. Dados tanto de “baixo nível”, entendíveis pelas máquinas, quanto de “alto nível” devem ser portados se solicitado pelo usuário. Portanto, é importante que o sistema ou plataforma presente em um ambiente IoT tenha a capacidade de portar ambas as categorias de dados. É uma discussão em aberto se é responsabilidade do sistema IoT em portar os métodos que podem agir sobre dados de “baixo nível”.

A Figura 3.1, adaptada de [14], apresenta um cenário de aplicação de um sistema de IoT em uma cidade inteligente. Neste cenário é possível perceber que dados de “baixo nível” podem gerar serviços de “alto nível”. O item 1, presente na Figura 3.1, simboliza um evento em uma cidade inteligente. O item 2 representa a detecção de dados de “baixo nível” realizados por dispositivos IoT (sensor de som, câmera de vigilância, sensor de movimento). Durante o item 3 os dados são processados e transformados em serviços de “alto nível” que podem ser vistos nos itens 4, 5 e 6. Ao portar somente os dados, excluindo os processamentos indiretos, um usuário perderia a funcionalidade de transformação dos dados de “baixo nível” em serviços de “alto nível”.

Mesmo antes da questão de portabilidade de dados virar um tópico de debate, a interoperabilidade foi e é uma grande questão de discussão na comunidade de desenvolvimento de soluções para Internet das Coisas [40]. A maioria dos cenários de sistemas IoT são tidos como complexos, por possuírem diversos tipos de dispositivos, produzindo diferentes tipos de dados em questão de formatação, tipo de dado, padronização, entre outros. Isto se deve ao fato de existirem diferentes fabricantes de dispositivos. Em alguns aspectos, como por exemplo protocolos de comunicação e topologias de rede, existe um padrão a ser seguido que é atendido por grande parte dos sistemas IoT [31]. Por outro lado, em alguns pontos existe um problema de interoperabilidade, em que diferentes sistemas podem não trabalhar da mesma maneira, dificultando diversos processos, como por exemplo a portabilidade de dados.

Figura 3.1 Cenário exemplificando uma informação de “baixo nível” gerando serviços de “alto nível”.

Nas questões de portabilidade de dados para IoT, a alternativa de criar um padrão global de dados para formato, tipo, características gerais, facilitaria o processo. Porém, com o grande aumento na criação de “padrões” para sistemas em ambiente IoT [51], a criação de um novo padrão parece entrar em um paradoxo. A cada novo “padrão” criado, será um padrão a mais que poderá não ser utilizado por todos. Por outro lado, soluções que permitem o compartilhamento de dados entre diferentes aplicações em sistemas IoT estão ganhando destaque nos últimos anos [12, 14, 31]. Percebeu-se que uma alternativa viável é a criação de métodos ou arquiteturas que sejam capazes de realizar a interpretação de diferentes formatos de dados e tenham como saída um formato de dados desejado. Desta maneira, independente do formato, tipo, ou característica geral do dado em questão, tais ferramentas podem ajudar no processo de interoperabilidade, facilitando a implementação ao direito a portabilidade de dados em tais ambientes.

3.3. QUEM SERÃO OS SUJEITOS DOS DADOS PORTADOS?

Em um primeiro momento, presume-se que somente os usuários solicitantes da portabilidade serão os sujeitos que terão seus dados portados. Porém, os dados de um determinado usuário podem afetar outros sujeitos. Um exemplo claro pode ser definido como de um usuário “A”, que possui dados em uma determinada rede social e deseja portá-los para outra plataforma. Suas informações pessoais serão portadas, assim como suas publicações, vídeos, fotos, entre outros. Por outro lado, outros usuários, como por exemplo o usuário “B”, podem aparecer nas fotos que serão portadas, gerando um problema complexo nesta situação. Portanto, é importante discutir como, e se, o usuário “B”, que está presente na foto, mas não solicitou a portabilidade, participará da portabilidade dos dados [25, 49].

Ambientes de Internet das Coisas podem possuir diversos sujeitos [31, 53]. Os sujeitos variam de acordo com as caraterísticas específicas do ambiente de aplicação. Grande parte dos sistemas de ambientes IoT possuem o usuário como ponto central da comunicação dos dados, na abordagem chamada de *user-centric* [8]. Nesta abordagem, o sistema IoT possui o objetivo final de beneficiar um determinado usuário. Este benefício pode ser interpretado como um serviço de (i) sensoriamento ou (ii) atuação. Um exemplo de (i) sensoriamento pode estar relacionado com informar ao usuário a temperatura de uma localidade relacionada, ou não, com a localização do usuário. Com relação a (ii) atuação, um exemplo pode ser visto como a abertura de um portão eletrônico a medida que o usuário se aproxima de sua casa, ou seja, atuando fisicamente sobre o ambiente.

