UNIVERSIDADE FEDERAL DE SÃO CARLOS

CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

MECANISMO DE PRESERVAÇÃO DE PRIVACIDADE DO USUÁRIO EM AMBIENTES IOT

Fagner Roger Pereira Couto

Orientador: Prof. Dr. Sergio Donizetti Zorzo

São Carlos – SP

Agosto/2018

UNIVERSIDADE FEDERAL DE SÃO CARLOS

CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

MECANISMO DE PRESERVAÇÃO DE PRIVACIDADE DO USUÁRIO EM AMBIENTES IOT

Fagner Roger Pereira Couto

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/ Privacidade e Segurança.
Orientador: Prof. Dr. Sergio Donizetti Zorzo

São Carlos – SP

Agosto/2018

Dedico este trabalho aos meus pais, Maria Aparecida e José Adelcio pelo exemplo de vida.

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 Fagner Roger Pereira Couto, realizada em 28/08/2018:

Prof. Dr. Sergio Donizetti Zorzo
UFSCar

Prof. Dr. Fredy João Valente
UFSCar

Prof. Dr. Robson Eduardo de Grande
uOttawa

Certifico que a defesa realizou-se com a participação à distância do(s) membro(s) Robson Eduardo de Grande 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

"*Se cheguei até aqui foi porque me apoiei no ombro dos gigantes*".

Isaac Newton

Resumo

A Internet das Coisas (IoT) é considerada umas das tecnologias emergentes na área de tecnologia da informação. A utilização dessa tecnologia proporciona uma melhoria para a população fornecendo melhores sistemas de transportes, saúde e infraestrutura elétrica, dentre outras. No entanto, a coleta de informações nesses espaços podem trazer sérios prejuízos à privacidade do usuário, o que representa um dos desafios a serem superados pela IoT. Em alguns cenários, o usuário pode fornecer informações pessoais sem estar ciente dos riscos a sua privacidade. Primitivas criptográficas com um alto custo computacional são utilizadas para manter a privacidade dos usuários em ambientes IoT, mas não são aplicáveis a todos os dispositivos, devido à heterogeneidade dos mesmos. Neste contexto, esse trabalho propõe um mecanismo de preservação de privacidade que objetiva mediar as trocas de informações que ocorrem em ambientes IoT. Esta proposta foi fundamentada por uma pesquisa realizada junto a usuários que visou validar as características e funcionalidades de um mecanismo com esses objetivos. O mecanismo de preservação de privacidade foi desenvolvido como um aplicativo para fornecer uma facilidade na interação do usuário com os ambientes IoT. A validação do aplicativo foi realizado por um experimento com os usuários, onde foram submetidos a vários cenários IoT. Os resultados evidenciam que, com a utilização do mecanismo, os usuários sentem-se mais confortáveis com a disponibilização de seus dados nesses ambientes. O processo de aprendizagem de preferências de privacidade do aplicativo obteve um percentual de acerto de 88,62% nos cenários previstos, sendo considerado satisfatório para processos decisórios de disponibilização de informações pessoais.

Palavras-chave: Internet das Coisas; Privacidade; Preferências de Privacidade.

Abstract

The Internet of Things (IoT) is considered one of the emerging technologies in the area of information technology. The use of this technology provides an improvement to the population by providing better transportation systems, health and electrical infrastructure, among others. However, collecting information in these spaces can cause serious damage to the user's privacy, which is one of the challenges to be overcome by IoT. In some scenarios, the user may provide personal information without being aware of the risks to their privacy. Cryptographic primitives with a high computational cost are used to maintain the privacy of users in IoT environments, but they are not applicable to all devices due to their heterogeneity. In this context, this work proposes a mechanism of preservation of privacy that aims to mediate the information exchanges that occur in IoT environments. This proposal was based on a research done with users that aimed to validate the characteristics and functionalities of a mechanism with these objectives. The privacy preservation mechanism was developed as an application to provide ease in user interaction with IoT environments. The validation of the application was performed by an experiment with the users, where they were submitted to several IoT scenarios. The results show that, with the use of the mechanism, users feel more comfortable with the availability of their data in these environments. The learning process of application privacy preferences obtained a success rate of 88.62% in the predicted scenarios and is considered satisfactory for decision making procedures for the provision of personal information..

Keywords: Internet of Things; Privacy; Privacy Preferences.

Lista de Figuras

Lista de Tabelas

Sumário

Capítulo 1

Introdução

1.1 Contextualização

Chegar-se à condição de onipresença dos dispositivos computacionais é tido como um dos grandes desafios do século 21 (WEISER, 1999). No entanto, para atingir essa onipresença, todos os dispositivos e objetos deverão estar entrelaçados e conectados a uma rede sem fio. Atualmente, a conexão desses objetos está sendo referenciada como “Internet das Coisas” (*Internet of Things* - IoT).

As “Coisas”, de Internet das Coisas, não se referem somente a objetos físicos, inclui também entidades vivas ou representações virtuais (ORIWOH; CONRAD, 2015). Desta forma, qualquer “Coisa” que se conecta a uma rede sem fio e que tenha capacidade de transmitir dados, é considerada um dispositivo IoT (ROUSE, 2017).

As aplicações IoT são os serviços oferecidos pelos dispositivos IoT, sendo que suas integrações com as demais aplicações permitem a concepção de ambientes inteligentes (ALABA et al., 2017). Essas aplicações têm possibilitado uma mudança radical na forma como as pessoas se comunicam com o mundo, transformando os atuais espaços físicos em ambientes pervasivos, nos quais serviços e recursos podem ser acessados de forma ubíqua (HERNáNDEZ-RAMOS et al., 2015).

Com essas mudanças, inúmeros benefícios podem ser obtidos nessa sociedade que utiliza a Internet das Coisas, devido ao potencial ilimitado em melhorar a vida diária das pessoas (WEBER, 2015). Em virtudes das suas capacidades computacionais, os serviços oferecidos pela IoT podem ser implementados em residências inteligentes, aplicações de transporte, *smart metering, smart grid*, dentre outros. Em contrapartida, essas aplicações também trazem riscos à privacidade e segurança

dos usuários.

Em ambientes inteligentes, a coleta constante de informações pelos dispositivos IoT dificultam o controle dos usuários sobre os seus dados. Com essas dificuldades, os usuários ficam receosos em utilizar essas aplicações. Assim, para que os indivíduos percebam o real potencial da IoT, devem estar cientes da divulgação de suas informações (NAEINI et al., 2017).

Os métodos de preservação da privacidade usualmente oferecidos nesses ambientes utilizam primitivas criptográficas nas transações de informações. No entanto, essas soluções não são aplicadas a todas as transações, devido ao alto custo computacional dessas primitivas (MALINA et al., 2016). Todavia, os métodos criptográficos não permitem ao usuário gerenciar o controle de seus dados, uma vez que eles apenas garantem a confiabilidade do canal de comunicação. Com isso, para que os usuários obtenham confiança na divulgação de seus dados, novas abordagens são necessárias para garantir a sua privacidade.

1.2 Motivação

A preservação da privacidade de dados é um dos aspectos demandados para obtenção de confiança em aplicações IoT (YAN; ZHANG; VASILAKOS, 2014), uma vez que a sua violação pode causar danos catastróficos ao usuário. Mesmo com um baixo custo de energia, os dispositivos IoT podem coletar um grande volume de dados do usuário (GUO; TANG; ZHANG, 2017), que posteriormente são compartilhados com outros dispositivos ou pessoas. No entanto, essas coletas de informações podem afetar diretamente a privacidade dos usuários, pois seus dados ficam expostos para esses dispositivos.

A dificuldade em controlar os seus dados faz com que os usuários divulguem suas informações sem estar cientes de que essa divulgação pode implicar na perda da sua privacidade. Uma informação divulgada de forma errônea pode trazer sérios danos à imagem do indivíduo. Consequentemente, os usuários devem possuir meios de controlar a sua informação de acordo com as suas preferências, pois a sua privacidade é um direito básico e inalienável (GURSES; BERENDT; SANTEN, 2006).

Com base nessas dificuldades, o usuário precisa ter um mecanismo para ajudá-lo a controlar a divulgação de seus dados. Diante dessa necessidade, a motivação é desenvolver um mecanismo que faça a medição das trocas de informações que

ocorrem em ambientes IoT.

Dar ao usuário a capacidade de controlar a divulgação de seus dados possibilita a ele saber quem realmente está coletando as suas informações. Com esse controle, ele tem ciência de quais dados podem ser divulgados. Assim, o usuário toma sua decisão de divulgar seus dados com base em suas preferências de privacidade.

1.3 Objetivo da pesquisa

Este trabalho apresenta um mecanismo de preservação de privacidade do usuário em ambientes IoT. Este mecanismo visa mediar as trocas de informações entre o consumidor de dados (quem solicita informação) e o produtor de dados (quem divulga a informação). O objetivo desta mediação é possibilitar ao usuário (produtor de dados) a capacidade de gerenciar a divulgação de seus dados para preservar a sua privacidade.

1.4 Contribuições e Limitações

A principal contribuição deste trabalho é apresentar um mecanismo de preservação de privacidade em ambientes IoT, contribuindo com os seguintes pontos.

- Um estudo para analisar a opinião dos usuários sobre os recursos a serem disponibilizados pelo mecanismo de preservação da privacidade.
- Uma abordagem para o usuário negociar as informações que são trocadas nesses ambientes IoT;
- O desenvolvimento de um modelo de aprendizagem que visa prever as informações das preferências de privacidade do usuário;
- A capacidade do usuário de definir um nível de confiança nas respostas fornecidas pelo modelo de predição das informações; e,
- O desenvolvimento de uma aplicação móvel do mecanismo de preservação da privacidade do usuário para ambientes de IoT.

É importante ressaltar que este trabalho possui algumas limitações durante o seu desenvolvimento:

- Os cenários dos ambientes IoT que foram aplicados aos usuários eram fictícios.
- A Internet das Coisas não é totalmente parte de nossa realidade, já que os usuários utilizados em nossos experimentos não estavam totalmente submersos nos recursos oferecidos pela IoT.

1.5 Estrutura e Organização do Trabalho

Este capítulo apresentou uma contextualização na qual este trabalho se insere, as motivações para a sua feitura, os objetivos a serem alcançados e as suas limitações.

No Capítulo 2 apresenta-se um levantamento teórico com o intuito de fornecer os principais conceitos referentes à Internet das Coisas e à Privacidade. Nesse capítulo também são apresentados os trabalhos relacionados referente a este tema de pesquisa.

No Capítulo 3 apresenta-se uma pesquisa feita com os usuários para verificar as opções e funcionalidades a serem disponibilizadas pelo mecanismo de preservação de privacidade.

No Capítulo 4 apresentam-se os detalhes referentes ao desenvolvimento do mecanismo proposto. Inicialmente é apresentada uma visão geral de seu funcionamento e posteriormente são apresentados a sua arquitetura, implementação e desenvolvimento.

No Capítulo 5 são apresentados os resultados referentes aos experimentos feitos com os usuários utilizando o mecanismo desenvolvido.

Por fim, no Capítulo 6, apresentam-se as conclusões e trabalhos futuros desta dissertação.

Capítulo 2

Fundamentação Teórica

2.1 Considerações Iniciais

Este Capítulo objetiva apresentar uma base de conhecimento que subsidiará os resultados a serem atingidos com este trabalho de pesquisa.

A organização deste capítulo obedece ao seguinte formato: primeiramente na Seção 2.2 é apresentada a conceituação de Internet das Coisas, assim como suas características e evoluções. Na Seção 2.3 são abordadas as definições de privacidade, focando-se em como ela se relaciona com a Internet das Coisas. Por fim, na Seção 2.4 são apresentados os trabalhos relacionados ao tema de pesquisa e na Seção 2.5, as considerações finais elencam os trabalhos relacionados a esta pesquisa.

2.2 Internet das Coisas

A frase *“Internet of Things"* foi utilizada pela primeira vez em 1999, em uma conferência da empresa Procter & Gamble (P&G), com o intuito de explicar que as *“Things"* poderiam obter informações por meios próprios, sendo capazes de observarem e compreenderem o mundo sem a interferência humana (ASHTON, 2009).

Com o passar dos anos, surgiram várias interpretações para essa frase, na qual a palavra *“Things"* foi substituída por diferentes termos dando origem a “*Internet of* α"(ORIWOH; CONRAD, 2015). Exemplos dessas variações são: *Internet of Everything* (IoE) (BUJARI; PALAZZI, 2014; ETZION; FOURNIER; ARCUSHIN, 2014), *Internet of Anything* (BOJANOVA; HURLBURT; VOAS, 2014), *Internet of People* (KERR, 2013),

Internet of Signs (O'LEARY, 2013), dentre outros.

Com essas variações, definir a *"Internet of Things"* não é uma tarefa trivial, devido não haver uma única e universal definição (ROSE; ELDRIDGE; CHAPIN, 2015). Entretanto, a Comissão Europeia considera a IoT como uma rede mundial de objetos inteligentes exclusivamente endereçáveis, baseados em protocolo de comunicação padrão (COMMISSION, 2008). Já segundo Perera et al. (2014), a IoT permite que as pessoas e as coisas sejam conectadas a qualquer momento, em qualquer lugar, com qualquer coisa e com qualquer um, independentemente do meio de comunicação e serviço, como ilustrado pela representação da Figura 2.1.

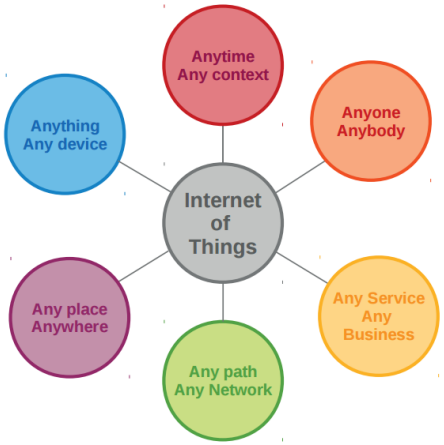


Figura 2.1: Definição da Internet das Coisas (PERERA et al., 2014).

No entanto, as definições apresentadas não necessariamente discordam, mas enfatizam os diferentes aspectos da IoT a partir de diferentes pontos de vista (TAN; WANG, 2010).

Neste trabalho será utilizada a definição proposta por Perera et al. (2014), na qual considera que a IoT permite que as pessoas e as coisas sejam conectadas a qualquer momento, em qualquer lugar, com qualquer coisa e com qualquer um, independentemente do meio de comunicação e serviço.

2.2.1 Evolução

A visão de Mark Weiser[1] criador do conceito da computação ubíqua teve um enorme impacto nos projetos de pesquisas, inspirando governos, pesquisadores e desenvolvedores do mundo todo a investigar sobre como os computadores se in-

[1] Mark Weiser é considerado o pai da computação ubíqua (ROGERS, 2006)

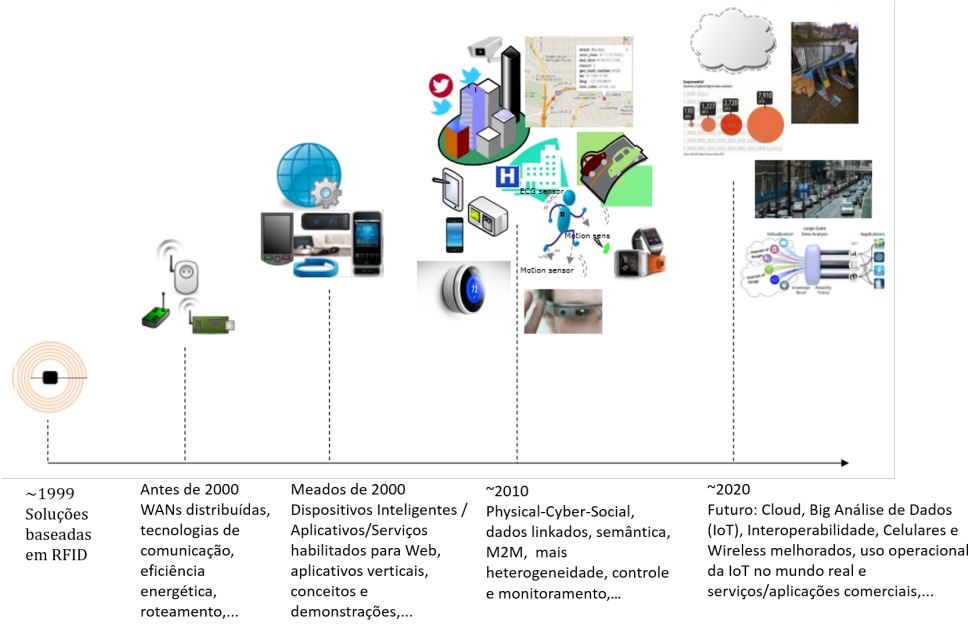


Figura 2.2: História da Internet das Coisas adaptado de (BARNAGHI; SHETH, 2014).

tegrariam na vida atual, de forma que se saberia tudo o que está acontecendo ao redor (ROGERS, 2006).

No entanto, para concretizar essa visão é necessário um conjunto de aplicações e serviços para alavancar tais tecnologias, abrindo novas oportunidades de negócios (MIORANDI et al., 2012). Neste contexto, surge a Internet das Coisas, que traz aos usuários uma perspectiva visível em áreas como automação residencial, transporte inteligente, manufatura industrial e tomada de decisões (ATZORI; IERA; MORABITO, 2010).

A IoT se tornou muito importante desde a sua concepção, sendo considerada a primeira evolução real da *Internet* (KARKOUCH et al., 2015), transformando-a em algo sensorial (temperatura, pressão, vibração, iluminação e estresse) permitindo assim ser mais proativa do que reativa (EVANS, 2011).

Conforme apresentado na Figura 2.2, a tecnologia RFID (*Radio-Frequency Identification*) desencadeou o surgimento da IoT, que era considerado um pré-requisito para que esta acontecesse. Os desenvolvedores acreditavam que se todos os dispositivos fossem "marcados" os computadores poderiam gerenciá-los (FOOTE, 2016). Posteriormente, as redes WSANs (*Wireless Sensor and Actor Networks*) e dispositivos inteligentes proporcionaram que as aplicações IoT se disseminassem no âmbito comercial.

2.2.2 Características

A Internet das Coisas possui diversas características que podem ser classificadas como sendo de aplicações e de infraestrutura (RAZZAQUE et al., 2016). As características de infraestrutura são apresentadas detalhadamente e ilustradas na Figura 2.3.

Figura 2.3: Características de infraestrutura IoT adaptado de (RAZZAQUE et al., 2016).

