UNIVERSIDADE FEDERAL DE SÃO CARLOS

CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

PRIVACY EVERYWHERE: MECANISMO PARA TOMADA DE DECISÕES E GARANTIA DA PRIVACIDADE EM AMBIENTES IOT

LEANDRO PRADO DE ANDRADE

ORIENTADOR: PROF. DR. SERGIO DONIZETTI ZORZO

São Carlos - SP
Dezembro/2019

UNIVERSIDADE FEDERAL DE SÃO CARLOS

CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

PRIVACY EVERYWHERE: MECANISMO PARA TOMADA DE DECISÕES E GARANTIA DA PRIVACIDADE EM AMBIENTES IOT

LEANDRO PRADO DE ANDRADE

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de São Carlos, como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação, área de concentração: Sistemas Distribuídos e Redes de Computadores.
Orientador: Prof. Dr. Sergio Donizetti Zorzo

São Carlos - SP
Dezembro/2019

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Ciência da Computação

Folha de Aprovação

Assinaturas dos membros da comissão examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato Leandro Prado de Andrade, realizada em 03/12/2019:

Prof. Dr. Sergio Donizetti Zorzo
UFSCar

Prof. Dr. Helio Crestana Guardia
UFSCar

Prof. Dr. Valderi Reis Quietinho Leithardt
UNIVALI

Certifico que a defesa realizou-se com a participação à distância do(s) membro(s) Valderi Reis Quietinho Leithardt e depois das arguições e deliberações realizadas, o(s) participante(s) à distância está(ao) de acordo com o conteúdo do parecer da banca examinadora redigido neste relatório de defesa.

Prof. Dr. Sergio Donizetti Zorzo

Dedico este trabalho à minha família e à minha noiva, meu porto seguro em momentos difíceis.

AGRADECIMENTO

Agradeço a Deus pela força e por tornar este momento possível.

Agradeço aos meus pais, à minha família e à minha noiva pelo apoio e por entenderem os momentos que estive ausente.

Agradeço ao professor Zorzo pela orientação, confiança e por todo conhecimento transmitido.

Agradeço a todos os professores que contribuíram para a minha formação.

E, por fim, agradeço a todos que contribuíram direta ou indiretamente para a realização deste trabalho.

"A persistência é o menor caminho do êxito".

Charles Chaplin

RESUMO

Por meio dos avanços tecnológicos, a sociedade tem se movido em direção ao paradigma “sempre conectado”. Uma variedade crescente de dispositivos está se tornando capaz de se conectar em uma rede, de captar informações ao seu redor e de enviar e receber informações. Por outro lado, o aumento no número de dispositivos de Internet das Coisas - do inglês Internet of Things (IoT), a possibilidade de integração de dispositivos com nuvens IoT e a diversidade de formas de interação podem tornar cansativo que o usuário tome uma decisão de privacidade sempre que entre em contato com um novo dispositivo IoT. Devido a sensibilidade de muitas das informações captadas por dispositivos IoT e também pelo fato de que serviços de nuvem IoT não possuem como foco a preservação da privacidade do usuário, se faz necessário que os dados captados por dispositivos IoT sejam tratados antes de serem enviados aos serviços de nuvem. Os ambientes IoT podem apresentar um número elevado de dispositivos coletores de dados que muitas vezes passam despercebidos pelos usuários. Informar o usuário sobre a presença de cada um destes dispositivos e pedir ao usuário que tome decisões de privacidade sobre a coleta de dados destes dispositivos pode ser inviável. Este trabalho apresenta o mecanismo Privacy Everywhere para tomada de decisões e garantia da privacidade do usuário em ambientes IoT. O mecanismo proposto trata as questões de privacidade do usuário e faz uso de redes neurais treinadas com dados coletados de uma comunidade pré-estabelecida. Com isso, minimiza a consulta ao usuário no momento da coleta de dados pelo dispositivo integrante de um ambiente IoT. Na validação do mecanismo, a verificação da precisão das redes neurais Allow/Deny e Privacy Action que compõem o mecanismo, apresentou uma precisão de 88,02% e 86,67% respectivamente. O mecanismo Privacy Everywhere se mostrou capaz de ajudar os usuários a preservarem a privacidade de seus dados nos ambientes IoT.

Palavras-chave: Internet das Coisas, privacidade em IoT, preferências de privacidade, tomada de decisão.

ABSTRACT

Through technological advances, society has moved toward the "always connected" paradigm. Growing varieties of devices are becoming able to connect to a network, capture information around them, and send and receive information. On the other hand, increasing in number of Internet of Things (IoT) devices, the ability to integrate IoT devices with IoT cloud services, and the diversity of forms of interaction can make it tiring to ask the user to make a privacy decision whenever it contacts a new IoT device. Due to sensitivity of many of information captured by IoT devices and because IoT cloud services do not focus on preserving user privacy, it is necessary that data captured by IoT devices be processed before being sent to cloud services. IoT environments can have a large number of data collection devices that often go unnoticed by users. Informing the user about the presence of each one of these devices and asking the user to make privacy decisions about data collection from these devices may be impracticable. This work presents the Privacy Everywhere mechanism for decision making and user privacy assurance in IoT environments. The proposed mechanism addresses user privacy issues and makes use of trained neural networks with data collected from a pre-established community. This minimizes user consultation at the time of data collection by the device that is part of an IoT environment. In validation of the mechanism, accuracy check of the Allow/Deny and Privacy Action neural networks that make up the mechanism presented an accuracy of 88.02% and 86.67%, respectively. Privacy Everywhere mechanism is able to help users preserve the privacy of their data in IoT environments.

Keywords: Internet of Things, IoT privacy, privacy preferences, decision making.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

CoT - *Cloud of Things*

IaaS - *Infrastructure as a Service*

IoT - *Internet of Things*

IP – *Internet Protocol*

LGPD – Lei Geral de Proteção de Dados

MQTT - *Message Queue Telemetry Transport*

OWASP - *Open Web Application Security Project*

PaaS - *Platform as a Service*

PDL – *Privacy Development Language*

RFID - *Radio Frequency Identification*

SaaS - *Software as a Service*

SDK – *Software Development Kit*

SenaaS - *Sensor as a Service*

TaaS - *Things as a Service*

TIC - *Tecnologia de Informação e Comunicação*

UML – *Unified Modeling Language*

UPECSI – *User-driven Privacy Enforcement for Cloud-based Services in the IoT*

WSN - *Wireless Sensor Network*

SUMÁRIO

Capítulo 1

INTRODUÇÃO

Este capítulo apresenta o contexto no qual o trabalho está inserido, a motivação para a sua realização, o objetivo, as contribuições e limitações desta pesquisa, bem como a forma como o trabalho está organizado.

1.1 Contexto

Por meio dos avanços tecnológicos, a sociedade tem se movido em direção ao paradigma “sempre conectado”. Uma variedade crescente de dispositivos está se tornando capaz de se conectar em uma rede, de captar as informações ao seu redor e de enviar e receber informações.

Neste contexto está inserida a Internet das Coisas, que é o que há de mais recente para descrever a tendência dos dispositivos a se tornarem mais inteligentes, mais comunicativos, mais conscientes e mais capazes de reagirem ao seu contexto (Rosner,2016).

Não existe uma definição precisa do que é Internet das Coisas. Existem vários conceitos sobrepostos para descrever um mundo de dispositivos que conversam entre si: inteligência ambiente, computação contextual e computação onipresente (Rosner,2016).

A definição de *Internet of Things* (IoT) que foi considerada para o desenvolvimento deste trabalho é a definição de Brown (2016) que definiu IoT como uma rede de dispositivos físicos, que permite que esses dispositivos se conectem e troquem dados. Cada dispositivo é identificável por meio de seu sistema de

computação embarcado e é capaz de interagir dentro de uma infraestrutura existente.

Para ser uma coisa integrante da Internet das Coisas o dispositivo precisa ter um identificador único, ter um meio de comunicação disponível e possuir sensores capazes de informar algo sobre a coisa ou sobre o ambiente. Um dispositivo IoT também possui a característica de realizar uma ponte entre o mundo físico e o mundo eletrônico.

No ambiente IoT surgem novas formas de comunicação e interação, com consequente surgimento de novas ameaças à privacidade e surge também uma grande quantidade de dados sensíveis. A privacidade é uma grande preocupação e um obstáculo para a maior difusão dos serviços de IoT (Kim *et al.*, 2019).

Para que se estabeleça a comunicação entre pessoas e objetos inteligentes, a infraestrutura computacional em nuvem vem sendo um componente crucial. Diversos provedores de serviços de nuvem IoT, como a IBM Cloud[1] e AWS IoT[2], estão surgindo no mercado com funcionalidades como gerenciamento de dispositivos, gerenciamento de dados, monitoramento e processamento dos dados.

Segundo Tanenbaum e Steen (2007), um sistema distribuído é uma coleção de computadores independentes entre si que se apresenta ao usuário como um sistema único e coerente. Um sistema em Internet das Coisas também pode ser considerado um sistema distribuído, porém cada coisa possui um poder de processamento menor se comparada a computadores integrantes de um sistema distribuído. Pois, apesar de terem poder de processamento, as coisas são projetadas para executar apenas algumas funções específicas.

1.2 Motivação

O aumento no número de dispositivos IoT e a possibilidade de integração de serviços e cruzamento de informações podem criar um ambiente extremamente benéfico, porém sujeito a problemas de privacidade com potenciais efeitos catastróficos. Uma checagem nos sensores de presença de uma residência poderia

[1] https://www.ibm.com/cloud/

[2] https://aws.amazon.com/pt/iot/

indicar a indivíduos mal-intencionados que a casa está vazia e dar sinal verde para uma tentativa de furto. A captação da localização dos usuários poderia indicar os locais que estes frequentam e facilitar a ação de sequestradores. A obtenção das preferências salvas em uma *smart tv* poderia resultar na criação de anúncios direcionados. Enfim os cenários e possibilidades são inúmeros. Um mecanismo que atue nestes cenários de coleta de dados pode poupar esforço e tempo dos usuários, e também garantir a privacidade dos usuários durante a coleta de dados.

As soluções IoT, comumente, necessitam de um serviço de nuvem IoT, onde é feito o controle de acesso, o processamento das informações, o gerenciamento da configuração dos dispositivos, dentre outras funcionalidades.

Visto que os serviços de nuvem IoT não possuem como foco a preservação da privacidade do usuário, se faz necessário então que os dados captados pelos dispositivos IoT sejam tratados antes de serem enviados aos serviços de nuvem IoT.

Os ambientes com elevada interação e comunicação, como são os ambientes IoT, possuem dispositivos coletores de dados que muitas vezes passam despercebidos pelos usuários. Estes ambientes também podem apresentar uma quantidade elevada de dispositivos coletores de dados. Pedir ao usuário que tome decisões de privacidade toda vez que entre em contato com um novo dispositivo ou algum serviço tente acessar determinada informação pode ser muito cansativo ou inviável.

1.3 Objetivo

Este trabalho tem como objetivo apresentar o mecanismo Privacy Everywhere para garantia da privacidade e tomada de decisão em ambientes IoT. O objetivo desse mecanismo é tomar decisões de privacidade pelos usuários nesses ambientes e executar ações de privacidade nos dados coletados por dispositivos IoT antes que os dados sejam enviados para os serviços de nuvem IoT; ou permitir que o usuário decida e defina qual ação de privacidade deve ser executada na coleta de dados em questão.

O mecanismo proposto trata as questões de privacidade do usuário e faz uso de redes neurais treinadas com dados coletados de uma comunidade pré-

estabelecida. Com isso, minimiza a consulta ao usuário no momento da coleta de dados pelo dispositivo integrante de um ambiente IoT.

1.4 Contribuições e limitações

Este trabalho possui como principal contribuição a apresentação do mecanismo Privacy Everywhere para tomada de decisão e realização de ações de privacidade de forma automatizada ou para que o usuário decida manualmente e indique a ação de privacidade a ser executada nos dados coletados. Esta pesquisa ainda apresenta as seguintes contribuições:

- São fornecidos insights sobre quais fatores influenciam a tomada de decisão de privacidade pelos usuários e também sobre como estão correlacionados o nível de conforto do usuário com a coleta de dados apresentada no cenário IoT com a decisão de permitir ou negar o envio do dado.
- As ações de privacidade realizadas pelo mecanismo nos dados coletados em ambientes de IoT, indicam alternativas para atenuar os riscos de privacidade inerentes ao surgimento de novas formas de interação e comunicação.
- São fornecidas indicações de que tanto as decisões de privacidade dos usuários quanto as ações de privacidade a serem executadas em cada cenário específico podem ser automatizadas.

Esta pesquisa apresenta como limitações:

- O número de fatores influentes na tomada de decisão de privacidade utilizados neste trabalho não contempla todas as situações possíveis de serem encontradas em ambientes IoT.
- O grupo de usuários pesquisados neste trabalho não apresenta diferentes níveis de formação, já que todos os usuários pesquisados eram estudantes de graduação de uma Universidade Federal.

1.5 Organização do Trabalho

O presente trabalho está organizado da seguinte forma: o Capítulo 2 apresenta características e desafios encontrados em Internet das Coisas. No Capítulo 3 são apresentadas ameaças à privacidade em ambientes IoT e também métodos e técnicas de preservação da privacidade. No Capítulo 4 são apresentadas plataformas de nuvem IoT e suas características. No Capítulo 5 são descritos trabalhos relacionados. No Capítulo 6 são apresentadas as pesquisas realizadas neste trabalho com usuários e com profissionais da área de redes e/ou segurança da informação. No Capítulo 7 o mecanismo Privacy Everywhere é apresentado. No Capítulo 8 é mostrado como foi feita a validação do mecanismo e é realizada uma discussão sobre os resultados obtidos. Por fim, no Capítulo 9, são apresentadas as conclusões e os trabalhos futuros.

Capítulo 2

INTERNET DAS COISAS

Neste capítulo é apresentado um modelo de referência para Internet das Coisas bem como suas características. Também é feita uma contextualização de Internet das Coisas em diversos domínios de aplicação. Por fim são apresentados alguns desafios gerais encontrados em ambientes IoT.

2.1 Considerações iniciais

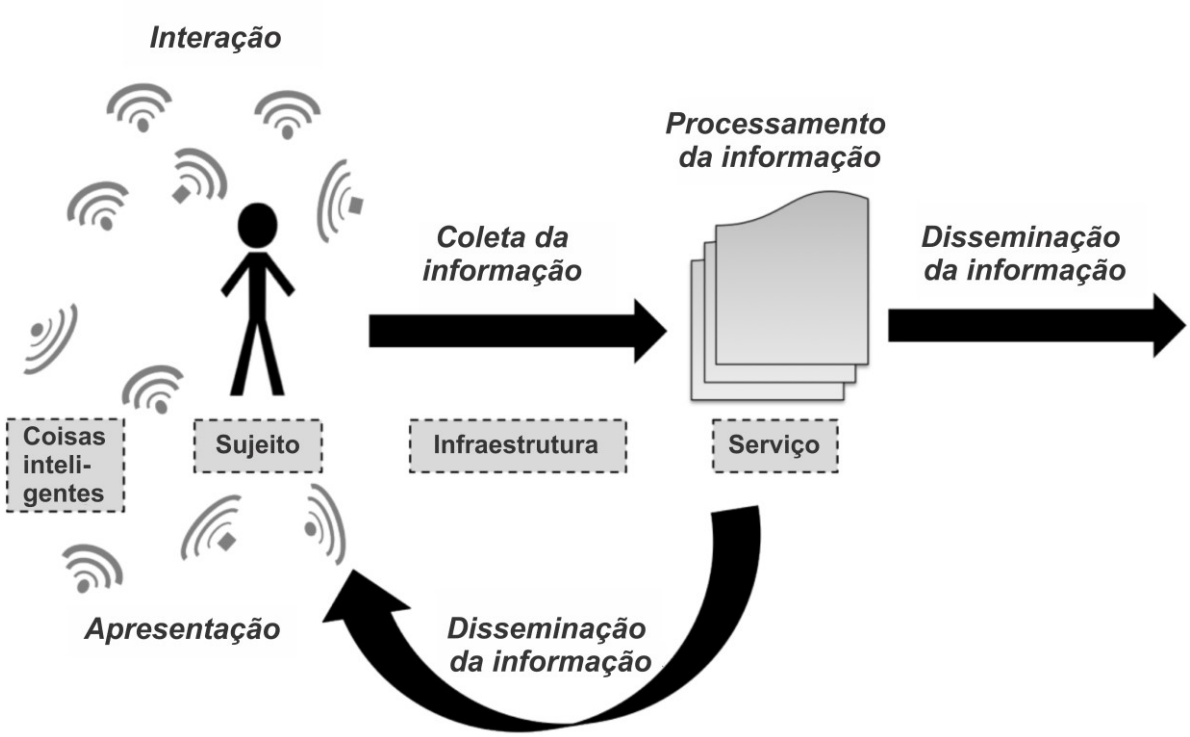
A internet das coisas surgiu como um novo paradigma capaz de realizar grandes transformações na forma de trabalho, nas formas de interação e nos modos de coleta e processamento de informações. Mercer (2017) estimou que no final de 2021 haverá 30 bilhões de dispositivos IoT conectados à Internet. Muitos podem ser os benefícios do paradigma IoT, porém surgem também diversos desafios a serem superados neste modelo.

Diante disso, é apresentado um modelo de referência IoT na seção 2.2. Na seção 2.3 são mostradas algumas áreas de aplicação da Internet das Coisas. Na seção 2.4 são mostrados alguns dos desafios encontrados em ambientes IoT.

2.2 Modelo de referência IoT

O modelo de referência IoT apresentado na Figura 2.1, foi escolhido para este trabalho porque considera como visão de Internet das coisas qualquer pessoa ou qualquer coisa conectada em qualquer lugar por meio de qualquer rede participante de qualquer serviço.

Figura 2.1 – Modelo de referência IoT com entidades relevantes e fluxos de dados em uma aplicação IoT típica



Fonte: Adaptado de Ziegeldorf, Morchon e Wehrle (2014).

O modelo de referência proposto por Ziegeldorf, Morchon e Wehrle (2014) considera quatro tipos de entidades: coisas inteligentes, sujeito, infraestrutura e serviço. As coisas inteligentes são capazes de coletar, processar e comunicar dados sobre elas mesmas e seu ambiente, bem como interagir com outras coisas e humanos.

Os humanos possuem dois diferentes papéis no modelo de referência: podem ser alvo da coleta de dados e podem ser também os destinatários dos serviços oferecidos.

As coisas inteligentes são conectadas a serviços por meio de uma infraestrutura que apresenta em sua composição desde redes de baixa potência até *backbones* poderosos.

Este modelo também considera cinco tipos de fluxo de dados: Interação, Apresentação, Coleta de Informação, Processamento da Informação e Disseminação da Informação.

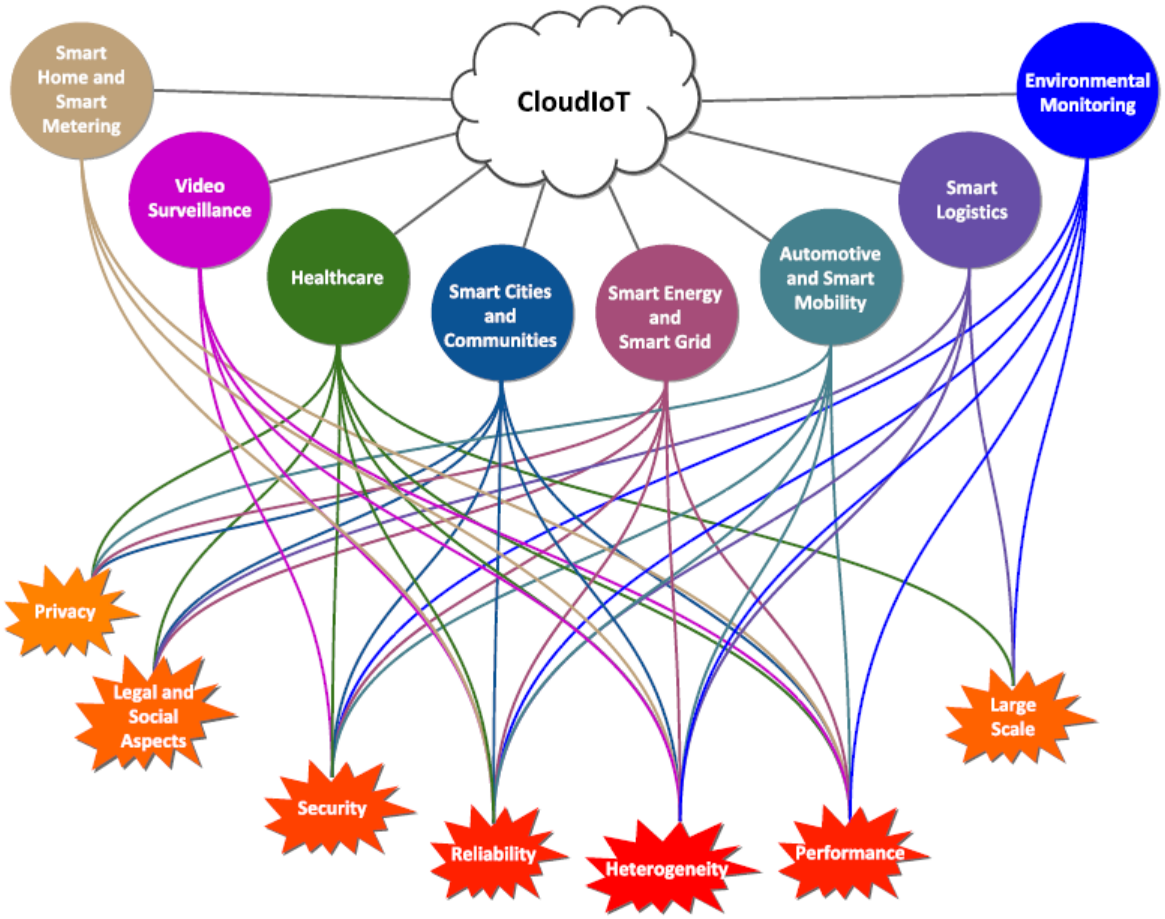
Segundo Ziegeldorf, Morchon e Wehrle (2014), na fase de Interação, a pessoa interage passiva ou ativamente com as coisas inteligentes em seu ambiente,

acionando um serviço. Coisas Inteligentes realizam, então, a coleta de informações e retransmitem as informações coletadas por meio da conexão disponível. Na fase de processamento, as informações são analisadas para fornecer o serviço solicitado. A divulgação da Informação constitui-se na quarta fase. Por fim, na fase de apresentação, o serviço é fornecido ao usuário de acordo com o resultado do processamento das informações.

2.3 Cenários de aplicação da IoT

Com a integração entre dispositivos e nuvens IoT, surge a possibilidade de implantação de novos serviços e surgem também novos desafios a serem superados. A Figura 2.2 mostra possíveis cenários de aplicação da IoT e seus respectivos desafios apresentados.

Figura 2.2 – Cenários de aplicação da IoT e seus respectivos desafios



Fonte: Botta, A. et al. (2014).

A Internet das coisas deverá oferecer soluções promissoras que provavelmente transformarão a forma de operação e o papel de muitos sistemas industriais existentes. Um exemplo de aplicação seria utilizar a IoT para criar sistemas de transportes inteligentes. Nesta aplicação, seria possível rastrear a localização de cada veículo, monitorar o seu movimento, prever a sua localização futura e indicar as melhores rotas para os veículos (Xu, He e Li, 2014).

Com o exemplo anterior também seriam impactados outros serviços. No mercado de seguros automotivos, um melhor rastreamento dos veículos e melhor monitoramento das rodovias poderia resultar em uma queda nos custos tanto para a seguradora quanto para o segurado. Se fossem geradas e processadas informações sobre a forma de condução, poderiam ser gerados e enviados alertas ao mau condutor com o objetivo de reduzir o número de acidentes. Perfis também poderiam ser criados para categorizar os condutores para auxiliar no cálculo do preço dos seguros.

Expandindo um pouco a ideia dos transportes inteligentes, se todos os componentes do veículo fossem integrantes da Internet das Coisas, poderiam ser criadas aplicações para o monitoramento dos componentes onde os proprietários dos veículos conseguiriam monitorar o estado destes componentes e saberiam o exato momento de se realizar a troca de um componente defeituoso ou com grande probabilidade de falha. Isto evitaria acidentes e geraria economia aos proprietários dos veículos.

Uma tecnologia fundamental para a IoT é a tecnologia *Radio Frequency Identification* (RFID), que permite que microchips transmitam as informações de identificação para um leitor por meio de comunicação sem fio (Xu, He e Li, 2014). Com o uso de leitores RFID, os objetos com tags RFID podem ser identificados, rastreados e monitorados automaticamente (Jia *et al.*, 2012). A tecnologia RFID tem sido amplamente utilizada em logística, produção farmacêutica e no gerenciamento da cadeia de suprimentos desde 1980 (Ngai *et al.,* 2008). Atualmente, a tecnologia RFID também é utilizada em aplicações diversas como pedágios, aplicações médicas e aplicações biométricas.

Outra tecnologia fundamental para IoT são as *Wireless Sensor Network*s (WSNs) que fazem uso de sensores inteligentes interconectados para realizar monitoramento e coleta de informações. As WSNs podem ser aplicadas no monitoramento industrial, no monitoramento de cuidados com a saúde, no monitoramento ambiental, no monitoramento de tráfego, entre outros serviços. Com os avanços tecnológicos, um número cada vez maior de dispositivos diferentes está sendo envolvido em IoT. Como resultado, essas tecnologias associadas à IoT têm causado grande impacto nas tecnologias de informação e comunicação (TIC) e nas tecnologias de sistemas empresariais (Li, Xu e Wang, 2013).

A seguir, serão apresentados alguns dos cenários de aplicação da IoT com seus respectivos desafios.

2.3.1 Integridade da cadeia de suprimentos e logística inteligente

Segundo Haller, Karnouskos e Schroth (2008) as tecnologias da Internet das Coisas permitem o rastreamento da localização e do estado de um objeto ao longo de todo o ciclo de vida do produto e em toda a cadeia de suprimentos. Isso já é usado para detectar desvios em mercados ilegais e na tentativa de impedir a

introdução de produtos falsificados (Lehtonen, Oertel e Vogt, 2007). Sensores podem ser usados para proteger a integridade física dos produtos. Pode ser verificado se um produto nunca foi exposto a condições ambientais potencialmente prejudiciais. Também pode ser verificada a integridade das rotas de transporte: pode ser verificado se um produto esteve em determinado local onde não deveria estar.

De acordo com Botta *et al*. (2014) a adoção de nuvens IoT em logística permite que seja feita a gestão automatizada de fluxos de mercadorias entre os pontos de origem e destino. Ao se fazer uso de uma arquitetura escalável e modularizada, a nuvem ajuda a tornar o sistema flexível e facilmente expansível.

Os desafios relacionados a este contexto são a heterogeneidade de recursos a serem monitorados e a seleção dos serviços adequados para cada empresa em seu ramo de atuação (Li *et al*., 2013).

2.3.2 Redes de energia inteligentes

De acordo com Hua, Junguo e Fantao (2014) as redes de energia inteligentes são altamente integradas com sensores de medição, tecnologias de informação e comunicação, tecnologias de tomada de decisão e tecnologias de rede elétrica. A rede inteligente permite otimização do controle de potência, flexibilização da estrutura de rede, otimização da alocação de recursos e melhora na qualidade dos serviços. Também é possível que se faça a predição na geração de energia eólica. Por meio de WSN, dados sobre os ventos podem ser coletados em tempo real e eventuais mudanças na quantidade de energia gerada podem ser previstas (Hua, Junguo e Fantao, 2014).

No processo de transmissão de energia, as tecnologias IoT permitem realizar o monitoramento das linhas de transmissão e identificar eventuais falhas mais rapidamente.

Ao se integrar dispositivos e nuvens IoT, o gerenciamento e o processamento de informações das redes de energia podem ser realizados na nuvem, amenizando a questão do baixo poder de processamento dos dispositivos IoT.

Para este tipo de aplicação os desafios relacionados são a heterogeneidade de dispositivos, o volume dos dados e a taxa de transmissão destes dados, e o comportamento da latência na transmissão destes dados (Yun e Yuxin, 2010).

2.3.3 Assistência médica

A tecnologia RFID também vem sendo utilizada em hospitais para localizar e rastrear equipamentos e medicamentos. Alguns hospitais também adotam o RFID como forma de identificação de recém-nascidos.