Abordagens *user-centric* geralmente trabalham com os dados do usuário em si, a fim de sugerir pontos de interesse, em um ambiente de cidade inteligente por exemplo, ou guardar informações para uma tomada de decisão futura, como por exemplo uma casa inteligente acionando dispositivos a medida que o morador ingressa nela. Portanto, em grande parte dos ambientes de aplicação de sistemas IoT, o usuário será o sujeito que terá os dados portados.

Por outro lado, também deve ser considerado o fato de que o usuário poderá possuir dados que são relacionados a outros usuários. Por exemplo, um usuário (sujeito) poderá ser uma indústria que possui sistemas de monitoramento da cadeia de produção, a qual deseja portar estes dados. Neste cenário citado como exemplo, outros usuários poderão fazer parte do sistema, como funcionários operando máquinas nesta cadeia de produção. Dependendo o nível de profundidade das informações a serem portadas que identifiquem estes usuários, eles também deveriam ser notificados da portabilidade em questão e também serão sujeitos que terão seus dados portados, mesmo de maneira indireta.

3.4. COMO DEVE-SE PERMITIR A PORTABILIDADE GARANTINDO A PROTEÇÃO DA PRIVACIDADE?

É importante que o usuário verifique as questões de privacidade da plataforma de destino no processo de portabilidade dos dados. Algumas plataformas podem prover diferentes métodos e maneiras de garantir a proteção da privacidade dos dados. O nível de privacidade das plataformas online pode-se tornar um fator de decisão ao portar os dados [9]. Outro fator de destaque no processo de portabilidade é a notificação, para o usuário, de todos os passos que serão realizados. Desta maneira tornando possível que o usuário tenha ciência exata de quais dados serão portados assim como os métodos de portabilidade. Na questão jurídica, é importante definir os níveis de privacidade que as informações portadas terão, pois em muitos casos usuários não relacionados diretamente com a portabilidade terão parte de seus dados portados, como por exemplo aqueles que possuem marcação em uma foto do usuário que está realizando a portabilidade dos dados [18]. Na questão técnica computacional, é importante garantir que as comunicações e dados sejam mantidos privados e íntegros, provendo assim um alto nível de segurança da informação.

A segurança é um dos principais tópicos de pesquisa e desenvolvimento em ambientes de sistemas IoT [42]. Nestes ambientes, a segurança pode ser complexa, já que possui diferentes possibilidades de implantação. Os dados necessitam de proteção, então percebe-se que é necessário um esforço no desenvolvimento de técnicas para mantê-los seguros. Porém, além de protegê-los quando armazenados, é mandatória a proteção enquanto os mesmos são transmitidos para diferentes entidades. Como na IoT a Internet está sempre presente, invariavelmente os dados serão transmitidos pela rede, abrindo possibilidades de ataques maliciosos para interceptação de dados [52]. Portanto, além de políticas de proteção de dados de maneira local, como por exemplo criptografia[2], anonimização[3], esteganografia[4], os dados também devem ser protegidos no canal de comunicação, com a implementação de tecnologias de comunicação considerados seguras, como por exemplo DTLS (*Datagram Transport Layer Security*), CoAP (*Constrained Application Protocol*), wolfSSL, entre outros [15].

A implementação de ferramentas seguras deve levar em conta as restrições de ambientes IoT [2]. Ambientes de Internet das Coisas muitas vezes possuem dispositivos com características restritas, seja relacionado ao poder de processamento, capacidade energética ou capacidade de armazenamento. Como dispositivos IoT são dispositivos do dia-a-dia com capacidade de processamento de dados e conexão na rede, muitos destes estão longe de ser considerados supercomputadores, dificultando a implementação da segurança, a qual deve ser pensada levando em conta este ambiente de características restritas.