- **Dispositivos Heterogêneos**: a IoT não é composta somente por sensores e atuadores (GARCíA et al., 2017). Ela também necessita de dispositivos que executam tarefas com um alto custo computacional, tais como processamento de dados, comutação e roteamento. Consequentemente, devido às diferenças nas capacidades dos dispositivos surge a heterogeneidade dos dispositivos;

- **Recursos Limitados**: o tamanho dos dispositivos IoT influencia em suas capacidades de processamento. Quanto menor é o dispositivo mais limitado ele tende a ser (MINERVA; BIRU; ROTONDI, 2015). Um exemplo de dispositivo com recurso limitado é o RFID. Os dispositivos podem não possuir nenhum tipo de capacidade de processamento, mas suas informações podem ser de grande valia para a aplicação IoT;

- **Interações Espontâneas**: com a movimentação dos dispositivos IoT, as infraestruturas devem prover a capacidade de interação espontânea com outros dispositivos e com o mínimo de interferência humana possível. Por exemplo, quando um usuário de *smartphone* se aproxima de um outro objeto IoT, eles espontaneamente podem trocar informações entre si;

- **Redes de grande escala e grande números de eventos**: em um ecossistema IoT, milhares de dispositivos trocaram informações entre si gerando um enorme número de eventos. Em larga escala essa troca de evento pode causar sérios problemas de infraestrutura, como, por exemplo, um congestionamento

de eventos. Esse congestionamento pode reduzir a capacidade de processamento do cenário, afetando assim as interações das aplicações;

- **Inteligência**: os dispositivos inteligentes e sistemas inteligentes são considerados os elementos chave de IoT, pois são interoperáveis e capazes de atuar de forma independente com base nas circunstâncias ou ambientes;
- **Distribuída**: assim como a Internet, a IoT também é uma rede global distribuída (COMMISSION, 2008). No entanto, essa rede pode ser distribuída em diferentes escalas, ou seja, globalmente como a internet ou localmente dentro da sua área de aplicação.

Apesar das características levantadas, ainda não se sabe como a infraestrutura IoT suportará toda essa heterogeneidade de dispositivos, pois o gerenciamento de IoT é um processo muito complexo (ANTUNES et al., 2016).

As características das aplicações IoT são ilustradas na Figura 2.4 e detalhadas a seguir:

Figura 2.4: Características das Aplicações IoT adaptado de (RAZZAQUE et al., 2016).

- **Diversas Aplicações**: a IoT possui diversos tipos de aplicações que podem ser agrupadas em domínios diferentes, tais como transporte e logística, *Healthcare*, ambientes inteligentes, dentre outros. Essas aplicações podem possuir arquiteturas e requisitos diferentes. No entanto, a maioria dos serviços de IoT que compõem esses domínios estão conectados à *Internet*;
- **Em Tempo Real**: nem todos os aplicativos IoT devem operar necessariamente em tempo real. No entanto, algumas aplicações IoT para agregar valor ao seu serviço devem operar dessa forma. Por exemplo, os serviços de cuidado de saúde (*Healthcare*) necessitam ter respostas rápidas aos eventos, pois uma informação entregue de forma tardia pode levar a complicações na saúde do paciente;
- **Tudo como um Serviço**: com o crescimento da utilização de objetos IoT, o modelo de tudo como um serviço (*Everything as a Service* - XaaS) proporciona eficiência, escalabilidade e reutilização dos serviços existentes;

- **Segurança**: as interações espontâneas na IoT podem levar a complicações na segurança das aplicações. Devido à conectividade global, a implantação de mecanismo de segurança eficiente, interoperáveis e escaláveis é um desafio presente na IoT;

- **Privacidade**: com a constante coleta de informação dos dispositivos IoT, muitos indivíduos temem que essas informações possam afetar a sua privacidade. Consequentemente, qualquer aplicação que não esteja em conformidade com suas preferências de privacidade pode lhes causar algum tipo de dano.

Essas características realçam a diversidade dos domínios existentes nas aplicações IoT e apresentam alguns aspectos essenciais nesses respectivos domínios.

2.3 Privacidade

Em um ambiente IoT é essencial manter a privacidade do usuário, devido à onipresença dos objetos inteligentes e aos riscos do que esses dados podem causar, caso não sejam manipulados por usuários legítimos (SFAR et al., 2017).

O compartilhamento de informações pessoais pode levar à violação de privacidade, pois no momento em que a pessoa compartilha uma informação pessoal, ela já não tem privacidade em relação a esses dados. Quanto mais informações pessoais forem divulgadas, menos controle e privacidade terá em relação a esses dados (GHANI; SIDEK, 2008).

2.3.1 Conceitos

A definição de privacidade foi evoluindo com o passar dos anos. Em 1890 Warren e Brandeis (1890) definiram que a privacidade era um direito de ser deixado sozinho, mas com o passar dos anos e à medida que a tecnologia evoluiu, essa definição também foi sofrendo algumas alterações. Em 1967, Westin (1967) definiu que a privacidade era o direito de o indivíduo, grupos ou instituições de determinar para si mesmo quando, como e quais informações sobre eles, serão divulgadas para os outros.

Já Clarke (1999) define que a privacidade é o interesse que o indivíduo tem em manter um espaço pessoal, livre de interferência de outras pessoas e organizações.

Além do mais, afirma que a privacidade possui várias outras dimensões sendo elas:

- **Privacidade pessoal ou privacidade corporal**: refere-se à privacidade do corpo do indivíduo. Procedimentos como transfusão de sangue, amostra de fluido corporal e tecidos, não devem ser feitos sem o seu consentimento;
- **Privacidade do comportamento pessoal**: todos os aspectos de comportamento estão relacionados a esse tipo de privacidade, dentre eles seus hábitos, atividades políticas e práticas religiosas;
- **Privacidade das comunicações pessoais**: as pessoas querem se comunicar entre si, sem ser monitoradas por outras pessoas ou organizações;
- **Privacidade dos dados pessoais**: mesmo que as pessoas compartilhem um dado pessoal com outra pessoa ou organização, elas querem ser capazes de exercer o controle substancial desses dados.

No entanto, apesar das várias dimensões de privacidade apresentadas por Clarke (1999), a definição de privacidade adotada para este trabalho será a definida por Westin (1967), consistindo no direito do indivíduo, grupos ou instituições de determinar para si mesmo quando, como e quais informações sobre eles serão divulgadas para os outros.

2.3.2 Privacidade na Internet das Coisas

Para garantir o atendimento à demanda de preservação da privacidade dos dados em dispositivos IoT, muitos autores se utilizam de mecanismos criptográficos. No entanto, soluções que envolvem criptografia podem não ser adequadas para todos os tipos de dispositivos.

Visando verificar o custo computacional das técnicas de preservação usualmente utilizadas, Malina et al. (2016) fizeram uma comparação do custo computacional para a utilização das técnicas que visam à preservação de privacidade, sendo que os resultados dos testes efetuados são apresentados na Figura 2.5

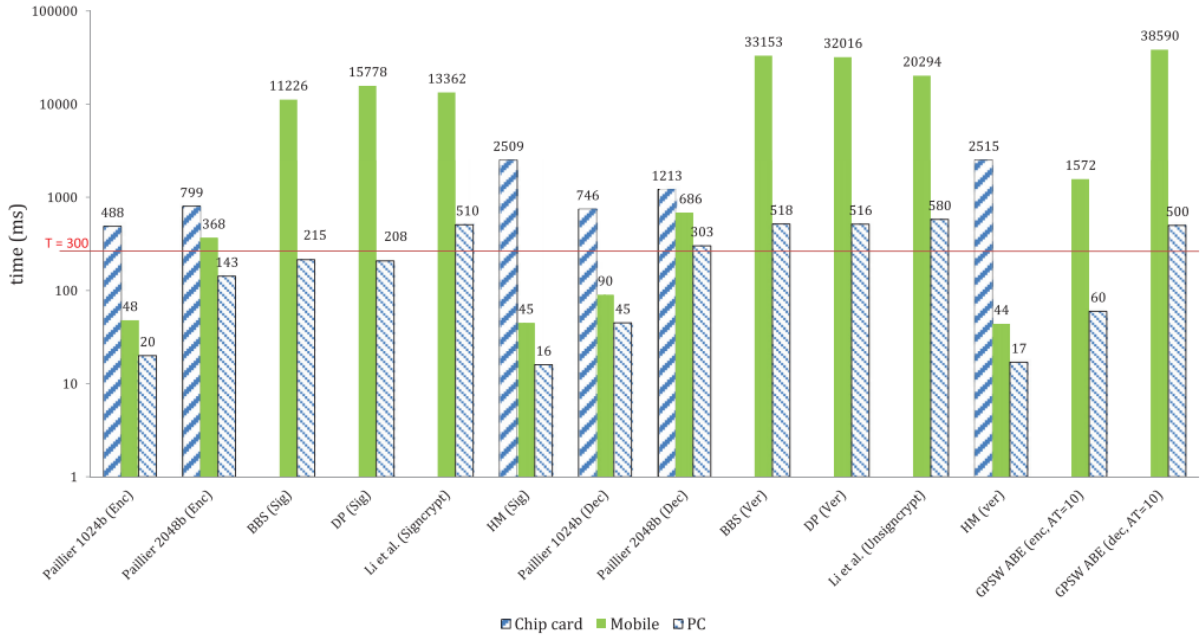


Figura 2.5: Tempos de execução das técnicas de preservação da privacidade nos dispositivos (MALINA et al., 2016).

As técnicas de preservação de privacidade utilizadas na avaliação de Malina et al. (2016), foram os esquemas de criptografia homomórfica de Paillier (PAILLIER, 1999), esquema de assinatura do grupo BBS (BONEH; BOYEN; SHACHAM, 2004), esquema de assinatura de grupo DP (DELERABLÉE; POINTCHEVAL, 2006), esquema de assinatura do anel (LI; ZHENG; JIN, 2016), esquema de assinatura baseada em atributos HM (HAJNY JANAND MALINA, 2013) e o esquema de criptografia baseada em atributos (GPSW) (GOYAL et al., 2006).

Nesta comparação foram utilizados três tipos de dispositivos IoT: um *chip card* com recursos limitados, um dispositivo com desempenho médio (*mobile* com Android 4.2) e um dispositivo de alto desempenho (Computador pessoal com *Windows* 7).

Nesta análise, os autores definiram um limiar de tempo de 300 ms (milissegundos) como o máximo de latência permitido nas operações criptográficas. A partir dessas premissas, concluíram que em muitos dispositivos IoT, as técnicas de preservação não se aplicam, pois esses métodos necessitam de um mínimo de poder de processamento.

Dispositivos com recursos limitados possuem pouca memória RAM (*Random Access Memory*) e, consequentemente, apresentam dificuldades em efetuar operações como emparelhamento bilineares e exponenciação modular, devido a essas

operações exigirem grande consumo de memória.

2.4 Trabalhos Relacionados

Como o aumento da conscientização das pessoas em manter a privacidade de seus dados, alguns autores propuseram na literatura mecanismos para assegurar que as suas privacidades não viessem a ser violadas.

Ukil et al. (2012) propuseram uma solução de privacidade na qual é feita uma negociação entre o consumidor de dados e o produtor de dados. O objetivo dessa negociação é que ambos entrem em acordo em como e quais dados serão divulgados.

Nesta abordagem, as preferências de privacidade do produtor de dados são armazenadas em uma matriz de negociação, formada por um conjunto sensível de informação e pelo consumidor de dados. Dependendo do resultado da negociação, é feita uma atualização na matriz de negociação. Após esse processo, o módulo de negociação cria uma regra de preservação de privacidade que é utilizada para reforçar a privacidade da plataforma IoT. Para impor a privacidade nos dados sensíveis, os autores propõem utilizar uma solução de mascaramento dinâmico denominada *SafeMask*.

Esse mascaramento é um processo de remoção ou modificação sistemática das informações sensíveis. Em seu processo, o *SafeMask* utiliza diferentes técnicas de preservação de privacidade, tais como: mascaramento hierárquico, quantização, perturbação e randomização. O modelo de negociação proposto pelos autores atua como uma plataforma de negociação para que as partes interessadas entrem em consenso sobre a divulgação dos dados.

A solução proposta por Ukil et al. (2012), sempre que um novo consumidor de dados solicitar uma informação e não tiver nenhuma regra de preservação relacionada a esses dados, a plataforma entra em contato com o produtor para verificar qual a sua decisão em relação a eles

Ortmann, Langendörfer e Maaser (2007) propuseram uma arquitetura de gerenciamento de privacidade fornecendo ao usuário uma forma de controle sobre os diversos dispositivos do ambiente. O objetivo desta arquitetura é gerenciar uma infinidade de sensores como se fossem um único dispositivo. Para satisfazer as

demandas de privacidade, o usuário pode dividir esses sensores em vários outros conjuntos de sensores, para permitir uma configuração flexível das exigências de privacidade dos usuários.

Essa arquitetura é estruturada em três camadas: *real sensor network, virtual sensor layer e Management layer*. *Management layer* é responsável por verificar se os requisitos de privacidade podem ser satisfeitos, dadas as configurações de usuário já aceitas.

Nesta abordagem o primeiro a chegar é o primeiro a ser servido, e três cenários devem ser considerados: *clear accept, conditional accept e clear reject*. *Virtual sensor layer* é o núcleo da arquitetura e tem acesso a todos os usuários registrados. Consequentemente, ele é responsável por fazer a leitura dos sensores corretamente e gerenciar todos os pedidos de assinatura. Além do mais, trata de todos os eventos relacionados ao usuário.

Pallapa, Kumar e Das (2007) propuseram uma entidade denominada *privon* para encapsular as informações relacionadas aos níveis de sensibilidade à privacidade. O objetivo do *privon* é permitir que os usuários entendam como suas informações pessoais podem ser usadas pelos outros e como eles e suas informações participam do sistema. Quando um utilizador estabelece uma sessão, o nível de privacidade ou coeficiente de privacidade é classificado com base nas políticas de privacidade do usuário.

As políticas de privacidade são previamente armazenadas em *cache* de diretivas do usuário. Após definido o nível de privacidade, o CIMU (*Context Information Management Unit*) extrai os elementos de contexto e os repassa para o *privon proxy*. O *privon proxy* acessa as políticas de privacidade da sessão por meio do monitor de privacidade e modifica os elementos repassados pelo CIMU. Os elementos modificados são separados em diferentes classes de dados e o gerador de *privon* gera um novo *privon*, que é armazenado no cache *privon* e enviado para o destinatário.

Com a utilização do *privon* o usuário pode definir um nível de privacidade para toda sessão e, dependendo deste nível, a natureza da informação é alterada. O usuário também pode visualizar os dados de forma transparente, protegida e privada. Caso considere necessário pode fazer modificações, podendo visualizar os dados armazenados em contexto sociais, pessoais e profissionais.

O trabalho de Schaub et al. (2012), verifica como a mudança de contexto pode

afetar a privacidade do usuário, com o intuito de buscar um modelo de contexto de privacidade genérico para poder decidir dinamicamente como os mecanismos de privacidade se adaptarão em cenários arbitrários.

O modelo proposto utiliza um grafo direcionado para representar a mudança de contexto, a fim de simplificar as implicações de privacidade. Com base nessa representação, as alterações se resumem a apenas dois tipos de operação ADD (Adicionar) e REMOVE (Remover). A operação ADD adiciona de forma granulada a fonte de informação e a operação REMOVE retira itens sensíveis à privacidade.

Em sua análise, os autores identificaram que à medida que os itens sensíveis às privacidades foram expostos, a operação ADD teve um impacto negativo na privacidade. Por outro lado, a operação REMOVE teve um impacto positivo quando menos itens sensíveis foram expostos.

Schaub et al. (2012) concluíram que o modelo proposto tem o potencial de reduzir a complexidade dos sistemas de privacidade adaptativos, sendo capazes de suportar a reconfiguração autônoma de mecanismos de privacidade e apoiar os usuários em decisões de privacidade.

Em ambientes IoT, as mudanças de contexto podem afetar significativamente a privacidade do usuário. Por exemplo: o usuário pode querer divulgar as suas informações vitais para as pessoas ao seu redor, mas pode desejar fazê-lo somente em caso de emergência. Nesse sentido, a mudança de contexto afeta a sua preferência de privacidade.

Copigneaux (2015) apresenta em seu trabalho uma abordagem para garantir o "consentimento informado" do usuário, com o objetivo de aumentar o controle e o entendimento do usuário sobre como são usados os seus dados, minimizando assim o número de operações feitas pelo usuário.

A proposta do autor é um sistema de *"privacy butler"* construído sobre uma plataforma denominada *BUTLER*. Esta plataforma utiliza uma interface gráfica que permite ao usuário definir um conjunto de regras, que posteriormente são usadas para tomada de decisão do sistema. O *privacy butler* é um agente semiautônomo capaz de autorizar ou negar operações de dados em nome do usuário. Esta proposta utiliza um sistema de reputação, no qual o usuário pode avaliar e classificar as aplicações IoT.

Copigneaux (2015) acredita que essa abordagem pode melhorar a forma de

como é tratada a questão de consentimento informado em ambientes IoT, devido ao controle detalhado fornecido ao usuário e também ao sistema de reputação baseado em comunidade que simplifica ainda mais a tarefa do utilizador final.

2.5 Considerações Finais

Este Capítulo apresentou um referencial teórico dos conceitos de Internet das Coisas e Privacidade, assim como os trabalhos relacionados a esta dissertação de mestrado. A partir desses trabalhos apresentados, o mecanismo proposto buscou absorver as características de cada abordagem para construir um modelo de preservação de privacidade eficiente e que satisfaça as necessidades dos usuários.

A Tabela 2.1 apresenta uma compilação de cada trabalho e as características que foram levadas em conta para desenvolver o mecanismo de preservação de privacidade.

Tabela 2.1: Compilação dos trabalhos relacionados

Autores	Descrição	Contribuição com o mecanismo
Ortmann, Langendörfer e Maaser (2007)	Este trabalho fornece a capacidade de controlar diversos sensores como se fosse um único dispositivo.	Esta visão proporcionou desenvolver um mecanismo capaz de controlar a divulgação de diversas informações sendo gerenciado por uma única aplicação.
Pallapa, Kumar e Das (2007)	Esse trabalho apresentou uma entidade capaz de encapsular as informações relacionada aos níveis de sensibilidade à privacidade.	O nível de privacidade incorporado pela entidade foi utilizado como um parâmetro pelo mecanismo.
Ukil et al. (2012)	Propôs uma solução de negociação nas trocas de informações entre o consumidor e produtor de dados.	Um processo de negociação de dados também foi utilizado no mecanismo.
Schaub et al. (2012)	Este trabalho propôs um modelo de contexto genérico para verificar as implicações de privacidade em cenários arbitrários.	A mudança de contexto no mecanismo não foi aplicada neste trabalho mas será considerada para trabalhos futuros.

Copigneaux (2015)	Este trabalho apresentou uma abordagem para garantir o consentimento informado do usuário.	O mecanismo proposto ao fornecer a capacidade de gerenciar a divulgação dos dados, possibilita ao usuário controlar as suas informações.

Essas características e visões levantadas pela revisão do estado da arte permitiram modelar o mecanismo agregando várias funcionalidades importantes. Tais combinações de abordagens proporcionam ao usuário um melhor entendimento sobre a divulgação de seus dados e fornecem a ele um meio de preservar a sua privacidade.

Capítulo 3

Levantamento das características do mecanismo

3.1 Considerações Iniciais

Este capítulo descreve uma pesquisa feita junto aos usuários para ser utilizado como apoio para o desenvolvimento do mecanismo de preservação de privacidade. A organização deste capítulo segue da seguinte forma: na Seção 3.2 são apresentados os objetivos e os resultados obtidos nesse levantamento e na Seção 3.3 são apresentadas as considerações finais.