É reconhecido que doentes crônicos, como aqueles com insuficiência cardíaca, hipertensão, diabetes ou doenças respiratórias, requerem serviços médicos, hospitalares e de emergência mais frequentemente do que pacientes regulares (Paré *et al.,* 2010). Assim, um conjunto de dispositivos interconectados em uma rede IoT dedicada à avaliação de saúde pode detectar automaticamente situações em que a intervenção médica é necessária.

Dispositivos modernos de medição, como aferidores de pressão sanguínea, medidores de peso e sensores de movimento, incorporam capacidade de comunicação e podem ser usados para criar redes IoT para telemonitoramento doméstico das condições de saúde dos pacientes. Estas redes podem ajudar alguns dos problemas associados ao envelhecimento da população, ao aumento das taxas de doenças crônicas e à escassez de profissionais de saúde (Tarouco *et al.,* 2012).

Com a aplicação de nuvens IoT neste campo, é possível que os dados vitais dos pacientes sejam coletados e enviados para uma nuvem de um centro médico para que seja feito o armazenamento e o processamento (Botta *et al.,* 2014).

O grande desafio enfrentado pelas aplicações de assistência médica é com relação à privacidade e à segurança das informações geradas devido ao alto grau de sensibilidade destas informações.

2.3.4 Casas Inteligentes

As casas inteligentes utilizam o conceito de ambiente doméstico do futuro onde sensores e atuadores instalados nas casas e presentes em diversos eletrodomésticos, são autoconfiguráveis e podem ser controlados remotamente. Estes dispositivos detectam e registram as atividades do usuário, registram sua

preferência e permitem uma variedade de tipos de monitoramento e aplicações de controle, com o objetivo de oferecer mais conveniência, conforto e segurança (Li *et al*, 2011).

Os exemplos de dispositivos e aplicações para casas inteligentes são muitos. Existem no mercado sensores de temperatura, sensores de movimento, câmeras, dispositivos que permitem ligar e desligar equipamentos eletrônicos por comandos enviados pela rede sem fio, dispositivos que permitem acender e apagar as luzes da casa e diversos outros.

Segundo Li *et al* (2011), uma expansão do conceito de casas inteligentes é o conceito de comunidades inteligentes, que possui como finalidade melhorar a segurança da comunidade, a segurança doméstica e a capacidade de resposta a emergências. Uma comunidade inteligente é um conjunto de casas inteligentes interligadas por meios de comunicação sem fio, que pode ser vista como um sistema ciber-físico, onde as casas são praticamente sensores multifuncionais com necessidades individuais (Li *et al,* 2011). Cada casa integrante da comunidade realiza o monitoramento de sua área de alcance e emite alertas quando acontece um evento ou comportamento fora do padrão.

A integração entre casas inteligentes e nuvens IoT permite a automação de atividades internas comuns (Botta *et al.,* 2014). Iluminação inteligente tem atraído a atenção de pesquisadores e os sistemas inteligentes de controle de iluminação provaram poupar até 45% da energia consumida com iluminação (Ye e Huang, 2011).

Os desafios relacionados a este contexto são relacionados a falta de padrões na produção de dispositivos IoT domésticos (Botta *et al.,* 2014).

2.3.5 Cidades inteligentes

Segundo Mohanty, Choppali e Kougianos (2016) o conceito de cidade inteligente ainda não está claramente definido. Estes autores sugerem uma definição simplista para cidades inteligentes: é um lugar onde redes tradicionais e serviços são feitos para serem mais flexíveis, eficientes e sustentáveis, que fazem uso de tecnologias de informação e de telecomunicações para melhorar as operações da cidade em benefício de seus habitantes.

As cidades inteligentes integram diferentes componentes tais como infra-estrutura inteligente, transporte inteligente, redes de energia inteligente, saúde inteligente e diversos outros.

Vermesan e Friess (2013) identificaram importantes desafios de pesquisa em aplicações para cidades inteligentes:

- Criar algoritmos e esquemas para descrever informações geradas por sensores em diferentes aplicações para permitir troca útil de informações entre diferentes serviços da cidade
- Garantir leituras confiáveis de uma infinidade de sensores
- Protocolos e algoritmos de baixa energia
- Algoritmos para análise e processamento dos dados adquiridos na cidade
- Implantação e integração em grande escala de dispositivos IoT

2.3.6 Transportes inteligentes e mobilidade inteligente

A integração entre dispositivos e nuvens IoT representa uma oportunidade promissora para transformar os sistemas de transporte e de mobilidade, o que pode aumentar a segurança das estradas, reduzir o congestionamento das estradas, gerenciar o tráfego e estacionamento, e recomendar manutenção nos veículos (He, Yan e Xu, 2014).

Um grande número de veículos já possui capacidade de coletar e enviar informações, trocar informações entre veículos (veículo para veículo – V2V) ou trocar informações com a infraestrutura de estradas inteligentes (veículo para infraestrutura – V2I) (Hank *et al.*, 2013).

Como desafios relacionados a este cenário de aplicações, pode-se citar a dificuldade de se desenvolver sistemas escaláveis devido ao grande número de veículos e também à falta de padrões globais e estudos experimentais para este tipo de aplicação (He, Yan e Xu, 2014).

2.3.7 Monitoramento ambiental

De acordo com Botta *et al.* (2014) a combinação entre dispositivos e nuvens IoT pode contribuir para a implantação de sistemas eficientes para monitoramento de ambientes com grandes áreas.

Pode-se citar como aplicações relacionadas a este cenário o monitoramento da concentração de gás no ar, o monitoramento do nível da água, a detecção de incêndios e o monitoramento de animais (Lazarescu, 2013).

O grande desafio relacionado ao monitoramento ambiental é fornecer uma infraestrutura adequada para o monitoramento de áreas muito extensas.

2.3.8 Vídeo vigilância inteligente

As nuvens IoT no contexto da vídeo vigilância inteligente permitem armazenar, gerenciar e processar conteúdos de câmeras, e também gerar conhecimento automaticamente a partir das cenas (Botta *et al.,* 2014).

Como desafio, tem-se a heterogeneidade e a falta de padrão na fabricação dos dispositivos.

2.4 Desafios gerais encontrados em ambientes IoT

Um dos desafios encontrados em ambientes IoT é realizar a comunicação entre dispositivos que fazem uso do *Internet Protocol* (IP) e dispositivos que não fazem uso de IP (Ma *et al.*, 2016). É necessário que cada componente IoT tenha um identificador único, porém ainda não está padronizado como deverá ser este identificador – se será utilizado algum padrão baseado em IP como o IPv6 ou alguma tecnologia não baseada em IP.

Bandyopadhyay e Sen (2011) apontam como desafios em ambientes IoT:

- Gerenciar a heterogeneidade de dispositivos.

- Gerenciar grande quantidade de informação e volumes de dados para prover serviços úteis.
- Projetar uma arquitetura eficiente para redes de sensores e armazenamento.
- Projetar mecanismos para descoberta de sensores.
- Padronizar dispositivos e interfaces de aplicações.

Por fim, há o desafio das questões de privacidade em ambientes IoT. Este assunto será tratado no próximo capítulo.

2.5 Considerações Finais

A Internet das coisas possui um grande número de áreas de aplicação e um grande número de desafios a serem superados. Para este trabalho, o desafio de maior relevância são as questões de privacidade em ambientes IoT, que serão discutidas no próximo capítulo.

Capítulo 3

PRIVACIDADE EM INTERNET DAS COISAS

Nesse capítulo é apresentada uma definição para privacidade no contexto geral e, mais especificamente, uma definição de privacidade adaptada para ambientes IoT. Serão apresentadas também ameaças à privacidade que surgem com as novas formas de interação presentes em cenários IoT e serão mostrados métodos e técnicas para a preservação da privacidade.

3.1 Considerações iniciais

As novas formas de interação que surgem com o aumento da adoção e com a evolução de dispositivos IoT fazem com que surjam também novas formas de ataque à privacidade. Ataques estes que, se bem-sucedidos, podem levar a efeitos catastróficos. Um pequeno vazamento de informações pode prejudicar seriamente a privacidade do usuário devido à interdependência e à sensibilidade dos dados (Porambage *et al.*, 2016). Além disso, a aceitação dos usuários da implantação de ambientes IoT está condicionada à segurança e confiabilidade na infraestrutura e também ao nível de preservação da privacidade.

Este capítulo apresenta então na seção 3.2 a definição de privacidade adotada para este trabalho. Na seção 3.3 são mostradas as ameaças à privacidade em ambientes de Internet das Coisas. Na seção 3.4 são apresentados métodos e técnicas de preservação da privacidade.

3.2 Definição de privacidade

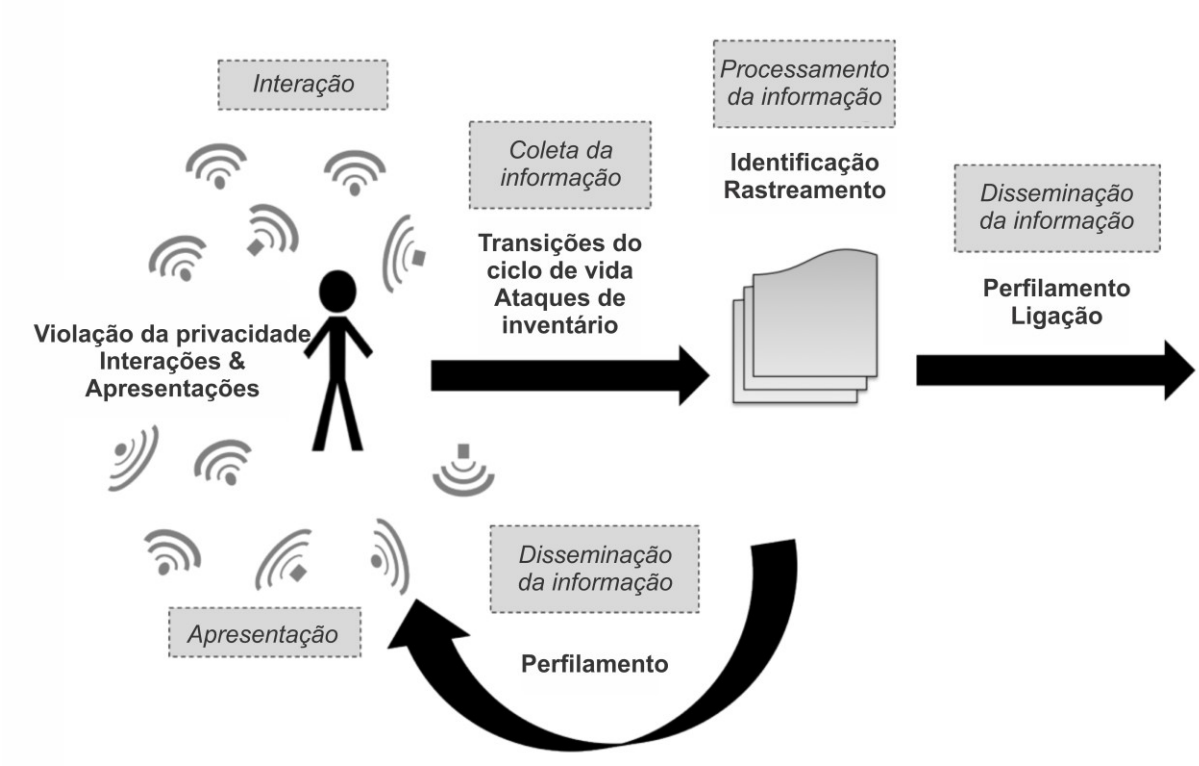
Privacidade é uma noção muito ampla e diversa para a qual a literatura oferece muitas definições e perspectivas (Renaud e Cruz, 2010). Westin em 1967, definiu privacidade como o direito de selecionar quais informações pessoais são divulgadas e para quais pessoas é feita esta divulgação. A definição de Westin apesar de ser para ambientes que não são eletrônicos, ainda é válida. Porém para este trabalho, será usada a definição adaptada de Ziegeldorf, Morchon e Wehrle (2014), que diz que privacidade em Internet das Coisas é a garantia ao usuário de:

- Consciência dos riscos de privacidade impostos por coisas inteligentes e serviços que envolvem dados dos usuários;
- Controle sobre a coleta e o processamento de informações pessoais pelas coisas inteligentes à sua volta;
- Conscientização e controle do uso e divulgação de informações pessoais coletadas por entidades localizadas fora da esfera de controle do usuário.

3.3 Ameaças à privacidade

A natureza evolutiva da IoT bem como as novas formas emergentes de interação levam a ameaças e desafios específicos de privacidade. A Figura 3.1 organiza as ameaças no modelo de referência de acordo com o local onde são mais propensas a aparecer.

Figura 3.1 – Ameaças à privacidade no modelo de referência IoT



Fonte**:** Adaptado de: Ziegeldorf, Morchon e Wehrle (2014).

3.3.1 Identificação

A ameaça de identificação está mais propensa a acontecer na fase de processamento de informações do modelo de referência onde grandes quantidades de informação estão concentradas em um lugar central fora do controle do usuário (Ziegeldorf, Morchon e Wehrle, 2014). Esta ameaça consiste em associar um identificador persistente a um indivíduo e aos dados coletados sobre ele.

Bases de dados faciais estão disponíveis a partes não governamentais, o que torna possível a identificação de indivíduos por meio de imagens de câmeras. A evolução do reconhecimento de fala e a proliferação da computação em nuvem também aumenta o vetor de ataque e os riscos de privacidade.

Proteção contra identificação ganhou atenção nas áreas de anonimização dos dados (Fung *et al,* 2010); porém, a maioria das técnicas de anonimização podem ser quebradas usando dados que provavelmente estarão disponíveis em algum ponto da comunicação no ambiente IoT (El *et al.,* 2011).

É importante que os usuários estejam conscientes de que prevenir a identificação é um grande desafio em ambientes IoT.

3.3.2 Perfilamento

Segundo Ziegeldorf, Morchon e Wehrle (2014) a ameaça de perfilamento ocorre na fase de disseminação das informações e consiste em compilar informações sobre os indivíduos, a fim de inferir interesses por correlação com outros perfis. A criação de perfis é muito utilizada para personalização em comércio eletrônico.

As abordagens existentes para impedir a criação de perfis incluem perturbação dos dados, anonimização e encriptação dos dados (Kobsa, 2007). Estas abordagens devem ser adaptadas para serem aplicadas em cenários de Internet das Coisas.

3.3.3 Localização e rastreamento

Localização e rastreamento é a ameaça de determinar e gravar a localização de um indivíduo em função do tempo e do espaço (Ziegeldorf, Morchon e Wehrle, 2014). O acompanhamento é possível por meio de diferentes meios como tráfego de Internet, localização do telefone celular, GPS, entre outros. Os usuários percebem como uma violação quando eles não têm controle sobre suas informações de localização ou desconhecem a sua divulgação.

Os principais desafios identificados por Ziegeldorf, Morchon e Wehrle (2014) foram: a conscientização do rastreamento na coleta de dados passiva, o controle de dados de localização compartilhados em ambientes internos e protocolos de preservação da privacidade para interação com sistemas IoT.

3.3.4 Ataques de inventário

Ataques de inventário referem-se à coleta não autorizada de informações sobre a existência e características de coisas pessoais. Este tipo de ataque

acontece na fase de coleta de informações do modelo de referência proposto por Ziegeldorf, Morchon e Wehrle (2014).

Ataques de inventário podem ser usados por ladrões para, por exemplo, em conjunto com as informações disponíveis em redes sociais, analisar casas, escritórios e fábricas para que possam determinar as vítimas potenciais (Bloxham, 2011). Também podem ser usados para determinar interesses pessoais de acordo com o conjunto de dispositivos presentes em uma casa e até mesmo como ação complementar de espionagem industrial, como notado por Mattern e Floerkemeier (2010).

3.3.5 Ataques na transição do ciclo de vida de dispositivos

Este tipo de ataque está relacionado com o acesso às informações que não foram efetivamente apagadas de dispositivos eletrônicos. O cenário IoT agravará este tipo de ameaça, visto que aumentará o número de dispositivos que coletarão e armazenarão informações sensíveis em conjunto com um aumento no índice de troca destes dispositivos (Ziegeldorf, Morchon e Wehrle, 2014).

3.3.6 Ataques de ligação

Esta ameaça consiste em ligar diferentes sistemas anteriormente separados tal que a combinação das fontes de dados revela informações não reveladas anteriormente e que o usuário não quis revelar (Ziegeldorf, Morchon e Wehrle, 2014). O ataque de ligação acontece principalmente na fase de disseminação da informação do modelo de referência utilizado neste trabalho.

Os usuários temem o efeito que pode ser alcançado quando dados de diferentes partes sob diferentes contextos e permissões são combinados (Spiekerman e Cranor, 2009). Os riscos de acesso não autorizado e vazamento de informações também podem aumentar quando é feita a combinação de dados de diferentes fontes.

Uma abordagem comum para tentar evitar ataques de ligação é trabalhar com dados anonimizados, porém a ação de combinar conjuntos diferentes de dados pode

permitir a reidentificação (El *et al,* 2011). Permanece como um desafio a criação de técnicas de anonimização robustas que resistam à reidentificação quando é feita a combinação de diferentes conjuntos de dados.

3.4 Métodos e técnicas de preservação da privacidade

Esta seção apresenta métodos e técnicas para preservação da privacidade. Apesar de serem métodos e técnicas de preservação para contextos mais gerais, podem ser adaptadas para uso em ambientes IoT.

3.4.1 Leis e políticas de privacidade

As leis e políticas de privacidade são os mais populares dos métodos de preservação. Incluem leis como a Diretiva de proteção de dados da União Europeia, o ato de privacidade dos Estados Unidos, e o HIPAA para informações médicas, entre outros instrumentos legais.

Dois elementos a serem lembrados nas políticas de privacidade são a conformidade voluntária e a conformidade forçada (Rosner, 2016). Algumas políticas encorajam o comportamento voluntário, enquanto outras utilizam sanções coercivas para alcançar a conformidade.

O Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/679, em inglês *General Data Protection Regulation* (GDPR), dispõe sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Parlamento Europeu e Conselho da União Europeia, 2016). O RGPD entrou em vigor em 25 de maio de 2018 e abrange todos os estados pertencentes à União Europeia.

Em agosto de 2018 no Brasil, foi sancionada a lei de número 13709 que dispõe sobre a proteção dos dados pessoais e objetiva proteger os direitos fundamentais de liberdade e privacidade (BRASIL, 2018). Esta lei aplica-se a operações de tratamento de dados quando a coleta dos dados seja realizada em território nacional.

Alguns princípios relevantes que devem ser observados durante a realização de tratamento dos dados pessoais foram destacados da lei brasileira:

- **finalidade:** o tratamento dos dados deve ser realizado para propósitos legítimos e específicos;
- **adequação:** o tratamento dos dados deve ser compatível com o contexto do tratamento;
- **necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades;
- **transparência:** garantia aos titulares dos dados, de informações sobre como o tratamento dos dados é realizado;
- **segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- **prevenção:** adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Pode-se observar também, que a lei brasileira indica que o titular do dado deve dar o seu consentimento para que o tratamento do dado seja realizado. O titular do dado também tem o direito a ter os seus dados anonimizados, bloqueados ou eliminados quando forem desnecessários ou excessivos.

Já em 8 de julho de 2019, foi sancionada a lei 13853 que cria a Autoridade Nacional de Proteção de Dados (BRASIL, 2019), da qual pode-se destacar as seguintes atribuições:

- zelar pela proteção dos dados pessoais, nos termos da legislação;
- zelar pela observância dos segredos comercial e industrial;
- elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
- fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação;
- promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

- e, promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade.

Para este trabalho, a Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira será o norte para o desenvolvimento da funcionalidade de execução de ações de privacidade no mecanismo Privacy Everywhere.

3.4.2 Certificação e selos

Os selos de privacidade certificam que um serviço oferecido possui e segue uma política de privacidade. A certificação obrigatória é rara, na maioria das vezes as empresas se candidatam a se certificar ou ao direito de exibir um selo voluntariamente, para sinalizar aos usuários que adotam um conjunto de diretrizes ou princípios (Rosner, 2016).

Uma das certificações e selos de privacidade existentes é o TRUSTe, que incorpora princípios das estruturas de privacidade estabelecidas pela APEC (*Asia-Pacific Economic Cooperation*), pela OECD (*Organization for Economic Co-operation and Development*) e pela FTC (*Federal Trade Comission*). Outro exemplo de certificação é a EuroPriSe, o selo de privacidade Europeu, que demonstra que o serviço oferecido cumpre as leis de proteção de dados da União Europeia.

3.4.3 Encriptação

Um esquema de encriptação é uma função que mapeia um texto simples para um texto cifrado com o uso de uma chave (Dragoi *et al.*, 2018). Se a chave é a mesma para criptografar e descriptografar (compartilhada entre o remetente e o destinatário) o esquema é chamado simétrico; se for usado um par de chaves (chave pública para criptografar e chave privada para decifrar), o esquema é chamado assimétrico (Dragoi *et al.*, 2018).

No contexto da IoT, encriptação, tipicamente, é usada na transmissão e no armazenamento de mensagens para que partes não autorizadas não tenham acesso à informação coletada.

3.4.4 Transparência

Transparência é um princípio central na formulação e no uso de políticas de privacidade. Refere-se às práticas utilizadas para assegurar que os usuários saibam o que está sendo coletado sobre eles, quando é feita a coleta, como os dados coletados são utilizados e com quem os dados coletados são compartilhados (Rosner, 2016).

3.4.5 Anonimização

A anonimização consiste em não permitir que uma pessoa seja identificada por meio da alteração ou remoção de suas informações pessoais identificáveis, dos dados relacionados a seus usos de sistemas computacionais.

Segundo o projeto *Open Web Application Security Project* (OWASP) (2018), dentre os métodos de anonimização estão a Substituição, a Supressão, a Generalização e a Perturbação. Na Substituição, as informações de identificação são substituídas. Na Supressão, os dados pessoais divulgados são omitidos parcial ou totalmente. No método de Generalização, os dados são substituídos por dados mais genéricos (uma data de nascimento pode ser substituída pelo ano de nascimento por exemplo). Na Perturbação são feitas alterações aleatórias nos dados divulgados.

3.4.6 Minimização da coleta e do uso dos dados

Esta é uma das táticas mais antigas de preservação da privacidade e consiste em limitar a quantidade de dados coletados, limitar o seu uso e o seu tempo de armazenamento.

Em IoT, a minimização pode em ocorrer em dois níveis (Rosner, 2016): no projeto e no armazenamento. No nível de projeto, os projetistas devem incluir somente os sensores e funções necessárias às funcionalidades chave do dispositivo. No nível de armazenamento, dispositivos não devem reter dados que não estão mais em uso ou não são relevantes.

3.4.7 Boas práticas

Governos, empresas e organizações sem fins lucrativos podem publicar um conjunto de boas práticas no tratamento dos dados e privacidade. Estas são subjetivas, mas podem ser eficazes quando criadas com a ajuda de especialistas, considerando praticidade, realismo e viabilidade, com objetivos claros e ética (Rosner, 2016). As boas práticas são quase sempre voluntárias.

3.5 Considerações finais

Este capítulo apresentou uma definição de privacidade adaptada para ambientes de Internet das Coisas que será utilizada neste trabalho. As novas formas de interação e comunicação emergentes com a evolução dos dispositivos IoT fazem que com que surja também uma maior quantidade de dados sensíveis e novos tipos de ameaça à privacidade dos usuários. Os métodos e as técnicas de preservação de privacidade apresentados podem e devem ser adaptados para uso em sistemas IoT.

Capítulo 4

SERVIÇOS DE NUVEM IOT

Nesse capítulo é apresentada uma definição para computação em nuvem e também é mostrada uma classificação das arquiteturas de serviços de nuvem disponíveis no mercado. É feita a apresentação e a comparação entre alguns serviços de nuvem IoT disponíveis.

4.1 Considerações iniciais

Os dispositivos inteligentes, em sua grande maioria, apresentam recursos de processamento e armazenamento extremamente limitados. Em outros casos, há um fator limitante relacionado à disponibilidade de energia. Para superar estas limitações, uma das abordagens mais promissoras é a de interconectar os dispositivos IoT com um serviço de nuvem, para que se beneficie dos recursos elasticamente escaláveis e sempre disponíveis fornecidos pelo paradigma da computação em nuvem (Botta *et al.,*2014). A Internet das Coisas baseada em nuvem simplifica o armazenamento e o processamento dos dados coletados, permite usar os mesmos dados em vários serviços, facilita a combinação de dados de vários usuários e impede a fragmentação da informação em vários bancos de dados (Henze *et al.,* 2016).

Este capítulo apresenta na seção 4.2 a definição de computação em nuvem bem como os tipos de arquiteturas existentes. Na seção 4.3 é feita uma apresentação e uma comparação entre algumas plataformas de nuvem IoT disponíveis no mercado.

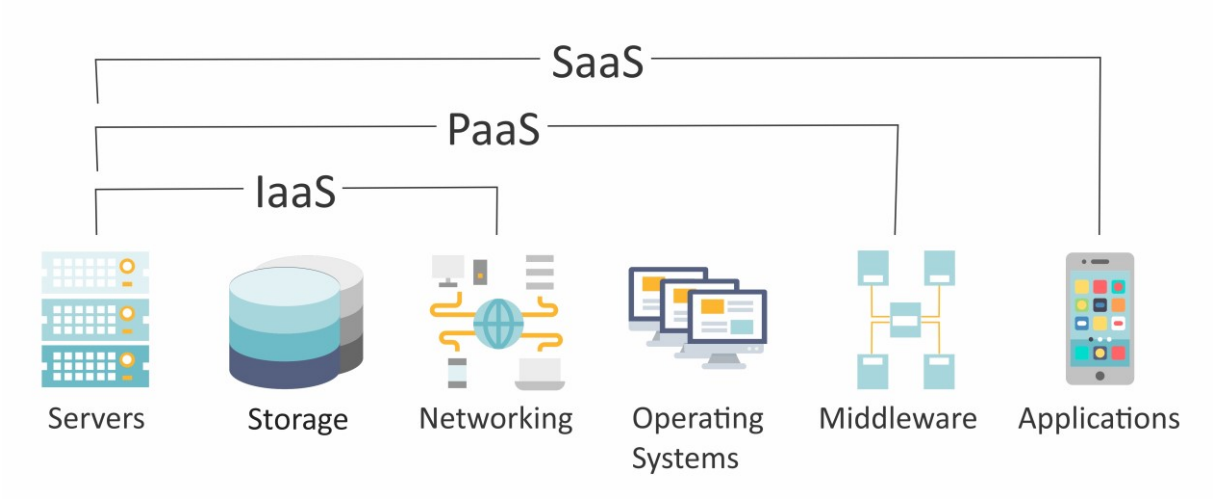
4.2 Computação em nuvem

A definição fornecida por Mell e Grance (2009) relata os aspectos essenciais da computação em nuvem: é um modelo que possibilita o acesso à rede para uso de recursos configuráveis e compartilhados que podem ser obtidos e liberados de forma rápida e com o mínimo de esforço de gerenciamento.

Existem diferentes categorias na computação em nuvem: Infraestrutura como Serviço, do inglês *Infrastructure as a Service* (IaaS), que é a camada de mais baixo nível na infraestrutura de nuvem e oferece servidores e armazenamento para computação, bem como as funcionalidades de rede; *Platform as a Service* (PaaS) que significa Plataforma como Serviço, é a camada de nível médio e fornece os sistemas operacionais e o middleware necessários para implantação dos serviços; e Software como Serviço, do inglês *Software as a Service* (SaaS), que oferece aplicações acessíveis ao usuário tal como é disponibilizado por IBM Bluemix, Google App Engine e Microsoft Azure (Díaz, Martín e Rubio, 2016). A Figura 4.1 ilustra as categorias IaaS, PaaS e SaaS na computação em nuvem. Outros modelos de computação em nuvem surgiram desde então.

A integração entre computação em nuvem e IoT, conhecida como *Cloud of Things* (CoT) (Aazam *et al.,* 2014), que significa nuvens de coisas inteligentes, além de resolver problemas como a limitação dos dispositivos IoT pode fazer com que surjam novas oportunidades como Coisas como Serviço, do inglês *Things as a Service* (TaaS) e Sensores como Serviço, do inglês *Sensors as a Service* (SenaaS) (Barbaran, Diaz e Rubio, 2014). Devido à proliferação e aos benefícios da integração de dispositivos IoT com computação em nuvem, vários projetos, protocolos, plataformas e sistemas surgiram para enfrentar os desafios desta integração.