Além disso, como demonstrado na Seção 2, ambientes com sistemas IoT podem ter uma grande capilaridade, possuindo diversas camadas de processamento, como *Edge* e *Fog*. Tais camadas podem solucionar diversos problemas de implantação de ambientes IoT, como diminuir a latência e aumentar escalabilidade, porém deve-se ter cuidado em relação a segurança destes ambientes [16]. É um consenso na área da Computação, e da IoT, de que os dispositivos na borda da rede (*Edge*) podem possuir uma maior vulnerabilidade quando comparado com servidores de grandes empresas (*Cloud*) [44]. Isto se deve ao fato de que muitas vezes, dispositivos *Edge* são desenvolvidos por entusiastas, sem a devida precaução na questão de segurança, além de que, tais dispositivos possuem menor poder de processamento do que a nuvem (*Cloud*), dificultando a implementação de técnicas mais robustas. Para tanto, a área de segurança para borda da rede (*Edge*) é um dos temas mais pesquisados atualmente, para garantir que tais dispositivos permaneçam protegidos, garantindo a segurança e privacidade das informações presentes em toda a topologia de ambientes de sistemas IoT [29, 44].

A Figura 3.2, adaptada de [42], apresenta uma taxonomia para segurança em camadas intermediárias na IoT. As camadas intermediárias envolvem diretamente a camada de Middleware (veja Seção 2), nas quais os dados são gerenciados. Geralmente situadas na topologia de *Fog Computing*.

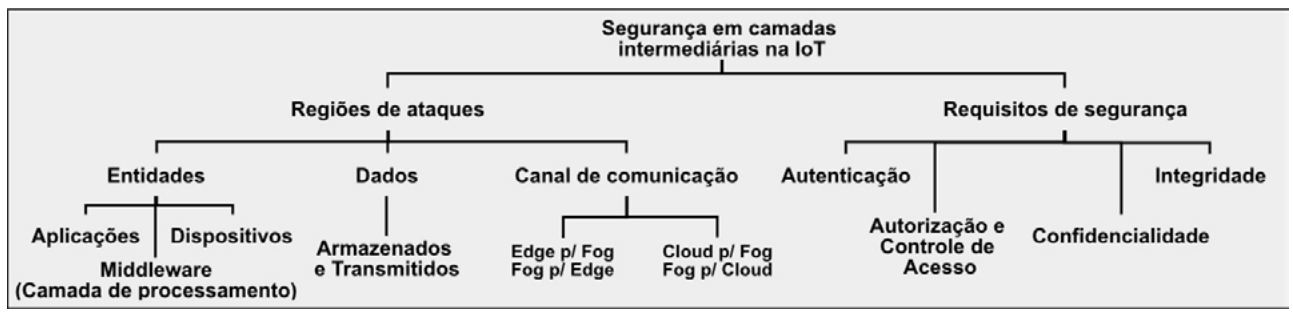


Figura 3.2 Taxonomia da segurança para IoT.

Através da Figura 3.2 percebe-se que são três as principais regiões de ataques: Entidades, Dados e Canal de comunicação. Tais regiões podem ter os dados roubados, modificados indevidamente, ou observados. São requisitos para estas regiões permanecerem seguras, a implementação de técnicas para Autenticação, Autorização e Controle de Acesso, Confidencialidade e Integridade. Um usuário acessando os dados precisa estar devidamente autenticado, através de métodos padrões como senhas ou PINs (*Personal Identification Number*). O mesmo deve possuir autorização para visualizar os dados, através de credenciais, ou via a categoria do usuário. Esta implementação é realizada através de mecanismos de controle de acesso, para validar a identidade do usuário. Os dados devem permanecer confidenciais, ou seja, somente o usuário devidamente autorizado poderá acessá-los. A aplicação de criptografia é uma técnica

relativamente comum para garantir a confidencialidade de dados armazenados, em que somente com a chave correta será possível realizar a visualização. Por fim, os dados devem ser mantidos íntegros, ou seja, imutáveis e completos. Canais de comunicação seguro podem garantir a integridade de dados enquanto trafegam via rede.

3.5. APÓS OS DADOS PORTADOS, SOBRE QUAL SUJEITO RECAI A RESPONSABILIDADE SE OS DADOS FOREM UTILIZADOS INDEVIDAMENTE OU MODIFICADOS?

A discussão sobre a portabilidade de dados tem como tópicos de debate não somente o processo de portabilidade em si, mas também questões envolvendo as possíveis repercussões da portabilidade, assim como a responsabilidade do sujeito de destino das informações [49]. Geralmente, a responsabilidade pela segurança e integridade dos dados é portada juntamente com os mesmos [6]. Portanto, uma vez que o usuário tenha todos os seus dados portados do serviço “A” para o serviço “B”, o serviço de destino (“B”) passaria a ter a responsabilidade sobre a segurança dos dados, o que inclui: garantir que os mesmos não sejam indevidamente utilizados, alterados ou compartilhados.