3.2 Objetivos e Resultados da Pesquisa

Nesta pesquisa objetivou-se fazer um levantamento para analisar a opinião dos usuários referente às funcionalidades a serem disponibilizadas pelo mecanismo de preservação de privacidade em ambiente IoT. Esse levantamento foi feito por meio de um questionário do *google forms* que foi aplicado aos alunos do curso da Pós-graduação em Ciência da Computação da Universidade Federal de São Carlos. Dos pontos abordados pelo questionário, os principais focos foram:

- Verificar o que influenciaria os usuários a disponibilizar mais informações pessoais;
- Verificar se as variáveis influentes iriam ser suficientes na tomada de decisão do usuário;

- Verificar se as divulgações de informações anônimas influenciariam ou não no processo de decisão do usuário. Verificar também se os métodos apresentados deixariam os usuários confortáveis nas divulgações das suas informações.

As questões apresentadas ao usuário no questionário podem ser visualizadas no Apêndice A. Um total de 68 alunos respondeu a esses questionários. Essa amostra representa um total de 39,5% da população escolhida. Embora esta amostra constitua um pequeno grupo de participantes, os resultados são representativos, pois de acordo com a Teoria do Limite Central (FISCHER, 2011), uma amostragem com mais de 30 elementos pode representar toda a população.

As primeiras perguntas do questionários remetem ao perfil do usuário. A Tabela 3.1 apresenta a distribuição demográfica desses alunos. Pode-se observar que a maioria dos alunos é de homens brasileiros com a faixa etária entre 21 a 29 anos de idade e eles se consideram experientes na utilização da internet.

Tabela 3.1: Dados demográficos da amostra.

Nacionalidade	**Participantes**	**(%)**		**Sexo**	**Participantes**	**(%)**
Brasileiros	64	94,1%		Feminino	15	22,1%
Outros	4	5,9%		Masculino	53	77,9%
Idade				**Nível em relação ao uso da Internet em**		
18 a 20 anos	8	11,8%		Especialista	20	29,4%
21 a 29 anos	41	60,3%		Experiente	39	57,4%
30 a 39 anos	13	19,1%		Intermediário	9	13,2%
40 a 49 anos	4	5,9%		Amador	0	0%
50 a 59 anos	2	2,9%		Iniciante	0	0%

A Figura 3.1 refere-se à opinião do usuário sobre a divulgação das suas informações pessoais. O intuito da pergunta foi verificar se as tomadas de decisões para divulgar uma informação são pensadas e não simplesmente divulgadas por impulso. Constata-se que, dentre as respostas dadas 23,5% dos usuários concordaram fortemente, 48,5% dos usuários concordaram, ou seja, os usuários costumam pensar mais de uma vez para divulgar uma informação pessoal. Um percentual de 17,6% não teve opinião sobre essa pergunta. Os outros 4,4% discordaram fortemente e 5,9% somente discordaram. De modo geral, pode-se perceber que os usuários estão preocupados com a divulgação de seus dados pessoais e consequentemente tomam suas decisões conscientemente.

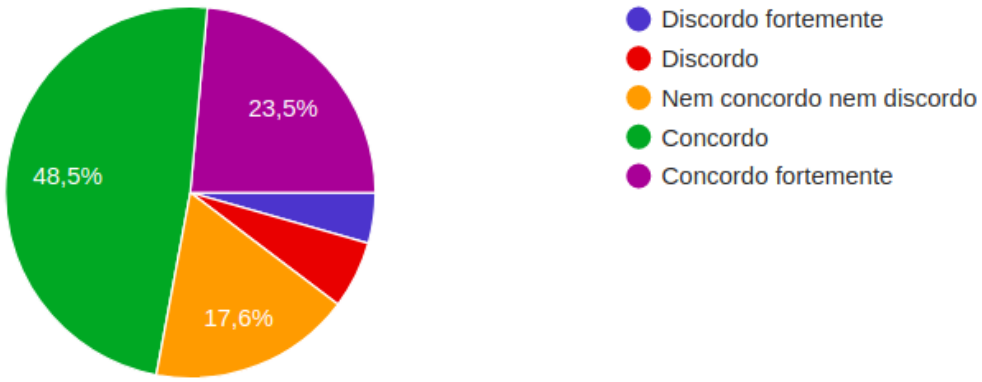


Figura 3.1: Quando algum dispositivo IoT me solicita informações pessoais, costumo pensar duas vezes em fornecer isso.

A Figura 3.2 refere-se à pergunta 7b do questionário que trata das informações pessoais do usuário. Perguntou-se aos usuários se eles acham que os sites ou dispositivos lidam com as suas informações pessoais de forma correta e confidencial. Dentre os participantes, 25% discordaram fortemente e 36,8% discordaram, evidenciando que eles não acreditam que suas informações estão sendo tratadas de forma correta e confidencial. Um total de 26,5% não soube opinar, 10,5% concordaram e 1,5% concordaram fortemente.

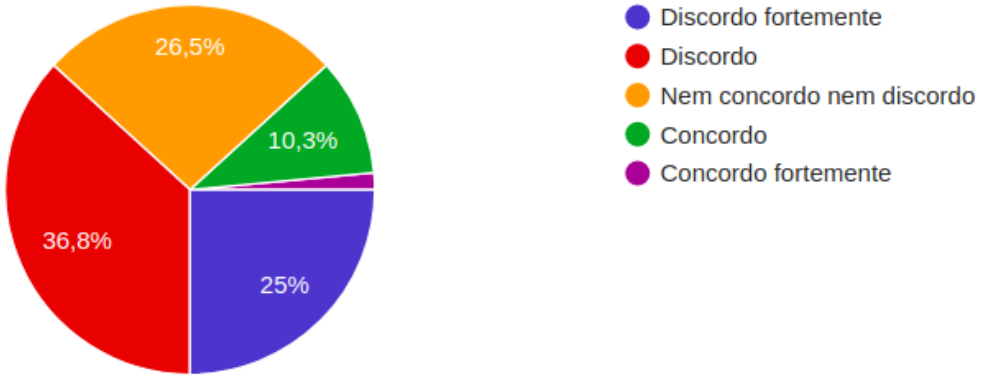


Figura 3.2: A maioria dos sites/dispositivos lidam com informações pessoais coletadas de forma correta e confidencial.

A Figura 3.3 refere-se às respostas dadas à pergunta 7c do questionário. O intuito dessa questão foi verificar se, ao utilizar um mecanismo que responda em seu nome em ambientes IoT, o usuário perde o controle de suas informações. Um total de 19,1% concorda fortemente, 45,6% concordam que perdem o controle de suas informações ao utilizar um mecanismo. Um total de 23,5% não teve uma opinião, 10,3% discordam e 1,5% discordam fortemente. Esses resultados evidenciam que mais da metade dos usuários considera que o uso de um mecanismo que responda

em seu nome pode representar perda do controle de suas informações.

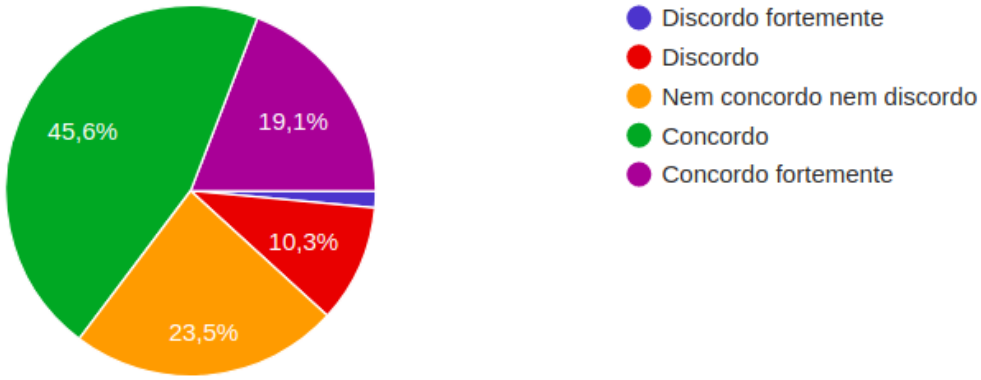


Figura 3.3: Você acha que tendo um mecanismo que responda em seu nome, você perde o controle sobre as suas informações.

Para que os usuários se sentissem mais confiantes com a utilização de um mecanismo que respondessem em seu nome, foi feito um conjunto de questões apresentados na Tabela 3.2 para verificar quais informações deveriam constar no mecanismo e que deixariam o usuário mais disposto a disponibilizar as suas informações.

Tabela 3.2: Conhecimento sobre a coleta de informações.

Eu estaria mais disposto a permitir a coleta de informações pessoais (ou seja, informações que podem ser usadas para me identificar e me contatar) se de alguma forma...	
Q1	Me permitisse escolher antecipadamente o que as empresas podem aprender sobre mim.
Q2	Me permitisse controlar quais empresas podem coletar e usar essas informações.
Q3	Me permitisse visualizar o que as empresas já conhecem sobre mim.
Q4	Me permitisse controlar quais dados serão coletados.

A questão apresentada na Tabela 3.2 foi dividida em quatro outras subperguntas (Q1, Q2, Q3 e Q4) e os resultados dessas perguntas são apresentados na Figura 3.4.

Nota-se no gráfico Q1, da Figura 3.4, que 76% dos usuários estariam mais dispostos a divulgar seus dados se pudessem de alguma forma escolher o que as empresas podem aprender sobre eles. No gráfico Q2, 83% dos usuários acreditam que o controle sobre quais empresas podem coletar seus dados influenciariam na sua tomada de decisão. Já no gráfico Q3, 82% dos usuários gostariam de visualizar o que as empresas sabem sobre eles. Por fim, no gráfico Q4 cerca de 91% dos usuários gostariam de controlar quais dados podem ser coletados pelas empresas.

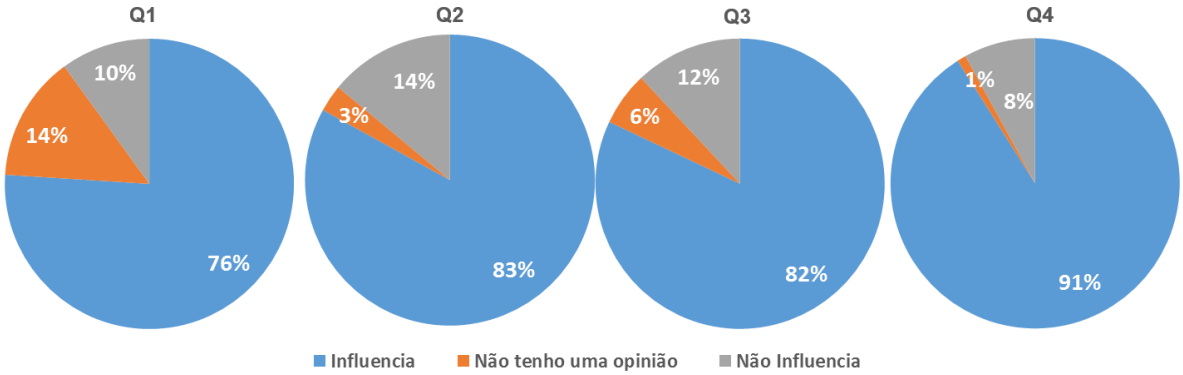


Figura 3.4: Resultados obtidos sobre a influência do conhecimento prévio da utilização dos dados solicitados.

Os resultados dessa questão evidenciam que, se o mecanismo de preservação de privacidade utilizasse essas características, deixaria os usuários mais confortáveis na disponibilização de seus dados e, consequentemente, daria a eles o controle da divulgação de suas informações.

Com base nas perguntas da Tabela 3.2 foram definidas algumas variáveis influentes. A literatura aponta um conjunto de variáveis influentes no processo de tomada de decisão na qual foram testadas separadamente pelos autores (LEDERER; MANKOFF; DEY, 2003; KLASNJA et al., 2009; BARUA; KAY; PARIS, 2013; LEON et al., 2013; LEE; KOBSA, 2016, 2017) e em conjunto pelo trabalho de Naeini et al. (2017). Consequentemente, essas variáveis foram adotadas e apresentadas aos participantes da pesquisa para verificar se existe alguma outra variável que eles considerariam influentes no seu processo de tomada de decisão. A Tabela 3.3 apresenta esse conjunto de variáveis.

Tabela 3.3: Variáveis influentes no processo de tomada de decisão.

Consumidor de dados	É quem está solicitando a informação.
Atributo	Informação que está sendo solicitada.
Motivo	Motivo da solicitação.
Benefício	Quem se beneficia da solicitação (usuário, consumidor ou ambos).
Retenção	Tempo em que a informação ficará armazenada.
Localização	É o local onde está sendo solicitada a informação.
Compartilhar	Se a informação será compartilhada com terceiros.
Inferência	Se pode ser inferida alguma outra informação a partir da informação solicitada.

A questão 9 do questionário refere-se à existência de alguma outra variável influente no processo de tomada de decisão. Essa pergunta foi feita no formato

aberto e nenhum dos participantes identificou outra variável que influenciasse em sua decisão.

Conforme apresentado no Capítulo 2.5, foram adotadas algumas características dos trabalhos. O processo de negociar a informação, proposto por Ukil et al. (2012) foi reavaliado pelos participantes e a Figura 3.5 apresenta os resultados dessa questão.

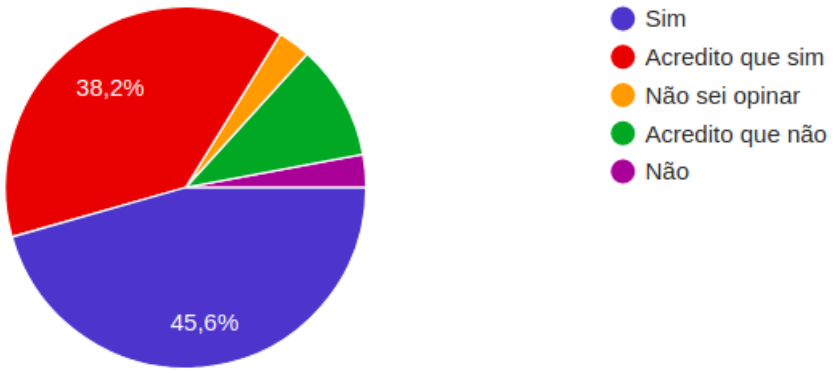


Figura 3.5: A possibilidade de disponibilizar uma informação de forma anônima, influência no seu processo de decisão.

Um total de 45,6% respondeu sim, ou seja, a possibilidade de disponibilizar uma informação anônima influencia no seu processo de decisão. Outros 38,2% não tiveram a plena certeza de responder sim, mas acredita que disponibilizar de forma anônima podem influenciar no seu julgamento. Um total de 10,3% acredita que isso não influencia, 2,9% disseram que não e apenas 2,9% não souberam opinar.

Com bases na capacidade de divulgar a informação de forma anônima, algumas perguntas referem-se aos tipos de métodos adotados para verificar se os participantes se sentem confortáveis na disponibilização de seus dados utilizando esses métodos.

A Figura 3.6 apresenta os resultados da pergunta referente à técnica de mascaramento hierárquico. É importante ressaltar que essas técnicas foram detalhadas para os participantes e apresentados exemplos de seu funcionamento. Um total de 20,65% respondeu que sim, 38,2% acreditam que sim, ou seja, os participantes se sentem confortáveis com a divulgação de seus dados utilizando essa técnica. Um percentual de 20,6% não soube opinar sobre essa pergunta, 10,3% acreditam que não e 4,4% responderam que não.

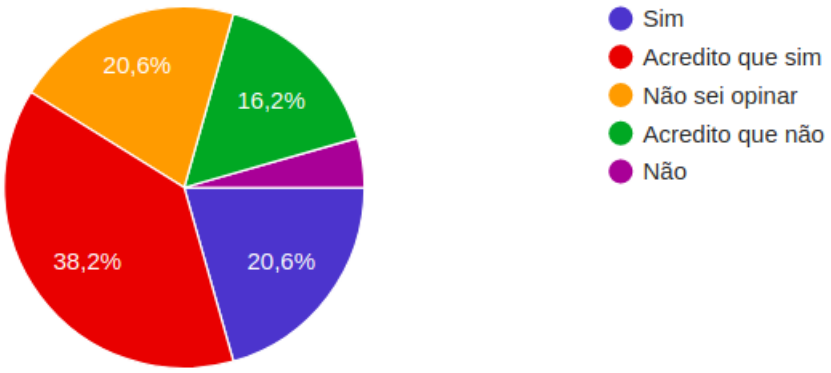


Figura 3.6: Neste contexto, você se sente confortável em disponibilizar seu bairro utilizando a técnica de mascaramento hierárquico.

A questão 13 refere-se à técnica de generalização. Essa técnica consiste em especificar um intervalo de um número e foi utilizado para anonimizar os atributos numéricos. A Figura 3.7 apresenta os resultados obtidos a partir dessa pergunta. Um total de 44,1% respondeu que sim, 36,8% acreditam que sim e 3% não souberam opinar. Os outros 14,7% tiveram uma opinião contraria, sendo que 10,3% acreditam que não e 4,4% não se sentem confortáveis em divulgar seus dados utilizando essa técnica.

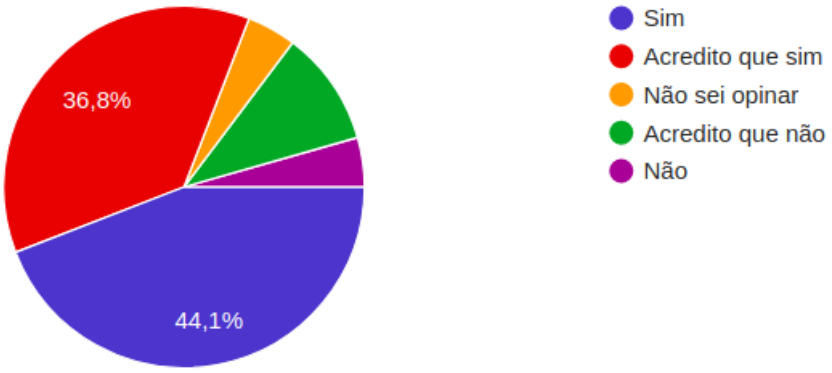


Figura 3.7: Neste contexto, você se sente confortável em disponibilizar a sua idade utilizando a técnica de generalização.

Para alguns dados foi adotado a técnica de pseudonimização por mascaramento, que consiste em substituir caracteres de uma informação por outros caracteres aleatórios ou fixos. A Figura 3.8 refere-se às respostas obtidas com a pergunta sobre pseudonimização fixa, ou seja, ao invés de usar o sexo masculino ou feminino foi definida uma palavra fixa, neste caso "indefinida". Um total de 19,1% respondeu que sim e se sentem confortáveis com a disponibilização de sua informação nesse formato, 29,4% acreditam que sim e 19,1% não souberam opinar. Os outros 32,3%

tiveram a opinião divergente, sendo que 14,7% responderam que não e 17,6% acreditam que não se sentem confortáveis.