Figura 4.1 – Categorias IaaS, PaaS e SaaS na computação em nuvem



Fonte: próprio autor.

4.2.1 Infraestruturas de nuvem

O IaaS é o componente chave em um datacenter em nuvem, pois é responsável pelo gerenciamento, provisionamento e por implantar componentes virtuais.

O OpenNebula[3] é um exemplo de uma Plataforma de nuvem IaaS que surgiu de um projeto da Universidade Complutense de Madri, realizado em 2005. O objetivo do projeto é fornecer uma camada aberta, flexível, extensível e gerenciável para abstrair rede, armazenamento, virtualização e monitoramento em diferentes nuvens públicas e privadas (Díaz, Martín e Rubio, 2016). Todos componentes do OpenNebula foram agrupados em um componente-chave, o sistema operacional em nuvem, que gerencia infraestruturas físicas e virtuais e controla o provisionamento de recursos virtuais de acordo com as necessidades dos serviços (Moreno-Vozmediano et al., 2012).

Outra plataforma IaaS bem conhecida é a plataforma de código aberto OpenStack[4]. Enquanto OpenNebula possui um sistema centralizado com componentes adicionais, OpenStack é composto por um conjunto de subcomponentes inter-relacionados com suas próprias APIs que devem ser instaladas e integradas para implantação do OpenStack (Díaz, Martín e Rubio, 2016).

[3] https://opennebula.org/

[4] https://www.openstack.org/

OpenStack possui quatro serviços principais: computação, armazenamento, rede e painel de instrumentos. O serviço de computação é responsável por gerenciar e controlar a plataforma de nuvem. OpenStack suporta dois tipos de armazenamento: Objeto e Bloco. O armazenamento de Objeto é adequado para armazenamento de dados redundante, tolerante a falhas e escalável, enquanto o armazenamento em bloco fornece um nível de bloqueio persistente adequado para cenários sensíveis ao desempenho (Díaz, Martín e Rubio, 2016). O serviço de rede permite conectividade de rede como um serviço para outros serviços do OpenStack e o painel de instrumentos permite gerenciar os recursos e serviços do OpenStack por meio de uma interface web que pode ser customizável para atender às necessidades do usuário.

4.3 Plataformas de nuvem IoT

Esta seção apresenta plataformas de nuvem IoT escolhidas para fornecer ideias sobre funcionamento, para apontar pontos fortes e limitações do uso destas tecnologias. Com relação ao critério de seleção para as soluções a serem apresentadas, foram priorizadas as soluções com suporte a Node-RED, soluções de código aberto e soluções de empresas já bem estabelecidas no mercado.

A Tabela 4.1 apresenta uma comparação entre as plataformas de nuvem IoT com relação às características da plataforma e à presença ou ausência de determinada funcionalidade. A presença da funcionalidade é indicada pelo sinal “+” e a ausência da funcionalidade é representada pela coluna vazia. A Tabela 4.2 apresenta uma comparação entre as plataformas com relação ao protocolo de aplicação suportado e linguagens de programação suportadas para o desenvolvimento das aplicações.

Tabela 4.1 – Comparação entre plataformas IoT com relação às características e funcionalidades presentes

Plataforma	Open Source	Análise em tempo real	Gerenciamento de configurações	Monitoramento dos dispositivos	Suporte a encriptação da comunicação
Kaa	+		+	+	+
IBM Cloud		+	+	+	+
AWS IoT			+	+	+
Oracle IoT		+	+	+	+
Microsoft Azure IoT		+	+	+	+
Dojot	+		+	+	+
Open IoT	+	+	+	+	+

Tabela 4.2 – Comparação entre plataformas IoT com relação ao protocolo de aplicação suportado e linguagens de programação suportadas

Plataforma	Protocolo de Aplicação			Linguagem suportada			
	HTTP	MQTT	CoAP	Java	Android	C	JavaScript
Kaa	+	+	+	+	+	+	+
IBM Cloud	+	+		+		+	+
AWS IoT	+	+				+	+
Oracle IoT	+	+		+	+	+	+
Microsft Azure IoT	+	+		+		+	+
Dojot	+	+	+				+
Open IoT	+	+	+	+	+		+

4.3.1 Kaa

Kaa[5] é uma plataforma de código aberto de *middleware* de propósitos múltiplos para a Internet das Coisas, que permite a criação de soluções IoT

[5] http://www.kaaproject.org/

completas fim-a-fim, aplicativos conectados e produtos inteligentes. A plataforma Kaa oferece um kit de ferramentas aberto e com recursos para o desenvolvimento de produtos IoT. Kaa também oferece um conjunto de recursos de IoT prontos para uso que podem ser facilmente conectados e usados para implementar casos de uso de IoT.

Dentre as características de Kaa está a independência de hardware, que o torna compatível com quase todos os dispositivos conectados, sensores e *gateways*. Ele também fornece recursos e extensões de IoT para diferentes tipos de aplicativos.

Dentre os recursos ativados por Kaa no dispositivo estão: gerência de um número ilimitado de dispositivos conectados, realizar provisionamento e configuração de dispositivos remotos, criar serviços em nuvem para produtos inteligentes, configurar interoperabilidade entre dispositivos, realizar o monitoramento de dispositivos em tempo real, coletar e analisar dados de sensores, distribuir atualizações de firmware, analisar o comportamento do usuário e distribuir notificações direcionadas.

4.3.2 IBM Cloud

A plataforma IBM Cloud[6] oferece conectividade fácil e segura entre dispositivos IoT e a nuvem. Dispositivos como Arduino e Raspberri Pi podem ser adicionados à nuvem utilizando o protocolo de mensagens leve e aberto *Message Queue Telemetry Transport* (MQTT). Quanto ao desenvolvimento de aplicações, IBM Cloud oferece suporte a Java, Spring, Ruby e Node.js. Também oferece suporte a MySQL, MongoDB, Redis e PostgreSQL. A solução da IBM faz uso de autenticação por token para que seja criada a conexão entre os dispositivos e a nuvem. Os tokens são gerados na ação de registro do dispositivo da nuvem onde deve ser fornecido um identificador único para cada dispositivo. Os usuários da IBM Cloud podem escolher entre operar em nuvens privadas, públicas, baseadas em OpenStack ou VMWare.

[6] https://www.ibm.com/cloud/

4.3.3 AWS IoT

AWS IoT[7] permite comunicação bidirecional entre dispositivos conectados à Internet e à nuvem AWS por meio de HTTP, WebSockets e MQTT. São disponibilizados ao usuário autenticação e criptografia na conexão, a fim de se comprovar a identidade antes que seja feito o envio de informações. O serviço de gerenciamento de dispositivos IoT da AWS permite que se registre serviços individualmente ou em grupo, permite gerenciar as permissões do dispositivo e também realizar o gerenciamento das configurações dos dispositivos cadastrados. Também é possível definir grupos de dispositivos e gerenciar políticas de acesso a estes grupos.

4.3.4 Oracle IoT

Oracle IoT[8] é uma solução baseada em nuvem e que trabalha sob o paradigma de plataforma como serviço (PaaS). Esta plataforma permite conectar dispositivos à nuvem, gerenciar e analisar dados gerados pelos dispositivos conectados em tempo real e realizar a integração destes dados com aplicações na nuvem. Oracle IoT possui mecanismos para prover autenticação e autorização para envio e recebimento de dados. Possui suporte à Javascript, Java, Android, C Posix, iOS e a APIs REST.

4.3.5 Microsoft Azure IoT

Microsoft Azure IoT[9] oferece serviços e soluções para comunicação entre dispositivos e a nuvem, disponibilizando soluções de software como serviço (SaaS) e também soluções de plataforma como serviço (PaaS). Na arquitetura dos serviços Azure, os dispositivos coletam dados e enviam para um gateway de nuvem. O *gateway* de nuvem disponibiliza os dados para processamento por outros serviços

[7] https://aws.amazon.com/pt/iot/

[8] https://cloud.oracle.com/iot

[9] https://azure.microsoft.com/pt-br/overview/iot/

de *back-end*. Os serviços de *back-end* podem fornecer os dados para outras aplicações ou apresentar estes dados aos usuários. Microsoft Azure IoT também possui *Software Development Kits* (SDKs) para facilitar a criação de aplicações para interação entre os dispositivos e a nuvem. Os SDKs estão disponíveis para .NET, Java, Node.js, Python e C.

4.3.6 Dojot

Dojot[10] é uma plataforma brasileira que objetiva facilitar o desenvolvimento de soluções IoT. A plataforma Dojot tem como base o projeto Fiware, o qual possui como missão construir um ecossistema público, padronizado, aberto e sustentável, para o desenvolvimento de aplicações inteligentes em diversas áreas.

Dojot possui uma interface de programação intuitiva, baseada em fluxos, que tem como base a ferramenta de programação em fluxos Node-RED[11]. Esta plataforma permite criar e gerenciar aplicações, permite o gerenciamento de dispositivos IoT e suporta a comunicação com dispositivos IoT por meio dos protocolos Message Queue Telemetry Transport (MQTT), Constrained Application Protocol (CoAP) e Hipertext Transfer Protocol (HTTP).

4.3.7 Open IoT

Open IoT[12] é um projeto de código aberto, que teve como um dos financiadores a Comissão Europeia, e que fornece uma plataforma de *middleware* que permite o desenvolvimento de aplicações IoT baseadas em nuvem, com esforço mínimo de programação (Zarko *et al.,* 2015).

Segundo Serrano, Hauswirth e Soldatos (2014), Open IoT é composto por sete elementos principais:

- O Sensor *Middleware* que coleta, filtra e combina fluxos de dados.
- O armazenamento de dados na nuvem que armazena os fluxos de dados coletados pelos sensores.

[10] http://www.dojot.com.br/

[11] https://nodered.org/

[12] http://www.openiot.eu/

- O Escalonador que controla o acesso aos recursos.
- O serviço de entrega e a funcionalidade de gerenciamento que entrega e monitora as métricas de cada serviço.
- O componente de definição de solicitação que permite que se faça a especificação de um serviço em tempo real.
- O componente apresentação de uma requisição que permite visualizar as saídas de um serviço.
- O componente de configuração e monitoramento que permite o gerenciamento visual e a configuração de funcionalidades nos sensores e serviços.

4.4 Considerações finais

Este capítulo apresentou uma definição de computação em nuvem revista neste trabalho. Também foram apresentadas categorias de computação em nuvem.

Existem hoje diversas plataformas de nuvem IoT disponíveis no mercado, foram apresentadas algumas delas neste capítulo, a fim de se conhecer algumas de suas características. Estas informações se fazem necessárias para melhor identificar a forma de atuação do mecanismo desenvolvido neste trabalho.

Capítulo 5

TRABALHOS RELACIONADOS

Este capítulo apresenta trabalhos relacionados com o tema abordado nesta pesquisa e destaca características daqueles que apresentam uma relação mais estreita com o mecanismo proposto por este trabalho.

5.1 Considerações iniciais

A integração entre dispositivos IoT e soluções de nuvem exige atenção no quesito privacidade do usuário, seja pelo grande volume de informações geradas ou pela criticidade das informações.

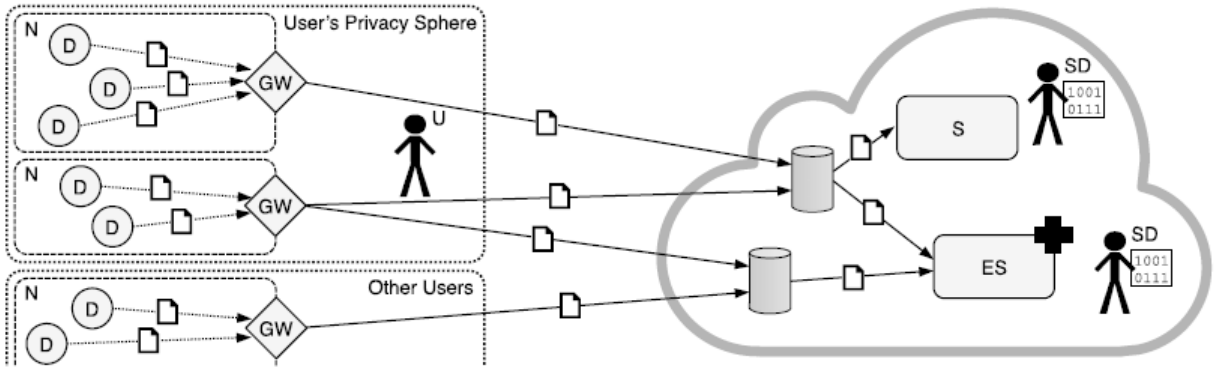
A seção 5.2 apresenta os trabalhos relacionados com a preservação da privacidade dos usuários em ambientes IoT. A seção 5.3 apresenta as considerações finais e uma comparação entre os trabalhos relacionados e o presente trabalho.

5.2 Trabalhos relacionados com a preservação da privacidade do usuário em ambientes IoT

Henze *et al.* (2016) propôs a solução UPECSI, do inglês *User-driven Privacy Enforcement for Cloud-based Services in the IoT*, a fim de fornecer uma solução integrada para cumprimento da privacidade focada nos usuários finais e nos desenvolvedores de serviços de nuvem.

O cenário de rede utilizado na proposição da solução UPECSI está representado na Figura 5.1. Neste cenário, um usuário (U) opera uma ou mais redes IoT (N). Os dispositivos IoT (D) enviam dados para a nuvem por meio do gateway (GW). A nuvem armazena os dados e os provê como serviços (S) ou como serviços de emergência (ES). Os serviços são fornecidos por desenvolvedores de serviços (SD).

Figura 5.1 – Cenário de rede da proposta UPECSI



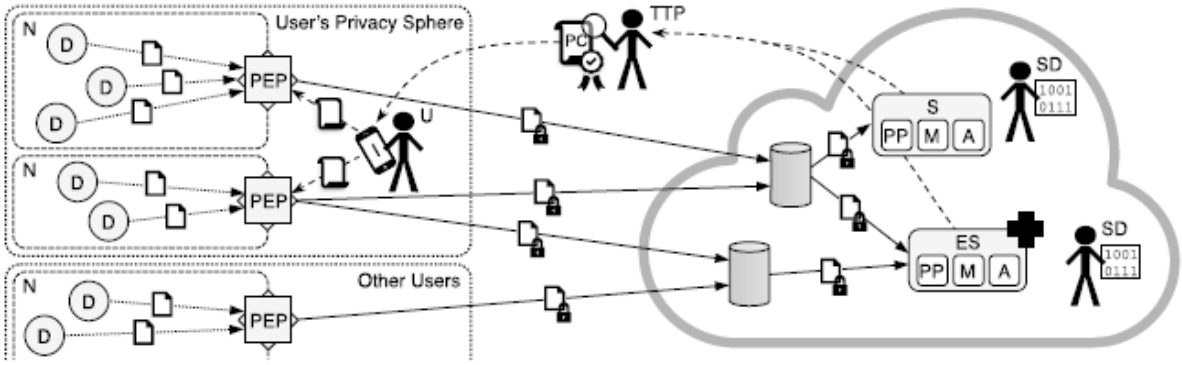
Fonte: Henze *et al.* (2016).

Ao projetar e implementar a solução UPECSI, os autores se concentraram nos requisitos para cumprimento da privacidade de Pearson (2009) que são: aviso, consentimento, auto-determinação, segurança adequada e uso com propósito.

A solução UPECSI é composta por três componentes principais: privacidade orientada a modelos, que obtém informações do processo de desenvolvimento de serviços na nuvem e gera uma política de segurança interativa e configurável pelo usuário ; interação com o usuário, que permite que usuários com diferentes visões de privacidade realizem as suas configurações de privacidade; e pontos de cumprimento da privacidade, que garantem que requisitos de privacidade sejam cumpridos antes que os dados sejam enviados do dispositivo para a nuvem.

A Figura 5.2 mostra uma visão geral mais detalhada da solução UPECSI. Os pontos de cumprimento da privacidade (PEPs) encriptam todos os dados antes de enviá-los para a nuvem. Cada serviço provê uma política de privacidade (PP), monitoramento do uso dos dados (M) e informação de auditoria a uma terceira parte confiável (TTP). A terceira parte confiável revisa a informação de todos os serviços e provê uma configuração de privacidade padrão para o usuário. O usuário identifica estas configurações por meio de uma interface (I) e configura os pontos de cumprimento da privacidade para permitir ou negar o acesso dos serviços aos dados.

Figura 5.2– Visão geral mais detalhada da solução UPECSI



Fonte: Henze *et al.* (2016).

O ato de encriptar todos os dados antes de enviá-los para uma nuvem pode gerar um custo computacional desnecessário para as aplicações. É necessário que se avalie o cenário de coleta de dados antes de se decidir pela realização da encriptação da informação.

Colnago (2016) desenvolveu um trabalho sobre como equilibrar a autonomia de agentes inteligentes e o controle do usuário nas decisões de privacidade. Para alcançar este equilíbrio, foi proposto o uso de soluções intermediárias chamadas no trabalho de coreografadas. Estas soluções se situam entre as soluções automatizadas, onde os usuários possuem pouco controle sobre as decisões, e as orquestradas, soluções onde o usuário deve consentir para que o envio de dado ocorra e fornece aos usuários um controle excessivo.

No trabalho de Colnago (2016), os usuários relataram: se sentirem mais ansiosos quando precisavam tomar uma decisão de privacidade do que quando delegavam a decisão; estar mais ocupados quando precisavam realizar uma tomada

de decisão do que quando delegavam esta decisão; e, ter uma maior interação social quando delegavam esta tomada de decisão.

São muitos os benefícios de se automatizar uma decisão de privacidade, porém ainda existem cenários de coleta de dados onde o usuário irá desejar realizar manualmente a tomada de decisão.

Chow (2017) propôs um framework conceitual denominado Privacy Stack para tratar de questões de privacidade do usuário em ambientes IoT. Privacy Stack é composto pelas camadas *Awareness, Inference, Preferences e Notification*.

A camada *Awareness* diz respeito à consciência do usuário de que uma coleta de dados está sendo realizada. A natureza potencialmente discreta da coleta de dados dos dispositivos IoT faz com que muitas vezes os usuários não percebam que dados foram coletados. Chow (2017) sugere que na camada *Awareness* seja tratada a questão de como criar um canal de comunicação entre usuários e dispositivos IoT para que estes dispositivos sejam descobertos com maior facilidade.

Na camada *Inference*, é proposto que se tenha uma abordagem equilibrada e não se confie somente nos usuários para entender as inferências possíveis dos dados coletados. É sugerido que os serviços forneçam explicitamente que inferências básicas são possíveis de se realizar.

A camada *Preferences* se refere às preferências de privacidade dos indivíduos. Chow (2017) diz que cada indivíduo tem uma percepção diferente sobre o grau de sensibilidade dos dados e que o contexto da coleta de dados também impacta diretamente no grau de sensibilidade do dado. Os fatores que determinam uma decisão de privacidade são muitos e é sugerido que sejam desenvolvidos mecanismos que facilitem a tomada de decisão de privacidade pelo usuário. Por fim, na camada *Notification* são tratadas as formas de se notificar o usuário e todas as camadas anteriores devem ser consideradas.

Segundo Chow (2017), a notificação representa uma forma de interação entre os dispositivos IoT e os usuários. Porém, muitas das vezes, os usuários não querem interagir com dispositivos IoT quando estes se tornam onipresentes. São necessários mecanismos para identificar quando a notificação se faz necessária para diferentes cenários de coleta de dados.

Jayaraman *et al.* (2017) propuseram uma abordagem em que o armazenamento dos dados coletados por dispositivos IoT é realizado em múltiplos servidores, que possuem como requisitos de segurança: conexão segura entre o

gateway e o servidor IoT; persistência segura no armazenamento dos dados; e controle de acesso aos dados nos servidores.

A ingestão dos dados da arquitetura proposta por Jayaraman *et al.* (2017) divide os dados em n partes, onde n é o número de servidores de armazenamento, que encriptam estes dados.

O trabalho de Jayaraman *et al.* (2017) motivou o presente trabalho a realizar a integração do mecanismo com soluções de nuvens IoT, a fim de aproveitar algumas das facilidades já presentes nas soluções de nuvem para facilitar o atendimento dos requisitos de segurança propostos por Jayaraman *et al.* (2017). O mecanismo proposto neste trabalho também procura realizar a encriptação dos dados de uma forma simplificada e somente em cenários de coleta de dados específicos.

Leithardt *et al.* (2018) desenvolveram um mecanismo para gerenciamento de privacidade com base em histórico de dados. Foi feita uma comparação entre diversos algoritmos de classificação e os algoritmos que apresentaram maior precisão foram os algoritmos “J48”, “Tabela de Decisão” e “Multilayer Perceptron”.

Para que haja a automatização da tomada de decisão se faz necessário o uso de algoritmos de aprendizado de máquina, principalmente para responder em cenários de coleta de dados onde não há uma configuração prévia de tomada de decisão. O algoritmo utilizado neste trabalho foi o “Multilayer Perceptron” devido à sua capacidade de generalização, à capacidade de responder por cenários de coleta de dados para os quais o algoritmo não foi treinado.

5.3 Considerações finais

Este capítulo apresentou trabalhos relacionados ao mecanismo desenvolvido neste trabalho. A Tabela 5.1 mostra uma comparação entre os trabalhos relacionados apresentados nesta seção e o presente trabalho.

Tabela 5.1 – Comparação entre os trabalhos relacionados

Características	Henze *et al.* *(*2016)	Colnago (2016)	Chow (2017)	Jayara-man *et al.* (2017)	Leithardt *et al.* (2018)	Este trabalho
Permite o controle da divulgação dos dados coletados	✓	✗	✗	✓	✓	✓
O controle da divulgação dos dados pode ser automatizado	✓	✗	✗	✗	✓	✓
Oferece insights teóricos sobre quais fatores influenciam a tomada de decisão pelo usuário	✗	✓	✗	✗	✗	✓
O usuário pode ser notificado quando informações pessoais são coletadas	✗	✓	✓	✗	✓	✓
São usados algoritmos de Inteligência Artificial no mecanismo de preservação da privacidade	✗	✓	✗	✗	✓	✓
O custo computacional da ação de privacidade realizada nos dados coletados é considerado	✗	✗	✗	✗	✗	✓

Como pode ser observado na Tabela 5.1, o desenvolvimento do mecanismo do Privacy Everywhere considerou características que não são abordadas pelos trabalhos relacionados.

Capítulo 6

ESTUDO SOBRE PREFERÊNCIAS DE PRIVACIDADE COM USUÁRIOS E PROFISSIONAIS

Este capítulo apresenta o estudo realizado com usuários de uma comunidade acadêmica a fim de se obter suas percepções de privacidade em cenários IoT. Estas percepções de privacidade foram utilizadas para o desenvolvimento do mecanismo Privacy Everywhere. Também é apresentado neste capítulo, o estudo realizado com profissionais de redes e segurança da informação que apoiou a automatização de ações de privacidade realizadas pelo mecanismo desenvolvido neste trabalho.

6.1 Considerações iniciais

Para apoiar o desenvolvimento do mecanismo Privacy Everywhere foram desenvolvidos dois estudos: um estudo com usuários de uma comunidade acadêmica para entender as preferências de privacidade dos usuários em ambientes IoT; e também, um estudo com profissionais de redes e segurança da informação

para apoiar a automatização de ações de privacidade a serem executadas em requisições de dados, antes que os dados sejam enviados.

Na seção 6.2 o método estatístico para seleção dos usuários participantes da pesquisa é demonstrado. A seção 6.3 apresenta os objetivos e resultados da pesquisa com os usuários. Na seção 6.4, podem ser visualizados os objetivos e resultados da pesquisa com os profissionais de redes e segurança da informação. Por fim, na seção 6.5 são apresentadas as considerações finais.

6.2 Seleção dos participantes da pesquisa

Os participantes do estudo com usuários foram selecionados dos cursos de graduação da Universidade Federal de Alfenas (UNIFAL-MG). Cochran (1977) indica como um contexto ideal, pesquisar todos os integrantes da população, porém restrições como tempo e disponibilidade dos usuários inviabilizam um estudo neste contexto. Devido a estas restrições, o estudo foi realizado com um subconjunto da população que foi investigada.

Para o cálculo do tamanho de uma amostra (cálculo amostral), Cochran (1977) destaca três variáveis que têm impacto direto sobre seu tamanho: o tamanho da população (quando conhecido), margem de erro e o nível de confiança. O cálculo é definido pela fórmula:

$$n = \frac{n_0}{1 + (n_0 - 1)/N}$$

Onde n é o número de indivíduos que compõem a amostra, e N o número de indivíduos que compõem a população. O valor de n_0 é obtido pela razão entre o grau de confiança (valor crítico de z) e a margem de erro adotada no estudo.

O cálculo amostral utilizado neste estudo para o primeiro momento da pesquisa foi composto pelos valores de 90% para o grau de confiança e 7% de margem de erro.

Segundo Cochran (1977) para um grau de confiança de 90%, tem-se o valor crítico de z igual a 1,649. O cálculo para obtenção do tamanho da amostra para o

primeiro momento do estudo é demonstrado a seguir:

$$N = 3737$$

$$e = 0{,}07$$

$$z^2\,(k) = 0{,}90 = 1{,}649 \text{ (Valor crítico de Z)}$$

$$n_0 = z^2\,(k) \,/\, 4e^2 = 1{,}649^2 \,/\, 4(0{,}07)^2 = 138{,}73$$

$$n = n_0 \,/\, (1 + (n_0 - 1)/N) = 138{,}73 \,/\, (1 + 137{,}73/3737) = 133{,}8$$

Sendo assim, foi tomado como amostra um conjunto de 136 alunos (134 alunos + 2, para que se tenha um número múltiplo de 4) de graduação da Universidade Federal de Alfenas (UNIFAL-MG) para o primeiro momento da pesquisa. Estes alunos de graduação estavam regularmente matriculados na UNIFAL-MG e possuíam disponibilidade de tempo para participação da pesquisa.

Já para o segundo momento da pesquisa foram selecionados 5 indivíduos profissionais da área de Redes e/ou Segurança da Informação.

6.3 Objetivos e resultados da pesquisa com usuários

Na pesquisa com usuários, objetivou-se obter as percepções de privacidade dos usuários em cenários IoT. O estudo foi realizado por meio de questionários impressos e apresentou como principais focos:

- Obter dados para automatização da tomada de decisão de privacidade na coleta de dados realizada por dispositivos IoT;
- Verificar a relação entre os fatores influentes na tomada de decisão de privacidade presentes nos cenários apresentados e o nível de conforto dos usuários com a coleta de dados.

A pesquisa foi realizada em espaços comuns a todos os estudantes de graduação a fim de se obter maior aleatoriedade e heterogeneidade na pesquisa.

Cada participante recebeu uma breve introdução sobre o conceito de IoT e também recebeu um questionário com 24 cenários de coleta de dados em ambientes IoT. Em cada cenário, os participantes responderam se permitem ou negam o envio de informações e quão confortáveis se sentem com a coleta de dados no cenário em questão. O tempo médio gasto pelos alunos para responder o questionário foi de 14 minutos. A Tabela 6.1 mostra a distribuição demográfica desses alunos.