Deve-se ter atenção às funcionalidades oferecidas para com os dados pelo serviço de destino, já que este terá a responsabilidade sobre os mesmos. Por exemplo, o serviço de destino pode implementar funcionalidades que compartilhem os dados do usuário automaticamente com terceiros — outros serviços ou plataformas. Muitos serviços, como por exemplo redes sociais, estão constantemente atualizando suas políticas de privacidade [21]. Tais políticas determinam de que maneira os dados do usuário podem ser utilizados. É importante o usuário ter conhecimento destas políticas no momento de portar seus dados, para confirmar que a portabilidade acontecerá dentro de suas expectativas.

Em ambientes de sistemas de Internet das Coisas, existem diversas plataformas gerenciadoras de dados, consideradas seguras contra ataques computacionais por possuírem ambiente descentralizado e seguirem normais internacionais de segurança [36]. Tais plataformas, geralmente estão situadas em camadas *Cloud*, tendo assim uma vasta capacidade de armazenamento para os dados dos usuários. O usuário poderá portar seus dados entre diferentes plataformas, sendo que a responsabilidade pela segurança dos mesmos recaia sobre a plataforma de destino. Em outro exemplo, o usuário pode desejar remover seus dados de uma determinada plataforma de armazenamento, e guardá-los localmente em seu computador ou servidor. Desta maneira, o usuário se torna inteiramente responsável por seus dados, devendo atentar para possíveis ataques computacionais que podem ocorrer sobre este ambiente.

4. DESAFIOS E CONCLUSÕES

Por herdar conceitos computacionais de abordagens prévias, como por exemplo Computação Pervasiva e Computação Ubíqua, a Internet das Coisas se trata de uma evolução de conceitos pré-existentes na computação [3]. Embora solidificada por conceitos bem definidos, ambientes de sistemas IoT possuem uma vasta quantidadede desafios que devem ser pesquisados e desenvolvidos [31]. Além disso, conceitos relativamente

novos como a GDPR e LGPD implicam em novos desafios para o pleno desenvolvimento e adequação da IoT [46, 48, 50]. A seguir, são listados e discutidos alguns dos principais desafios para o desenvolvimento da IoT considerando possíveis implicações relacionadas a portabilidade dos dados.

- **Interoperabilidade**: Ambientes com sistemas de IoT muitas vezes possuem características heterogêneas [31]. Isto se deve pelo fato de existirem diferentes fabricantes de dispositivos IoT, os quais podem ter diferentes formatos para dados, tipos de representação, e maneiras de realizar a comunicação entre dispositivos e entre usuários. É importante atingir interoperabilidade entre as diferentes entidades de um determinado ambiente de aplicação de tecnologias IoT para uma comunicação fluída e uniforme. Em alguns aspectos, pode-se elencar padrões amplamente utilizados pela indústria, como por exemplo em protocolos de comunicação. Por outro lado, em alguns aspectos, como no gerenciamento de dados, é difícil encontrar um padrão amplamente estabelecido em ambientes de sistemas IoT [14]. Portanto, a interoperabilidade acaba sendo um desafio na portabilidade de dados para sistemas de Internet das Coisas. Existem soluções sendo pesquisadas e desenvolvidas para solucionar tal problema [12, 31, 33, 40]. Boa parte delas foca em criar uma camada de entendimento semântico entre os diferentes tipos de dados da IoT, através de processamento léxico e uso de tecnologias como ontologias.

- **Comércio de dados:** Um dos principais objetivos da portabilidade dos dados do usuário é a escolha de um serviço que lhe atenda de maneira mais satisfatória. Além disso, como uma área em ascensão na IoT, está o comércio dos dados de usuários, o que pode tornar a escolha pela portabilidade, também uma questão monetária. Mercados de dados, conhecidos na área da pesquisa de Internet das Coisas como *IoT Data Marketplaces*, são uma abordagem emergente que vem ganhando espaço no mercado. Esta abordagem tem como objetivo realizar o comércio de dados, sendo este o principal ativo deste cenário, aumentando assim as possibilidades dos donos de dispositivos IoT [24]. Vamos imaginar o seguinte cenário hipotético, em que o usuário “A” possui dispositivos monitorando os dados climáticos de seu terreno, em sua casa. Por outro lado, o usuário “B” é um desenvolvedor de software que tem como objetivo o desenvolvimento de um aplicativo móvel para mostrar dados climáticos de diferentes pontos de uma determinada região. Através de uma plataforma de mercado de dados para IoT, o usuário “A” poderá vender seus dados para o usuário “B”, que não necessitará de comprar os dispositivos físicos de monitoramento climático e instalá-los ao redor da região. Diversas plataformas de IoT estão em diferentes fases de desenvolvimento e aplicação para este fim [24, 26, 28, 45]. Tal abordagem pode significar uma diferente ramificação da porta-