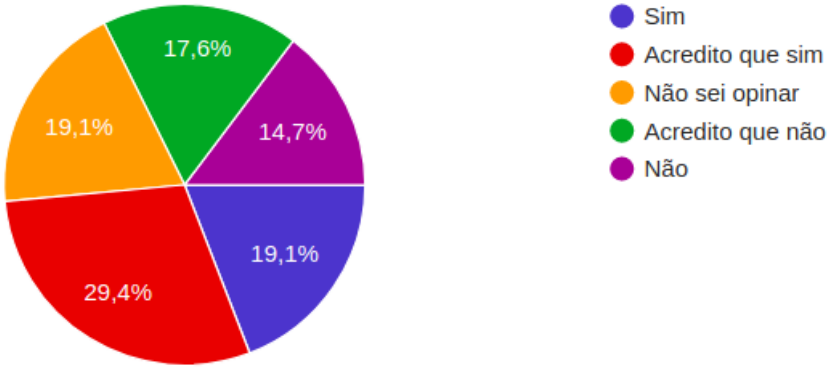


Figura 3.8: Neste contexto, você se sente confortável disponibilizar o seu sexo pseudonimizado como "indefinido".

A Figura 3.9 refere-se às respostas da pseudonimização aleatória. Essa técnica foi aplicada nos dados que não tivessem nenhum outro tipo de anonimização associado. Um total de 11,8% respondeu que sim, 36,8% acreditam que sim, ou seja, a técnica os deixa confortáveis em disponibilizar suas informações. Uma porcentagem de 27,9% não soube opinar, 14,7% acreditam que não e 8,8% não se sentem confortáveis com essa técnica.

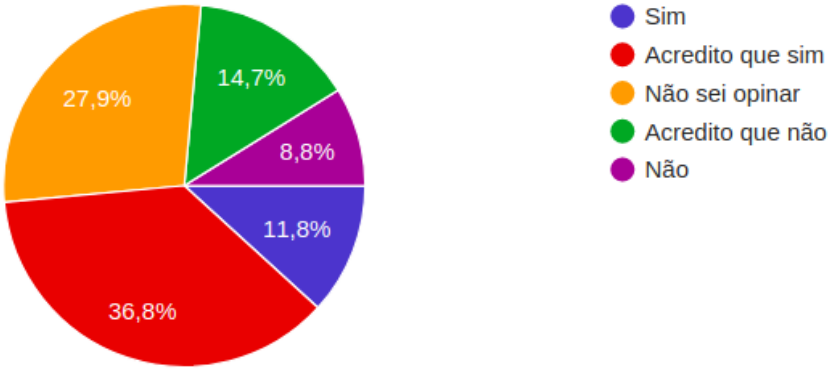


Figura 3.9: Ainda no contexto de pseudonimização, você se sente confortável disponibilizar qualquer outro tipo de informação utilizando a pseudonimização aleatória.

Por fim, a Figura 3.10 refere-se às respostas sobre a técnica de ajuste de precisão. Esta técnica consiste em disponibilizar a localização de forma a torná-la anônima, fazendo um deslocamento da localização original para qualquer direção dentro de um raio aleatório. Um total de 20,6% respondeu sim, 38,2% acreditam que sim, que se sentem confortáveis com essa técnica. Um percentual de 17,6%

respondeu que não, 20,6% acreditam que não se sentem confortáveis e apenas 2,9% não souberam responder.

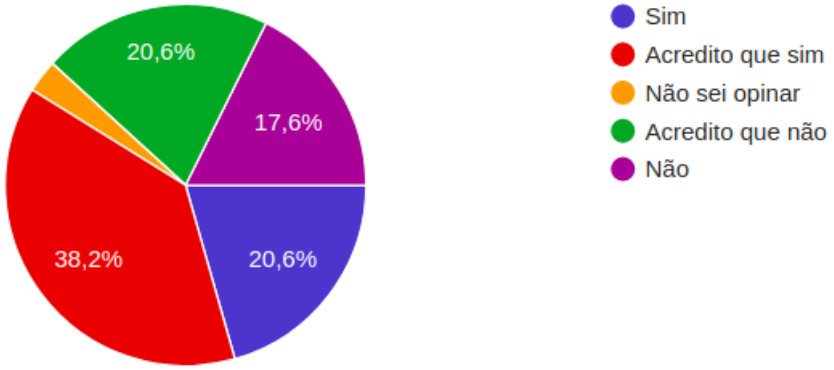


Figura 3.10: Neste contexto, você se sente confortável em disponibilizar sua localização, desde que o seu anonimato esteja assegurado

3.3 Considerações Finais

Este capítulo objetivou apresentar um levantamento feito com uma amostra de usuários sobre as características e funcionalidades a serem disponibilizadas pelo mecanismo de preservação de privacidade.

As perguntas e afirmações submetidas aos usuários tiveram os resultados aceitáveis. As características de coleta de dados apresentadas pela pesquisa evidenciam que 83% dos usuários concordam que essas informações influenciariam as suas decisões, 6% não tiveram uma opinião e apenas 11% acreditam que essas características não influenciariam a sua decisão.

As variáveis influentes também foram avaliadas pelos usuários, e os respondentes as consideraram suficientes no processo de tomada de decisão. Na avaliação da capacidade de divulgar as informações de forma anônima, 83,8% dos participantes acreditam que essa capacidade influenciará na sua tomada de decisão, 13,2% não acreditam que isso influenciaria e 2,9% não souberam responder.

Os métodos de anonimização propostos na avaliação foram respondidos pelos participantes e em média 59,12% dos usuários sentem-se confortáveis com a disponibilização dos seus dados nesses formatos, 25,86% não se sente confortável e 14,98% não tiveram uma opinião.

Os resultados evidenciam que vários aspectos se disponibilizados aos usuários influenciam grandemente na sua decisão de disponibilizar os seus dados pessoais.

Capítulo 4

Mecanismo de Preservação de Privacidade

4.1 Considerações Iniciais

Neste Capítulo da dissertação de mestrado é apresentado o mecanismo desenvolvido, cujo modelo de funcionamento é uma das principais contribuições deste trabalho. O mecanismo proposto visa a fornecer ao usuário a capacidade de controlar as informações que são disponibilizadas em ambientes IoT.

A Seção 4.2 apresenta a visão geral do mecanismo e a Seção 4.3 descreve a sua arquitetura apresentando os detalhes de seu funcionamento. Na Seção 4.4 são descritas as informações de implementação, bem como os diagramas de casos de uso e de classe.Na Seção 4.5 é apresentada uma aplicação deste mecanismo. O intuito dessa aplicação é testar o seu funcionamento. Finalmente, a Seção 4.7 apresenta as considerações finais deste capítulo.

4.2 Visão Geral do Mecanismo

O mecanismo de preservação de privacidade visa mediar as trocas de informações em ambientes IoT. Esta mediação busca ajudar o usuário a preservar sua privacidade, fornecendo meios para controlar como suas informações podem ser divulgadas.

Esse mecanismo foi projetado com bases nos trabalhos encontrados na literatura (descrito no Capítulo 2) e no levantamento feito com os usuários apresentado no Capítulo 3. A combinação das abordagens levantadas pelo estado da arte juntamente com a pesquisa realizada, proporcionou desenvolver um mecanismo eficiente

e que auxilia o usuário a controlar a divulgação de suas informações.

O principal intuito desse mecanismo proposto é melhorar o controle e gerenciamento da divulgação de dados do usuário pelo uso de algumas variáveis que são consideradas influentes no processo de tomada de decisão. O processo utiliza uma negociação dos dados para auxiliar o usuário a manter a sua privacidade, possibilitando divulgar somente a informação que foi solicitada e com a anuência do usuário.

Os benefícios fornecidos pelo mecanismo são visíveis tanto para o consumidor de dados (quem solicita uma informação) quanto para o produtor de dados/usuário (quem disponibiliza uma informação). O usuário beneficia-se da capacidade de gerenciar a sua privacidade e, pelo fato de controlar a divulgação de seus dados, sente-se mais confortável em disponibilizá-los. É evidente que quanto mais dados são disponibilizados pelo produtor de dados, maior será o benefício para o consumidor de dados, bem como para o próprio produtor de dados.

O mecanismo atua como um mediador entre o consumidor de dados e o produtor de dados. Ao mediar essa troca de informação, ele possibilita o produtor de dados a capacidade de autorizar, negar ou negociar. A Figura 4.1 apresenta uma visão geral do funcionamento do mecanismo.

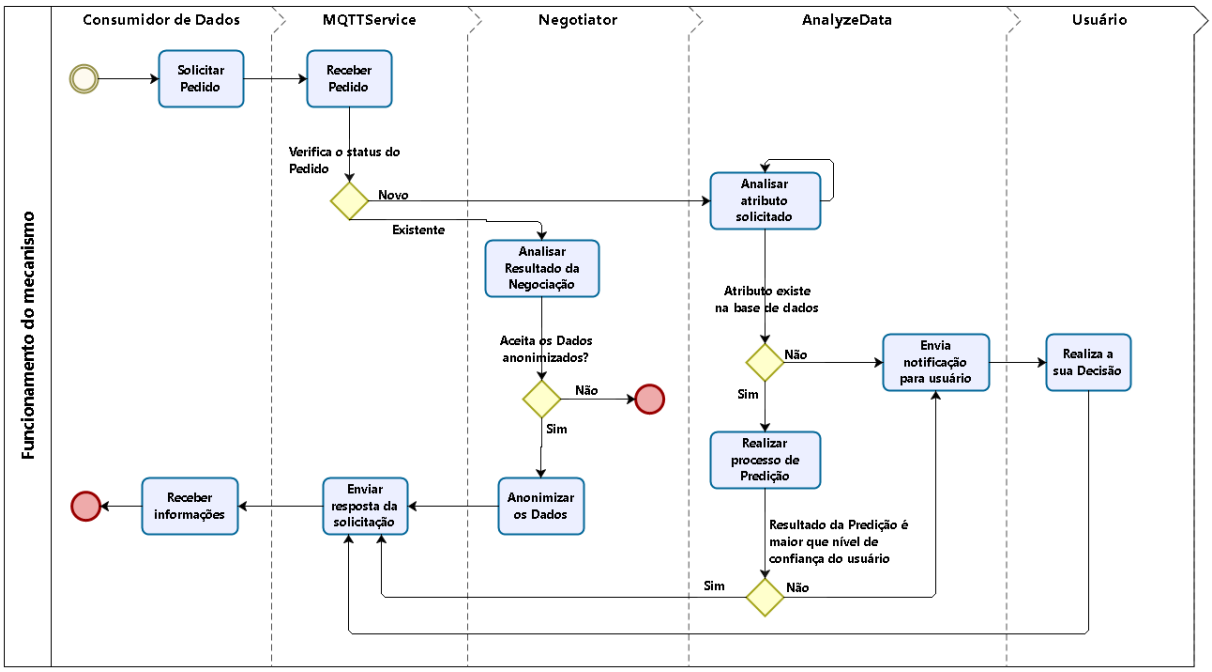


Figura 4.1: Visão geral do funcionamento do mecanismo.

O consumidor de dados possui a capacidade de solicitar uma informação ao pro-

dutor de dados. Ao solicitar uma informação, o mecanismo recebe esse pedido de dados e faz uma análise para verificar se é um pedido novo ou um pedido existente. Se for um pedido novo, os dados solicitados passam por uma análise para verificar se eles existem na base de dados do usuário. Casos eles existam, os dados são submetidos a um modelo de aprendizagem para verificar o quanto de confiança que o mecanismo tem em responder essa solicitação automaticamente. Se a confiança do resultado da predição for maior que a confiança estipulada pelo usuário, o próprio mecanismo responderá em nome do usuário.

No entanto, se os dados solicitados não existirem na base de dados do usuário ou se a confiança da predição for menor que a confiança estipulada, esse pedido de dados é enviado para o usuário decidir sobre ele. O usuário então decide em relação a esse pedido e os resultados dessa decisão são enviados ao consumidor de dados.

As possíveis respostas que o consumidor de dados pode receber nessa troca de informação são:

- **Autorizar**: as informações solicitadas serão disponibilizadas para o consumidor de dados;
- **Negar**: as informações solicitadas serão negadas pelo produtor de dados;
- **Negociar**: o produtor de dados irá disponibilizar as informações para o consumidor de dados em um formato que não viole a suas preferências de privacidade, isto é, os dados solicitados serão submetidos a um processo de anonimização (descrito na Seção 4.3.4). Nessa negociação o consumidor de dados pode decidir se quer ou não aceitar as informações nesse formato.

Quando o consumidor de dados recebe uma notificação sobre o processo de anonimização, ele tem a opção de aceitar ou não os dados de maneira anônima. Se o consumidor optar por aceitar os dados anonimizados, deve então responder a essa solicitação com uma informação de aceite.

No processo de mediação das trocas de informação, o mecanismo desenvolve a capacidade de aprender as possíveis respostas do usuário. Esse processo de aprendizagem foi utilizado para aliviar a carga do usuário em ambientes nos quais existem várias trocas de informações. O modelo de aprendizagem utilizado pelo mecanismo será descrito em mais detalhes na Seção 4.3.3.

Para que o usuário tenha controle de suas informações e possa manter assim a privacidade de seus dados, o mecanismo utiliza como parâmetro um conjunto de variáveis (descritas na Seção 4.3.2) fundamental no seu processo de decisão. Essas variáveis auxiliam o usuário a entender como os seus dados e informações são utilizados pelo consumidor de dados.

4.3 Arquitetura

Esta Seção apresenta a arquitetura do mecanismo de preservação de privacidade, detalhando o modelo de comunicação. Apresenta, ainda, o protocolo de comunicação que foi utilizado entre o mecanismo e os dispositivos IoT, as variáveis que ajudam no processo de tomada de decisões, o modelo de aprendizagem que foi utilizado, as estruturas das trocas de informações e os métodos de anonimização utilizados pelo mecanismo.

4.3.1 Modelo de Comunicação

O *Message Queue Telemetry Transport* (MQTT) é um protocolo projetado com o propósito de ser ideal para aplicações móveis e foi utilizado no mecanismo por ser um modelo de conectividade máquina-a-máquina (M2M). Além de possuir um baixo custo de energia é excelente para o mundo IoT, por ser leve e atingir redes de longo alcance citeMQTT.

O padrão de troca de mensagem do MQTT funciona de maneira assíncrona (*push*) por meio da arquitetura *Publish* e *Subscribe* (Figura 4.2). Nessa arquitetura é implementado um *Broker* que trabalha como um mediador responsável por receber, enfileirar e disparar as mensagens recebidas.

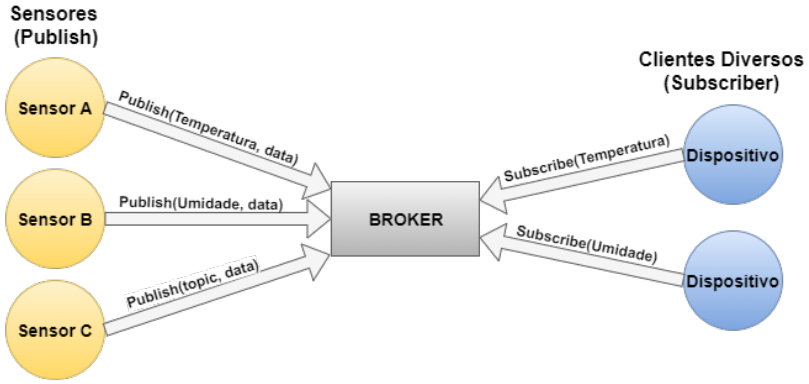


Figura 4.2: Visão geral do protocolo MQTT (MQTT, 2018).

O *Broker* interliga dois papéis: o *Publish* e *Subscribe*. O *Publish* é o responsável por enviar as informações para um determinado tópico e possui dois principais parâmetros: o *topic* e o *data*. O *topic* é o tópico no qual a mensagem será publicada e *data* são os dados da mensagem. O *Subscribe* é o responsável por receber as mensagens que foram publicadas no seu tópico de interesse. Para que o cliente MQTT possa dar *Subscribe* em um determinado tópico é necessário informar os parâmetros *topic*, que trabalha como um identificador de mensagens e o tipo de Qualidade do Serviço (QoS), responsável por garantir a qualidade de entrega das mensagens.

Um exemplo do funcionamento desse protocolo é imaginar uma rede de sensores na qual cada sensor envia um determinado tipo de informação em tópicos diferentes. Por exemplo, observando a Figura 4.2, o sensor A publica a informação no tópico temperatura, o B no tópico de umidade e assim por diante. Os dispositivos ou pessoas que estiverem inscritos nesses tópicos receberão as informações que forem publicadas pelos sensores.

A sua estrutura simples é uma peculiaridade muito relevante para a IoT, mas mesmo assim não deixa de contemplar as características importantes como segurança, qualidade de serviço e a facilidade de implementação. Nesse contexto, para garantir a segurança nas transações o protocolo MQTT apresenta dois níveis de autenticação, um nível é feito na camada de transporte e outro na camada de aplicação.

Na camada de transporte, a conexão *Transport Layer Security* (TLS) pode garantir a autenticação utilizando certificados de cliente. Já no nível de aplicação, o protocolo MQTT disponibiliza um usuário e senha. Após a autenticação na camada de aplicação, o servidor libera os recursos que esse cliente MQTT pode acessar.

O principal recurso do cliente é publicar ou subscrever em um determinado tópico. Para efetuar o procedimento, o cliente MQTT precisa de uma autorização especifica para essa operação. Essas autorizações são feitas por meio de *Acess Control List* (ACL), ou seja, uma lista que contêm as permissões de acesso de um usuário. Essa ACL gerencia as políticas de controle de cada recurso do cliente e as permissões de acesso são configuradas e ajustadas pelo *Broker* em tempo de execução.

No mecanismo proposto, as trocas de informações feitas pelas "*things*" seguem conforme apresentado na Figura 4.3. Quando um consumidor de dados (*thing*)

deseja solicitar uma informação para o usuário, ele utiliza o protocolo MQTT para fazer uma publicação em um tópico especifico definido pelo mecanismo. O tópico de publicação foi padronizado para que os consumidores de dados solicitem as informações no mesmo tópico.

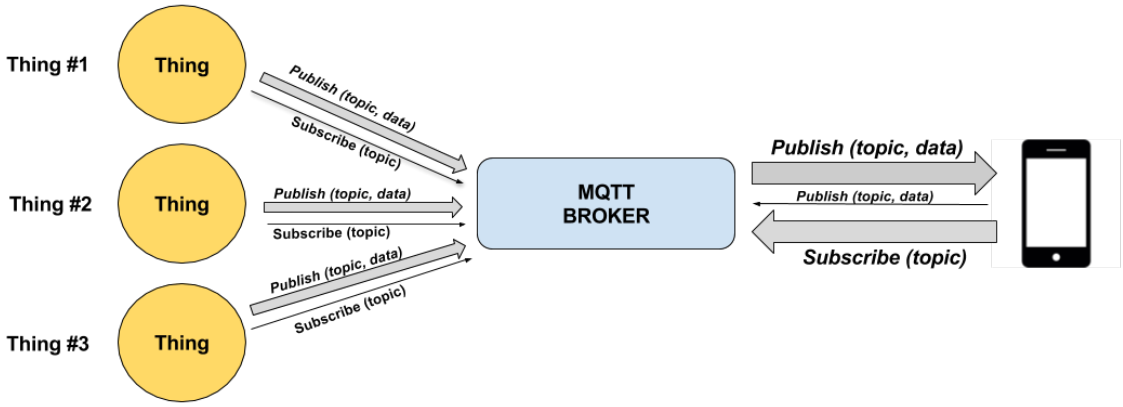


Figura 4.3: Funcionamento do MQTT no mecanismo.