Tabela 6.1 – Distribuição demográfica dos participantes

Idade	**Participantes**	**%**
<21	45	33,1
21 a 25	73	53,7
26 a 30	11	8,1
31 a 35	4	2,9
>35	3	2,2
Sexo		
Feminino	69	50,7
Masculino	67	49,3

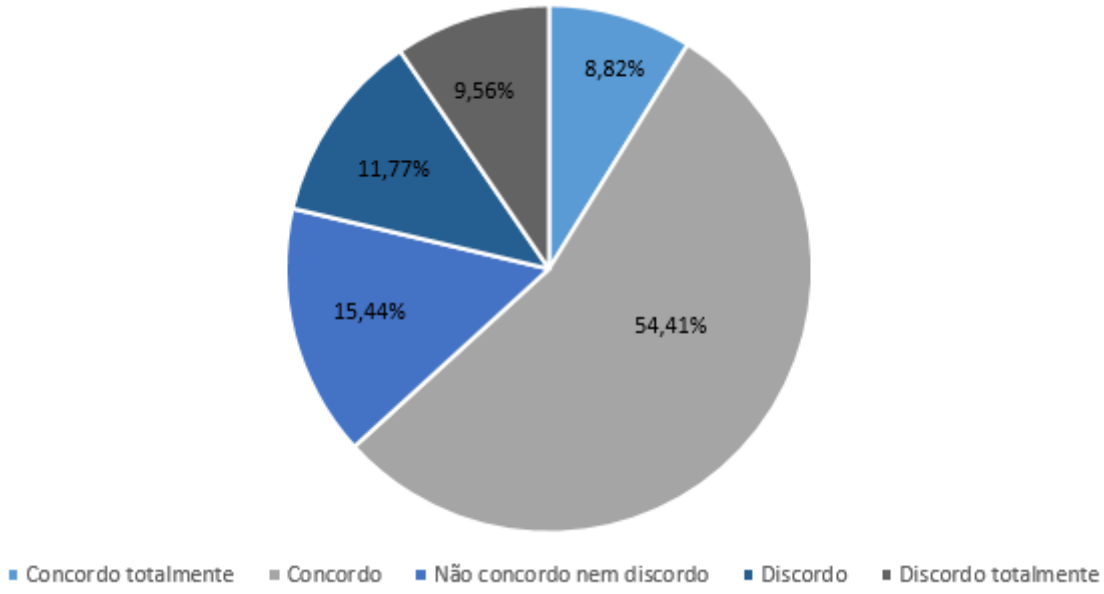
Área da graduação	**Participantes**	**%**
Ciências biológicas	59	43,4
Ciências exatas	38	27,9
Ciências humanas	39	28,7
Nível de preocupação com privacidade		
Muito preocupados	47	34,5
Intermediário	84	61,8
Despreocupados	5	3,7

Após as perguntas referentes à demografia dos usuários, os participantes responderam se gostariam que um mecanismo tomasse por eles decisões de privacidade em ambientes com uma grande quantidade de dispositivos capazes de coletar informações. Também responderam se sentir-se-iam mais confortáveis em permitir o envio de determinadas informações coletadas por dispositivos sabendo que os dados seriam tratados com base no conhecimento de profissionais de redes de computadores e segurança da informação antes de seriam enviados.

Como pode ser observado na Figura 6.1, 8,82% dos respondentes concordaram totalmente e 54,51% concordaram com a ideia de um mecanismo tomar decisões de privacidade por eles em ambientes IoT. Um percentual de 15,44% não concordou nem discordou da ideia, 11,77% discordaram e 9,56% discordaram totalmente. Com estas respostas, pode-se observar que não há unanimidade no desejo de automatização das decisões de privacidade. Diante disso, foi adicionada

ao mecanismo desenvolvido neste trabalho uma forma dos usuários realizarem as suas decisões de privacidade de forma manual.

Figura 6.1 – Resultado obtido ao se perguntar aos usuários se concordam em ter suas decisões de privacidade automatizadas

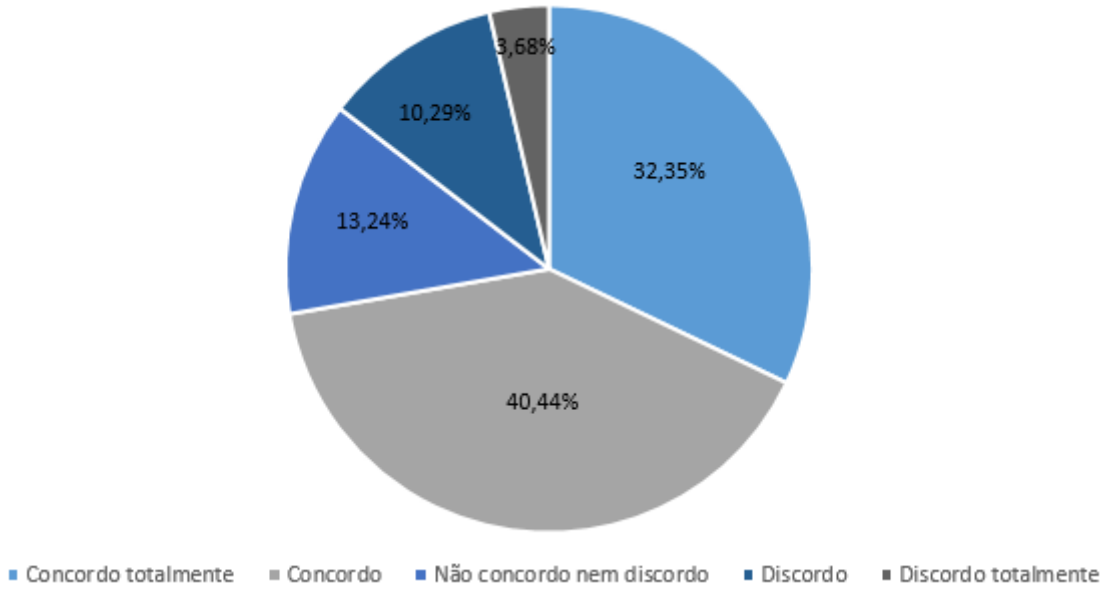


Fonte: próprio autor.

Na Figura 6.2 é mostrado que, dos entrevistados, 32,35% concordaram totalmente e 40,44% concordaram se sentir mais confortáveis com o envio de determinadas informações se estas informações forem tratadas por um mecanismo que atue de forma a garantir a privacidade dos usuários. Um percentual de 13,24% não concordou nem discordou, 10,29% discordaram e 3,68% discordaram totalmente da afirmação de que tratar os dados antes que eles sejam enviados proporcionaria maior conforto aos usuários em permitir o envio de determinadas informações. Estas respostas indicam que, para a maioria dos entrevistados, o tratamento dos dados por um mecanismo de garantia de privacidade antes que eles fossem enviados, deixaria os usuários mais confortáveis em permitir o envio destes dados.

Após os usuários responderem às perguntas referentes ao perfil do participante e também às perguntas mostradas nas Figuras 6.1 e 6.2, iniciou-se a sessão do questionário referente a coleta de dados nos cenários de coleta de dados em ambientes IoT.

Figura 6.2 – Resultado obtido ao se perguntar aos usuários se concordam que sentir-se-iam mais confortáveis com a coleta de dados se fossem executadas ações de privacidade nos dados antes que estes fossem enviados



Fonte: próprio autor.

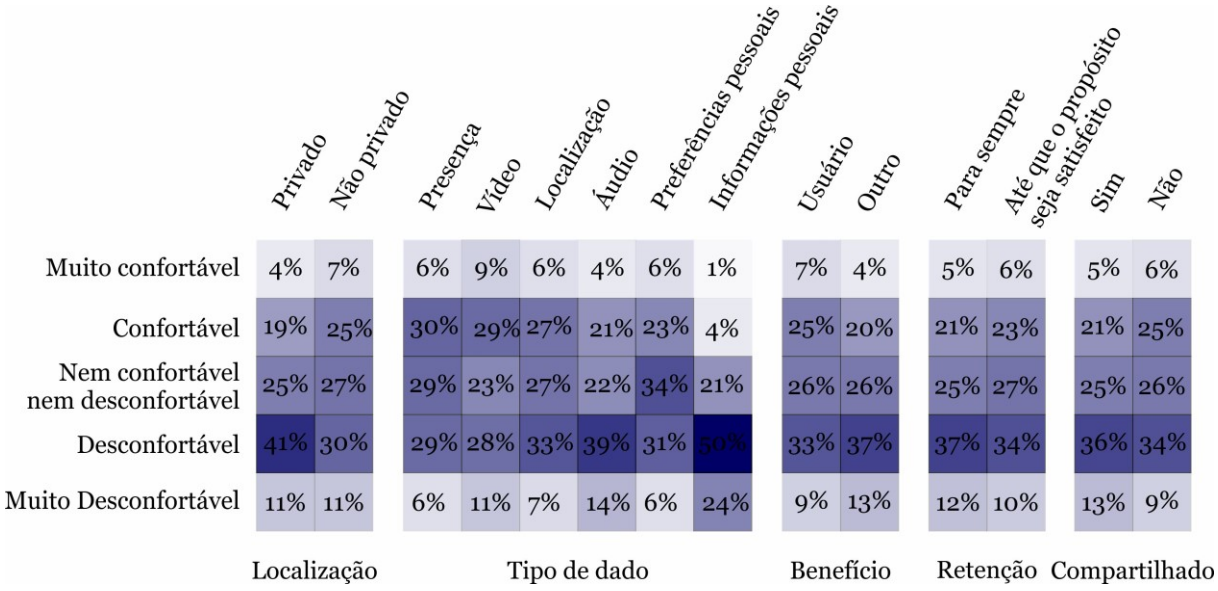
Os cenários de coleta de dados IoT apresentados aos participantes podem ser visualizados no Apêndice A. Estes cenários foram construídos a partir da combinação de fatores que influenciam a tomada de decisão de privacidade do usuário, considerados relevantes por autores como Lee e Kobsa (2016) e Naeini et al. (2017). A Tabela 6.2 apresenta os fatores com seus respectivos valores possíveis, utilizados para criar os cenários deste trabalho.

Tabela 6.2 – Fatores influentes na tomada de decisão de privacidade e seus possíveis valores utilizados para criar os cenários

Variáveis de entrada	**Valores possíveis**
Local da coleta	Privado, não privado
Tipo do dado	Presença, vídeo, localização, áudio, preferências pessoais, informações pessoais
Benefício da coleta	Usuário, coletor do dado
Retenção	Para sempre, até que o propósito seja satisfeito
Compartilhado	Sim, não

Nesta pesquisa, após apresentar cada cenário e solicitar ao entrevistado que respondesse se o envio das informações solicitadas seria permitido ou negado, também foi perguntado como o entrevistado se sentiu em relação à coleta de dados apresentada. O conforto dos participantes foi medido em uma escala Likert de 5 pontos, de "Muito confortável" a "Muito desconfortável". A representação estatística que mostra a relação entre os fatores presentes nos cenários e o nível de conforto dos participantes com os dados coletados pode ser visualizada na Figura 6.3. Por exemplo, 25% dos participantes se sentiram confortáveis quando a coleta de dados ocorreu em local não privado.

Figura 6.3 – Representação estatística que mostra a relação entre os fatores presentes nos cenários e o nível de conforto dos participantes. Células com valores mais altos são mais escuras.



Fonte: próprio autor.

Como pode ser visto na Figura 6.3, os usuários ficaram mais desconfortáveis quando a coleta de dados ocorreu em locais privados. Quanto ao tipo de dados, os usuários ficaram mais confortáveis quando a coleta foi realizada por sensores de presença e apresentaram maior desconforto quando suas informações pessoais foram solicitadas. Os participantes ficaram um pouco mais confortáveis quando a coleta de dados foi em benefício deles. Em relação ao tempo de retenção, não houve diferença significativa entre retenção para sempre e retenção até que o propósito fosse satisfeito. Os participantes também ficaram um pouco mais confortáveis em cenários em que os dados coletados não eram compartilhados.

As respostas obtidas da pesquisa com os estudantes foram utilizadas para construir o conjunto de treinamento da rede neural Allow/Deny componente do mecanismo Privacy Everywhere para automatização da tomada de decisões de privacidade.

6.4 Pesquisa com profissionais

Após a pesquisa com os estudantes de graduação, iniciou-se o segundo momento deste estudo: os 96 cenários de coleta de dados em ambientes IoT utilizados para realizar a pesquisa com os 136 alunos de graduação foram apresentados a 5 profissionais. Neste trabalho, entendeu-se como profissional, discentes, ex-discentes ou docentes do programa de pós-graduação em Ciência da Computação da UFSCar na área de Redes e Sistemas Distribuídos; ou profissionais da área de Redes e/ou Segurança da Informação.

O objetivo deste segundo momento da pesquisa foi obter informações para realização de ações de privacidade pelo mecanismo Privacy Everywhere em dados coletados em ambientes IoT.

Aos participantes foi solicitado que respondessem, para cada cenário de coleta de dados IoT apresentado, qual ação de privacidade deveria ser executada para que a privacidade do usuário fosse preservada com o menor custo computacional possível, e também tendo como norte a Lei Geral de Proteção de Dados (LGPD) brasileira. As ações de privacidade a serem realizadas nos dados coletados que poderiam ser indicadas pelos profissionais foram: não realizar nenhuma ação de privacidade, notificar o usuário, anonimizar o dado ou cifrar o dado.

Os 96 cenários apresentados aos estudantes de graduação no primeiro momento da pesquisa foram divididos em 4 grupos de cenários, o que deu origem a 4 questionários com 24 cenários. Para os profissionais, foi apresentado um único questionário com os 96 cenários. A Tabela 6.3 mostra a distribuição demográfica dos profissionais consultados.

Tabela 6.3 – Distribuição demográfica dos profissionais consultados

Idade	**Participantes**	**%**		**Tempo de atuação na área de redes e/ou segurança da informação**	**Participantes**	**%**
<20	0	0,0		<5 anos	0	0,0
21 a 30	0	0,0		5 a 10 anos	2	40,0
31 a 40	2	40,0		11 a 15 anos	0	0,0
41 a 50	1	20,0		16 a 20 anos	1	20,0
>50	2	40,0		>20 anos	2	40,0
				Nível de preocupação com privacidade		
Sexo				Muito preocupados	5	100,0
Feminino	0	0,0		Intermediário	0	0,0
Masculino	5	100,0		Despreocupados	0	0,0

As respostas fornecidas pelos profissionais foram utilizadas para construir o conjunto de treinamento da rede neural Privacy Action componente do mecanismo Privacy Everywhere e consultada para realizações de ações de privacidade em dados coletados em ambientes IoT.

6.5 Considerações finais

Este capítulo teve como objetivo apresentar como foi conduzida a pesquisa com usuários e profissionais realizada neste trabalho. Na pesquisa com usuários foi possível obter informações para que o mecanismo desenvolvido indique em cenários de coleta de dados IoT, se o envio do dado solicitado deve ser permitido ou negado. Também foi possível observar qual é o nível de conforto dos usuários com a coleta de dados do cenário IoT em questão.

Na pesquisa com profissionais, foi possível obter informações para que ações de privacidade possam ser executadas pelo mecanismo desenvolvido nas requisições de dados realizadas em ambientes IoT.

Capítulo 7

MECANISMO PRIVACY EVERYWHERE

Este capítulo apresenta o mecanismo Privacy Everywhere para tomada de decisão e garantia de privacidade dos usuários em ambientes IoT desenvolvido neste trabalho. Este mecanismo objetiva automatizar a decisão de privacidade dos usuários e realizar ações de privacidade nos dados coletados em ambientes IoT.

7.1 Considerações iniciais

É apresentado neste capítulo o mecanismo Privacy Everywhere desenvolvido neste trabalho. Este mecanismo tem como objetivo realizar decisões de privacidade pelos usuários em ambientes com uma grande quantidade de dispositivos capazes de coletar e enviar informações; e também, realizar ações de privacidade em dados coletados em ambientes IoT.

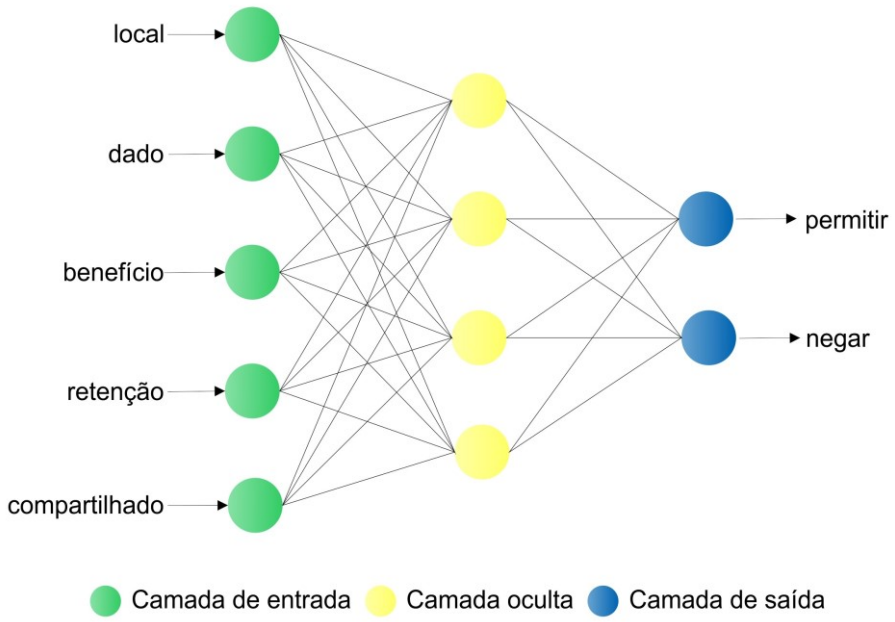
A seção 7.2 apresenta as redes neurais componentes do mecanismo. Na seção 7.3, a implementação do mecanismo Privacy Everywhere é descrita. A seção 7.4 descreve a arquitetura e apresenta um resumo sobre o modo de operação do mecanismo Privacy Everywhere. Por fim, na seção 7.5 são apresentadas as considerações finais deste capítulo.

7.2 Redes neurais do mecanismo Privacy Everywhere

A inclusão de duas redes neurais no mecanismo foi necessária para que o mecanismo pudesse automatizar a tomada de decisões de privacidade pelos usuários e também pudesse automatizar as ações de privacidade a serem executadas nos dados coletados pelos dispositivos IoT. Essas redes neurais são *multilayer perceptron* (MLP), que são redes compostas de vários neurônios interconectados com pesos atribuídos às conexões.

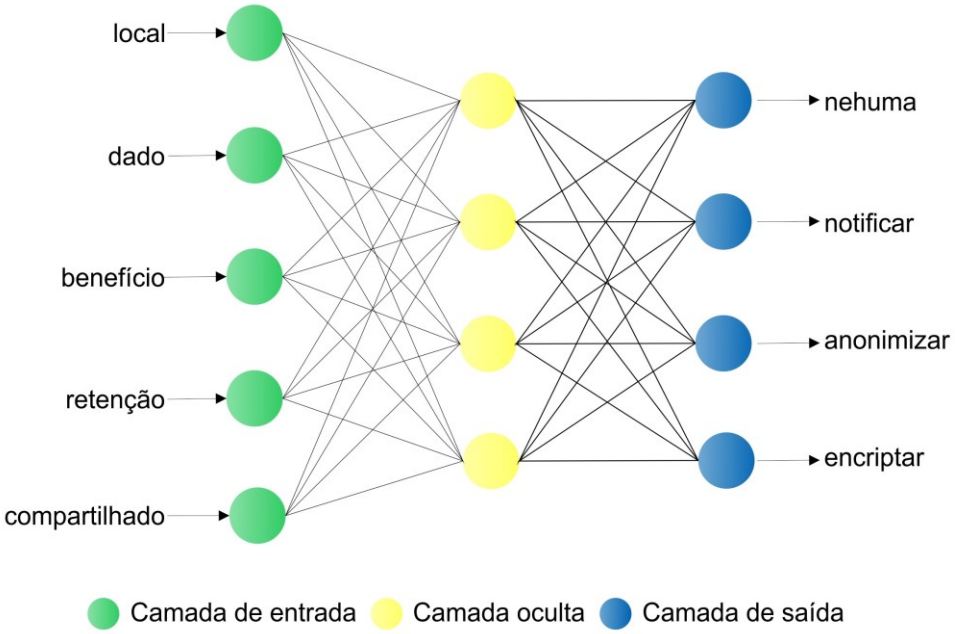
Essas redes neurais presentes no mecanismo Privacy Everywhere possuem o mesmo conjunto de entradas, mas diferem nas saídas (respostas fornecidas). A rede neural Allow/Deny apresenta como possíveis saídas permitir ou negar. Entretanto, a rede neural Privacy Action apresenta como possíveis saídas: não executar qualquer ação de privacidade, notificar o usuário, anonimizar os dados e cifrar os dados. O conjunto de dados de treinamento gerado a partir da pesquisa com os alunos realizada neste trabalho foi utilizado para treinar a rede neural Allow/Deny. A rede neural Privacy Action foi treinada com o conjunto de dados de treinamento gerado a partir da pesquisa com os profissionais realizada neste trabalho. A rede neural Allow/Deny pode ser visualizada na Figura 7.1, enquanto a rede neural Privacy Action pode ser visualizada na Figura 7.2.

Figura 7.1 – Rede neural Allow/Deny



Fonte: próprio autor.

Figura 7.2 – Rede neural Privacy Action



Fonte: próprio autor.

As variáveis utilizadas na camada de entrada para o treinamento de redes neurais são as variáveis que foram usadas para criar os cenários utilizados nas pesquisas com usuários e profissionais realizadas neste trabalho. A camada de saída fornece as decisões de privacidade: permitir ou negar o envio do dado (rede neural Allow/Deny) e qual a ação de privacidade a ser executada no dado coletado (rede neural Privacy Action).

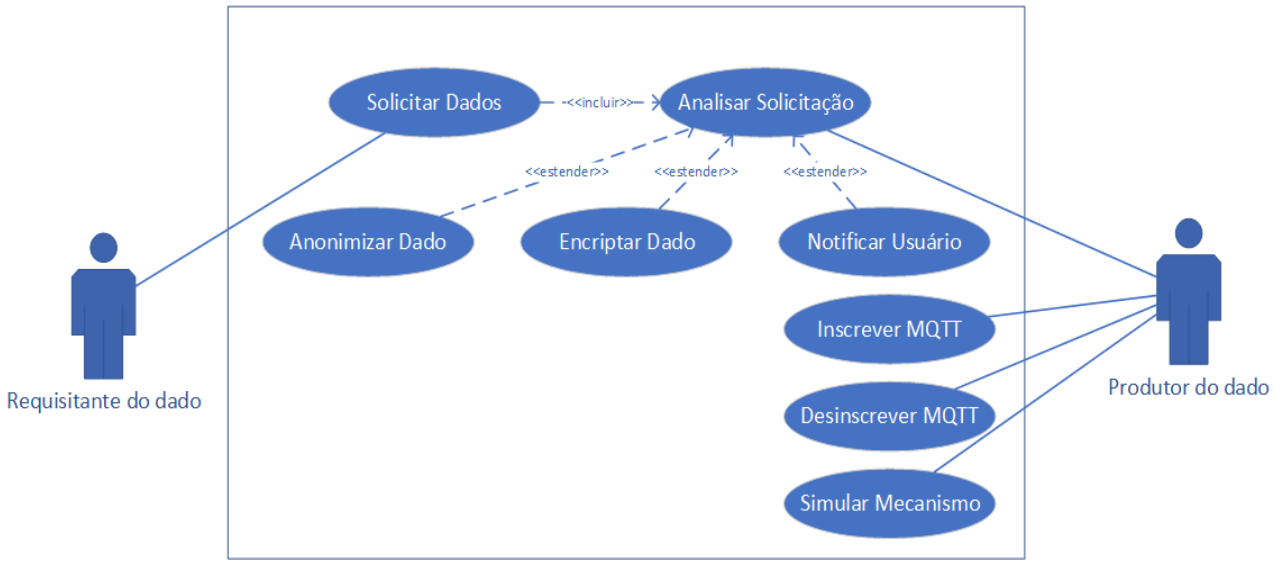
A escolha pelas redes neurais MLP para comporem o mecanismo foi motivada pela capacidade de generalização destas redes, ou seja, pela capacidade das redes responderem por cenários de coleta de dados diferentes dos cenários utilizados no treinamento das redes neurais.

7.3 Implementação do mecanismo Privacy Everywhere

Para facilitar a implementação do mecanismo e identificar os componentes da solução a ser desenvolvida, o diagrama de casos de uso da linguagem de modelagem *Unified Modeling Language* (UML) foi utilizado. Esta linguagem é utilizada para visualizar, especificar e documentar artefatos componentes de uma

solução de software. O diagrama de casos de uso utilizado para identificar os componentes da solução a ser desenvolvida pode ser visualizado na Figura 7.3.

Figura 7.3 – Diagrama de casos de uso



Fonte: próprio autor.

Como pode ser visto na Figura 7.3 os casos de uso possíveis são:

- **Solicitar Dados:** Neste caso de uso, o requisitante solicita o dado desejado e será analisado para verificar se o requisitante terá ou não terá acesso ao dado solicitado.
- **Analisar Solicitação:** todas as solicitações de dados, quando o mecanismo está no modo de operação automático, passam por duas análises onde, de acordo com o cenário da solicitação, o envio do dado pode ser permitido ou negado (definido por meio de uma consulta à rede neural Allow/Deny do mecanismo); e, se o envio for permitido, é feita uma segunda análise para verificar se é necessário que se realize alguma ação de privacidade antes do envio do dado (definida por meio de uma consulta à rede neural Privacy Action do mecanismo). Já, se o mecanismo estiver no modo de operação manual, o usuário é consultado para que ele decida se o envio será permitido ou negado, e, se permitido, qual é a ação de privacidade a ser realizada no dado solicitado.
- **Anonimizar Dado:** neste caso de uso é realizada a anonimização do dado quando o envio do dado for permitido e a ação de privacidade a ser executada no dado for anonimizar.

- **Encriptar Dado:** a encriptação do dado é realizada quando o envio do dado for permitido e a ação de privacidade a ser executada no dado for encriptar.
- **Notificar Usuário:** quando o envio do dado for permitido e a ação de privacidade a ser executada no dado antes do envio for notificar, o usuário receberá uma notificação em seu aplicativo móvel caso esteja inscrito no tópico *Message Queuing Telemetry Transport* (MQTT), que é um protocolo para envio e recebimento de mensagens, correspondente ao ambiente da coleta de dados. A escolha pelo MQTT foi motivada por este ser um protocolo leve e possuir meios de controle para inscrição nos tópicos (esta última é desejável para controle de dispositivos instalados em locais privados).
- **Inscrever MQTT:** uma das ações possíveis aos usuários ao utilizar o mecanismo Privacy Everywhere, é se inscrever no tópico MQTT correspondente ao ambiente que se deseja receber notificações. Cada ambiente que coleta dados tem o seu próprio tópico MQTT e o usuário pode selecionar em quais tópicos MQTT deseja se inscrever.
- **Desinscrever MQTT:** este caso de uso realiza a desinscrição dos usuários nos tópicos MQTT, dos quais os usuários não desejam mais receber notificações.
- **Simular Mecanismo:** este caso de uso é responsável por simular o mecanismo, onde os usuários fornecem as entradas correspondentes ao cenário, e podem observar qual é a saída resultante (se o envio do dado será permitido ou negado e qual a ação de privacidade a ser executada antes do envio, caso o envio seja permitido).

Com os componentes da solução a ser desenvolvida identificados, passou-se para o desenvolvimento de cada um dos componentes do Privacy Everywhere.

7.3.1 Módulo privacy-IoT-analyzer

O módulo privacy-IoT-analyzer foi o primeiro módulo a ser desenvolvido no mecanismo. No modo de operação automático, este módulo analisa as requisições de dados por meio de consultas às redes neurais artificiais a fim de verificar se o

envio do dado será permitido e qual é a ação de privacidade a ser executada. No modo de operação manual é feita uma consulta ao usuário para que ele responda se o envio do dado deve ser permitido ou negado e qual ação de privacidade deve ser realizada pelo mecanismo.

As requisições e as respostas das requisições são efetuadas no formato *JavaScript Object Notation* (JSON) e um exemplo de requisição e resposta à requisição podem ser visualizados nos Quadros 7.1 e 7.2 respectivamente. O identificador único universal (do inglês *universally unique identifier* - UUID) componente da requisição e da resposta, é um número de 128 bits e identifica o dispositivo IoT cadastrado na nuvem IoT. O atributo *code* identifica a requisição e a resposta à requisição univocamente. Os atributos *location*, *data_type, benefit, retention* e *shared* identificam o cenário onde a coleta de dados aconteceu. O atributo *data* na estrutura da requisição indica qual é a informação desejada. Já na resposta, o atributo *data* contém (quando permitido o envio) a informação requisitada.

Quadro 7.1 – Exemplo de requisição de dados

```
{       "uuid": "67ac49b2-78c3-4783-5d41-53c287b1d412"
        "code": "34b271ad984c",
        "location": "private",
        "data_type": "location",
        "benefit": "data_collector",
        "retention":  "forever",
        "shared":  "yes",
        "data": {
                "attribute":  "device_location",   }
}
```

Quadro 7.2 – Exemplo de resposta à requisição de dados

```
{       "uuid": "67ac49b2-78c3-4783-5d41-53c287b1d412"
        "code": "34b271ad984c",
        "location": "private",
        "data_type": "location",
        "benefit": "data_collector",
        "retention":  "forever",
        "shared":  "yes",
        "decision":  "deny",
        "action":  "none",
        "data": {
                "attribute":  "device_location",
                "value":  "",    }}
```

Como pode ser observado no Quadro 7.2, a estrutura da resposta possui dois atributos adicionais: *decision* e *action*. O atributo *decision* indica se o mecanismo, após a consulta à rede neural Allow/Deny ou após a consulta direta ao usuário, permite ou nega o envio do dado. O atributo *action* indica qual foi a ação de privacidade realizada no cenário em questão de acordo com a resposta obtida com a consulta à rede neural Privacy Action ou após a consulta direta ao usuário.