bilidade de dados, em que envolva interesse monetário, tendo o dado como um ativo.

- **Segurança e Privacidade:** Por trabalhar com dados pessoais dos usuários, os quais são considerados dados sensíveis, o tópico de segurança e privacidade é um dos principais desafios no desenvolvimento e aplicabilidade de ambientes com sistemas IoT [42]. Além disso, a portabilidade pode adicionar um risco a mais na segurança dos dados, uma vez que os mesmos terão de trafegar pela rede entre a plataforma de origem e a plataforma de destino. Diversos pesquisadores e indústrias estão trabalhando para aumentar o nível de segurança e privacidade para a aplicações da IoT [35, 41, 44, 52]. São diversas as áreas de desenvolvimento da segurança na IoT. Pesquisas para a segurança no nível de *hardware* fazem com que o dispositivo permaneça seguro e inalterável desde o momento de sua conexão na rede até o momento de sensoriamento e envio de dados [44]. O canal de comunicação também é testado para que os dados trafeguem de maneira segura [43]. Diversas aplicações de segurança na camada de software, com decisão baseada em dois fatores, e decisões de segurança baseada no contexto do ambiente também são pesquisadas [13, 41, 52]. Além disso, diferentes tecnologias emergentes são utilizadas para aumentar a segurança em ambientes computacionais sensíveis, como a IoT [14, 27]. Exemplos destas tecnologias são: blockchain[1] [34], segurança baseada no contexto, protocolos de comunicação leves, entre outros. Embora existam diversas pesquisas na área de segurança e privacidade para IoT, a portabilidade de dados amplia as possibilidades de ataques para tais ambientes, necessitando o desenvolvimento específico de soluções para diminuir os riscos aos dados de usuários.

A Internet das Coisas é uma área em franca expansão, atingindo a cada ano um número maior de soluções e usuários. Juntamente dos diversos benefícios provenientes de aplicações que utilizem tecnologias IoT, como conectividade, agilidade e prestação de serviços personalizados, a área traz uma vasta gama de desafios na sua implementação. Além disso, o direito a portabilidade de dados, unido aos ambientes inteligentes de Internet das Coisas, pode aumentar a complexidade na soluções de tais desafios. Por estes motivos, é importante a contínua pesquisa e desenvolvimento em ambas as áreas, de maneira conjunta, para a mitigação destes desafios e para o pleno desenvolvimento e aplicação na prática da portabilidade de dados em ambientes conectados de Internet das Coisas.

NOTAS

CAPÍTULO 3

1 Dados dinâmicos em ambientes IoT são considerados aqueles passíveis de mudanças ao decorrer do tempo, como por exemplo dados de localização, status, climáticos, entre outros.

2 Método utilizado para tornar dados ilegíveis, possibilitando a visualização dos mesmos apenas com o uso de uma chave pré-definida. Pode ser simétrica, através do uso de chave única, ou assimétrica, através do uso de chaves pública e privada

3 Método que torna o dado anônimo, retirando a possibilidade de conectar o dado ao seu provedor.

4 Método que pode camuflar uma mensagem em um texto ou imagem que parece não carregar dados sensíveis. Exemplos são: (i) embutir mensagens apenas nas letras inicias de uma frase, ou (ii) inserir mensagens dentre os pixels de uma imagem.

CAPÍTULO 4

1 Cadeia de blocos. Abordagem computacional emergente para encadeamento e registro de informações/dados de maneira distribuída como medida de segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] Amaral, L. A.; Matos, E.; Tiburski, R. T.; Hessel, F.; Lunardi, W. T.; Marczak, S. “Internet of Things (IoT) in 5G Mobile Technologies”. Cham: Springer International Publishing, 2016, cap. Middleware Technology for IoT Systems: Challenges and Perspectives Toward 5G, pp. 333–367.