O protocolo MQTT sendo uma arquitetura assíncrona permite que qualquer *things* se escreva e publique em qualquer tópico. No entanto, no mecanismo aqui proposto quando uma *thing* faz uma publicação solicitando informações do produtor de dados, somente essa *thing* deve receber a resposta vindo do mecanismo. Portanto, para que o mecanismo garanta que outras *things* não recebam as informações publicadas o recurso de subscribe foi vedado por meio da ACL. Com isso, é garantido que somente o mecanismo tem acesso as informações de solicitações publicadas pelas *things*.

4.3.2 Variáveis Influentes no Processo de Decisão

O consumidor de dados que deseja solicitar uma informação ao usuário (produtor de dados) deve seguir os padrões estabelecidos pelo mecanismo. Conforme mencionado anteriormente, o mecanismo utiliza um conjunto de variáveis que são consideradas influentes no processo da tomada de decisão. Esse conjunto de variáveis foi testado separadamente por diversos autores (LEDERER; MANKOFF; DEY, 2003; KLASNJA et al., 2009; BARUA; KAY; PARIS, 2013; LEON et al., 2013; LEE; KOBSA, 2016, 2017) e em conjunto no trabalho de Naeini et al. (2017).

Tais variáveis denotam aspectos que podem ser considerados relevantes na avaliação da violação da privacidade do usuário. A descrição de cada variável utilizada

neste trabalho é apresentada na Tabela 4.1

Tabela 4.1: Variáveis influentes no processo de tomada de decisão visando a privacidade.

Variável	**Descrição**
Consumidor de dados	dispositivo ou pessoa que está solicitando uma informação.
Atributo	informação que está sendo solicitada.
Motivo	motivo da coleta dos dados.
Benefício	quem se beneficia desta troca de informação (usuário, consumidor ou ambos).
Retenção	tempo em que a informação solicitada ficará retida pelo consumidor de dados.
Localização	local onde os dados são coletados (público, privado, semipúblico).
Compartilhar	se a informação solicitada será compartilhada com terceiros (sim ou não).
Inferência	Se é possível inferir alguma outra informação a partir da informação solicitada (sim ou não).

Cada variável remete ao usuário uma avaliação na sua tomada de decisão. Variáveis como consumidor de dados, atributo e motivo têm um maior impacto nessa decisão, pois apresentam ao usuário quem é o solicitante, o atributo que está sendo solicitado e motivo dessa solicitação. Já as demais variáveis complementam a sua decisão e em alguns casos são consideradas decisórias na divulgação das informações (NAEINI et al., 2017; LEDERER; MANKOFF; DEY, 2003).

O emprego dessas variáveis em um só contexto possibilita ao usuário entender como as informações são utilizadas pelo consumidor de dados e como isso pode se refletir na preservação da sua privacidade.

4.3.3 Modelo de Aprendizagem

A capacidade de aprendizagem é uma característica fundamental no desenvolvimento de aplicações IoT. Essa competência alivia o usuário quanto à tomada de decisões rotineiras que tomam o seu tempo no decorrer do dia a dia. Nesse mecanismo, o modelo de aprendizagem utilizado foram as redes neurais *Multilayer*

Perceptron (MLP).

A MLP é um modelo de rede neural artificial que utiliza técnicas de aprendizagem supervisionada, ou seja, é necessário um conjunto de treinamento para predizer uma determinada informação. A Figura 4.4 apresenta a arquitetura de uma MLP que consiste em uma camada de entrada, uma ou mais camadas ocultas e uma camada de saída.

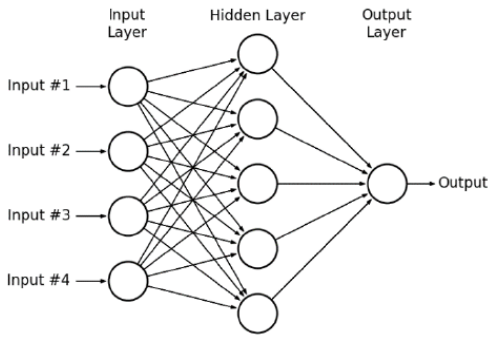


Figura 4.4: Arquitetura do Multilayer Perceptron (MOHAMED et al., 2015).

Nesse modelo de aprendizagem, as variáveis são inseridas na camada de entrada e, a partir dela, os cálculos são feitos para cada padrão de entrada até que uma saída seja obtida (DRISS et al., 2017) . A camada de saída da MLP é responsável pela saída de um valor ou vetor de valores que correspondem ao formato de seu problema.

Na MLP utilizada pelo mecanismo as variáveis obrigatórias são utilizadas como parâmetros de entrada e têm como saída as três possíveis respostas: Allow (Autorizar), Deny (Negar) ou Negotiate (Negociar). A Figura 4.5 ilustra o modelo dessa MLP.

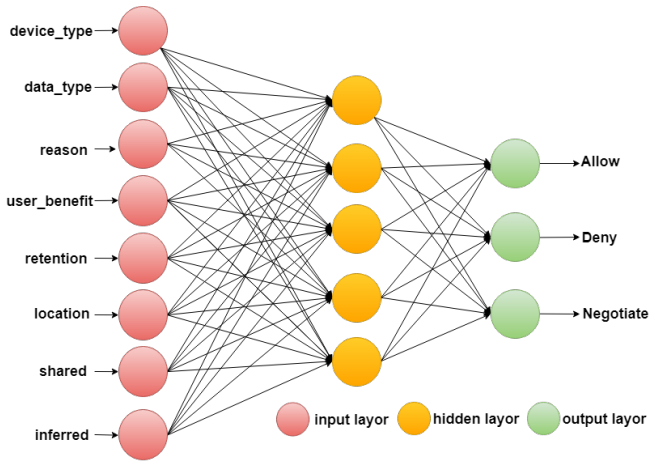


Figura 4.5: Representação da MLP no Mecanismo.

Nesse modelo de MLP, a camada de saída tem uma probabilidade de prever cada uma das possíveis respostas. Como uma segurança adicional, o mecanismo só aceita uma predição se a probabilidade da resposta for maior que a probabilidade definida pelo usuário. Essa probabilidade imposta pelo usuário é definida como o nível de confiança que ele tem em deixar o mecanismo responder em seu nome.

4.3.4 Métodos de anonimização

Nos casos em que o usuário decida disponibilizar as suas informações de forma anônima, os dados solicitados pelo consumidor de dados são submetidos a um processo de anonimização. Nesse processo, as informações são aplicadas às técnicas de preservação de privacidade para serem disponibilizados em um formato que não viole a privacidade do usuário.

As técnicas de anonimização utilizadas no mecanismo foram avaliadas pela pesquisa apresentada na Seção 3.2 e são descritas a seguir:

- **Mascaramento hierárquico**: é uma técnica capaz de agregar uma informação no formato de hierarquia. Por exemplo, os bairros (Vila Nery, Faga e Vila Prado) podem ser agregados para cidade de São Carlos. Já a cidade de São Carlos pode ser agregado para o estado de São Paulo e assim por diante (UKIL et al., 2012).

- **Generalização**: é uma técnica que permite especificar um intervalo de um determinado número ou extrair um membro de um conjunto desse número. Por exemplo, considerando que o usuário tenha 26 anos, ao utilizar essa técnica de anonimização a idade do usuário poderia ser anonimizada para 22-29 (NELSON, 2015);

- **Pseudonimização**: é uma técnica que consiste em substituir caracteres de uma informação por outros conjuntos de caracteres fixos ou aleatórios. Na pseudonimização fixa os dados são substituídos por um conjunto de informações fixas. Por exemplo, o sexo de uma pessoa (masculino ou feminino) pode ser pseudonimização para "indefinido". Já na pseudonimização aleatório cada carácter da informação é substituído por outro carácter aleatório (NELSON, 2015).

- **Ajuste de Precisão**: faz um deslocamento da localização original do usuário para qualquer outra direção dentro de um raio aleatório (ROSA, 2015).

Essa capacidade de anonimizar as informações permite ao usuário desfrutar de um serviço fornecido pelo consumidor de dados, ao mesmo tempo, fornecendo as informações no formato que preserve a sua privacidade.

4.3.5 Estrutura das trocas de mensagens

Para solicitar uma informação ao usuário, é necessário que o consumidor de dados utilize uma estrutura de dados definida pelo mecanismo. Essa estrutura definida segue o formato JSON (*JavaScript Object Notation*) conforme apresentado na Figura 4.6. Foi utilizado esse formato por ser uma estrutura simples e ao mesmo tempo eficiente para as trocas de mensagem em ambientes IoT (PöHLS, 2015).

```
{
  "uuid": "39d17a79-6a56-4013-b55d-b0f6d42dfcd6",
  "location": "public",
  "user_benefit": "consumer",
  "reason": "Para cadastrar essas informações em seu sistema com
    intuito de manter um registro de seus abastecimentos",
  "data": [{
      "attribute": "modelo_carro",
      "shared": true,
      "retention": "forever",
      "inferred": true
    },{
      "attribute": "ano_carro",
      "shared": true,
      "retention": "forever",
      "inferred": true
    },{
    "attribute": "placa_carro",
      "shared": true,
      "retention": "forever",
      "inferred": true
  }],
  "consumer": [{
      "attribute": "Nome",
      "value": "Posto de Gasolina"
    },
    {
      "attribute": "Endereço",
      "value": "Av. São Carlos"
    }]
}
```

Figura 4.6: Estrutura da solicitação de dados.

Conforme apresentado na Figura 4.6 os parâmetros obrigatórios para solicitar uma informação são descritos na Tabela 4.2.

Tabela 4.2: Descrição dos parâmetros da solicitação de dados.

uuid	Corresponde a um identificador único gerado pelo consumidor de dados quando ele vai se autenticar no servidor MQTT.
location	Local onde está situado o consumidor de dados (publico, semi_publico ou privado).
user_benefit	Informação de quem se beneficia desta troca de informação (usuário, consumidor ou ambos).
attribute	Informação que está sendo solicitado.
shared	Corresponde que esse atributo será compartilhar com mais alguém.
retention	Mede quanto tempo a informação será mantida pelo consumidor de dados.
inferred	Informa se a partir do atributo solicitado pode ser inferido alguma outra informação.
consumer	Um *array* de objeto no qual o consumidor deve informar mais detalhes sobre as suas informações. Esse *array* é constituído por um *attribute* e um *value*. O *attribute* corresponde ao rotulo da informação e o *value* é valor desse *attribute*.

Ao receber uma solicitação de dados, o mecanismo processa esse pedido de dados e retorna ao consumidor uma resposta no formato apresentado na Figura 4.7. Nesse retorno, o consumidor de dados recebe dois parâmetros o *request_code* e o *data* (descritos na Tabela 4.3).

Tabela 4.3: Descrição dos parâmetros de retorno da solicitação de dados.

Variável	**Descrição**
request_code	refere-se ao código da solicitação.
data	é uma *array* que contém as informações dos dados solicitados. Esse *array* possui um objeto contendo em sua composição até 3 (três) atributos: • *attribute*: refere-se ao dado que está sendo solicitado; • *state*: refere-se aos estado da informação solicitada. Pode assumir 3 (três) possíveis valores, 1 (um) para aceite, 2 (dois) para negar e 3 (três) para negociar; • *value*: corresponde ao valor do atribute.

```
{
    "request_code": "962012d09b8170d912f",
    "data":[{
      "attribute":"modelo_carro",
      "state": 1,
      "value" : "chevrolet onix"
      },{
      "attribute":"ano_carro",
      "state": 3
     },{
      "attribute":"placa_carro",
      "state": 3
     }],
    "consumer":[{
      "attribute":"Nome",
      "value":"Posto de Gasolina"
    },{
      "attribute":"Endereço",
      "value":"Av. São Carlos"
    }]
}
```


Figura 4.7: Resposta da solicitação de dados.

Nos casos em que o consumidor de dados recebe como resposta um atributo com o "*state*=3", significa que o usuário deseja disponibilizar esta informação de maneira anonimizada. Dessa forma, o consumidor de dados tem a autonomia de escolher se ele deseja ou não uma informação nesse formato. Se o consumidor de dados aceitar a informação nesse formato, ele envia outra solicitação de dados (Figura 4.8) informando os mesmos atributos anteriores acrescentando o *request_code* como um indicativo ao pedido anterior e respondendo se aceita ou não os dados anonimizados. Dessa forma, quando o mecanismo receber uma solicitação com um *request_code*, ele faz uma busca para verificar esse pedido de dados em aberto e uma análise nas respostas do consumidor para poder disponibilizar os dados solicitados.


```
{
    "uuid":"39d17a79-6a56-4013-b55d-b0f6d42dfcd6",
    "request_code": "962012d09b8170d912f",
    "data":[{
      "attribute":"modelo_carro",
      "answer": true
      },{
      "attribute":"ano_carro",
      "answer": true
     },{
      "attribute":"placa_carro",
      "answer": false
     }],
    "consumer":[{
      "attribute":"Nome",
      "value":"Posto de Gasolina"
    },{
      "attribute":"Endereço",
      "value":"Av. São Carlos"
    }]
}
```


Figura 4.8: Estrutura da solicitação de dados de um pedido existente.

4.4 Especificações de Implementação

Para especificar o desenvolvimento da implementação do mecanismo, foi utilizada a linguagem de modelagem UML (*Unified Modeling Language*). Esta linguagem facilita construir, especificar e documentar os artefatos utilizados (LARMAN, 2006).

O diagrama de caso de uso foi utilizado para um melhor entendimento do funcionamento do mecanismo. As suas principais funcionalidades são apresentadas pelo diagrama de caso de uso da Figura 4.9.

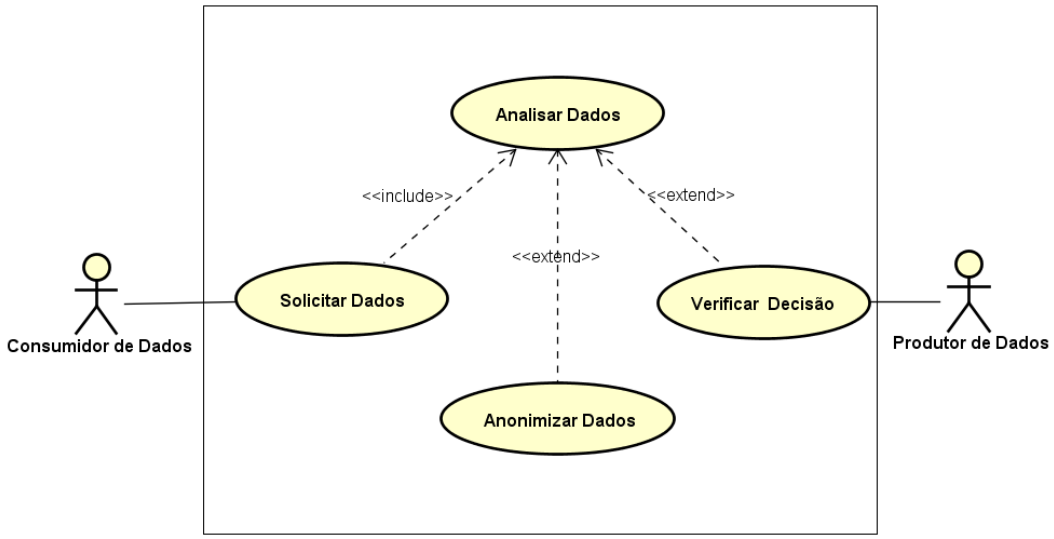


Figura 4.9: Diagrama de casos de uso.

A seguir são descritos detalhadamente para cada um dos casos de uso apresentados no diagrama da Figura 4.9.

1. **Solicitar dados**: neste caso de uso o consumidor faz um pedido de dados por meio de uma solicitação bem estruturada e definida, conforme apresentado na Seção 4.3.5. Posteriormente, a solicitação é processada pelo mecanismo e um retorno é enviado ao consumidor de dados;

2. **Analisar Dados**: ao receber um pedido de informação, os dados solicitados passam por uma análise na qual se verifica se o mecanismo possui a informação que está sendo pedida. Se o mecanismo possuir essa informação, é então feita uma predição visando a verificar o grau de confiança confiança do mecanismo para responder de forma automática a essa solicitação. Se a confiança da predição for maior que a confiança estipulada pelo usuário, o mecanismo

responderá em seu nome, isto é, autorizará, negará ou negociará as informações automaticamente. No entanto, se a informação solicitada não estiver na base de dados do mecanismo ou se a confiança da predição for menor que a estipulada pelo usuário, esse pedido de informação será enviado ao usuário para que ele mesmo decida em relação a eles;

3. **Verificar Decisão**: Caso o mecanismo não consiga responder uma solicitação automaticamente, o usuário precisará responder (autorizar, negar ou negociar) manualmente esta solicitação. Após a escolha de uma dessas opções, o pedido será finalizado e uma resposta será enviada ao consumidor de dados;

4. **Anonimizar Dados**: este caso de uso é responsável por anonimizar uma informação (Seção 4.3.4). Nesse caso, o produtor de dados pode decidir utilizar o método de anonimização disponível no mecanismo. Vale a pena ressaltar que o consumidor de dados pode decidir se aceita ou não os dados de maneira anonimizada.