O módulo privacy-IoT-analyzer após analisar a solicitação pode realizar uma das seguintes decisões:

- **negar o envio do dado:** nesta situação, o mecanismo retorna a resposta à requisição com o atributo *decision* com o valor igual a *deny* e o fluxo de dados se encerra.
- **permitir o envio do dado e não realizar nenhuma ação de privacidade:** neste caso o mecanismo envia a informação à nuvem IoT e não realiza nenhuma ação de privacidade sobre o dado coletado.
- **permitir o envio do dado e notificar o usuário:** aqui o fluxo é direcionado para o módulo privacy-IoT-notify para que o usuário seja notificado antes que o dado seja enviado para o requisitante.
- **permitir o envio do dado e anonimizar o dado:** nesta situação o fluxo é direcionado para o módulo privacy-IoT-anonymize para que o dado seja anonimizado antes de ser enviado para o requisitante.
- **Permitir o envio do dado e encriptar o dado:** neste caso, o fluxo é direcionado para o módulo privacy-IoT-encrypt para que o dado seja encriptado antes de ser enviado para o requisitante.

Assim, o mecanismo Privacy Everywhere realiza o direcionamento do fluxo de dados de acordo com a análise da coleta de dados.

7.3.2 Módulo privacy-IoT-anonymize

O módulo privacy-IoT-anonymize realiza a anonimização do dado antes que o mesmo seja enviado ao solicitante. Os tipos de dados controlados pelo mecanismo são presença, vídeo, localização, áudio, preferências pessoais e informações pessoais. A ação de anonimização acontece por perturbação nos dados do tipo

localização, preferências pessoais e informações pessoais. Os dados do tipo presença não necessitam de anonimização. Já a anonimização dos dados do tipo áudio acontece por meio do processamento deste áudio, transformando-o primeiramente em texto, e após isso, o texto é convertido em áudio novamente utilizando-se uma voz padronizada predefinida.

Um trecho de código do módulo privacy-IoT-anonymize onde acontece a anonimização de informações pessoais por perturbação pode ser visualizado no Quadro 7.3.

Quadro 7.3 – Trecho de código do módulo privacy-IoT-anonymize

```
(…)
If (msg.payload.data_type == personal_information){
    If (name.length != 0)   anonymized_name = anonymizePI (name);
    If (email.length != 0)
       anoymized_email = anonymizePI (email);
    If (phone.length != 0)
       anonymized_phone = anonymizePI (phone);
    If (street.length != 0)
       anonymized_street = anonymizePI (street);
    If (credit_card.length != 0)
       anonymized_credit_card = anonymizePI (credit_card);
    If (birth_date.length != 0)
       anonymized_birth_date = anonymizePI (birth_date);
    If (gender.length != 0)
       anonymized_gender = anonymizePI (gender);
    If (id_number.length != 0)
       anonymized_id_number = anonymizePI (id_number);    }
      (...)
   function anonymizePI(string) {
     var result = '';
     while (!result)
       result = Math.random().toString(36).substring(2, string.length + 2);
   return result;       } }
```

Já a anonimização de dados do tipo áudio é realizada com o uso de duas interfaces de programação de aplicativos, do inglês Application Programming Interface (API), disponibilizadas pela IBM: a API “Speech to Text”, que converte áudio em texto; e a API “Text to Speech”, que realiza o processo inverso e converte texto em áudio em uma voz padrão predefinida. Este processo garante que técnicas de desanonimização não restaurarão a voz original do áudio.

7.3.3 Módulo privacy-IoT-encrypt

O módulo privacy-IoT-encrypt realiza a cifragem do dado antes que o mesmo seja enviado ao solicitante. A cifragem do dado se faz necessária em informações sensíveis (números de cartões de crédito, CPF e muitas outras), onde se deseja adicionar uma camada de segurança adicional.

As operações de cifragem e decifragem do dado utilizam um algoritmo de chave simétrica que faz uso do Advanced Encryption Standard (AES) que é uma especificação para criptografia de dados eletrônicos. O comprimento de chave utilizado foi de 256 bits. A escolha pelo AES com comprimento de chave de 256 bits foi devido ao fato deste algoritmo ser amplamente utilizado e seguro. O AES é a cifra de bloco de chave simétrica mais usada em segurança de computadores devido a sua padronização pelo Instituto Nacional de Padrões e Tecnologia – do inglês *National Institute of Standards and Technology* (NIST) – dos Estados Unidos e também por resistir a diversos tipos de ataques (Saraiva *et al.*, 2019).

O mecanismo Privacy Everywhere gera uma chave criptográfica para cada ambiente de coleta de dados cadastrado no mecanismo. O requisitante do dado para solicitar a chave para decifragem do dado, deve estar autorizado na nuvem IoT e, preencher, assinar e submeter um termo de compromisso com normas de uso adequado do dado solicitado.

No Quadro 7.4 podem ser vistas as funções utilizadas pelo módulo privacy-IoT-encrypt para cifragem e decifragem dos dados.

Quadro 7.4 – Trecho de código do módulo privacy-IoT-encrypt

```
(...)
const data_encrypt= {
   algorithm : "aes256",
   type : "hex"
   secret : "key",  };
(...)
function encrypt(data) {
        const cipher = crypto.createCipher(data_encrypt.algorithm,
data_encrypt.secret);
        cipher.update(data);
        return cipher.final(data_encrypt.type);    };

function decrypt(data) {
        const decipher = crypto.createDecipher(data_encrypt.algorithm,
data_encrypt.secret);
        decipher.update(data, data_encrypt.type);
        return decipher.final();    };
```

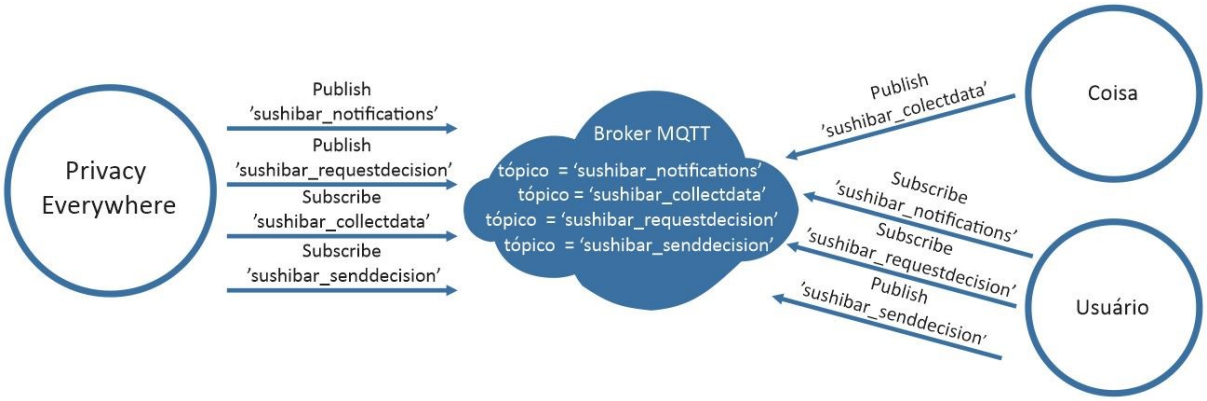
7.3.4 Módulo privacy-IoT-notify

O módulo privacy-IoT-notify é responsável por notificar o usuário antes que o dado seja enviado ao requisitante. As notificações são enviadas por meio de um tópico do MQTT para o aplicativo móvel componente do mecanismo Privacy Everywhere do usuário.

Para cada ambiente coletor de dados são criados quatro tópicos MQTT: um tópico “notifications” por onde o mecanismo envia as notificações de coleta de dados aos usuários quando esta ação se fizer necessária; um tópico “requestdecision” para que o mecanismo divulgue o cenário de coleta de dados ao usuário para que este informe qual é a sua decisão no modo de operação manual; um tópico “senddecision” para que o usuário envie suas decisões de privacidade no modo de operação manual; e, um tópico “collectdata” onde as coisas publicam as informações

coletadas. Um exemplo de como o mecanismo trabalha com os tópicos MQTT pode ser visualizado na Figura 7.4.

Figura 7.4 – Exemplo de como o mecanismo Privacy Everywhere trabalha com os tópicos MQTT



Fonte: próprio autor.

Como pode ser observado na Figura 7.4, o ambiente coletor de dados “sushibar” possui os tópicos “sushibar_notifications”, “sushibar_requestdecision”, “sushibar_collectdata” e “sushibar_senddecision”. O mecanismo Privacy Everywhere: publica no tópico “notifications” para enviar notificações aos usuários quando houver necessidade desta ação; publica no tópico “sushibar_requestdecision” para enviar aos usuários os cenários onde a decisão do usuário se faz necessária; se inscreve no tópico “sushibar_collectdata” para receber as informações das coisas coletoras de dados presentes no ambiente “sushibar”; e, se inscreve no tópico “sushibar_senddecision”, para receber as decisões realizadas pelos usuários no modo de operação manual. As coisas publicam no tópico “sushibar_collectdata” para informar os dados coletados. Já os usuários, se inscrevem no tópico “suhibar_notifications” para receber as notificações enviadas pelo mecanismo; se inscrevem no tópico “sushibar_requestdecision” a fim de receber as solicitações de tomada de decisão no modo de operação manual, e, publicam no tópico “sushibar_senddecision” para que suas decisões de privacidade sejam informadas ao mecanismo Privacy Everywhere no modo de operação manual.

Para que as notificações e as solicitações de tomada de decisão sejam mostradas aos usuários, estes devem estar inscritos no tópico MQTT correspondente ao local coletor de dados que originou a notificação, e também devem estar presentes no local coletor do dado com o aplicativo móvel do

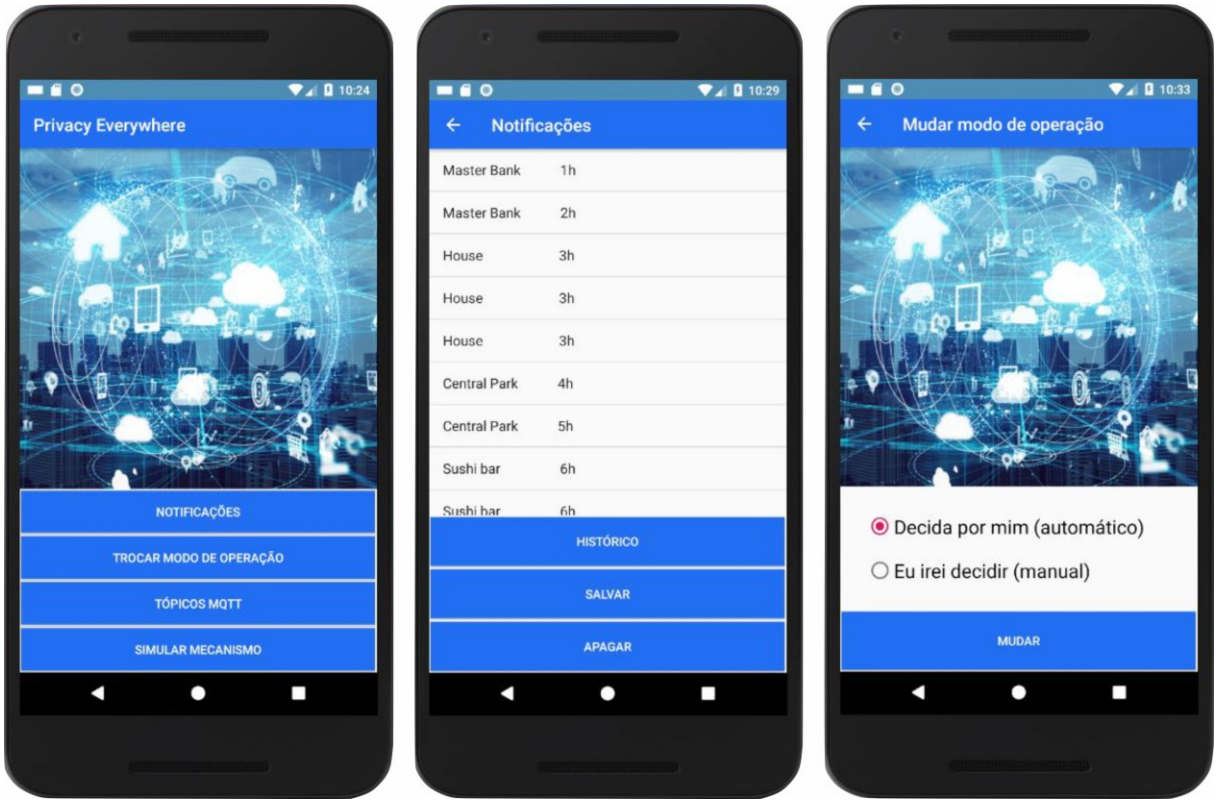
mecanismo Privacy Everywhere instalado e com a localização de seu dispositivo móvel ativada.

7.3.5 Interface do aplicativo móvel do mecanismo Privacy Everywhere

O aplicativo móvel componente do mecanismo Privacy Everywhere foi projetado para o usuário receber notificações de sistemas e dispositivos IoT quando o resultado da análise de solicitação de dados realizada pelo mecanismo for notificar o usuário. Esta aplicação móvel também permite ao usuário escolher entre os modos manual e automático de operação do mecanismo. No modo de operação manual, o usuário deve informar, mediante solicitação, se ele permite ou nega o envio das informações e qual é a ação de privacidade desejada (no modo manual, as ações de privacidade possíveis de serem executadas são anonimizar ou cifrar o dado). Os usuários também podem se inscrever ou cancelar a inscrição nos tópicos MQTT disponíveis e simular o comportamento do mecanismo Privacy Everywhere neste aplicativo móvel.

A Figura 7.5 mostra as telas principal, de notificações e de troca de modo de operação do aplicativo móvel componente do mecanismo Privacy Everywhere. Na tela principal, apresentada na Figura 7.5a, o usuário pode escolher entre as funcionalidades de notificações, de troca do modo de operação do mecanismo, de inscrição e desinscrição nos tópicos MQTT disponíveis no mecanismo e de simulação do mecanismo. Na tela de notificações mostrada na Figura 7.5b, o usuário pode visualizar as notificações recentes, salvar ou apagar notificações recentes e também escolher ir a uma outra tela (por meio da seleção do botão “HISTÓRICO”) onde o usuário pode visualizar e apagar as suas notificações salvas.

Figura 7.5 – Telas principal, de notificações e de troca de modo de operação do aplicativo móvel componente do mecanismo Privacy Everywhere

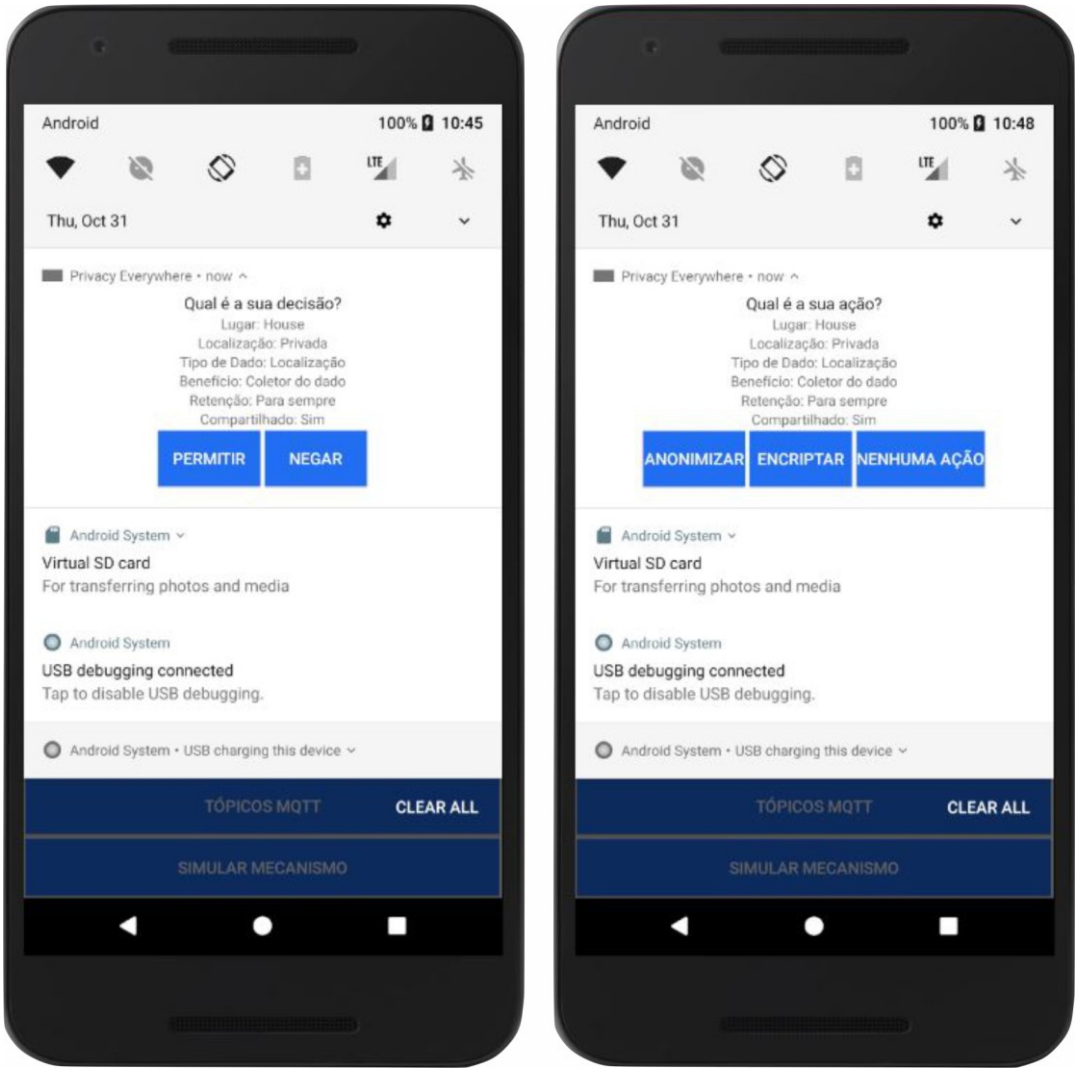


(a)Principal **(b)Notificações** **(c)Troca de modo**

Fonte: próprio autor.

Na Figura 7.5c é mostrada a tela de troca do modo de operação do mecanismo, onde o usuário pode escolher entre os modo “Decida por mim (automático)” e “Eu irei decidir (manual)”. No modo automático de operação, as decisões sobre permitir ou não o envio de determinada informação e qual é a ação de privacidade a ser realizada sobre o dado coletado são automatizadas. No modo de operação manual, o usuário deve informar se permite ou nega o envio do dado coletado e qual é a ação de privacidade a ser executada. São mostrados na Figura 7.6 exemplos de notificações utilizadas no modo manual de operação do mecanismo. Estas notificações contêm: o local onde o dado é coletado; se este local é público ou privado; qual é o tipo de dado coletado; quem é o beneficiário da coleta de dados; por quanto tempo o dado será retido; e, se o dado será ou não compartilhado.

Figura 7.6 – Exemplos de notificações utilizadas no modo manual de operação do mecanismo



(a)Allow/Deny **(b)Privacy Action**

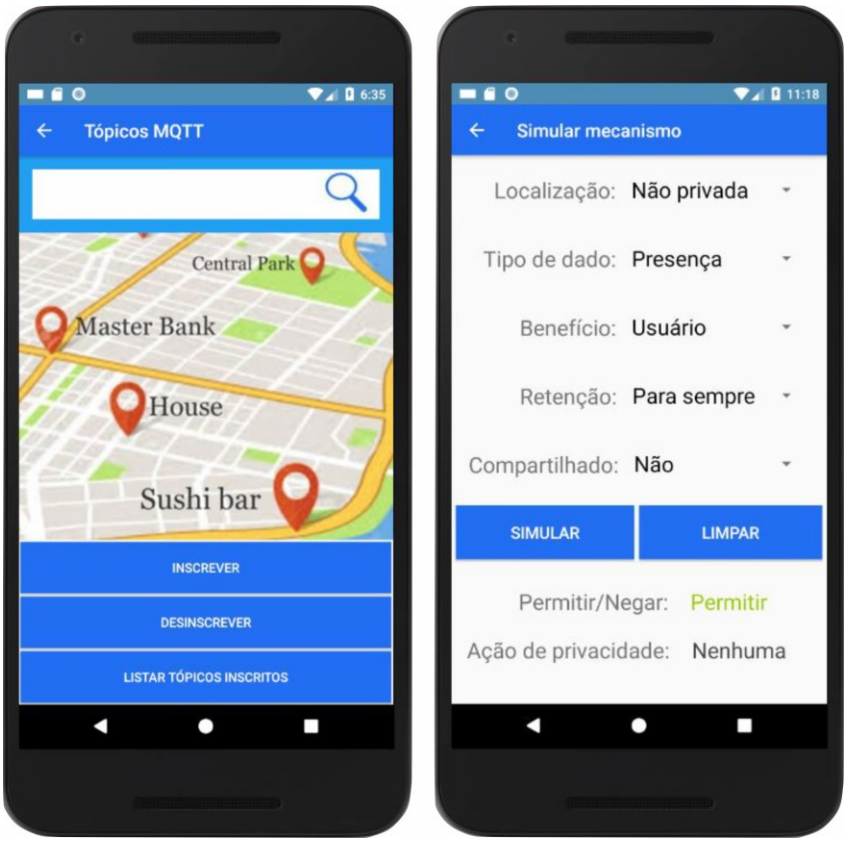
Fonte: próprio autor.

Com essas informações, o usuário deve fornecer a sua decisão de permitir ou negar o envio do dado como pode ser visualizado na Figura 7.6a, e qual ação de privacidade deve ser executada como pode ser observado na Figura 7.6b.

Os tópicos MQTT disponíveis no mecanismo são únicos para cada local de coleta de dados. Assim, o usuário que queira receber ou deixar de receber notificações de um local de coleta de dados deve se inscrever ou se desinscrever no tópico MQTT correspondente ao local. Nos tópicos MQTT não privados, a inscrição não é protegida por autenticação. Já nos tópicos privados, é necessária a autenticação do usuário para concluir a inscrição. A tela de inscrição ou desinscrição no tópico MQTT do mecanismo pode ser visualizada na Figura 7.7a.

Neste aplicativo móvel do mecanismo, o usuário também pode simular o comportamento do mecanismo inserindo valores para os fatores influentes na tomada de decisão utilizados para a construção dos cenários de coleta de dados e observar a saída fornecida pelo mecanismo como pode ser observado na Figura 7.7b.

Figura 7.7 – Telas de inscrição e desinscrição nos tópicos MQTT disponíveis e de simulação do mecanismo Privacy Everywhere



(a)Tópicos MQTT **(b)Simulação do mecanismo**

Fonte: próprio autor.

Na simulação do mecanismo, o usuário pode fornecer como valores de entrada: onde ocorre a coleta de dados; qual o tipo do dado coletado; quem se beneficia com a coleta; por quanto tempo os dados são retidos e se os dados são compartilhados ou não. Depois de fornecidas as entradas para simulação, o usuário pode observar se o mecanismo permite ou nega o envio do dado e qual é a ação de privacidade realizada no cenário informado: não executar nenhuma ação de privacidade, notificar o usuário, anonimizar os dados ou cifrar os dados. O trecho de código que contém a consulta e a resposta à simulação do mecanismo pode ser visualizado do Quadro 7.5.

Quadro 7.5 – Trecho de código da consulta e obtenção da resposta na simulação do mecanismo

```
(...)
private String SIMULATE_MECHANISM_REQUEST_URL =
 "http://192.168.10.10/ query?location=” +
spinnerLocation.getSelectedItem().toString() + “&datatype=” +
spinnerDataType.getSelectedItem().toString()" + “&benefit=” +
spinnerBenefit.getSelectedItem().toString() + “&retention=” +
spinnerRetention.getSelectedItem().toString() + “&shared=” +
spinnerShared.getSelectedItem().toString() ;

URL url = generateUrl(SIMULATE_MECHANISM_REQUEST_URL);
        String responseJson = "";
        try {
           responseJson = makeRequest(url);
        } catch (IOException e) {
            (...)
        }

(...)

private URL generateUrl(String urlString) {
        URL url = null;
        try {  url = new URL(urlString); } catch (MalformedURLException exception) {
           Log.e(LOG_TAG, "Error with generating URL", exception);
           return null;  }
        return url;    }

private String makeRequest(URL url) throws IOException {
        String responseJson = "";
        HttpURLConnection connection = null;
        InputStream inputStream = null;
        try {
           connection = (HttpURLConnection) url.openConnection();
           connection.setRequestMethod("GET");
           connection.setReadTimeout(10000 );
           connection.setConnectTimeout(15000);
           connection.connect();
           inputStream = urlConnection.getInputStream();
           responseJson = readFromStream(inputStream);
        } catch (IOException e) {   (...)   }
        finally {
           if (connection != null) {  connection.disconnect(); }
           if (inputStream != null) {    inputStream.close();   }
        }
        return responseJson;
      }
```

Como pode ser observado no Quadro 7.5, durante a simulação é realizada uma consulta ao *web service,* que após realizar uma consulta às redes neurais do mecanismo Privacy Everywhere, retorna uma resposta no formato Json. A resposta então é interpretada e mostrada ao usuário.

7.4 Arquitetura e resumo do modo de operação do mecanismo Privacy Everywhere

Conforme apresentado na seção anterior, o mecanismo Privacy Everywhere é composto pelas redes neurais Allow/Deny e Privacy Action; pelos módulos privacy-IoT-analyzer, privacy-IoT-notify, privacy-IoT-anonymize e privacy-IoT-encrypt; e também por um aplicativo móvel que é responsável por receber as notificações enviadas ao usuário. O mecanismo Privacy Everywhere possui dois modos de operação: modo automático e modo manual. No modo automático de operação, as decisões de privacidade e as ações de privacidade são executadas pelo mecanismo. No modo manual de operação, o usuário deve responder se deseja ou não que os dados sejam enviados e também se os dados (se enviados) devem ser anonimizados ou cifrados.

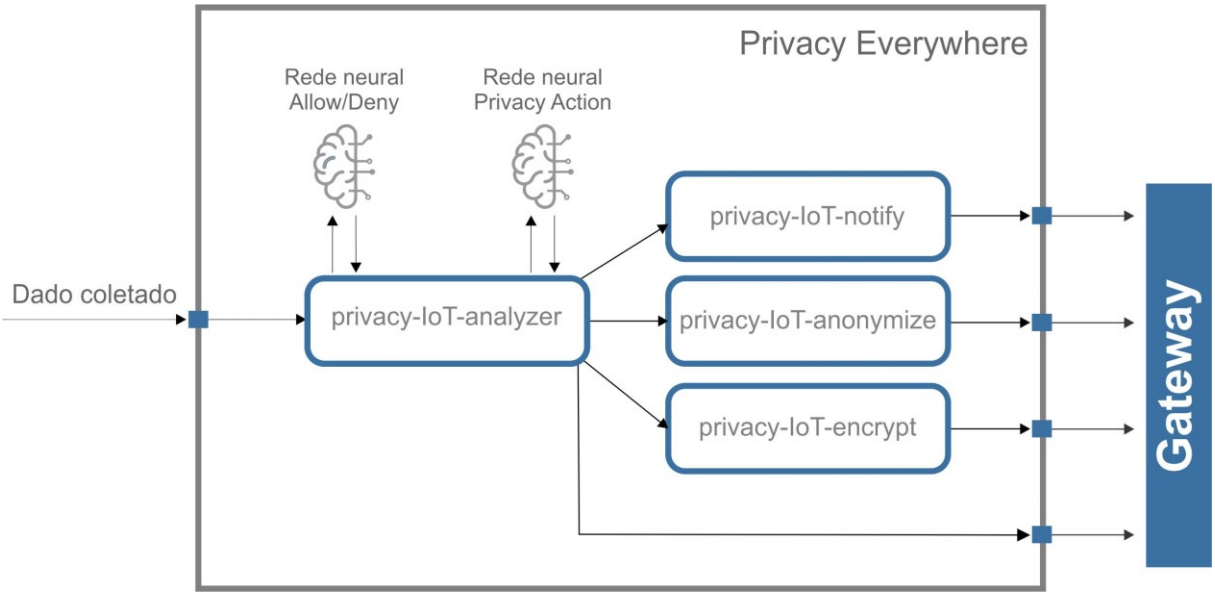
Os dispositivos IoT coletam informações que antes de serem enviadas ao requisitante das informações, passam pelo mecanismo de garantia de privacidade desenvolvido neste trabalho. Este mecanismo contém um módulo chamado pivacy-IoT-analyzer. Este módulo envia no formato *JavaScript Object Notation* (JSON) uma consulta à rede neural Allow/Deny ou ao usuário, com o cenário no qual a solicitação de informação está inserida. Se a resposta obtida pelo mecanismo for negar o envio, o fluxo da requisição se encerra e a informação não é enviada. Por outro lado, se a resposta for permitir o envio, uma nova consulta agora à rede neural Privacy Action ou ao usuário é então realizada.