[2] Amaral, L. A.; Tiburski, R. a. T.; de Matos, E.; Hessel, F. “Cooperative Middleware Platform as a Service for Internet of Things Applications”. In: Proceedings of the 30th Annual ACM Symposium on Applied Computing, 2015, pp. 488–493.

[3] Atzori, L.; Iera, A.; Morabito, G. “The internet of things: A survey”, *Computer Networks*, vol. 54–15, Oct 2010, pp. 2787–2805.

[4] Bandyopadhyay, D.; Sen, J. “Internet of things: Applications and challenges in technology and standardization”, *Wireless Personal Communications*, vol. 58–1, Apr 2011, pp. 49–69.

[5] Botta, A.; De Donato, W.; Persico, V.; Pescapé, A. “Integration of cloud computing and internet of things: a survey”, *Future generation computer systems*, vol. 56, 2016, pp. 684–700.

[6] Bowman, J.; Gufflet, M. “Meeting the challenge of a global gdpr and bcr programme”, *Eur. Data Prot. L. Rev.*, vol. 3, 2017, pp. 257.

[7] Canto Moniz, G. “Direitos do titular dos dados pessoais: o direito à portabilidade (data subjects rights: The right to data portability)”, *Anuário da Proteção de dados*, vol. 1–1, 2018.

[8] Datta, S. K.; Gyrard, A.; Bonnet, C.; Boudaoud, K. “onem2m architecture based user centric iot application development”. In: 3rd International Conference on Future Internet of Things and Cloud, 2015, pp. 100–107.

[9] De Hert, P.; Papakonstantinou, V.; Malgieri, G.; Beslay, L.; Sanchez, I. “The right to data portability in the gdpr: Towards user-centric interoperability of digital services”, *Computer Law & Security Review*, vol. 34–2, 2018, pp. 193 – 203.

[10] de Matos, E.; Amaral, L. A.; Hessel, F. “Context-Aware Systems: Technologies and Challenges in Internet of Everything Environments”. Cham: Springer International Publishing, 2017, cap. 1, pp. 1–25.

[11] de Matos, E.; Amaral, L. A.; Tiburski, R. T.; Schenfeld, M.; Hessel, F.; de Azevedo, D. “A Sensing-as-a-Service Context-Aware system for internet of things environments” In: Proceedings of the 14th IEEE Annual Consumer Communications & Networking Conference, 2017, pp. 725–728.

[12] de Matos, E.; Tiburski, R. T.; Amaral, L. A.; Hessel, F. “Context Interoperability for IoT Through an Edge-Centric Context Sharing Architecture”. In: Proceedings of the 23th IEEE Symposium on Computers and Communications, 2018, pp. 00667–00670.

[13] de Matos, E.; Tiburski, R. T.; Amaral, L. A.; Hessel, F. “Providing Context-Aware Security for IoT Environments Through Context Sharing Feature”. In: Proceedings of the 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, 2018, pp. 1711–1715.

[14] de Matos, E.; Tiburski, R. T.; Moratelli, C. R.; Filho, S. J.; Amaral, L. A.; Ramachandran, G.; Krishnamachari, B.; Hessel, F. “Context information sharing for the Internet of Things: A survey”, *Computer Networks*, vol. 166, Jan 2020, pp. 1–19.

[15] de Oliveira, N. S. “Segurança da informação para internet das coisas (iot): uma abordagem sobre a lei geral de proteção de dados (lgpd)”, *Revista Eletrônica de Iniciação Científica em Computação*, vol. 17–4, 2019.

[16] Dolui, K.; Datta, S. K. “Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing”. In: Proceedings of the Global Internet of Things Summit, 2017, pp. 1–6.

[17] Doneda, D. “Reflexões sobre proteção de dados pessoais em redes sociais”, *Revista Internacional de Protección de Datos Personales*, vol. 1–1, 2012, pp. 1–12.

[18] Egan, E. “Data portability and privacy”. Capturado em: https://about.fb.com/wp-content/ uploads/2020/02/data-portability-privacy-white-paper.pdf, 2019.

[19] Erickson, A. “Comparative analysis of the eu’s gdpr and brazil’s lgpd: Enforcement challenges with the lgpd”, *Brook. J. Int’l L.*, vol. 44, 2018, pp. 859.

[20] Ericsson. “IoT connections outlook”. Capturado em: https://www.ericsson.com/en/mobility-report/reports, July 2019.