Essa descrição do caso de uso possibilita visualizar as sequências de eventos que podem ocorrer para se chegar ao resultado desejado. A Figura 4.10 apresenta o diagrama de classe do mecanismo para demonstrar as classes, os atributos e as relações dos objetos. As classes do diagrama de caso de uso são descritas a seguir:

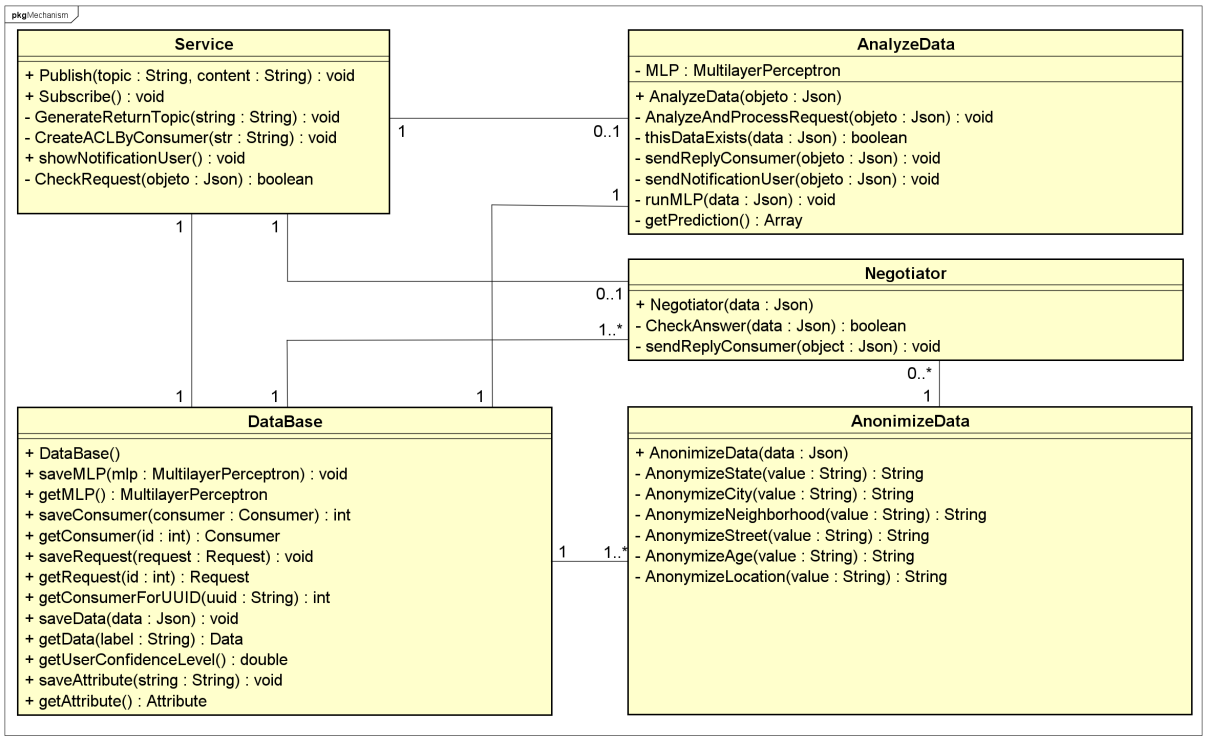


Figura 4.10: Diagrama de classes.

1. ***Service***: essa classe tem como objetivo receber as interações feitas pelo consumidor de dados. Possui apenas três funções, uma destinada a analisar a estrutura dos dados solicitados, outra destinada a enviar os dados solicitados para análise e a outra para enviar o resultado da decisão do consumidor de dados ao *Negotiator*;

2. ***AnalyzeData***: é responsável por fazer uma análise dos dados solicitados. Dentro das várias operações contidas no seu escopo, sua principal operação é a *AnalyzeAndProcessRequest*. Esta operação é responsável por verificar se os dados solicitados estão presentes na base de dados. Se estiverem, ela executa o processo de inferência de decisão;

3. ***Negotiator***: é responsável por verificar a resposta do consumidor de dados. Se a sua resposta for de aceite, os dados solicitados são enviados para o processo de anonimização;

4. ***AnonimizeData***: é responsável por aplicar as técnicas de preservação de privacidade descritas na Seção 4.3.4;

5. ***DataBase***: faz a interação com o banco de dados e fornece os métodos de acesso necessários;

Para descrever a sequência de interação das mensagens trocadas, assim como as operações, são apresentados os diagramas de sequência. A utilização dos diagramas fornece uma visão gráfica mais rigorosa do funcionamento do mecanismo.

Na Figura 4.11, é apresentado o diagrama de sequência para solicitar uma informação ao mecanismo. Inicialmente o consumidor por meio do método *publish* envia um pedido de dados. Este pedido é recebido pelo *MQTTBroker* que por sua vez envia para o serviço do mecanismo, o *Service* recebendo essa solicitação faz uma verificação para identificar se é um pedido novo ou um pedido já existente.

Após executar uma dessas condicionais (pedido novo ou existente), um tópico de retorno é criado no servidor MQTT para que o mecanismo possa publicar a sua resposta ao consumidor. Em seguida, são atribuídas as permissões de acesso nesse tópico criado. Por fim, uma mensagem de retorno é publicada para o consumidor no seu tópico específico.

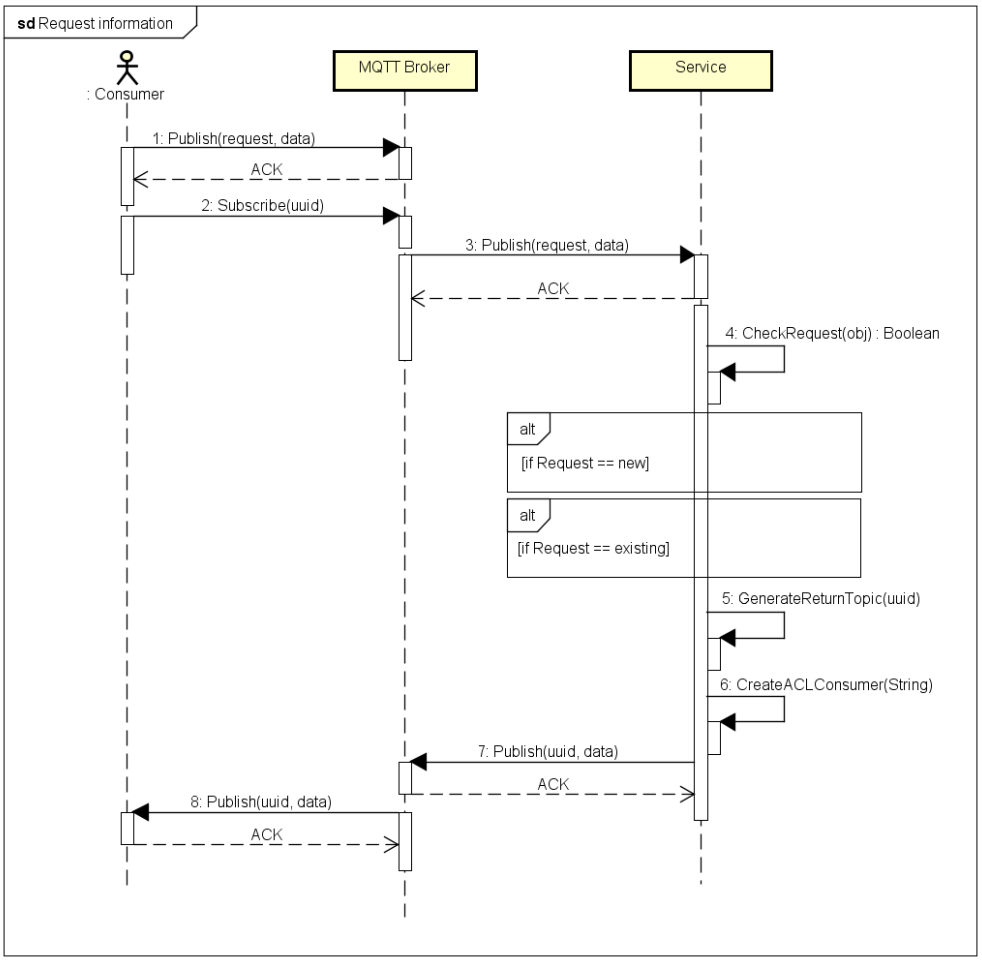


Figura 4.11: Diagrama de Sequência: Solicitar informação.

A Figura 4.12 apresenta as trocas de mensagem de uma nova solicitação. Inicialmente, o *AnalizeAndDataProcessRequest* pelo seu método *thisDataExists* verifica na base de dados, se o usuário possui os dados solicitados. Caso ele não possua, uma solicitação é enviado ao *Service* e ele reencaminha a notificação para o usuário decidir sobre esse pedido de dados. Um retorno é dado pelo usuário, e consequentemente segue o fluxo conforme descrito na Figura 4.11.

No entanto, quando os dados solicitados contem na base de dados do usuário, uma predição é feita por meio da função *runMLP*. Após essa predição, uma probabilidade na resposta é gerada pela MLP. O método *getPrediction* faz uma análise para verificar se a probabilidade da confiança da resposta é maior que o nível de confiança estipulado pelo usuário. Se for menor, o pedido de dados é enviado ao *Service* que notifica o usuário sobre esse pedido de dados. Caso seja maior ou igual, os dados são enviados para o *Service* que, por sua vez os publica para o consumidor de dados.

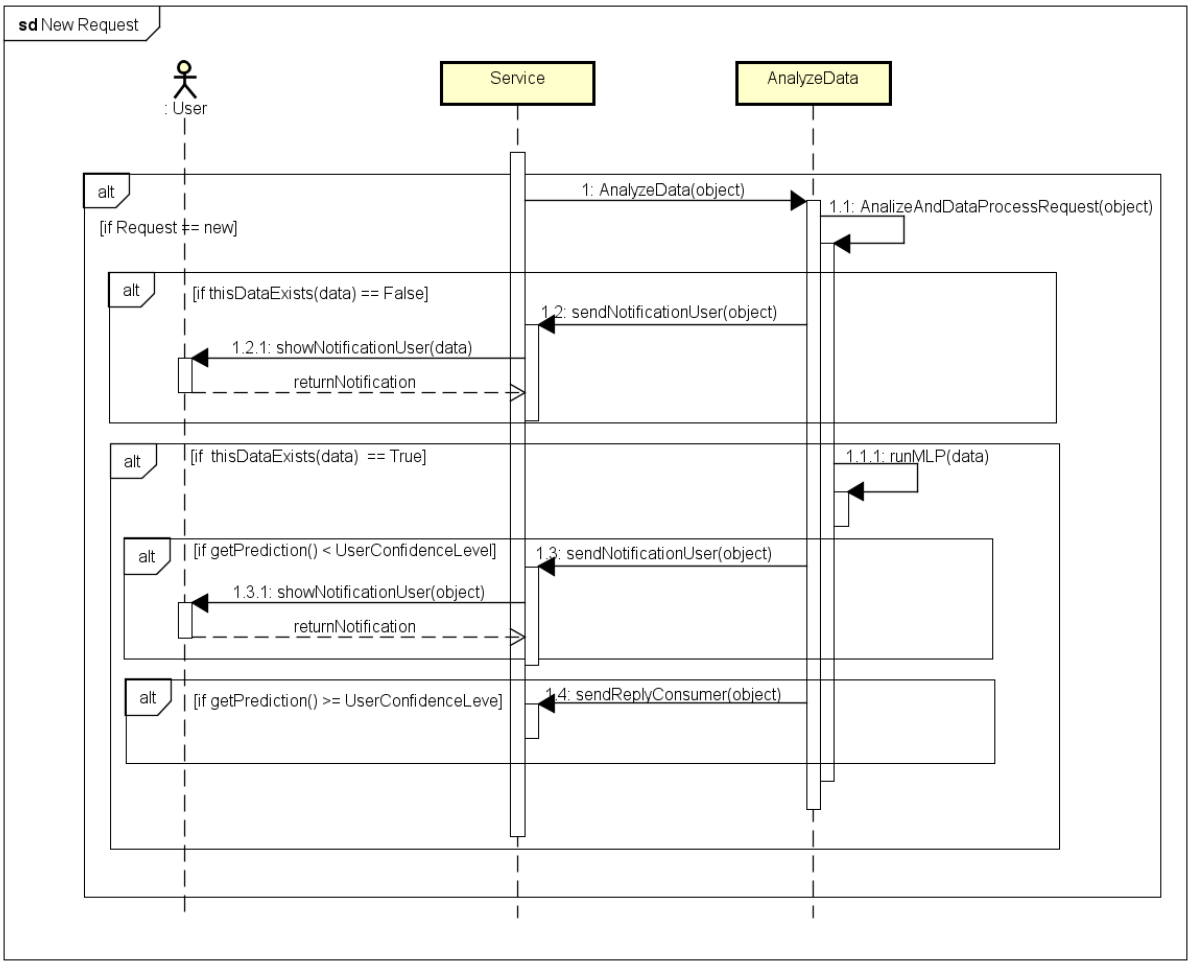


Figura 4.12: Diagrama de Sequência: Nova solicitação detalhada.

Já a Figura 4.13 apresenta o diagrama de sequência das trocas de mensagens de um pedido de dados existente.

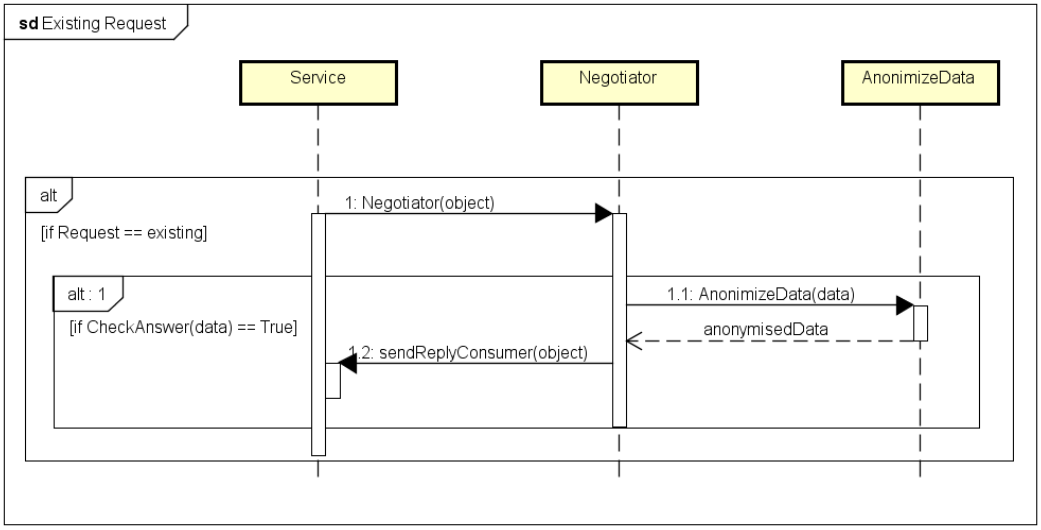


Figura 4.13: Diagrama de Sequência: Solicitação existente detalhada.

Nesta ocorrência, os dados são enviados pelo *Service* para o *Negotiator*, que, após receber esse pedido de dados, faz uma análise para verificar a resposta do consumidor. Se for uma resposta de aceite, os dados são enviados para a classe *AnonimizeData* que retorna os dados anonimizados. Na sequência, após o recebimento dos dados anonomizados, as informações solicitadas são enviadas pelo método *sendReplyConsumer* as informações solicitadas e o *Service* publica essas informações para o consumidor de dados.

4.5 Desenvolvimento

Utilizando a arquitetura e as especificações apresentadas nas Seções 4.3 e 4.4 foi desenvolvido um aplicativo *Android* para validar o funcionamento e a viabilidade desse mecanismo.

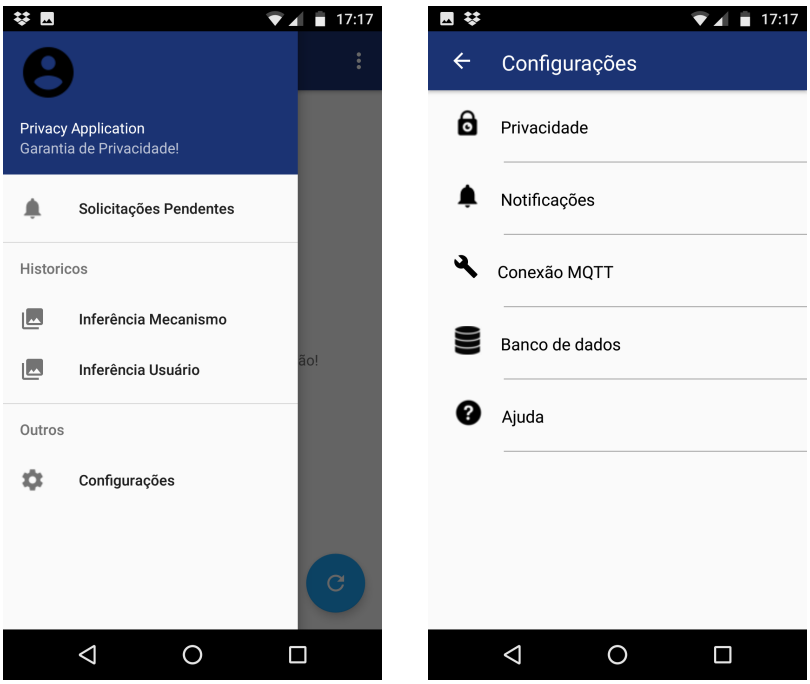
Para atingir um maior público de dispositivo foi utilizado a versão do *Android* 4.4 *KitKat* devido à sua compatibilidade com mais de 80% dos dispositivos ativos. A escolha por desenvolver a aplicação em uma plataforma móvel deveu-se à facilidade de interação com o usuário.

4.5.1 PrivacyApplication

O *PrivacyApplication* é uma aplicação *mobile* desenvolvida para validar o funcionamento de todas as funcionalidades propostas pelo mecanismo. A Figura 4.14 apresenta o menu do *PrivacyApplication* e as suas principais funcionalidades.

Neste menu da Figura 4.14a temos 4 (quatro) funcionalidades:

- **Solicitações Pendentes**: essa opção acessa a lista de pedidos que ainda não foram respondidos pelo usuário;
- **Inferência Mecanismo**: são listados para o usuário os pedidos de dados que foram respondidos pelo mecanismo, ou seja, os pedidos que foram respondidos automaticamente pelo processo de aprendizagem;
- **Inferência Usuário**: são listados os pedidos de dados que foram respondidos pelo usuário;



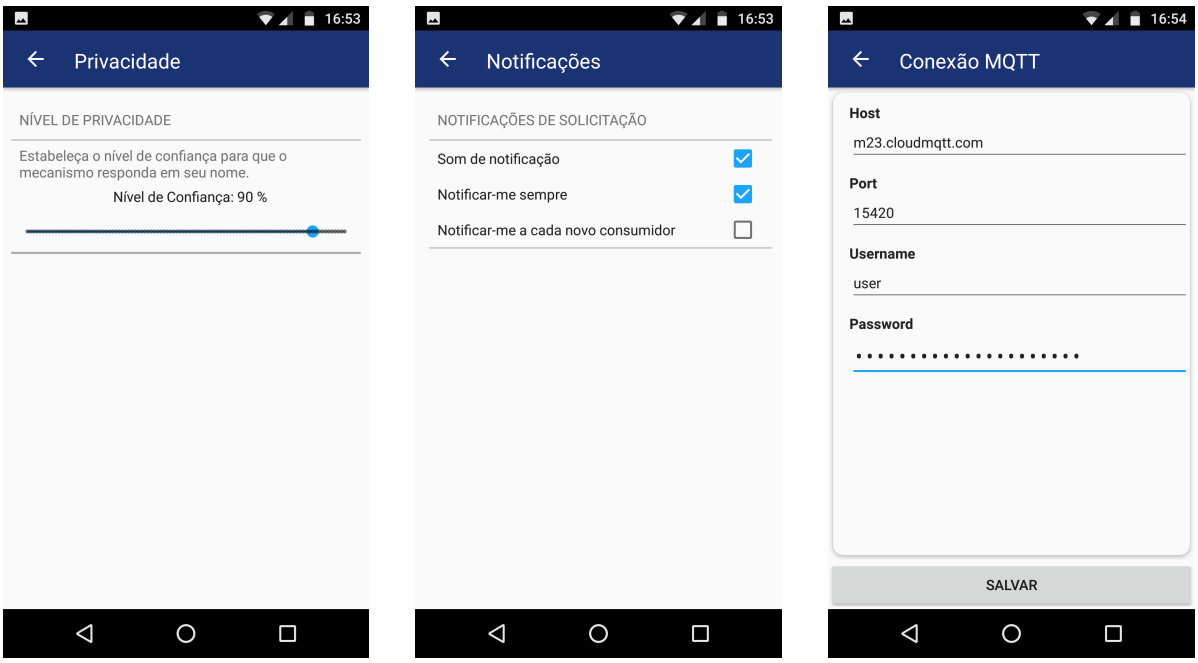
(a) Menu Principal. (b) Menu das Configurações.