Se a resposta obtida com a nova consulta for que nenhuma ação de privacidade precisa ser realizada, as informações serão enviadas para a nuvem IoT para serem processadas, armazenadas ou transmitidas para alguma solicitação do usuário ou algum dispositivo IoT. Realizado este procedimento, a ação do

mecanismo nesta solicitação é finalizada. Se a resposta for notificar, o fluxo será direcionado para o módulo privacy-IoT-notify. Se a resposta for anonimizar, o fluxo será direcionado para o módulo privacy-IoT-anonymize. E se a resposta for cifrar o dado, o fluxo será direcionado para o módulo privacy-IoT-encrypt.

A Figura 7.8 mostra a arquitetura da análise de fluxo de uma solicitação de dados no mecanismo do Privacy Everywhere no modo de operação automática antes que os dados sejam enviados.

Figura 7.8 – Arquitetura de análise de fluxo de uma solicitação de dados no mecanismo Privacy Everywhere no modo de operação automática



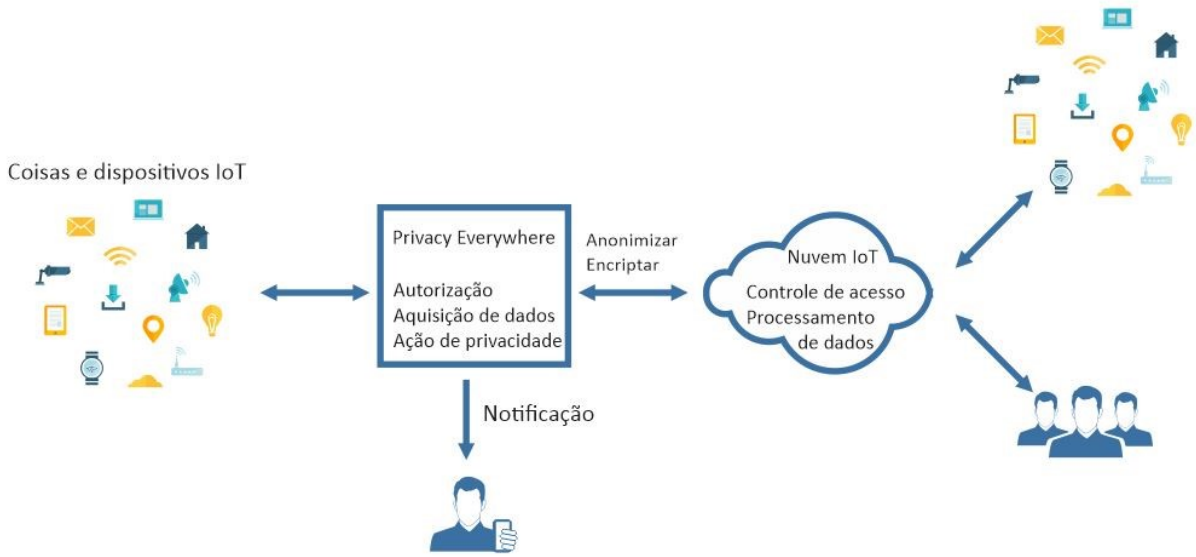
Fonte: próprio autor.

O mecanismo Privacy Everywhere faz uso do MQTT para notificar o usuário. O módulo privacy-IoT-notify envia uma notificação por meio de um tópico do MQTT para o aplicativo móvel componente do mecanismo Privacy Everywhere do usuário antes que a informação seja enviada ao solicitante e o tratamento da solicitação seja encerrado. O módulo privacy-IoT-anonymize realiza a anonimização dos dados do usuário contidos na solicitação antes de enviar as informações para o solicitante e terminar o fluxo. E, o módulo privacy-IoT-encrypt, executa a cifragem dos dados antes que as informações sejam enviadas para o solicitante e o fluxo seja encerrado.

Como pode ser observado na Figura 7.9, o mecanismo Privacy Everywhere é responsável por tomar as decisões de privacidade, autorizando ou negando o envio do dado, controla a aquisição de dados e realiza a ação de privacidade

apropriada para cada cenário em questão antes que os dados sejam enviados para a nuvem IoT. Fica sob a responsabilidade da nuvem IoT executar o processamento dos dados e o controle de acesso.

Figura 7.9 – Visão geral do mecanismo do Privacy Everywhere para tomada de decisão e garantia da privacidade em ambientes de IoT



Fonte: próprio autor.

A solicitação da informação pode pode ser realizada por um usuário ou por algum dispositivo IoT autorizado pela nuvem IoT. Estar autorizado pela nuvem IoT é um requisito primário para enviar uma solicitação de dados. Após a devida autorização pela nuvem IoT, a requisição do dado chega ao dispositivo IoT. O mecanismo Privacy Everywhere atua no fluxo de retorno da solicitação do dado, permitindo ou negando a envio do dado e executando a ação de privacidade apropriada para cada cenário em questão antes que as informações solicitadas sejam retornadas ao solicitante.

O mecanismo deve estar integrado à aplicação que irá realizar a coleta de dados. Se não fosse desta forma, o mecanismo não conseguiria acesso ao conteúdo das requisições quando a aplicação de coleta de dados fizesse uso de um canal de comunicação criptografado.

7.5 Considerações finais

Neste capítulo foram apresentados: as redes neurais Allow/Deny e Privacy Action, os demais componentes do mecanismo, e a arquitetura e um resumo do modo de operação do mecanismo Privacy Everywhere. No capítulo seguinte, será descrito como o mecanismo Privacy Everywhere foi validado e os resultados obtidos desta validação.

Capítulo 8

VALIDAÇÃO DO MECANISMO E DISCUSSÃO

Este capítulo apresenta como o mecanismo Pivacy Everywhere foi validado e uma discussão sobre os resultados obtidos.

8.1 Considerações iniciais

Neste capítulo, é apresentada a validação do mecanismo Privacy Everywhere e uma discussão sobre os resultados do trabalho. Para a validação, foram realizados: uma verificação da acurácia das redes neurais componentes do mecanismo; uma verificação das funcionalidades do mecanismo com o envio de requisições de dados com cenários IoT aleatórios; e uma verificação da média de aumento do tempo de resposta ao se adicionar o mecanismo Privacy Everywhere no modo automático de operação para processar a requisição antes desta ser enviada

Na seção 8.2 é descrito como a acurácia das redes neurais componentes do mecanismo foi verificada. É descrito na seção 8.3 como foi realizada a verificação das funcionalidades do mecanismo e como foi verificada a média de aumento do tempo de resposta a uma requisição ao se fazer uso do mecanismo. Na seção 8.4 é

realizada uma discussão sobre os resultados obtidos. E, por fim, na seção 8.5 são feitas as considerações finais.

8.2 Verificação da acurácia das redes neurais

Na coleta de dados para a construção do mecanismo, foram apresentados cenários de IoT para estudantes e profissionais. Um exemplo de cenário de IoT utilizado nos questionários pode ser visualizado abaixo:

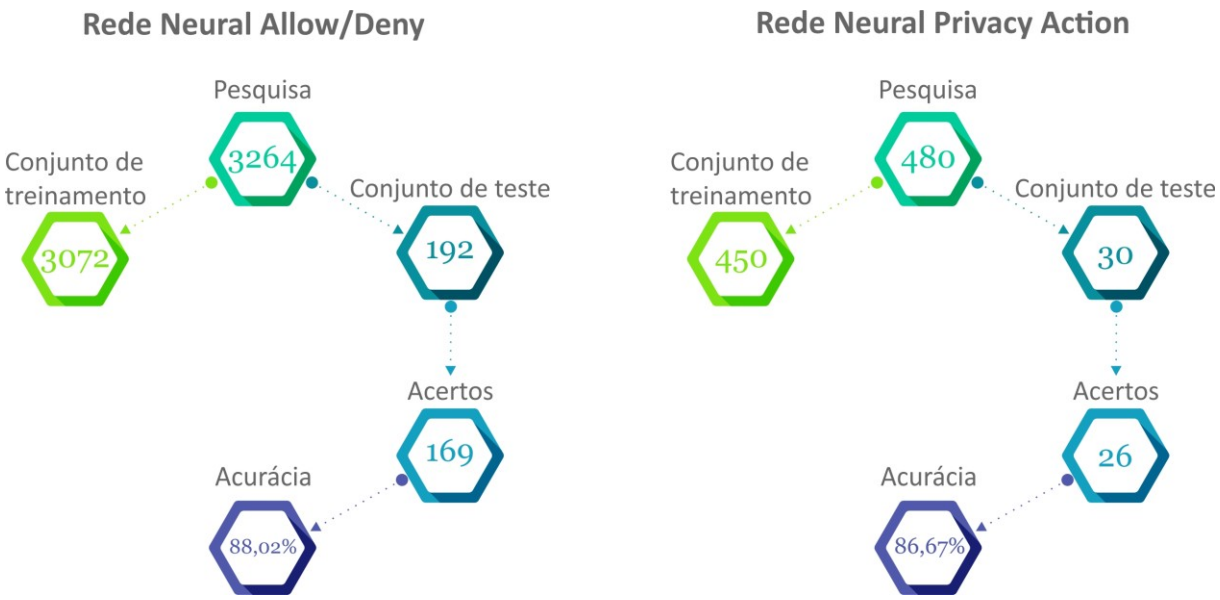
“A empresa de segurança SEG+ quer acessar o sensor de presença de sua residência para registrar em seu sistema os horários mais frequentes em que seus clientes estão em casa. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito”.

Os estudantes foram então solicitados a responder se permitiam ou negavam o envio dos dados para cada cenário de IoT apresentado. Os profissionais foram consultados sobre qual ação de privacidade era apropriada para cada cenário IoT apresentado. Foram apresentados 24 cenários para cada aluno e 96 cenários para cada profissional. Foram geradas 3264 respostas dos alunos e 480 respostas dos profissionais.

As respostas foram divididas em dois conjuntos de dados: o conjunto de dados de treinamento da rede neural do mecanismo e o conjunto de dados de teste. As respostas dos estudantes foram divididas em 3072 respostas (94,12% das respostas) para o conjunto de dados de treinamento da rede neural Allow/Deny e 192 respostas (5,88% das respostas) para o conjunto de dados de teste. As respostas dos profissionais foram divididas em 450 respostas (93,75% das respostas) para o conjunto de dados de treinamento da rede neural Privacy Action e 30 respostas (6,25% das respostas) para o conjunto de dados de teste.

Para a validação do mecanismo, foram utilizados os conjuntos de dados de teste (que não foram utilizados no treinamento das redes neurais) e foi observada a precisão das redes neurais do mecanismo Privacy Everywhere. Os resultados das previsões podem ser visualizados na Figura 8.1.

Figura 8.1 – Resultados das predições realizadas pelas redes neurais Allow/Deny e Privacy Action componentes do mecanismo



Fonte: próprio autor.

Assim, o mecanismo realizou 192 previsões com a rede neural Allow/Deny e 30 previsões com a rede neural Privacy Action. Das 192 previsões realizadas com a rede neural Allow/Deny, 169 estavam corretas. Isso corresponde a uma precisão de 88,02%. A rede neural Privacy Action teve sucesso em 26 das 30 previsões, resultando em uma precisão de 86,67%.

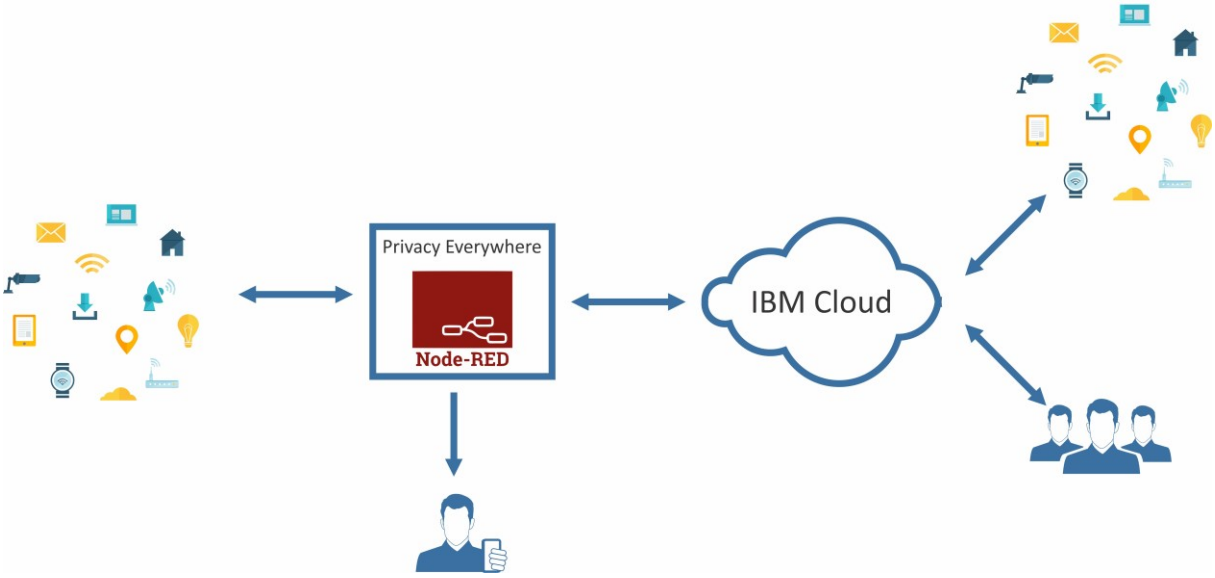
8.3 Verificação das funcionalidades do mecanismo

Foi realizada uma verificação das funcionalidades do mecanismo a fim de se observar o comportamento do mecanismo com relação às ações de privacidade a serem executadas. Esta verificação foi realizada com o uso do mecanismo Privacy Everywhere em conjunto com a plataforma Node-RED, que é uma IDE para programação em fluxos para IoT integrado com a nuvem da IBM, a IBM cloud. A nuvem da IBM foi a escolhida para testar as funcionalidades do mecanismo, devido à facilidade de integração com a plataforma Node-RED, facilidade de configuração de dispositivos coletores de dado e por atender aos requisitos de segurança

desejados nesta verificação (a nuvem IoT da IBM orefece a funcionalidade de encriptação da comunicação e de autenticação).

Foi criada uma aplicação na *Internet of Things Cloud Platform* da IBM hospedada na região Dallas que fez uso do hub IoT da IBM, o qual permite configurar e gerenciar os dispositivos conectados. Esta aplicação foi utilizada para simular requisições de dados passando pela nuvem IoT da IBM e sendo tratadas pelo mecanismo Privacy Everywhere. Uma visão geral da arquitetura utilizada para verificação das funcionalidades do mecanismo pode ser observada na Figura 8.2.

Figura 8.2 – Visão geral da arquitetura utilizada para verificação das funcionalidades do mecanismo.



Fonte: próprio autor.

Um broker MQTT, componente do mecanismo Privacy Everywhere, também foi instalado e configurado em um servidor da rede local. No servidor da rede local também foram implementados um webservice (também componente do mecanismo Privacy Everywhere) que possui como funcionalidade principal realizar consultas às redes neurais e retornar as respostas das consultas realizadas.

Foram então enviadas 30 requisições com cenários aleatórios para o mecanismo a fim de observar como o mecanismo se comporta. O resultado das requisições pode ser observado na Tabela 8.1.

Tabela 8.1 – Resultado das requisições enviadas a fim de se observar o comportamento do mecanismo Privacy Everywhere

Cenário	Ação esperada (rede Allow/Deny)	Ação do mecanismo	Ação esperada (rede Privacy Action)	Ação do mecanismo	Ação de privacidade proposta foi devidamente executada?
Cenário 1	allow	allow	No action	No action	sim
Cenário 2	deny	deny	-	-	sim
Cenário 3	allow	allow	Anonymize	Anonymize	sim
Cenário 4	deny	deny	-	-	sim
Cenário 5	deny	deny	-	-	sim
Cenário 6	allow	allow	Anonymize	Anonymize	sim
Cenário 7	allow	allow	Encrypt	Encrypt	sim
Cenário 8	deny	deny	-	-	sim
Cenário 9	deny	deny	-	-	sim
Cenário 10	deny	deny	-	-	sim
Cenário 11	allow	allow	Notify	Notify	sim
Cenário 12	allow	allow	No action	No action	sim
Cenário 13	allow	allow	Notify	Notify	sim
Cenário 14	allow	allow	Anonymize	Anonymize	sim
Cenário 15	deny	deny	-	-	sim
Cenário 16	allow	allow	Encrypt	Encrypt	sim
Cenário 17	allow	allow	Encrypt	Encrypt	sim
Cenário 18	deny	deny	-	-	sim
Cenário 19	allow	allow	Notify	Notify	sim
Cenário 20	allow	allow	Anonymize	Anonymize	sim
Cenário 21	deny	deny	-	-	sim
Cenário 22	allow	allow	No action	No action	sim
Cenário 23	allow	allow	Anonymize	Anonymize	sim
Cenário 24	allow	allow	Anonymize	Anonymize	sim
Cenário 25	deny	deny	-	-	sim
Cenário 26	allow	allow	Encrypt	Encrypt	sim

Cenário 27	deny	deny	-	-	sim
Cenário 28	deny	deny	-	-	sim
Cenário 29	allow	allow	Encrypt	Encrypt	sim
Cenário 30	deny	deny	-	-	sim

Como pode ser observado na Tabela 8.1, o mecanismo se comportou de forma satisfatória nos cenários simulados e negou o envio do dado quando esta ação foi a proposta pelo mecanismo. Também as funcionalidades de notificar o usuário, anonimizar e encriptar o dado funcionaram conforme o esperado. Estas requisições não possuem como objetivo verificar novamente a acurácia das redes neurais na realização de predições. Esta verificação foi realizada a fim de se observar o comportamento do mecanismo com suas respectivas funcionalidades durante a requisição de um dado.

Após a verificação de comportamento das funcionalidades, foi realizada uma verificação do aumento do tempo de resposta ao se adicionar o mecanismo Privacy Everywhere para processar uma requisição antes desta ser enviada. Foram enviadas cinco requisições idênticas para cada cenário específico, onde já era esperada uma ação de privacidade específica para o cenário em questão no modo de operação automática.

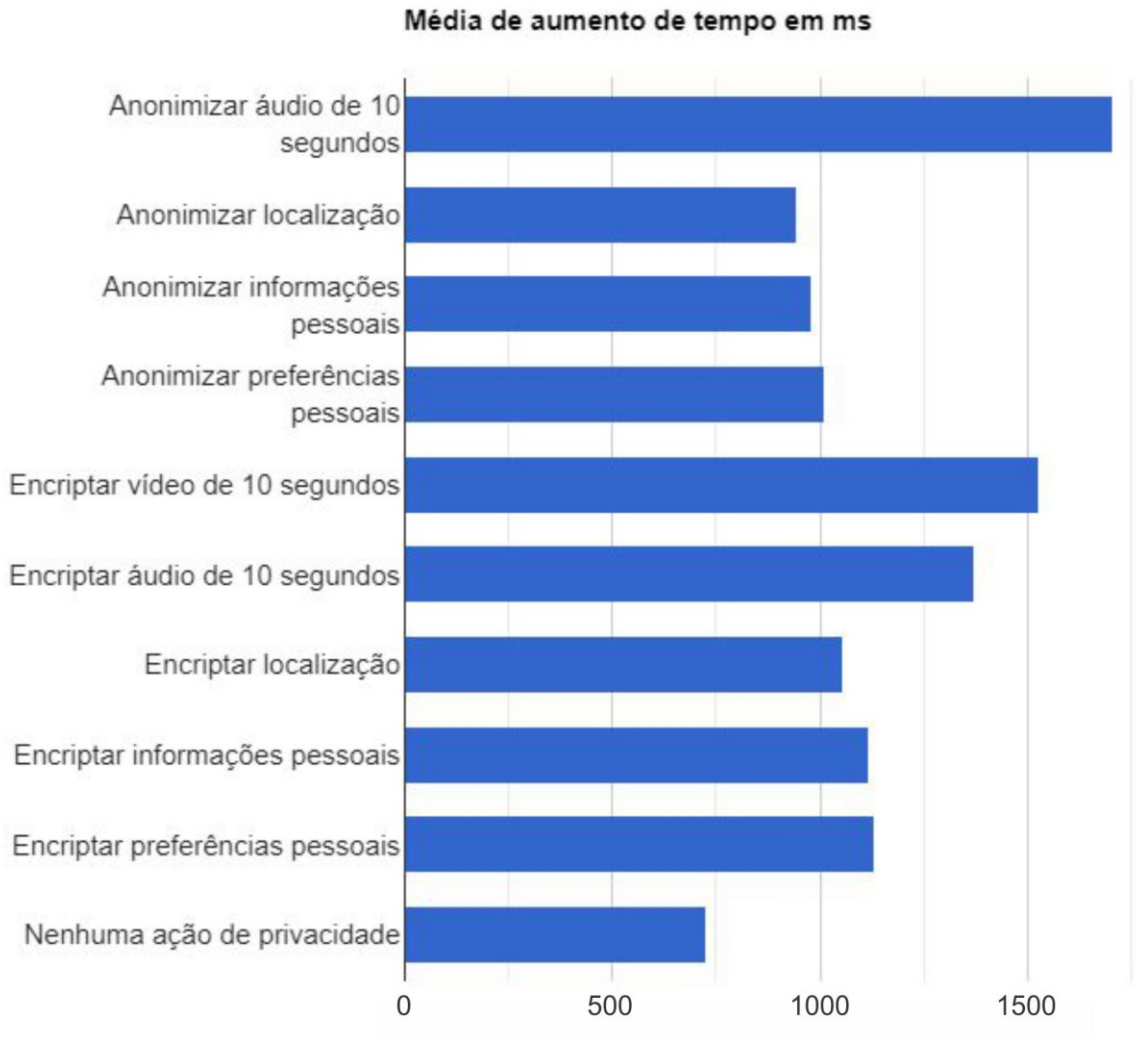
A aplicação criada na IBM cloud para esta verificação contou com 256 MB de memória. O servidor local que estava simulando os dispositivo IoT e tratava das requisições e das respostas foi definido virtualizado com 4096 MB de memória RAM, 4 processadores, com os processadores sem restrição de execução, com 64 MB de memória de vídeo e com a aceleração 3D da controladora gráfica ativada. Os resultados desta verificação podem ser visualizados na Figura 8.3.

Para esta verificação foram utilizadas as ações de anonimizar áudio, anonimizar localização, anonimizar informações pessoais, anonimizar preferências pessoais, encriptar áudio, encriptar localização, encriptar informações pessoais e encriptar preferências pessoais.

Em dados do tipo “presença”, não são realizadas ações de privacidade. O tratamento de dados do tipo “presença” é realizado pelo mecanismo apenas permitindo ou não o envio da informação.

O mecanismo Privacy Everywhere também não realiza a ação de anonimizar um vídeo, pois esta ação demanda uma elevada complexidade de implementação e está fora do escopo do mecanismo Privacy Everywhere.

Figura 8.3 – Média de aumento do tempo de resposta ao se fazer uso do mecanismo Privacy Everywhere no modo automático de operação



Fonte: próprio autor.

8.4 Discussão

O surgimento de novas ameaças à privacidade decorrentes das novas formas de interação e comunicação introduzidas pelos ambientes IoT, exige soluções para proteção da privacidade a serem desenvolvidas. Divulgar informações privadas

indiscriminadamente sem tratamento adequado resulta em perda de privacidade (Adelhamid, Sharman & Bezawada, 2015).

Este estudo representa uma tentativa de explorar a eficácia em se tomar decisões de privacidade por usuários em ambientes de IoT e executar ações de privacidade sobre os dados coletados por dispositivos IoT. A precisão de 88,02% da rede neural Allow/Deny indica que esse valor é satisfatório e suficiente para o mecanismo tomar uma decisão de privacidade pelo usuário em ambientes com um grande número de dispositivos de IoT e em situações em que o usuário não deseja ser perturbado. Este estudo também fornece insights teóricos sobre quais fatores influenciam a tomada de decisão pelos usuários.

A precisão de 86,67% da rede neural Privacy Action do mecanismo proposto indica que esse valor é suficiente para executar ações de privacidade adequadas em dados coletados antes que esses dados sejam enviados ao solicitante. Essas ações de privacidade em ambientes de IoT fornecem insights sobre como os riscos de privacidade inerentes ao surgimento de novas formas de interação e comunicação podem ser mitigados.

A funcionalidade de simulação das saídas das redes neurais foi adicionada ao aplicativo móvel Privacy Everywhere para que o usuário possa ver como o mecanismo se comporta em determinados cenários. Esta simulação é necessária para que o usuário possa usar com mais confiança o modo automático do mecanismo.

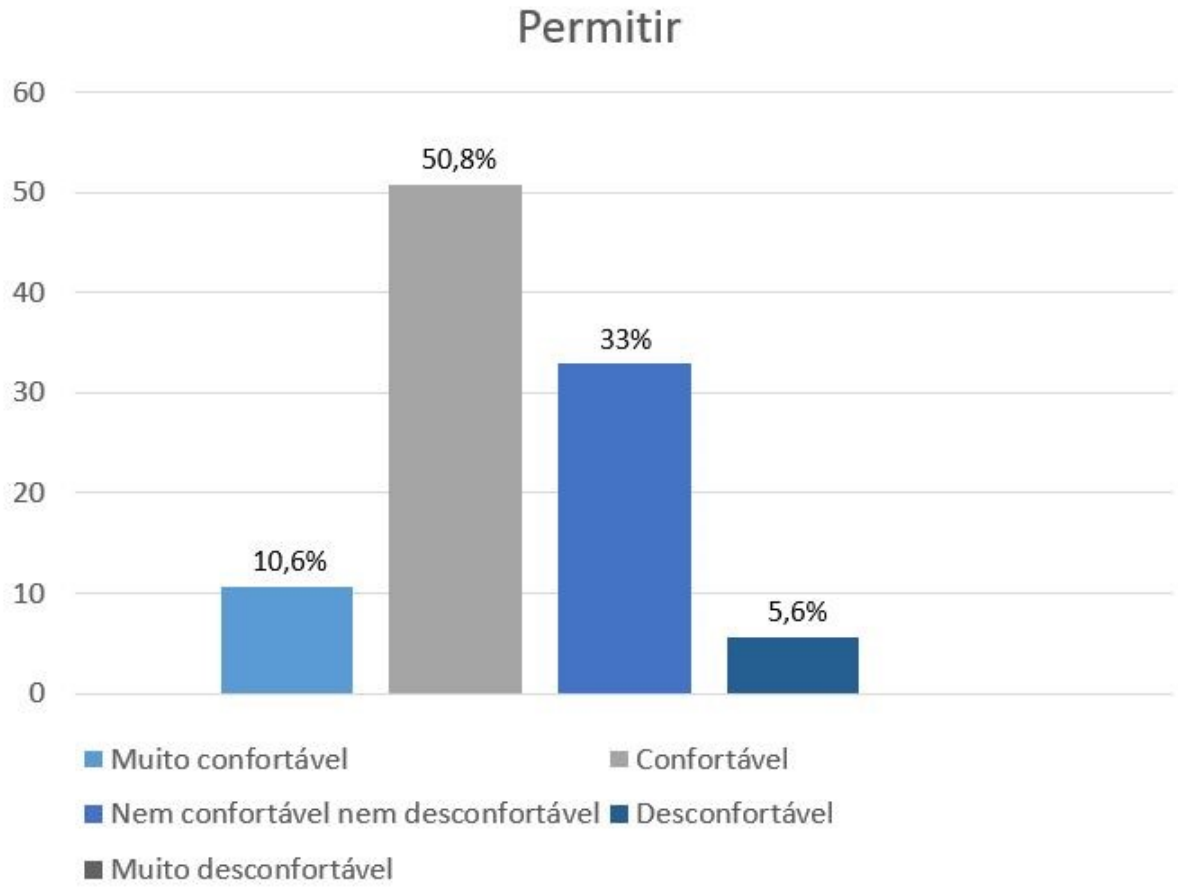
Como pode ser visto na Figura 8.3, a ação de privacidade do mecanismo que apresentou maior aumento no tempo de resposta foi a ação de anonimizar um áudio. Este maior aumento se deve à complexidade desta ação de privacidade: primeiro o áudio é convertido para texto pela API “Speech to Text” e depois o texto é convertido novamente para áudio para uma voz padrão previamente definida na API “Text to Speech”. Este procedimento impede que técnicas de desanonimização sejam aplicadas no áudio anonimizado para que se obtenha o áudio original.