[21] Fowler, L. R.; Gillard, C.; Morain, S. R. “Readability and accessibility of terms of service and privacy policies for menstruation-tracking smartphone applications”, *Health Promotion Practice*, vol. 21–5, 2020, pp. 679–683, pMID: 32037887, https://doi.org/10.1177/1524839919899924.

[22] Gartner. “Gartner says worldwide iot security spending will reach $1.5 billion in 2018”. Capturado em: https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018, Mar 2020.

[23] Gomes, M. C. O. “Portabilidade de dados reputacionais: a problemática da sua aplicabilidade na economia compartilhada”. Capturado em: https://www.academia.edu/37027420/Portabilidade_de_dados_reputacionais_a_problem%C3%A1tica_da_sua_aplicabilidade_na_economia_compartilhada, Ago 2020.

[24] Krishnamachari, B.; Power, J.; Kim, S. H.; Shahabi, C. “I3: An iot marketplace for smart communities”. In: Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services, 2018, pp. 498–499.

[25] Leonard, P. G. “Regulatory trends and emerging practices in access to customer data, portability and data sharing in the financial services sector”, *Data Synergies Pty Limited*, vol. 2, 2017.

[26] Mišura, K.; Žagar, M. “Data marketplace for internet of things”. In: 2016 International Conference on Smart Systems and Technologies (SST), 2016, pp. 255–260.

[27] Moratelli, C. R.; Tiburski, R. T.; de Matos, E.; Portal, G.; Johann, S. F.; Hessel, F. “Privacy and security of Internet of Things devices”. In: *Real-Time Data Analytics for Large Scale Sensor Data*, Das, H.; Dey, N.; Balas, V. E. (Editores), Academic Press, 2020, *Advances in Ubiquitous Sensing Applications for Healthcare*, vol. 6, cap. 9, pp. 183 – 214.

[28] Nagorny, K.; Scholze, S.; Ruhl, M.; Colombo, A. W. “Semantical support for a CPS data marketplace to prepare Big Data analytics in smart manufacturing environments”. In: Proceedings of the 1st IEEE Industrial Cyber-Physical Systems, 2018, pp. 206–211.

[29] Ngu, A. H.; Gutierrez, M.; Metsis, V.; Nepal, S.; Sheng, Q. Z. “IoT Middleware: A Survey on Issues and Enabling Technologies”, *IEEE Internet of Things Journal*, vol. 4– 1, Feb 2017, pp. 1–20.

[30] Nogueira, C. A. G.; MOTA, M. D. O.; de Almeida, F. C.; de Lima, P. G. N.; de Moura, H. J. “Uma análise avaliativa e comportamental dos consumidores do setor de telefonia móvel antes e depois da portabilidade numérica”, *Revista Base (Administração e Contabilidade) da UNISINOS*, vol. 9–4, 2012, pp. 340–356.

[31] Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. “Context Aware Computing for The Internet of Things: A Survey”, *IEEE Communications Surveys Tutorials*, vol. 16– 1, First Quarter 2014, pp. 414–454.

[32] Ponce, P. P. “Direito à portabilidade de dados: entre a proteção de dados e a concorrência”, *Revista de Defesa da Concorrência*, vol. 8–1, 2020, pp. 134–176.

[33] Rahman, H.; Hussain, M.; et al.. “LiO-IoT: A Light-weight Ontology to provide Semantic Interoperability in Internet of Things”, *International Journal of Computational Intelligence & IoT*, vol. 2–4, Mar 2019, pp. 571–575.

[34] Ramachandran, G. S.; Krishnamachari, B. “Blockchain for the iot: Opportunities and challenges”, *CoRR*, vol. abs/1805.02818, 2018, 1805.02818.

[35] Ramos, J. L. H.; Bernabe, J. B.; Skarmeta, A. F. “Managing Context Information for Adaptive Security in IoT Environments”. In: Proceedings of the 29th IEEE International Conference on Advanced Information Networking and Applications Workshops, 2015, pp. 676–681.

[36] Ray, P. P. “A survey of iot cloud platforms”, *Future Computing and Informatics Journal*, vol. 1–1, 2016, pp. 35 – 46.

[37] Ray, P. P. “A survey on internet of things architectures”, *Journal of King Saud University-Computer and Information Sciences*, vol. 30–3, 2018, pp. 291–319.

[38] Roman, R.; Lopez, J.; Mambo, M. “Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges”, *Future Generation Computer Systems*, vol. 78, 2018, pp. 680–698.