Figura 4.14: Telas das funcionalidades disponíveis pelo *PrivacyApplication*.

- **Configurações**: essa opção acessa as configurações das informações referentes ao *PrivacyApplication*. A Figura 4.14b apresenta a lista de configurações disponível para ao usuário.

A "Privacidade" disponível na opção configuração conforme apresentado na Figura 4.14b, possibilita ao usuário definir o nível de confiança que ele tem em deixar o mecanismo responder em seu nome. A Figura 4.15a apresenta a tela dessa opção. Por meio de uma barra deslizante o usuário informa em uma escala de 0 à 100% o nível de confiança empregado no mecanismo.

A tela de configuração de "Notificação" é apresentada na Figura 4.15b e por meio dessa funcionalidade, o usuário possui a capacidade de escolher ser quer ser notificado ao receber um pedido de informação. O usuário possui três opções nesta configuração: 1) som de notificação - possibilita ao usuário desativar o som ao receber uma notificação; 2) notificar-me sempre - fornece ao usuário a possibilidade de sempre receber as notificações; 3) notificar-me a cada novo consumidor - possibilita ao usuário escolher receber notificação somente quando for a primeira vez que o consumido de dados está pedindo uma informação. É importante ressaltar que quando a opção 2 (notificar-me sempre) estiver ativa, a opção 3 (Notificar-me a cada novo consumidor) estará desativada, pois uma regra se sobrepõe à outra.



(a) Privacidade. (b) Notificações. (c) Conexão MQTT.

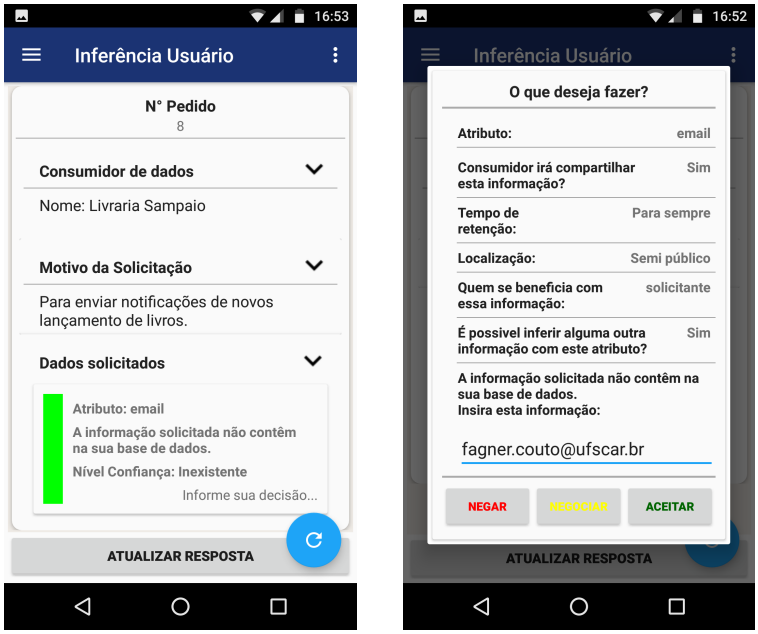
Figura 4.15: Telas das Configurações.

Na tela de configuração do MQTT, apresentada na Figura 4.15c, o usuário deve informar as configurações de seu servidor MQTT. Os parâmetros para acessar o servidor são: 1) *host* - é url (*Uniform Resource Locator*) do servidor; 2) *port* - é o número da porta designada para o acesso; 3) *username* - é o nome de usuário; e por fim 4) *password* - é a senha do seu *username*. As informações de acesso ao servidor MQTT precisam ser informadas para que ele possa disponibilizar e receber as informações de pedidos de dados.

Quando o mecanismo recebe um pedido de dados e a informação solicitada não consta na base de dados do usuário, ele então recebe uma notificação. Ao acessar essa notificação, o usuário visualiza esse pedido de dados na forma apresentada pela Figura 4.16a. Nessa visualização, são apresentados primeiramente para o usuário as informações sobre o consumidor de dados, o motivo da solicitação e os atributos que estão sendo solicitados. No caso em que o usuário não tem a informação solicitada, o nível de confiança é inexistente. Para o usuário informar uma decisão em relação a esse dado solicitado, o usuário clica no atributo e outra tela lhe é apresentada. A Figura 4.16b apresenta os detalhes desse atributo e as informações referente a eles.

As informações detalhadas desse atributo são referentes às variáveis descritas na Seção 4.3.2. Nessa tela o usuário possui três opções de escolha, que são refe-

rentes à sua tomada de decisão. Pelo fato de o mecanismo não conter a informação solicitada, se o usuário se escolher aceitar ou negociar, será obrigado a informar esse atributo. Para manter um modelo mental nas escolhas do usuário, optou-se por deixar os botões cada um de uma cada cor (Aceitar = verde, Negar = vermelho e Negociar = amarelo),visando a facilitar a visualização da sua decisão.

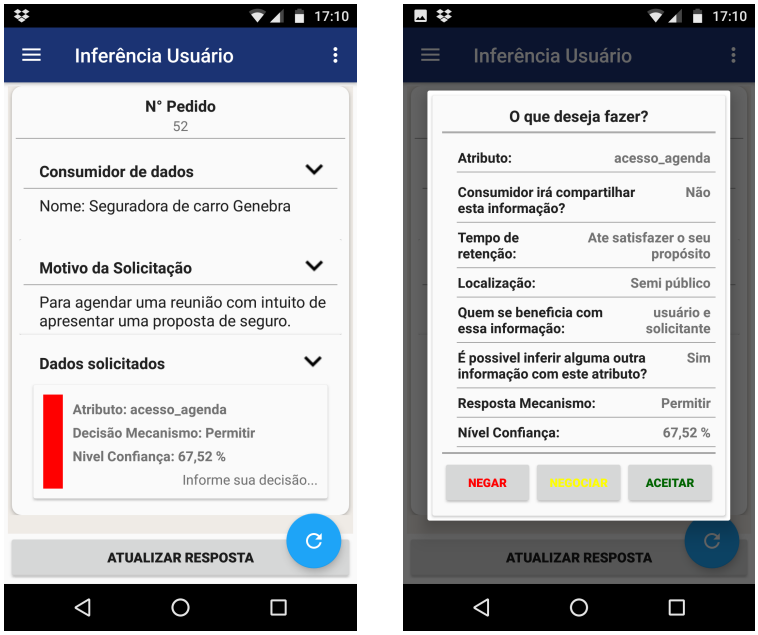


(a) Informações iniciais. (b) Informações detalhadas.

Figura 4.16: Telas das solicitações sem predição.

Nos casos em que a informação solicitada já existe no banco de dados do usuário, esta informação é submetida a um processo de inferência para o próprio mecanismo predizer o resultado da solicitação. No entanto, dependendo do atributo solicitado, o mecanismo não tem confiança o suficiente para responder a essa solicitação. Nesse caso, a solicitação é repassada ao usuário tomar uma decisão em relação a ela. A Figura 4.17a apresenta a tela desse pedido de dados. A diferença dessa tela em relação à tela da Figura 4.16a é que o mecanismo informa ao usuário a sua possível decisão e a sua confiança em relação a essa tomada de decisão.

Nesse caso, quando o usuário visualiza os detalhes desse atributo (Figura 4.17b) não é necessário informar a informação referente a ele, e sim somente a sua escolha de resposta. O mecanismo, disponibilizando a informação da sua possível decisão, passa ao usuário uma perspectiva da sua progressão de aprendizado. Dessa forma, o usuário toma ciência de sua escolha de resultado e consequentemente deve sentir mais confortável com a escolha de decisão do mecanismo.



(a) Informações iniciais. (b) Informações detalhadas.

Figura 4.17: Telas das solicitações com predição.

4.6 Comparação do PrivacyApplication com as ferramentas abordadas nos trabalhos relacionados

Com o desenvolvimento do PrivacyApplication, foi feita uma comparação dos recursos oferecidos por ele em comparação com as ferramentas proposta por Ukil et al. (2012) e Copigneaux (2015). O objetivo desta análise é sintetizar os principais benefícios que são apresentados ao usuário no uso do mecanismo de preservação da privacidade em ambientes de IoT.

A Tabela 4.4 apresenta a comparação dessas ferramentas considerando as características que influenciam os usuários no seu processo de tomada de decisão.

Tabela 4.4: Comparação entre as ferramentas

	Ukil et al. (2012)	**Copigneaux (2015)**	**Privacy Application**
Você pode escolher antecipadamente quais dados os consumidores podem aprender sobre você?	✓	✗	✓
Você pode rastrear quais empresas podem coletar e usar suas informações pessoais?	✓	✓	✓

Você pode controlar quais dados serão coletados pelas empresas?	✓	✓	✓
Você pode ver quais dados já foram divulgados?	✓	×	✓
Você pode saber o motivo da solicitação dos dados?	×	×	✓
Você pode anonimizar / ofuscar as informações que serão disponibilizadas?	✓	×	✓
Você pode controlar as notificações de solicitações de informações?	×	×	✓
Você pode negar os dados solicitados?	✓	✓	✓
Você pode negociar os dados solicitados?	✓	×	✓
Você pode aprender as preferências de privacidade do usuário?	✓	×	✓
Os usuários podem estabelecer um nível de confiança para o mecanismo responder em seu nome?	×	×	✓

A comparação destas ferramentas permite ao usuário verificar as características essenciais que podem influenciá-lo em seu processo de tomada de decisão. Além disso, permite verificar que características importantes que não foram abordadas em outras ferramentas foram contempladas pelo mecanismo aqui proposto.

4.7 Considerações Finais

Neste capítulo foi apresentada, inicialmente uma visão geral do mecanismo e o seu funcionamento. No decorrer do capítulo foi apresentada a arquitetura do mecanismo, demonstrando os métodos de comunicação, as variáveis influentes, o processo de aprendizagem e os métodos de anonimização que foram utilizadas. Por fim, foi apresentada uma aplicação desenvolvida com base nas especificações descritas pelo mecanismo e uma comparação das ferramentas dos trabalhos relacionados em relação ao PrivacyApplication.

No capítulo seguinte serão apresentados uma avaliação da aplicação desenvolvida e os seus respectivos resultados.

Capítulo 5

Experimentos e Resultados

5.1 Considerações Iniciais

Neste Capítulo, é apresentado o experimento realizado com os usuários. O intuito desse experimento foi avaliar a viabilidade e o funcionamento do *PrivacyApplication*. Assim, a Seção 5.2 descreve os detalhes da execução do experimento. A Seção 5.2.1 apresenta a demografia dos usuários que testaram a aplicação. A Seção 5.2.2 apresenta os resultados da análise do processo de aprendizagem. Por fim, a Seção 5.2.3 aborda os resultados da análise do *PrivacyApplication* de modo geral.

5.2 Metodologia empregada para o Experimento de Avaliação do *PrivacyApplication*

Para avaliar o *PrivacyApplication*, foi feito um experimento com os usuários para verificar a viabilidade e o funcionamento. Esse experimento foi aplicado aos alunos do Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de São Carlos.

Os alunos foram convidados por meio de um *e-mail* enviado pelo Departamento de Ciência da Computação e também por intermédio de convites feitos pelos próprios autores. O experimento foi executado individualmente com cada participante e foi dividido em três partes.

- **1ª parte**: os alunos responderam a um questionário demográfico contendo informações para identificar seu perfil;

- **2ª parte**: os alunos foram convidados a usar o *PrivacyApplication*;
- **3ª parte**: os alunos responderam aos questionários referentes ao uso do *PrivacyApplication*.

Na 1ª parte do experimento, foi aplicado aos alunos um questionário contendo informações para identificar a demografia da população foi aplicado aos alunos (Apêndice B). Na 2° parte, os alunos foram convidados a usar o *PrivacyApplication* e foram submetidos a vários cenários que poderiam ocorrer em ambientes IoT. Um total de 63 cenários foram aplicados e estava no formato de vinhetas, que são como histórias curtas sobre personagens hipotéticos em circunstâncias específicas - vide Naeini et al. (2017). As vinhetas utilizadas são descritas no apêndice C, sendo que um deles é apresentado a seguir como ilustração.

"O seu local de trabalho quer acesso à sua agenda para marcar uma reunião. A informação será mantida até seu propósito ser concluído e não será compartilhada com terceiros."

Após responder às questões de todos os cenários da 2° parte, os usuários foram submetidos aos questionários referentes à 3° parte do experimento. Dois questionários foram aplicados na 3° parte do experimento. O primeiro questionário reporta às respostas fornecidas pelo processo de aprendizagem do mecanismo (exemplo no Apêndice D) e o segundo questionário trata da usabilidade e viabilidade do PrivacyApplication (descrito no Apêndice E).

5.2.1 Demografia dos participantes do experimento

Os participantes da pesquisa foram alunos de Pós-Graduação de Ciência da Computação da Universidade Federal de São Carlos (PPGCC). Ao todo 20 alunos participaram do experimento e, por estarem cursando uma pós-graduação foram considerados como especialista no tema avaliado. Esse valor representa 17,54% do total da população, que corresponde aos alunos matriculados no PPGCC.

A Tabela 5.1 apresenta a demografia dos participantes, sendo que 17 são brasileiros, 1 colombiano, 1 peruano e 1 paraguaio. O sexo masculino corresponde a 70% dos pesquisados e o feminino 30%.

Tabela 5.1: Demografia dos participantes do experimento.

Nacionalidade	**Participantes**	**Porcentagem (%)**
Brasileiros	17	85%
Outros	3	15%
Sexo	**Participantes**	**Porcentagem (%)**
Masculino	14	70%
Feminino	6	30%

5.2.2 Resultados da Avaliação do Processo de Aprendizagem

Para avaliar a capacidade do processo de aprendizagem do mecanismo proposto, foi realizada uma avaliação manual do usuários. Nessa avaliação foi apresentado ao usuário cada um dos cenários que tiveram ações tomadas automaticamente pelo processo de aprendizagem. Foi então solicitado ao usuário, tido como um especialista, que assinalasse se a tomada de decisão feita pelo mecanismo foi correta ou não. Caso a decisão do mecanismo fosse incorreta, o usuário informava a sua decisão para aquele determinado cenário. O Apêndice D ilustra um exemplo dos cenários que foi apresentados aos participantes para que pudessem avaliar a tomada de decisão feita pelo mecanismo.

As respostas fornecidas pelos usuários foram sistematizadas e apresentadas na Tabela 5.2. Os nomes dos participantes foram ocultados para preservar a sua privacidade. A coluna 2 apresenta o nível de confiança que foi especificado pelo usuário no *PrivacyApplication*. Conforme apresentado na Seção 4.3.3, o nível de confiança é utilizado como um parâmetro para medir a aceitabilidade de uma inferência feito pelo processo de aprendizagem e fornece ao usuário uma confiança nas respostas inferidas em seu nome.

A coluna 3 apresenta a quantidade de cenários que foram respondidos pelo processo de aprendizagem do mecanismo. Pode-se verificar que esse número variou de participante para participante, pois para alguns houve mais previsões e para outro menos. Essa variação de quantidade de cenários preditos tem relação com o nível de confiança que foi definido pelo usuário.

Após a aplicação do questionário contendo os cenários que foram respondidos automaticamente, foi possível verificar a quantidade de cenários que o mecanismo respondeu de forma errônea. A coluna 4 apresenta a quantidade de cenários que foram respondidos erroneamente e a coluna 5 apresenta um percentual da quan-

tidade de acerto obtidos pelo mecanismo, comparado com a resposta dada pelo usuário especialista.

Tabela 5.2: Dados do questionário avaliado.

Participantes	Nível de confiança	Qtd. Cenários Preditos	Qtd. Cenários Preditos Errados	Acertos %
Participante 1	75%	26	3	88,4615%
Participante 2	75%	22	2	90,9090%
Participante 3	70%	23	3	86,9565%
Participante 4	50%	18	2	88,8888%
Participante 5	75%	15	3	80%
Participante 6	98%	7	0	100%
Participante 7	50%	36	5	86,1111%
Participante 8	74%	35	4	88,5714%
Participante 9	75%	29	3	89,6551%
Participante 10	90%	8	2	75%
Participante 11	90%	9	2	77,7777%
Participante 12	50%	23	2	91,3043%
Participante 13	50%	16	2	87,5%
Participante 14	95%	8	1	87,5%
Participante 15	80%	9	2	77,7777%
Participante 16	65%	31	3	90,3225%
Participante 17	75%	23	2	91,3043%
Participante 18	85%	30	1	96,6666%
Participante 19	90%	24	2	91,6666%
Participante 20	90%	21	3	85,7142%

Analisando os resultados das predições de informações de todos os participantes, obtivemos uma precisão de 88,62% dos cenários preditos. Esse resultado foi calculado com base no total da quantidade de cenários previstos de forma errônea dividido pela quantidade total de cenários preditos. A Fórmula abaixo apresenta como é feito esse cálculo.

$$100 - ((\sum Qtd_Erro) * 100) / \sum Qtd_Cenarios_Preditos) \quad (5.1)$$

Conforme apresentado pela Figura 5.1, ao todo 63 cenários foram aplicados aos participantes. Destes, o mecanismo previu em nome do usuário uma média de 20,65 cenários, o que corresponde a 32,77% do total de cenários aplicados. Desses 20,65 cenários preditos, uma média de 2,34 cenários foram preditas de maneira errônea pelo mecanismo, constituindo um percentual de 11,38%.

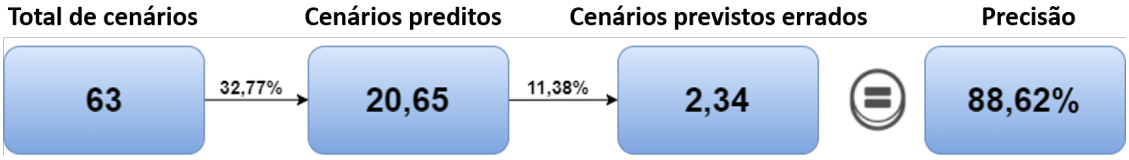


Figura 5.1: Análise dos resultados das predições.

De modo geral, o *PrivacyApplication* obteve em média um percentual de acerto de 88,62% nos cenários preditos. O resultado obtido é muito satisfatório e, de certa forma, esperado. Isso porque o mecanismo permite ao usuário definir um nível de confiança nas respostas inferidas em seu nome, e quanto maior o nível de confiança, maior será a precisão do mecanismo.