A média de aumento de tempo em milissegundos que ocorre ao se fazer uso do mecanismo Privacy Everywhere, indica que no modo de operação automática do mecanismo, este não prejudica a coleta de dados, pois a maior média de tempo foi de 1706 milissegundos adicionados ao se anonimizar um áudio de 10 segundos. Porém, ao se utilizar o modo manual de operação do mecanismo, o tempo de resposta da requisição é aumentado. No modo de operação manual, é necessário

aguardar que o usuário responda a solicitação para se realizar a ação de privacidade, ou que após um timeout pré-definido, se inicie o modo de operação automática do mecanismo. O tempo de resposta da requisição no modo de operação automática sempre será menor que o tempo de resposta no modo de operação manual.

Nas Figuras 8.4 e 8.5, pode-se observar a tendência do usuário em permitir ou negar o envio de um dado com relação ao nível de conforto do usuário com a coleta de dados. Como pode ser observado, todos os usuários que relataram se sentir confortáveis ou muito confortáveis com a coleta do dado, permitiram o envio da informação no cenário em questão. Na maioria das decisões de permitir o envio do dado, os usuários relataram se sentir confortáveis com a coleta. Alguns usuários que relataram se sentir desconfortáveis com a coleta de dados no cenário, permitiram o envio. Este fato é justificado pelo oferecimento de algum serviço ou benefício para o usuário em troca da informação solicitada.

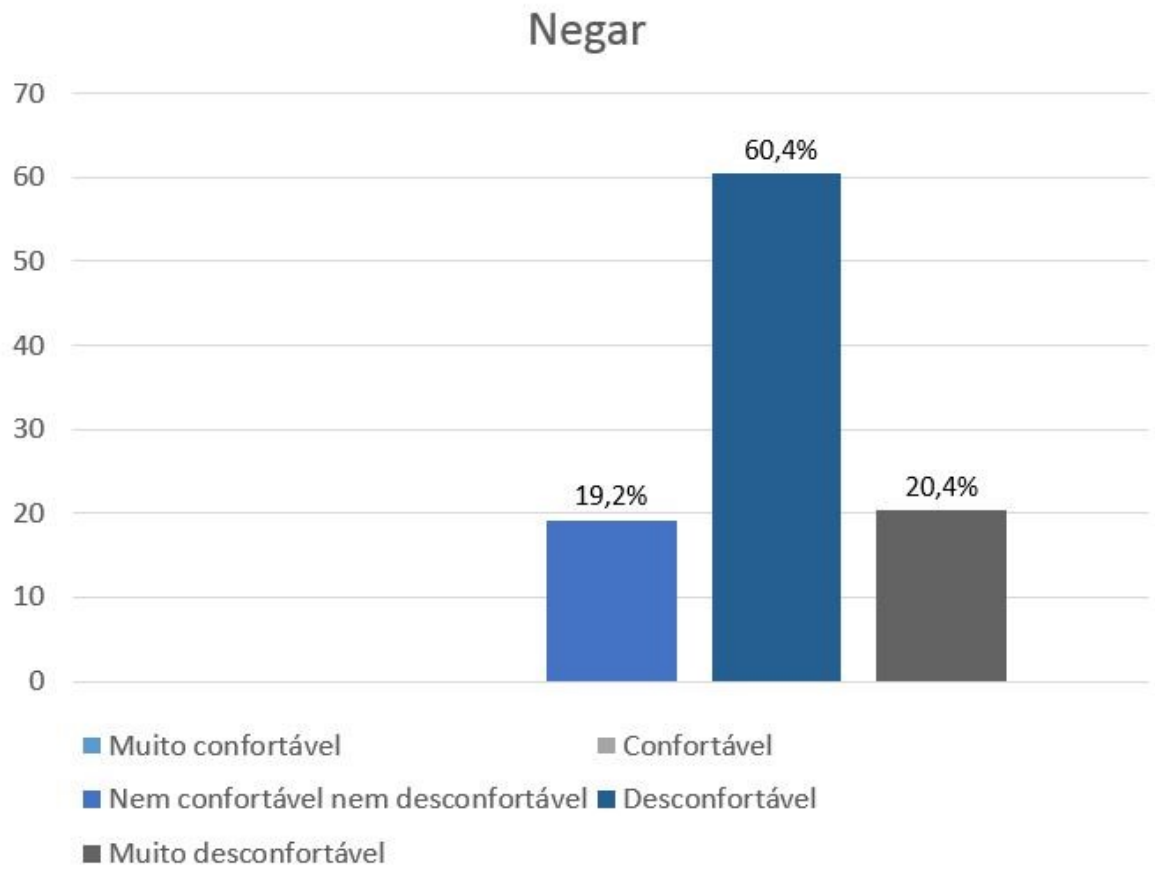
Figura 8.4 – Percentuais de níveis de conforto com a coleta de dados nas decisões de permitir o envio do dado pelos usuários



Fonte: próprio autor.

Já nas decisões de negar o envio do dado, pode-se observar que a maioria dos usuários que negaram o envio relataram se sentir desconfortáveis com a coleta de dados apresentada pelo cenário. Todos os usuários que relataram se sentir muito desconfortáveis com a coleta de dados apresentada pelo cenário, negaram o envio do dado. Pode-se observar também, como mencionado anteriormente, que nenhum usuário que relatou se sentir confortável ou muito confortável com a coleta de dados, negou o envio do dado.

Figura 8.5 – Percentuais de níveis de conforto com a coleta de dados nas decisões de negar o envio do dado pelos usuários



Fonte: próprio autor.

De uma perspectiva prática, este estudo tem implicações em várias áreas de aplicação - casas inteligentes, vigilância por vídeo, saúde, cidades inteligentes, mobilidade inteligente, monitoramento ambiental e outras áreas que fazem uso de soluções de IoT. Esses tipos de aplicativos geram uma grande quantidade de fluxo de dados que requer autorização e tratamento devido à privacidade antes de serem enviados. Os resultados sugerem que tanto as decisões de privacidade dos usuários

quanto as ações de privacidade a serem executadas em cada cenário específico podem ser automatizadas.

As ações de privacidade realizadas pelo mecanismo Privacy Everywhere visam não apenas preservar a privacidade do usuário, mas também adicionar uma camada extra de segurança na troca de dados entre usuários e requisitantes.

8.5 Considerações finais

Este capítulo descreveu como foi feita a validação do mecanismo e como foi verificada a acurácia das redes neurais que compõem o mecanismo Privacy Everywhere. Também foi realizada uma discussão sobre os resultados obtidos com a validação do mecanismo e sobre as implicações teóricas e práticas do mecanismo proposto.

No capítulo seguinte, são apresentadas as conclusões e os trabalhos futuros.

Capítulo 9

CONCLUSÕES E TRABALHOS FUTUROS

Este capítulo apresenta as conclusões, os trabalhos futuros e a publicação resultante do desenvolvimento deste trabalho.

9.1 Conclusões

A evolução tecnológica e a crescente adoção de soluções integradas e conectadas estão se movendo em direção a ambientes cada vez mais invasivos em relação às questões de privacidade.

O mecanismo Privacy Everywhere foi apresentado neste trabalho. O objetivo deste mecanismo é realizar decisões de privacidade pelos usuários e executar ações de privacidade nos dados coletados por dispositivos IoT de forma automática ou permitir que o usuário decida e defina qual ação de privacidade deve ser executada na coleta de dados em questão.

A motivação para o desenvolvimento deste trabalho foi o aumento no número de dispositivos IoT com consequente aumento nas formas de interação, comunicação e coleta de dados, fato este que gera a necessidade de se criar

mecanismos para tratar questões de privacidade do usuário durante a coleta de dados.

A precisão de 88,02% da rede neural Allow/Deny indica que esse valor é satisfatório para o mecanismo tomar uma decisão de privacidade pelo usuário em cenários IoT de coleta de dados. A precisão de 86,67% da rede neural Privacy Action indica que esse valor é suficiente para executar ações de privacidade adequadas em dados coletados em cenários IoT.

A média de aumento de tempo de resposta apresentada no uso do mecanismo em seu modo de operação automática indica que fazer uso do Privacy Everywhere não impede a coleta de dados em tempo real.

Este mecanismo se mostrou capaz de ajudar os usuários com questões de privacidade nos ambientes de IoT, ao se mostrar capaz de automatizar decisões e ações de privacidade nos dados coletados; ou mesmo ao permitir que o usuário decida e defina qual ação de privacidade deve ser executada no dado coletado. O Privacy Everywhere também se apresentou como uma ferramenta adicional para preservar a privacidade do usuário.

Este estudo também fornece insights sobre quais fatores influenciam a tomada de decisões de privacidade pelos usuários e também mostra a correlação entre o nível de conforto do usuário com a coleta de dados apresentada no cenário IoT com a decisão de permitir ou negar o envio do dado.

9.2 Trabalhos futuros

Para se obter uma melhoria do mecanismo em trabalhos futuros, é necessário fazer uma ampla coleta de dados com os potenciais usuários do mecanismo, a fim de melhorar as respostas da rede neural em permitir ou negar o envio dos dados. Diferenças regionais e culturais também devem ser consideradas na coleta de dados e na avaliação do mecanismo.

Também é indicado para melhorar o mecanismo, aumentar o número de fatores para tomada de decisão de privacidade utilizados para a construção das redes neurais. Isso aumentaria as possibilidades de tomada de decisão do

mecanismo, mas também aumentaria consideravelmente o número de cenários possíveis e necessários para a construção das redes neurais.

A criação de uma taxonomia de privacidade em conjunto com a criação de perfis de privacidade para os usuários também seriam interessantes para melhora do mecanismo.

Por fim, também é indicado como trabalho futuro, verificar outros algoritmos de aprendizado de máquina a fim de tentar melhorar a acurácia das redes neurais e possivelmente construir novos modelos de predição.

9.3 Publicação de trabalhos

Durante o desenvolvimento deste trabalho o seguinte artigo foi publicado:

Andrade, L. P., Zorzo, S. D. “Privacy Everywhere: a Mechanism for Decision Making and Privacy Assurance in IoT Environments”, The 25th Americas Conference on Information Systems (AMCIS), 15 a 17 de Agosto de 2019, Cancún, México.

REFERÊNCIAS

AAZAM, M.*et al.* Cloud of things: integrating internet of things and cloud computing and the issues involved. In: Applied sciences and technology (IBCAST), 2014 *11th International Bhurban conference on Anchorage*, Alaska, USA: IEEE; June 2014. p. 414–9.

Abdelhamid, M., Sharman, R., and Bezawada, R., 2015. "Better Patient Privacy Protection with Better Patient Empowerment about Consent in Health Information Exchanges". WISP 2015 Proceedings. 14.

BANDYOPADHYAY, D; SEN, J. Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Pers Commun*, 58:49–69. April, 2011.

BARBARAN, J.; DIAZ, M.; RUBIO, B. A virtual channel-based framework for the integration of wireless sensor networks in the cloud. In: *Proceedings of the 2nd international conference on future internet of things and cloud (FiCloud-2014*). Barcelona, Spain; Aug 2014. p. 334–9. http://dx.doi.org/10.1109/FiCloud.2014.59

BLOXHAM, A. Most burglars using Facebook and Twitter to target victims, survey suggests. *The Telegraph*. http://bit.ly/pOL8MX [Online. Last accessed: 2018-05-27], 2011.

BOTTA, A. *el al.* On the integration of cloud computing and internet of things, in: 2014 *International Conference on Future Internet of Things and Cloud, IEEE*, 2014, pp. 23–28. http://dx.doi.org/10.1109/FiCloud.2014.14.

BRASIL. Lei nº 13709 de 14 de Agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 8 de setembro de 2019.

BRASIL. Lei nº 13853 de 8 de Julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em 15 de outubro de 2019.

BROWN, E. *Who Needs the Internet of Things?.* Linux.com. Retrieved 23 October 2016.

CHOW, R. 2017. “The last mile for iot privacy”. IEEE Security & Privacy, 15(6):73-76.
DÍAZ, M.; MARTÍN, C.; RUBIO, B. State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing**.** *J. Netw. Comput***.** Appl. 67, C (May 2016), 99-117. DOI: http://dx.doi.org/10.1016/j.jnca.2016.01.010

COCHRAN, W. G. Sampling techniques. 3. ed. Westlake Village: John Wiley & Sons, 1977. 428 p. (Wiley series in probability and mathematical statistics: Applied probability and statistics). ISBN 0-471-16240-X.

COLNAGO, J. H. Privacy agents in the IoT: considerations on how to balance agent autonomy and user control in privacy decisions. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de São Carlos. São Carlos, 2016.

DRAGOI, V. *et al.* Survey on cryptanalysis of code-based cryptography: From theoretical to physical attacks. *7th International Conference on Computers Communications and Control (ICCCC*), Oradea, 2018, pp. 215-223.

EL, E. K. *et al.* A Systematic Review of Re-Identification Attacks on Health Data. *PLoS ONE* 2011; 6(12), doi:10.1371/journal.pone.0028071.

Ericsson Consumerlab Wearable Technology and the Internet of Things. Disponível em: https://www.ericsson.com/en/trends-and-insights/consumerlab/consumer-insights/reports/wearable-technology-and-the-internet-of-things. Acesso em: 26/05/2018.

FUNG, B. C. M. Wang K, Chen R, Yu PS. Privacypreserving data publishing: A survey of recent developments. *ACM Comput. Surv*. 2010; 42(4):14:1–14:53, doi:10.1145/1749603.1749605.

HALLER, S.; KARNOUKOS, S.; SCHROTH, C. The Internet of Things in an Enterprise Context. In: *Future Internet – FIS 2008*. Lecture Notes in Computer Science, vol 5468. Springer, Berlin, Heidelberg.

HANK, P. *et al.* Automotive ethernet: invehicle networking and smart mobility, in: Proceedings of the Conference on Design, Automation and Test in Europe, *EDA Consortium*, 2013, pp. 1735–1739.

HE, W.; YAN, G.; XU, L.D.Developing vehicular data Cloud services in the IoT environment**,** *IEEE* Trans. Ind. Inf. 10 (2) (2014) 1587–1595.

HENZE, M. *et al.* A comprehensive approach to privacy in the cloud-based Internet of Things. *Future Gener. Comput. Syst. 56*, C (March 2016), 701-718. DOI: https://doi.org/10.1016/j.future.2015.09.016

HUA, L.; JUNGUO, Z.; FANTAO, L. Internet of Things Technology and its Applications in Smart Grid. *TELKOMNIKA Indonesian Journal of Electrical Engineering***.** Vol.12, No.2, February 2014, pp. 940-946.

JAYARAMAN, P. *et al.* 2017, Privacy preserving Internet of Things: From privacy techniques to a blueprint architecture and efficient implementation, *Future Generation Computer Systems*, 2017, vol. 76, pp. 540-549.

JIA, X. *et al*. RFID technology and its applications in internet of things (IoT). *Proc. 2nd IEEE Int. Conf. Consum. Electron., Commun. Netw. (CECNet)*, Yichang, China, Apr. 21–23, 2012, pp. 1282–1285.

KIM, D. *et al.* Willingness to provide personal information: Perspective of privacy calculus in iot services Comput. Hum. Behav., 92 (2019), pp. 273-281, 10.1016/j.chb.2018.11.022

KOBSA, A. Privacy-enhanced web personalization. The adaptive web. *Springer-Verlag*, 2007; 628–670.

LEE, H.; KOBSA, A. Understanding user privacy in Internet of Things environments, 2016 *IEEE 3rd World Forum on Internet of Things (WF-IoT),* Reston, VA, 2016, pp. 407-412.

LEITHARDT, V. R. Q. et al. Mechanism for Privacy Management Based on Data History (UbiPri-His). Journal of ubiquitous systems and pervasive networks (PRINT), v. 10, p. 11-19, 2018. ISSN/ISBN: 19237324

LAZARESCU, M. Design of a wsn platform for long-term environmental monitoring for IoT applications, *IEEE* J. Emerg. Sel. Top. Circuits Syst. 3 (1) (2013) 45–54.

LEHTONEN, M.; OERTEL, N.; VOGT, H. Features, Identity, Tracing, and Cryptography in Product Authentication. *13th International Conference on Concurrent Enterprising*, 2007.

LI, S.; XU, L.; WANG, X. Compressed sensing signal and data acquisition in wireless sensor networks and internet of things. *IEEE Trans. Ind. Informat*., vol. 9, no. 4, pp. 2177–2186, Nov. 2013.

LI, W. *et al.* Resource virtualization and service selection in Cloud logistics, *J. Netw. Comput. Appl*. 36 (6) (2013) 1696–1704.

LI, X. *et al.* Smart Community: An Internet of Things Application. *IEEE Communications Magazine*. November, 2011.
MA, H. *et al.* On Networking of Internet of Things: Explorations and Challenges. *IEEE internet of things jornal*. Vol. 3, no. 4, August 2016.

MELL, P.; GRANCE, T. The NIST definition of Cloud computing, Natl. *Inst. Stand. Technol*. 53 (6) (2009) 50.

MERCER, D. Connected World: Smart Home Is Key To Tomorrow's Internet Of Things. *Report*. October, 2017.

MOHANTY, S. P.; CHOPPALI, U.; KOUGIANOS, E. Everything You Wanted to Know About Smart Cities. *IEEE Consumer Electronics Magazine***.** July, 2016.

MORENO-VOZMEDIANO *et al.* Iaas cloud architecture: from virtualized datacenters to federated cloud infrastructures. *Computer* 2012;12:65–72.

NAEINI, P. E. Privacy Expectations and Preferences in an IoT World. *Symposium on Usable Privacy and Security (SOUPS)* 2017, July 12–14, 2017, Santa Clara, California.

NGAI, E. W. T. *et al.* RFID research: An academic literature review (1995–2005) and future research directions. *Int. J. Prod. Econ*., vol. 112, no. 2, pp. 510–520, 2008.

OWASP. Anonimização. Diponível em: https://www.owasp.org/index.php/Anonymization. Acesso em: 28/05/2018.

PAQUIN, C.; ZAVERUCHA, G. *U-Prove Cryptographic Specification V1.1* (Revision 3)", December, 2013.

PARÉ, G. *et al.* Clinical effects of home telemonitoring in the context of diabetes, asthma, heart failure and hypertension: a systematic review. *J Med Internet Research*, June 2010. Available at: http://www.jmir.org/2010/2/e21/ doi: 10.2196/jmir.1357

PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados (RGPD) (UE) 2016/79. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=PT. Acesso em: 8 de dezembro de 2019.

PEARSON, S. Taking account of privacy when designing cloud computing services, in: 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, *IEEE*, 2009, pp. 44–52. http://dx.doi.org/10.1109/CLOUD.2009. 5071532.

PORAMBAGE, P. *et al.* The Quest for Privacy in the Internet of Things. *IEEE Cloud Computing*, vol. 3, no. 2, pp. 36-45, Mar.-Apr. 2016.

RENAUD, K; CRUZ, D. G. Privacy: Aspects, definitions and a multi-faceted privacy preservation approach. *Information Security for South Africa*, Sandton, Johannesburg, 2010, pp. 1-8.

ROSNER, G. *Privacy and the Internet of Things*. O´Reilly Media. October, 2016.

SARAIVA, D. A. F. *et al*. PRISEC: Comparison of Symmetric Key Algorithms for IoT Devices. Sensors 2019, Volume 19, Issue 19, 4312. doi:10.3390/s19194312

SERRANO, M.; HAUSWIRTH, M.; SOLDATOS, J. Design principles for utility-driven services and cloud-based computing modelling for the internet of things. *Int. J. Web Grid Serv*. 10(2–3),139–167 (2014).

SPIEKERMANN, S.; CRANOR, L. Engineering Privacy. Software Engineering, *IEEE Transactions* on 2009; 35(1):67 –82, doi:10.1109/TSE.2008.88.

TANENBAUM, A. S.; STEEN, M. V. *Distributed Systems: Principles and Paradigms*. Pearson, 2nd Edition, 2007.

TANK, B; UPADHYAY, H; PATEL, H. A Survey on IoT Privacy Issues and Mitigation Techniques. *ICTS*. March, 2016. Udaipur, India.

TAROUCO *et al.* Internet of Things in Healthcare: Interoperatibility and Security Issues. *IEEE International Conference on Communications (ICC)*. June, 2012.

TOGAN, M. T. et al. A Smart-phone Based Privacy-Preserving Security Framework for IoT Devices. *ECAI 2017 - International Conference*. Electronics, Computers and Artificial Intelligence. July, 2017.

WALTER, C. *et al.* Toward Predicting Secure Environments for Wearable Devices. *Proceedings of the 50th Hawaii International Conference on System Sciences***.** 2017.

WESTIN, A.F. *Privacy and Freedom*. New York, NY: Atheneum, 1967.

XU, L. D.; He, W; Li, S. Internet of Things in Industries: A Survey. *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, VOL. 10, NO. 4, NOVEMBER 2014.

YE, X.; HUANG, J. A framework for Cloud-based smart home, in: Computer Science and Network Technology *(ICCSNT)*, 2011 International Conference on. Vol. 2, December 2011, pp. 894–897.

YUN, M.; YUXIN, B. Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid, in: Advances in Energy Engineering (ICAEE), 2010 International Conference on, *IEEE*, 2010, pp. 69–72.

ZARKO, P. *et al. FP7 OpenIoT Project Workshop*, LNCS 9001, pp. 13–25, 2015.

ZIEGELDORF, J. H; MORCHON, O.G; WEHRLE, K. Privacy in the Internet of Things: Threats and Challenges. *Security and Communication Networks* 7.12 (2014): 2728-2742.

Apêndice A

QUESTIONÁRIO 1 APLICADO AOS USUÁRIOS

Características do participante

1. Idade

( ) < 20 anos ( ) 21 a 25 anos ( ) 26 a 30 anos ( ) 31 a 35 anos ( ) > 35 anos

2. Sexo

( ) Masculino ( ) Feminino

3. Área do curso

( ) Ciências exatas ( ) Ciências biológicas ( ) Ciências humanas

4. Como você se classifica quanto ao seu nível de preocupação com privacidade:

( ) Muito preocupado(a) ( ) Intermediário ( ) Despreocupado(a)

5. Eu gostaria que um mecanismo tomasse por mim decisões de privacidade em ambientes com uma grande quantidade de dispositivos capazes de coletar informações.

( ) Concordo totalmente ( ) Concordo ( ) Não concordo nem discordo

( ) Discordo ( ) Discordo totalmente

6. Me sentiria mais confortável em permitir o envio de determinadas informações coletadas por dispositivos sabendo que um mecanismo desenvolvido com base no conhecimento de profissionais de redes de computadores e segurança da informação realizará o tratamento das informações (anonimização ou encriptação dos dados) antes que elas sejam enviadas.

( ) Concordo totalmente ( ) Concordo ( ) Não concordo nem discordo

( ) Discordo ( ) Discordo totalmente

Preferências de privacidade

Agora com relação às suas preferências de privacidade responda se você permite ou nega o envio da informação de acordo com cada cenário IoT apresentado. Responda também como você se sentiria com a coleta de dados em cada cenário.

7. A empresa de segurança SEG+ quer acessar o sensor de presença de sua residência para definir a atitude a ser tomada com o disparo do seu alarme residencial. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

8. A empresa de segurança SEG+ quer acessar o sensor de presença de sua residência a fim de registrar em seu sistema os horários mais frequentes em que seus clientes estão casa. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

9. O novo sistema da polícia recebeu uma notificação de roubo próximo à sua residência e quer acessar as câmeras de vigilância de sua residência para verificar se você está com problemas. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

10. Uma empresa especialista em segurança residencial quer acessar as câmeras de vigilância de sua residência a fim de observar comportamentos e melhorar os produtos da empresa. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

11. O sistema da empresa de refrigeradores inteligentes recebeu uma notificação de mal funcionamento do seu refrigerador. A empresa quer acessar a localização do seu refrigerador inteligente a fim de mandar um técnico à sua casa para verificar o problema. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

12. O sistema "sugestões do dia" quer acessar a localização de seu refrigerador inteligente a fim de lhe enviar as promoções dos supermercados mais próximos. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável
( ) Desconfortável ( ) Muito desconfortável

13. A polícia recebeu uma denúncia de violência doméstica e quer acessar o microfone de sua smart TV para verificar se há algum indício de violência. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável
( ) Desconfortável ( ) Muito desconfortável

14. A empresa analytics quer acessar o microfone de sua Smart TV para coletar dados, processá-los, e verificar se há algo útil desse processamento para melhora de seus serviços. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável
( ) Desconfortável ( ) Muito desconfortável

15. A empresa de segurança cibernética CyberSec quer coletar as configurações de sua Smart TV para lhe enviar dicas sobre segurança. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável
( ) Desconfortável ( ) Muito desconfortável

16. A empresa de streaming de vídeos vídeo+ quer acessar o conteúdo recente de sua Smart TV a fim de alimentar a base de dados da empresa com os tipos de conteúdo mais assistidos pelos usuários. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

17. A empresa de corretagem de criptomoedas SmartCrypto gostaria de acessar seu nome e email salvos no seu smartphone para lhe enviar um link onde você pode se cadastrar e ganhar uma pequena quantidade de uma determinada cryptomoeda. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

18. A empresa BetterApp que comercializa aplicativos para smartphone quer acessar seu nome e email salvos no seu smartphone para lhe enviar o conjunto de aplicativos da empresa em promoção. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

19. A iluminação da cidade inteligente gostaria de coletar a informação do sensor de presença do local onde você está passando para ativar a iluminação do local. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

20. A biblioteca central gostaria de coletar a informação do sensor de presença da sala onde você está presente para estimar quão próximo do final

do expediente os usuários encerram seus estudos. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

21. O banco Master Bank quer coletar as imagens da câmera do caixa em que você está realizando uma transação bancária e fazer o reconhecimento facial a fim de adicionar um fator de segurança a mais para movimentação de grandes quantias de dinheiro. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

22. O banco Master Bank quer coletar as imagens da câmera por onde você está passando no banco e realizar o reconhecimento facial como parte do sistema de segurança do banco de tentar reconhecer criminosos procurados. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

23. A empresa de seguros Seu Seguro quer acesso à localização de seu veículo para aplicar um desconto automático na renovação de seu seguro. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

24. A empesa tráfego rápido quer acesso à localização do seu veículo para estimar as regiões de trânsito mais intenso e direcionar melhor os recursos para melhora da infraestrutura das vias. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

25. O banco Master Bank quer captar o áudio do microfone do caixa em que você está realizando uma transação para fazer o reconhecimento de voz como parte da política de segurança do banco em transações bancárias que envolvam grandes quantias de dinheiro. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

26. A empresa de monitoramento Monitora Tudo quer coletar o áudio da câmera instalada na rua em que você está passando a fim de aprimorar as ações de segurança pública da empresa. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

27. O restaurante Boa Refeição quer acessar os pedidos de refeições salvos em seu celular realizados em outros restaurantes para lhe sugerir uma promoção personalizada. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

28. O restaurante Boa Refeição quer acessar os pedidos de refeições salvos em seu celular realizados em outros restaurantes a fim de melhor reformular o seu cardápio. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

29. A Loja Tem de tudo quer acessar suas informações pessoais salvas em seu smartphone a fim de já realizar o seu cadastro na loja para agilizar uma possível compra. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

30. A Loja Tem de tudo quer acessar suas informações pessoais salvas em seu smartphone a fim de lhe enviar um cartão para parcelamento de compras na loja. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

Apêndice B

QUESTIONÁRIO 2 APLICADO AOS USUÁRIOS

Características do participante

1. Idade

( ) < 20 anos ( ) 21 a 25 anos ( ) 26 a 30 anos ( ) 31 a 35 anos ( ) > 35 anos

2. Sexo

( ) Masculino ( ) Feminino

3. Área do curso

( ) Ciências exatas ( ) Ciências biológicas ( ) Ciências humanas

4. Como você se classifica quanto ao seu nível de preocupação com privacidade:

( ) Muito preocupado(a) ( ) Intermediário ( ) Despreocupado(a)

5. Eu gostaria que um mecanismo tomasse por mim decisões de privacidade em ambientes com uma grande quantidade de dispositivos capazes de coletar informações.