[39] Schenfeld, M.; Amaral, L.; de Matos, E.; Hessel, F. “Arquitetura para fog computing em sistemas de middleware para internet das coisas”. In: Anais do XLIII Seminário Integrado de Software e Hardware, 2016, pp. 199–209.

[40] Sinha Roy, D.; Behera, R. K.; Reddy, K. H. K.; Buyya, R. “A Context-Aware Fog Enabled Scheme for Real-Time Cross-Vertical IoT Applications”, *IEEE Internet of Things Journal*, vol. 6–2, Apr 2019, pp. 2400–2412.

[41] Tao, M.; Zuo, J.; Liu, Z.; Castiglione, A.; Palmieri, F. “Multi-layer cloud architectural model and ontology-based security service framework for iot-based smart homes”, *Future Generation Computer Systems*, vol. 78, Jan 2018, pp. 1040 – 1051.

[42] Tiburski, R. T.; Amaral, L. A.; Matos, E. D.; Hessel, F. “The importance of a standard security architecture for SOA-based IoT middleware”, *IEEE Communications Magazine*, vol. 53–12, Dec 2015, pp. 20–26.

[43] Tiburski, R. T.; de Matos, E.; Hessel, F. “Evaluating the DTLS Protocol from CoAP in Fog-to-Fog Communications”. In: Proceedings of the 14th IEEE International Conference on Service-Oriented System Engineering, 2019, pp. 90–905.

[44] Tiburski, R. T.; Moratelli, C. R.; Johann, S. F.; Neves, M. V.; d. Matos, E.; Amaral, L. A.; Hessel, F. “Lightweight Security Architecture Based on Embedded Virtualization and Trust Mechanisms for IoT Edge Devices”, *IEEE Communications Magazine*, vol. 57–2, Feb 2019, pp. 67–73.

[45] Travizano, M.; Minnoni, M.; Ajzenman, G.; Sarraute, C.; Della Penna, N. “Wibson: A decentralized marketplace empowering individuals to safely monetize their personal data”. Capturado em: https://wibson.org/wp-content/uploads/2019/04/Wibson-Technical-Paper-v1.1.pdf, Nov 2019.

[46] Turner, S.; Quintero, J. G.; Turner, S.; Lis, J.; Tanczer, L. M. “The exercisability of the right to data portability in the emerging internet of things (iot) environment”, *New Media & Society*, vol. 0–0, 2020, pp. 1461444820934033, https://doi.org/10.1177/1461444820934033.

[47] Urquhart, L.; Sailaja, N.; McAuley, D. “Realising the right to data portability for the domestic internet of things”, *Personal and Ubiquitous Computing*, vol. 22–2, 2018, pp. 317–332.

[48] Urquhart, L.; Sailaja, N.; McAuley, D. “Realising the right to data portability for the domestic internet of things”, *Personal and Ubiquitous Computing*, vol. 22–2, 2018, pp. 317–332.

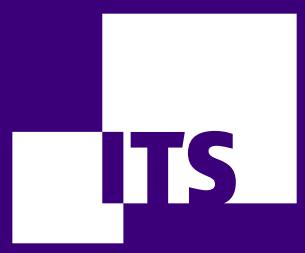
[49] Ursic, H. “Unfolding the new-born right to data portability: Four gateways to data subject control”, *SCRIPTed*, vol. 15, 2018, pp. 42.

[50] Wachter, S. “The gdpr and the internet of things: a three-step transparency model”, *Law, Innovation and Technology*, vol. 10–2, 2018, pp. 266–294, https://doi.org/10.1080/17579961.2018.1527479.

[51] Washizaki, H.; Ogata, S.; Hazeyama, A.; Okubo, T.; Fernandez, E. B.; Yoshioka, N. “Landscape of architecture and design patterns for iot systems”, *IEEE Internet of Things Journal*, vol. 1–1, 2020, pp. 1–12.

[52] Zhang, L.; Li, Y.; Wang, L.; Lu, J.; Li, P.; Wang, X. “An Efficient Context-Aware Privacy Preserving Approach for Smartphones”, *Security and Communication Networks*, vol. 2017, Apr 2017, pp. 1–11.

[53] Zheng, S.; Apthorpe, N.; Chetty, M.; Feamster, N. “User perceptions of smart home iot privacy”, *Proc. ACM Hum.-Comput. Interact.*, vol. 2–CSCW, nov. 2018.



Acesse nossas redes

itsrio.org