( ) Concordo totalmente ( ) Concordo ( ) Não concordo nem discordo

( ) Discordo ( ) Discordo totalmente

6. Me sentiria mais confortável em permitir o envio de determinadas informações coletadas por dispositivos sabendo que um mecanismo desenvolvido com base no conhecimento de profissionais de redes de computadores e segurança da informação realizará o tratamento das informações (anonimização ou encriptação dos dados) antes que elas sejam enviadas.

( ) Concordo totalmente ( ) Concordo ( ) Não concordo nem discordo

( ) Discordo ( ) Discordo totalmente

Preferências de privacidade

Agora com relação às suas preferências de privacidade responda se você permite ou nega o envio da informação de acordo com cada cenário IoT apresentado. Responda também como você se sentiria com a coleta de dados em cada cenário.

7. A empresa de segurança SEG+ quer acessar o sensor de presença de sua residência para definir a atitude a ser tomada com o disparo do seu alarme residencial. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

8. A empresa de segurança SEG+ quer acessar o sensor de presença de sua residência a fim de registrar em seu sistema os horários mais frequentes em que seus clientes estão casa. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

9. O novo sistema da polícia recebeu uma notificação de roubo próximo à sua residência e quer acessar as câmeras de vigilância de sua residência para verificar se você está com problemas. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

10. Uma empresa especialista em segurança residencial quer acessar as câmeras de vigilância de sua residência a fim de observar comportamentos e melhorar os produtos da empresa. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

11. O sistema da empresa de refrigeradores inteligentes recebeu uma notificação de mal funcionamento do seu refrigerador. A empresa quer acessar a localização do seu refrigerador inteligente a fim de mandar um técnico à sua casa para verificar o problema. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

12. O sistema "sugestões do dia" quer acessar a localização de seu refrigerador inteligente a fim de lhe enviar as promoções dos supermercados mais próximos. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

13. A polícia recebeu uma denúncia de violência doméstica e quer acessar o microfone de sua smart TV para verificar se há algum indício de violência. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

14. A empresa analytics quer acessar o microfone de sua Smart TV para coletar dados, processá-los, e verificar se há algo útil desse processamento para melhora de seus serviços. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

15. A empresa de segurança cibernética CyberSec quer coletar as configurações de sua Smart TV para lhe enviar dicas sobre segurança. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

16. A empresa de streaming de vídeos vídeo+ quer acessar o conteúdo recente de sua Smart TV a fim de alimentar a base de dados da empresa com

os tipos de conteúdo mais assistidos pelos usuários. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

17. A empresa de corretagem de criptomoedas SmartCrypto gostaria de acessar seu nome e email salvos no seu smartphone para lhe enviar um link onde você pode se cadastrar e ganhar uma pequena quantidade de uma determinada cryptomoeda. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

18. A empresa BetterApp que comercializa aplicativos para smartphone quer acessar seu nome e email salvos no seu smartphone para lhe enviar o conjunto de aplicativos da empresa em promoção. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

19. A iluminação da cidade inteligente gostaria de coletar a informação do sensor de presença do local onde você está passando para ativar a iluminação do local. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

20. A biblioteca central gostaria de coletar a informação do sensor de presença da sala onde você está presente para estimar quão próximo do final do expediente os usuários encerram seus estudos. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

21. O banco Master Bank quer coletar as imagens da câmera do caixa em que você está realizando uma transação bancária e fazer o reconhecimento facial a fim de adicionar um fator de segurança a mais para movimentação de grandes quantias de dinheiro. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

22. O banco Master Bank quer coletar as imagens da câmera por onde você está passando no banco e realizar o reconhecimento facial como parte do sistema de segurança do banco de tentar reconhecer criminosos procurados. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

23. A empresa de seguros Seu Seguro quer acesso à localização de seu veículo para aplicar um desconto automático na renovação de seu seguro. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

24. A empesa tráfego rápido quer acesso à localização do seu veículo para estimar as regiões de trânsito mais intenso e direcionar melhor os recursos para melhora da infraestrutura das vias. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

25. O banco Master Bank quer captar o áudio do microfone do caixa em que você está realizando uma transação para fazer o reconhecimento de voz como parte da política de segurança do banco em transações bancárias que envolvam grandes quantias de dinheiro. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

26. A empresa de monitoramento Monitora Tudo quer coletar o áudio da câmera instalada na rua em que você está passando a fim de aprimorar as ações de segurança pública da empresa. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

27. O restaurante Boa Refeição quer acessar os pedidos de refeições salvos em seu celular realizados em outros restaurantes para lhe sugerir uma promoção personalizada. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

28. O restaurante Boa Refeição quer acessar os pedidos de refeições salvos em seu celular realizados em outros restaurantes a fim de melhor reformular o seu cardápio. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

29. A Loja Tem de tudo quer acessar suas informações pessoais salvas em seu smartphone a fim de já realizar o seu cadastro na loja para agilizar uma possível compra. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

30. A Loja Tem de tudo quer acessar suas informações pessoais salvas em seu smartphone a fim de lhe enviar um cartão para parcelamento de compras na loja. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

Apêndice C

QUESTIONÁRIO 3 APLICADO AOS USUÁRIOS

Características do participante

1. Idade

( ) < 20 anos ( ) 21 a 25 anos ( ) 26 a 30 anos ( ) 31 a 35 anos ( ) > 35 anos

2. Sexo

( ) Masculino ( ) Feminino

3. Área do curso

( ) Ciências exatas ( ) Ciências biológicas ( ) Ciências humanas

4. Como você se classifica quanto ao seu nível de preocupação com privacidade:

( ) Muito preocupado(a) ( ) Intermediário ( ) Despreocupado(a)

5. Eu gostaria que um mecanismo tomasse por mim decisões de privacidade em ambientes com uma grande quantidade de dispositivos capazes de coletar informações.

( ) Concordo totalmente ( ) Concordo ( ) Não concordo nem discordo

( ) Discordo ( ) Discordo totalmente

6. Me sentiria mais confortável em permitir o envio de determinadas informações coletadas por dispositivos sabendo que um mecanismo desenvolvido com base no conhecimento de profissionais de redes de computadores e segurança da informação realizará o tratamento das informações (anonimização ou encriptação dos dados) antes que elas sejam enviadas.

( ) Concordo totalmente ( ) Concordo ( ) Não concordo nem discordo

( ) Discordo ( ) Discordo totalmente

Preferências de privacidade

Agora com relação às suas preferências de privacidade responda se você permite ou nega o envio da informação de acordo com cada cenário IoT apresentado. Responda também como você se sentiria com a coleta de dados em cada cenário.

7. A empresa de segurança SEG+ quer acessar o sensor de presença de sua residência para definir a atitude a ser tomada com o disparo do seu alarme residencial. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

8. A empresa de segurança SEG+ quer acessar o sensor de presença de sua residência a fim de registrar em seu sistema os horários mais frequentes em que seus clientes estão casa. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

9. O novo sistema da polícia recebeu uma notificação de roubo próximo à sua residência e quer acessar as câmeras de vigilância de sua residência para verificar se você está com problemas. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

10. Uma empresa especialista em segurança residencial quer acessar as câmeras de vigilância de sua residência a fim de observar comportamentos e melhorar os produtos da empresa. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

11. O sistema da empresa de refrigeradores inteligentes recebeu uma notificação de mal funcionamento do seu refrigerador. A empresa quer acessar a localização do seu refrigerador inteligente a fim de mandar um técnico à sua casa para verificar o problema. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

12. O sistema "sugestões do dia" quer acessar a localização de seu refrigerador inteligente a fim de lhe enviar as promoções dos supermercados mais próximos. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

13. A polícia recebeu uma denúncia de violência doméstica e quer acessar o microfone de sua smart TV para verificar se há algum indício de violência. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

14. A empresa analytics quer acessar o microfone de sua Smart TV para coletar dados, processá-los, e verificar se há algo útil desse processamento para melhora de seus serviços. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

15. A empresa de segurança cibernética CyberSec quer coletar as configurações de sua Smart TV para lhe enviar dicas sobre segurança. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

16. A empresa de streaming de vídeos vídeo+ quer acessar o conteúdo recente de sua Smart TV a fim de alimentar a base de dados da empresa com os tipos de conteúdo mais assistidos pelos usuários. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

17. A empresa de corretagem de criptomoedas SmartCrypto gostaria de acessar seu nome e email salvos no seu smartphone para lhe enviar um link onde você pode se cadastrar e ganhar uma pequena quantidade de uma determinada cryptomoeda. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

18. A empresa BetterApp que comercializa aplicativos para smartphone quer acessar seu nome e email salvos no seu smartphone para lhe enviar o conjunto de aplicativos da empresa em promoção. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

19. A iluminação da cidade inteligente gostaria de coletar a informação do sensor de presença do local onde você está passando para ativar a iluminação do local. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

20. A biblioteca central gostaria de coletar a informação do sensor de presença da sala onde você está presente para estimar quão próximo do final do expediente os usuários encerram seus estudos. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

21. O banco Master Bank quer coletar as imagens da câmera do caixa em que você está realizando uma transação bancária e fazer o reconhecimento facial a fim de adicionar um fator de segurança a mais para movimentação de grandes quantias de dinheiro. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

22. O banco Master Bank quer coletar as imagens da câmera por onde você está passando no banco e realizar o reconhecimento facial como parte do sistema de segurança do banco de tentar reconhecer criminosos procurados. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

23. A empresa de seguros Seu Seguro quer acesso à localização de seu veículo para aplicar um desconto automático na renovação de seu seguro. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

24. A empesa tráfego rápido quer acesso à localização do seu veículo para estimar as regiões de trânsito mais intenso e direcionar melhor os recursos para melhora da infraestrutura das vias. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

25. O banco Master Bank quer captar o áudio do microfone do caixa em que você está realizando uma transação para fazer o reconhecimento de voz como parte da política de segurança do banco em transações bancárias que envolvam grandes quantias de dinheiro. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

26. A empresa de monitoramento Monitora Tudo quer coletar o áudio da câmera instalada na rua em que você está passando a fim de aprimorar as ações de segurança pública da empresa. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

27. O restaurante Boa Refeição quer acessar os pedidos de refeições salvos em seu celular realizados em outros restaurantes para lhe sugerir uma promoção personalizada. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

28. O restaurante Boa Refeição quer acessar os pedidos de refeições salvos em seu celular realizados em outros restaurantes a fim de melhor reformular o seu cardápio. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

29. A Loja Tem de tudo quer acessar suas informações pessoais salvas em seu smartphone a fim de já realizar o seu cadastro na loja para agilizar uma possível compra. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

30. A Loja Tem de tudo quer acessar suas informações pessoais salvas em seu smartphone a fim de lhe enviar um cartão para parcelamento de compras na loja. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

Apêndice D

QUESTIONÁRIO 4 APLICADO AOS USUÁRIOS

Características do participante

1. Idade

( ) < 20 anos ( ) 21 a 25 anos ( ) 26 a 30 anos ( ) 31 a 35 anos ( ) > 35 anos

2. Sexo

( ) Masculino ( ) Feminino

3. Área do curso

( ) Ciências exatas ( ) Ciências biológicas ( ) Ciências humanas

4. Como você se classifica quanto ao seu nível de preocupação com privacidade:

( ) Muito preocupado(a) ( ) Intermediário ( ) Despreocupado(a)

5. Eu gostaria que um mecanismo tomasse por mim decisões de privacidade em ambientes com uma grande quantidade de dispositivos capazes de coletar informações.

( ) Concordo totalmente ( ) Concordo ( ) Não concordo nem discordo

( ) Discordo ( ) Discordo totalmente

6. Me sentiria mais confortável em permitir o envio de determinadas informações coletadas por dispositivos sabendo que um mecanismo desenvolvido com base no conhecimento de profissionais de redes de computadores e segurança da informação realizará o tratamento das informações (anonimização ou encriptação dos dados) antes que elas sejam enviadas.

( ) Concordo totalmente ( ) Concordo ( ) Não concordo nem discordo

( ) Discordo ( ) Discordo totalmente

Preferências de privacidade

Agora com relação às suas preferências de privacidade responda se você permite ou nega o envio da informação de acordo com cada cenário IoT apresentado. Responda também como você se sentiria com a coleta de dados em cada cenário.

7. A empresa de segurança SEG+ quer acessar o sensor de presença de sua residência para definir a atitude a ser tomada com o disparo do seu alarme residencial. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

8. A empresa de segurança SEG+ quer acessar o sensor de presença de sua residência a fim de registrar em seu sistema os horários mais frequentes em que seus clientes estão casa. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

9. O novo sistema da polícia recebeu uma notificação de roubo próximo à sua residência e quer acessar as câmeras de vigilância de sua residência para verificar se você está com problemas. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

10. Uma empresa especialista em segurança residencial quer acessar as câmeras de vigilância de sua residência a fim de observar comportamentos e melhorar os produtos da empresa. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

11. O sistema da empresa de refrigeradores inteligentes recebeu uma notificação de mal funcionamento do seu refrigerador. A empresa quer acessar a localização do seu refrigerador inteligente a fim de mandar um técnico à sua casa para verificar o problema. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

12. O sistema "sugestões do dia" quer acessar a localização de seu refrigerador inteligente a fim de lhe enviar as promoções dos supermercados mais próximos. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

13. A polícia recebeu uma denúncia de violência doméstica e quer acessar o microfone de sua smart TV para verificar se há algum indício de violência. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

14. A empresa analytics quer acessar o microfone de sua Smart TV para coletar dados, processá-los, e verificar se há algo útil desse processamento para melhora de seus serviços. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

15. A empresa de segurança cibernética CyberSec quer coletar as configurações de sua Smart TV para lhe enviar dicas sobre segurança. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

16. A empresa de streaming de vídeos vídeo+ quer acessar o conteúdo recente de sua Smart TV a fim de alimentar a base de dados da empresa com

os tipos de conteúdo mais assistidos pelos usuários. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

17. A empresa de corretagem de criptomoedas SmartCrypto gostaria de acessar seu nome e email salvos no seu smartphone para lhe enviar um link onde você pode se cadastrar e ganhar uma pequena quantidade de uma determinada cryptomoeda. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

18. A empresa BetterApp que comercializa aplicativos para smartphone quer acessar seu nome e email salvos no seu smartphone para lhe enviar o conjunto de aplicativos da empresa em promoção. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

19. A iluminação da cidade inteligente gostaria de coletar a informação do sensor de presença do local onde você está passando para ativar a iluminação do local. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

20. A biblioteca central gostaria de coletar a informação do sensor de presença da sala onde você está presente para estimar quão próximo do final do expediente os usuários encerram seus estudos. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

21. O banco Master Bank quer coletar as imagens da câmera do caixa em que você está realizando uma transação bancária e fazer o reconhecimento facial a fim de adicionar um fator de segurança a mais para movimentação de grandes quantias de dinheiro. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

22. O banco Master Bank quer coletar as imagens da câmera por onde você está passando no banco e realizar o reconhecimento facial como parte do sistema de segurança do banco de tentar reconhecer criminosos procurados. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

23. A empresa de seguros Seu Seguro quer acesso à localização de seu veículo para aplicar um desconto automático na renovação de seu seguro. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

24. A empesa tráfego rápido quer acesso à localização do seu veículo para estimar as regiões de trânsito mais intenso e direcionar melhor os recursos para melhora da infraestrutura das vias. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

25. O banco Master Bank quer captar o áudio do microfone do caixa em que você está realizando uma transação para fazer o reconhecimento de voz como parte da política de segurança do banco em transações bancárias que envolvam grandes quantias de dinheiro. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

26. A empresa de monitoramento Monitora Tudo quer coletar o áudio da câmera instalada na rua em que você está passando a fim de aprimorar as ações de segurança pública da empresa. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

27. O restaurante Boa Refeição quer acessar os pedidos de refeições salvos em seu celular realizados em outros restaurantes para lhe sugerir uma promoção personalizada. Os dados serão compartilhados e esta informação será mantida para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

28. O restaurante Boa Refeição quer acessar os pedidos de refeições salvos em seu celular realizados em outros restaurantes a fim de melhor reformular o seu cardápio. Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

29. A Loja Tem de tudo quer acessar suas informações pessoais salvas em seu smartphone a fim de já realizar o seu cadastro na loja para agilizar uma possível compra. Os dados não serão compartilhados e serão armazenados para sempre.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

30. A Loja Tem de tudo quer acessar suas informações pessoais salvas em seu smartphone a fim de lhe enviar um cartão para parcelamento de compras na loja. Os dados serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Permitir ( ) Negar

Sentimento com relação a coleta de dados deste cenário:

( ) Muito confortável ( ) Confortável ( ) Nem confortável nem desconfortável

( ) Desconfortável ( ) Muito desconfortável

Apêndice E

QUESTIONÁRIO APLICADO AOS PROFISSIONAIS

Características do participante

1. Idade

( ) < 20 anos ( ) 21 a 25 anos ( ) 31 a 40 anos ( ) 41 a 45 anos ( ) > 50 anos

2. Sexo

( ) Masculino ( ) Feminino

3. Tempo de atuação na área de redes e/ou segurança da informação.

( ) < 5 anos ( ) 5 a 10 anos ( ) 11 a 15 anos ( ) 16 a 20 anos ( ) > 20 anos

4. Como você se classifica quanto ao seu nível de preocupação com privacidade:

( ) Muito preocupado(a) ( ) Intermediário ( ) Despreocupado(a)

Ações de privacidade

Agora, para cada cenário IoT apresentado, indique qual ação de privacidade seria mais adequada com o objetivo de preservar a privacidade do usuário com o mínimo de processamento computacional necessário.

6. A empresa de segurança SEG+ quer acessar o sensor de presença de sua residência para definir a atitude a ser tomada com o disparo do seu alarme residencial.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

7. A empresa de segurança SEG+ quer acessar o sensor de presença de sua residência a fim de registrar em seu sistema os horários mais frequentes em que seus clientes estão casa.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

8. O novo sistema da polícia recebeu uma notificação de roubo próximo à sua residência e quer acessar as câmeras de vigilância de sua residência para verificar se você está com problemas.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

9. Uma empresa especialista em segurança residencial quer acessar as câmeras de vigilância de sua residência a fim de observar comportamentos e melhorar os produtos da empresa.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

10. O sistema da empresa de refrigeradores inteligentes recebeu uma notificação de mal funcionamento do seu refrigerador. A empresa quer acessar a localização do seu refrigerador inteligente a fim de mandar um técnico à sua casa para verificar o problema.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

11. O sistema "sugestões do dia" quer acessar a localização de seu refrigerador inteligente a fim de lhe enviar as promoções dos supermercados mais próximos.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

12. A polícia recebeu uma denúncia de violência doméstica e quer acessar o microfone de sua smart TV para verificar se há algum indício de violência.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

13. A empresa analytics quer acessar o microfone de sua Smart TV para coletar dados, processá-los, e verificar se há algo útil desse processamento para melhora de seus serviços.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

14. A empresa de segurança cibernética CyberSec quer coletar as configurações de sua Smart TV para lhe enviar dicas sobre segurança.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

15. A empresa de streaming de vídeos vídeo+ quer acessar o conteúdo recente de sua Smart TV a fim de alimentar a base de dados da empresa com os tipos de conteúdo mais assistidos pelos usuários.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

16. A empresa de corretagem de criptomoedas SmartCrypto gostaria de acessar seu nome e email salvos no seu smartphone para lhe enviar um link onde você pode se cadastrar e ganhar uma pequena quantidade de uma determinada cryptomoeda.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

17. A empresa BetterApp que comercializa aplicativos para smartphone quer acessar seu nome e email salvos no seu smartphone para lhe enviar o conjunto de aplicativos da empresa em promoção.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

18. A iluminação da cidade inteligente gostaria de coletar a informação do sensor de presença do local onde você está passando para ativar a iluminação do local.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

19. A biblioteca central gostaria de coletar a informação do sensor de presença da sala onde você está presente para estimar quão próximo do final do expediente os usuários encerram seus estudos.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

20. O banco Master Bank quer coletar as imagens da câmera do caixa em que você está realizando uma transação bancária e fazer o reconhecimento facial a fim de adicionar um fator de segurança a mais para movimentação de grandes quantias de dinheiro.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

21. O banco Master Bank quer coletar as imagens da câmera por onde você está passando no banco e realizar o reconhecimento facial como parte do sistema de segurança do banco de tentar reconhecer criminosos procurados.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

22. A empresa de seguros Seu Seguro quer acesso à localização de seu veículo para aplicar um desconto automático na renovação de seu seguro.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

23. A empesa tráfego rápido quer acesso à localização do seu veículo para estimar as regiões de trânsito mais intenso e direcionar melhor os recursos para melhora da infraestrutura das vias.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

24. O banco Master Bank quer captar o áudio do microfone do caixa em que você está realizando uma transação para fazer o reconhecimento de voz como parte da política de segurança do banco em transações bancárias que envolvam grandes quantias de dinheiro.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

25. A empresa de monitoramento Monitora Tudo quer coletar o áudio da câmera instalada na rua em que você está passando a fim de aprimorar as ações de segurança pública da empresa.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

26. O restaurante Boa Refeição quer acessar os pedidos de refeições salvos em seu celular realizados em outros restaurantes para lhe sugerir uma promoção personalizada.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

27. O restaurante Boa Refeição quer acessar os pedidos de refeições salvos em seu celular realizados em outros restaurantes a fim de melhor reformular o seu cardápio.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

28. A Loja Tem de tudo quer acessar suas informações pessoais salvas em seu smartphone a fim de já realizar o seu cadastro na loja para agilizar uma possível compra.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

29. A Loja Tem de tudo quer acessar suas informações pessoais salvas em seu smartphone a fim de lhe enviar um cartão para parcelamento de compras na loja.

Os dados serão compartilhados e mantidos para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados serão compartilhados e armazenados até a satisfação de seu propósito

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados para sempre.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Os dados não serão compartilhados e serão armazenados até a satisfação de seu propósito.

( ) Nenhuma ação a ser realizada ( ) Notificar

( ) Anonimizar ( ) Encriptar

Apêndice F

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO APRESENTADO AOS USUÁRIOS

Termo de Consentimento Livre e Esclarecido

1. Você está sendo convidado para participar da pesquisa intitulada “Privacy Everywhere: mecanismo para tomada de decisão e garantia da privacidade em ambientes IoT”.
2. Você foi selecionado pela sua formação acadêmica e pelo fato de ser um entusiasta em novas tecnologias, no entanto sua participação não é obrigatória.
3. A qualquer momento você pode desistir de participar e retirar seu consentimento.
4. Sua recusa não trará nenhum prejuízo em sua relação com o pesquisador ou com a instituição onde esse estudo é aplicado.
5. O objetivo deste estudo é o desenvolvimento de um mecanismo que tome decisões de privacidade pelo usuário em ambientes com elevada interação e comunicação como são os ambientes de Internet of Things (IoT).
6. Sua participação nesta pesquisa consistirá em responder um questionário impresso onde, para cada cenário apresentado, deve-se responder se o envio da informação é permitido ou negado.
7. Esta pesquisa pode causar algum desconforto com relação ao tempo dedicado à leitura e interpretação do cenário apresentado, e também devido ao preenchimento do questionário. Faremos o possível para minimizar possíveis desconfortos.
8. A sua contribuição é voluntária e realizada de forma anônima, e tem o objetivo de auxiliar no desenvolvimento do mecanismo *Privacy Everywhere* para tomada de decisões e garantia da privacidade na integração entre dispositivos e nuvens IoT.
9. As informações obtidas por meio desta pesquisa serão confidencias e asseguramos o sigilo sobre sua participação.
10. Os dados não serão divulgados de forma a possibilitar sua identificação. As informações coletadas não estarão vinculadas à sua identidade.
11. Caso desejar, você poderá receber uma cópia deste termo onde consta o telefone e o endereço do pesquisador principal, podendo tirar suas dúvidas sobre o projeto e sua participação, agora ou a qualquer momento.

Leandro Prado de Andrade

Universidade Federal de São Carlos – Departamento de Computação Rodovia Washington Luis, km 235, Cep: 13565-905 São Carlos – SP Tel: (16) 3351-8626
Endereço e Telefone do Pesquisador R. Adelardo Franco de Carvalho, 204 - Centro 37130-125 – Alfenas – MG Tel: (35) 98875-2930

Declaro que entendi os objetivos, riscos e benefícios de minha participação na pesquisa e concordo em participar. O pesquisador me informou que o projeto foi aprovado pelo Comitê de Ética em Pesquisa com Seres Humanos da UFSCar que funciona na Pró-Reitoria de Pós- Graduação e Pesquisa da Universidade Federal de São Carlos, localizada na Rodovia Washington Luiz, Km. 235 - Caixa Postal 676 - CEP 13.565-905 - São Carlos - SP – Brasil. Fone

(16) 3351-8110. Endereço eletrônico: cephumanos@power.ufscar.br

Participante da Pesquisa

Apêndice G

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO APRESENTADO AOS PROFISSIONAIS

Termo de Consentimento Livre e Esclarecido

1. Você está sendo convidado para participar da pesquisa intitulada “Privacy Everywhere: mecanismo para tomada de decisão e garantia da privacidade em ambientes IoT”.
2. Você foi selecionado pela sua formação acadêmica e experiência profissional. Também foi selecionado pelo fato de se interessar por questões de tratamento da privacidade do usuário, no entanto sua participação não é obrigatória.
3. A qualquer momento você pode desistir de participar e retirar seu consentimento.
4. Sua recusa não trará nenhum prejuízo em sua relação com o pesquisador ou com a instituição onde esse estudo é aplicado.
5. O objetivo deste estudo é o desenvolvimento de um mecanismo que realize ações adequadas de privacidade em dados coletados em ambientes com elevada interação e comunicação como são os ambientes de Internet of Things (IoT).
6. Sua participação nesta pesquisa consistirá em responder um questionário online onde, para cada cenário apresentado, deve-se responder qual é a ação de privacidade adequada com um mínimo de custo computacional: não realizar nenhuma ação de privacidade, notificar o usuário, anonimizar os dados ou encriptar os dados.
7. Esta pesquisa pode causar algum desconforto com relação ao tempo dedicado à leitura e interpretação do cenário apresentado, e também devido ao preenchimento do questionário. Faremos o possível para minimizar possíveis desconfortos.
8. A sua contribuição é voluntária e realizada de forma anônima, e tem o objetivo de auxiliar no desenvolvimento do mecanismo *Privacy Everywhere* para tomada de decisões e garantia da privacidade na integração entre dispositivos e nuvens IoT.

9. As informações obtidas por meio desta pesquisa serão confidencias e asseguramos o sigilo sobre sua participação.
10. Os dados não serão divulgados de forma a possibilitar sua identificação. As informações coletadas não estarão vinculadas à sua identidade.
11. Aceitar participar da pesquisa e responder ao questionário online, corresponderá à assinatura do TCLE, o qual poderá ser impresso se assim o desejar.

Universidade Federal de São Carlos – Departamento de Computação Rodovia Washington Luis, km 235, Cep: 13565-905 São Carlos – SP Tel: (16) 3351-8626
Endereço e Telefone do Pesquisador R. Adelardo Franco de Carvalho, 204 - Centro 37130-125 – Alfenas – MG Tel: (35) 98875-2930

Declaro que entendi os objetivos, riscos e benefícios de minha participação na pesquisa e concordo em participar. O pesquisador me informou que o projeto foi aprovado pelo Comitê de Ética em Pesquisa com Seres Humanos da UFSCar que funciona na Pró-Reitoria de Pós- Graduação e Pesquisa da Universidade Federal de São Carlos, localizada na Rodovia Washington Luiz, Km. 235 - Caixa Postal 676 - CEP 13.565-905 - São Carlos - SP – Brasil. Fone

(16) 3351-8110. Endereço eletrônico: cephumanos@power.ufscar.br

_____

Participante da Pesquisa