Em geral, o nível de confiança estipulado pelos usuários foi de 75,1%. Com isso, ao analisarmos os resultados individuais (Figura 5.2), percebemos que, quanto maior o nível de confiança estipulado pelo usuário, menor é a quantidade de cenários previstos. Isso se justifica pelo fato de que, quanto maior a confiança, mais cenários se fazem necessários para treinar o modelo de aprendizagem. Consequentemente, os usuários que definiram sua confiança baixa tiveram mais cenários previstos.

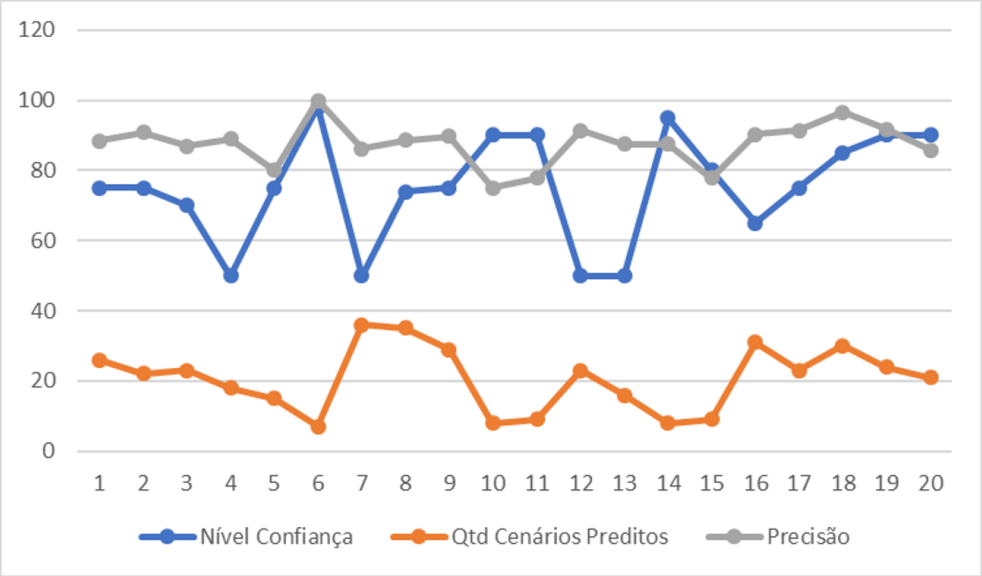


Figura 5.2: Relação individual do número de cenários preditos de cada participante.

A precisão obtida pelo *PrivacyApplication* em comparação com os resultados do trabalho de Naeini et al. (2017), mostrou que utilizar uma ferramenta de preservação de privacidade individual proporciona um ganho muito significativo, pois o modelo de predição de dados é baseado somente em informações disponibilizadas pelo usuário e não leva em consideração informações de terceiros. Com isso, as informações preditas pelo processo de aprendizagem são mais eficientes e correspondem exatamente com às suas preferências de privacidade do usuário.

5.2.3 Usabilidade e Aceitabilidade do *PrivacyApplication*

O segundo questionário da 3° parte do experimento foi aplicado para verificar a usabilidade e aceitabilidade do *PrivacyApplication*. O questionário aplicado aos participantes pode ser visualizado no apêndice E.

A usabilidade do *PrivacyApplication* foi avaliada sendo que 80% das respostas concordaram que a "A usabilidade do *PrivacyApplication* é fácil". A Figura 5.3 apresenta os percentuais dados pelos respondentes em formato de gráfico pizza.

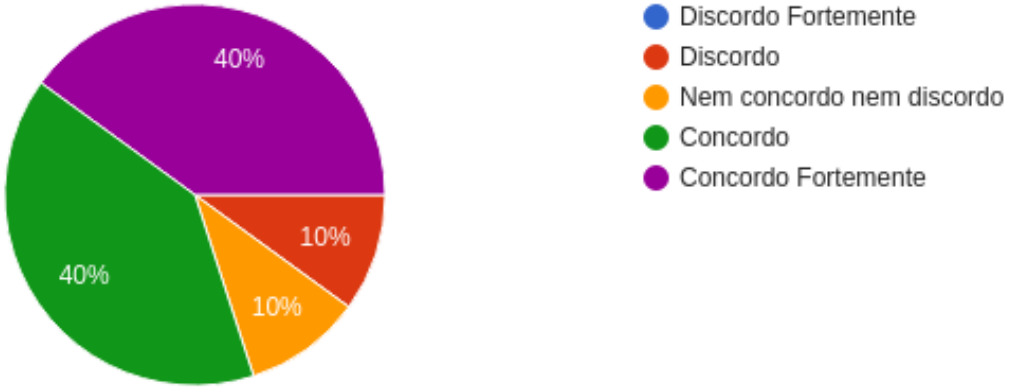


Figura 5.3: P1 - A usabilidade do *PrivacyApplication* é fácil.

A Figura 5.4 refere-se à compreensão das informações apresentadas pelo *PrivacyApplication*. Dentre os pesquisados, 85% concordaram que "As informações apresentadas pelo *PrivacyApplication* é de fácil compreensão". Apenas 5% discordaram e os 10% restantes nem concordaram e nem discordaram.

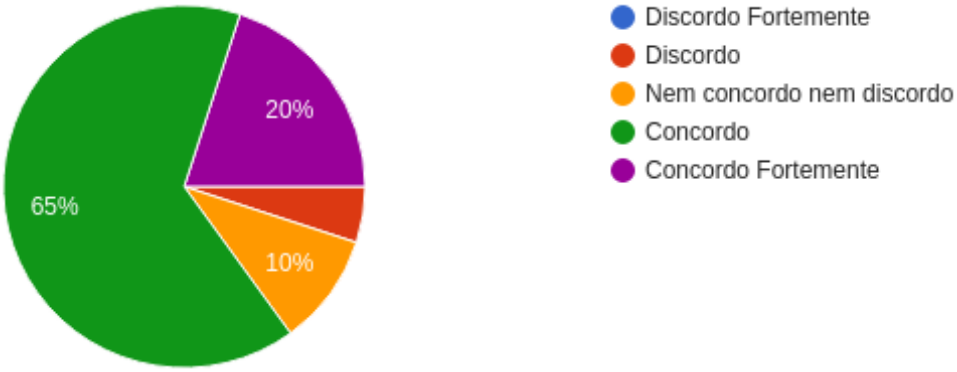


Figura 5.4: P2 - As informações apresentadas pelo *PrivacyApplication* é de fácil compreensão.

A utilidade do *PrivacyApplication* quanto a responder em nome do usuário foi avaliada pelos participantes. A Figura 5.5 apresenta os dados referentes à seguinte afirmação "É útil utilizar o *PrivacyApplication* em ambientes inteligentes para responder em seu nome". Nesta avaliação, 65% dos participantes concordaram que essa funcionalidade é útil e 5% discordaram. Os outros 30% dos participantes não tiveram uma opinião.

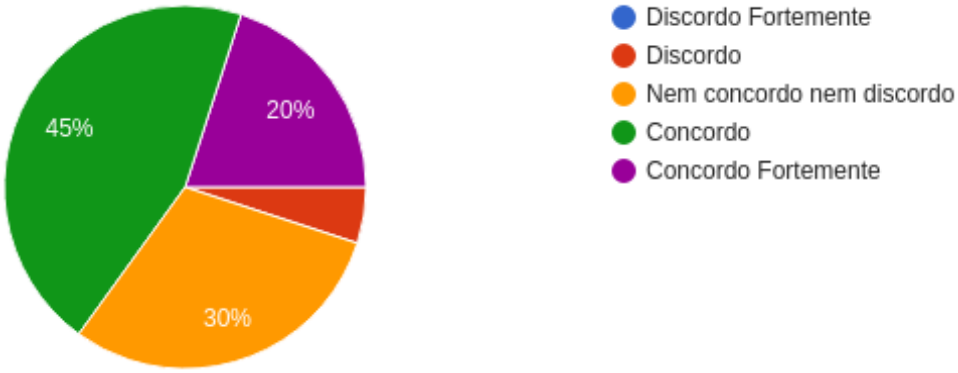


Figura 5.5: P3 - É útil utilizar o *PrivacyApplication* em ambientes inteligentes para responder em seu nome.

As respostas que foram dadas em nome do usuário também foram avaliadas pelos respondentes. A Figura 5.6 apresenta os resultados da seguinte afirmação "As solicitações respondidas automaticamente pelo App te traz resultados satisfatórios". Um total de 95% concordou fortemente ou simplesmente concordou que as informações são satisfatórias. Nenhum dos participantes discordou dessa afirmação e apenas 5% não tiveram uma opinião.

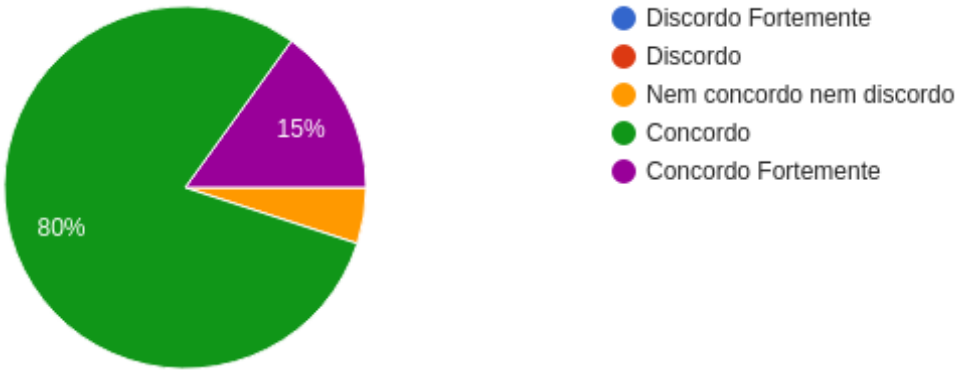


Figura 5.6: P4 - As solicitações respondidas automaticamente pelo App te trazem resultados satisfatórios.

Os métodos de anonimização que foram utilizados no mecanismo e avaliados pela pesquisa descrita na Seção 3 foram reavaliados após o uso do *PrivacyApplication*. A Figura 5.7 apresenta os resultados dessa reavaliação. Um total de 65% dos participantes concordou que esses métodos são adequados, 10% discordaram e outros 25% não tiveram uma opinião.

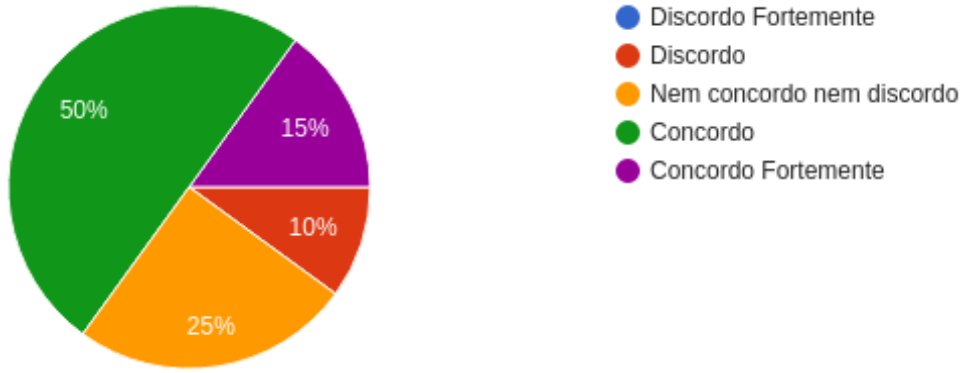


Figura 5.7: P5 - Você considera os métodos de anonimização adequados para anonimizar as suas informações pessoais.

Com o intuito de verificar o benefício do *PrivacyApplication* em um contexto geral, a seguinte afirmação foi submetida aos participantes: “Utilizar o *PrivacyApplication* te traz algum benefício relevante". Um total de 85% dos respondentes concordou que o PrivacyApplication traz benefícios relevantes, 10% não tiveram opinião e outros 5% discordaram.

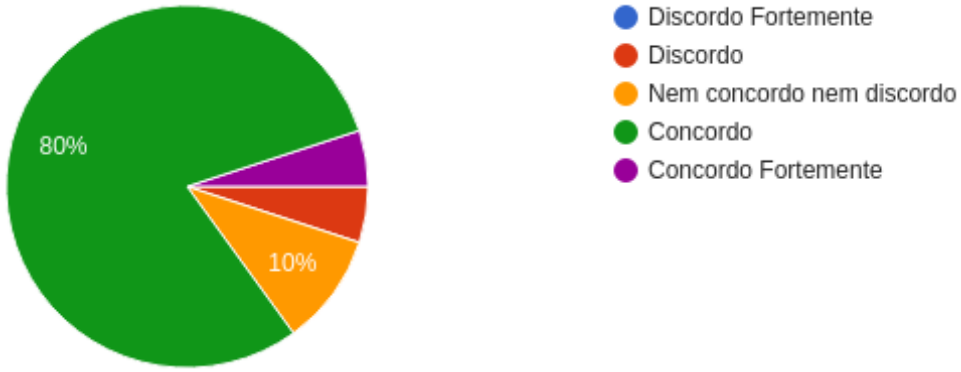


Figura 5.8: P6 - Utilizar o *PrivacyApplication* te traz algum beneficio relevante.

Em um ambiente IoT, várias interações e solicitações de informação acontecem a todo momento. Essas interações podem ser rotineiras e ocupar muito tempo do usuário. Diante disso, verificou-se junto aos usuários se a utilização do *PrivacyApplication* nesses ambientes reduziria o seu tempo de interação com esses dispositivos (Figura 5.9). Um total de 90% dos respondentes concordou que essa utilização reduz o tempo de interação e os outros 10% discordaram .

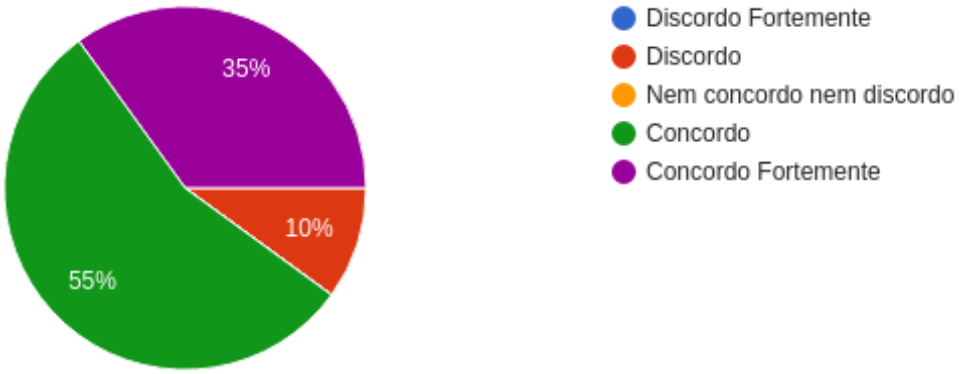


Figura 5.9: P7 - Em ambientes nos quais existem muitas interações entre dispositivos IoT, a utilização do *PrivacyApplication* minimizaria o seu tempo de interação com esses dispositivos.

Por fim, verificou-se com os participantes se o aplicativo apresentado é uma boa ideia. A Figura 5.10 apresenta os resultados obtidos junto aos respondentes. Um total de 95% dos alunos concordou que o *PrivacyApplication* é uma boa ideia e os 5% não tiveram uma opinião sobre essa afirmação.

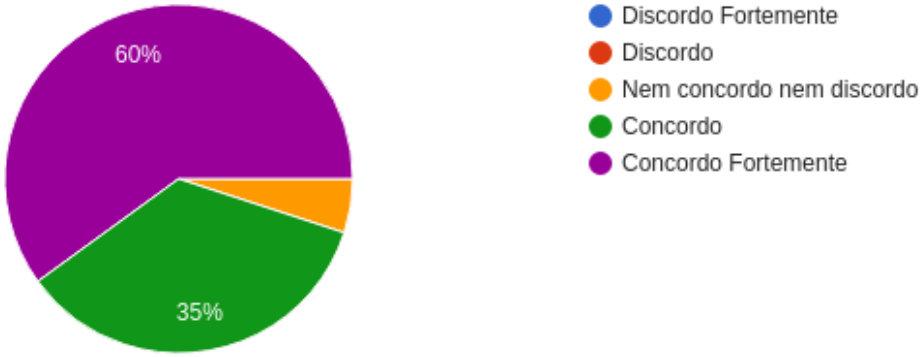


Figura 5.10: P8 - O App apresentado é uma boa ideia.

Com base nos resultados dessa avaliação, pode-se concluir que as funcionalidades disponíveis no *PrivacyApplication* foram aceitas pelos pesquisados. As informações apresentadas foram compreensíveis e a usabilidade foi considerada fácil pela maioria dos participantes.

5.3 Considerações Finais

Neste Capítulo foram apresentados os resultados do experimento feito com os usuários. Nesse experimento, os alunos utilizaram o *PrivacyApplication* e respon-

deram aos questionários referentes ao processo de aprendizagem e sobre a usabilidade e aceitabilidade do *PrivacyApplication*.

Os resultados do modelo de aprendizagem utilizado pelo *PrivacyApplication* foram bem significativos, alcançando uma precisão de 88,62% de acerto nos cenários preditos. Esse resultado é satisfatório e corresponde exatamente às preferências de privacidade do usuário, pois o processo de aprendizado é baseado somente nas informações disponibilizadas por ele, não levando em consideração informações de terceiros.

Fez-se, também, uma análise da usabilidade e aceitabilidade do aplicativo. De modo geral, os participantes consideraram o *PrivacyApplication* uma aplicação de fácil utilização, com as informações apresentadas de forma coesas e com resultados úteis e satisfatórios. Uma avaliação geral das respostas dadas pelos participantes nas afirmações apresentadas indica que, um total de 81,25% concordou, 4,375% discordaram e 14,375% nem concordaram e nem discordaram. Esse resultado evidencia que o *PrivacyApplication* teve uma boa aceitação por parte dos usuários participantes.

Capítulo 6

Conclusões e Trabalhos Futuros

6.1 Conclusões

Este trabalho apresentou um mecanismo de preservação de privacidade para ambientes IoT. O objetivo deste mecanismo é mediar as trocas de informações que ocorrem nesses ambientes visando a fornecer ao usuário a capacidade de controlar a divulgação de seus dados.

A concepção deste trabalho foi motivada pela perda do controle, por parte do usuário na divulgação de suas informações, dada a crescente interação com os ambientes inteligentes. Essa falta de controle leva o usuário a divulgar as suas informações privadas de forma descontrolada e isto acaba afetando a sua privacidade.

A proposta do mecanismo de preservação de privacidade considerou o estado da arte na literatura e se deu por meio de uma consulta a uma amostra de usuários, que evidenciaram as características essenciais na divulgação de uma informação. A implementação do mecanismo foi feita com o recurso a um aplicativo que considerou também a usabilidade na disponibilização dos dados pessoais.

O mecanismo proposto foi desenvolvido como um aplicativo móvel para facilitar a interação do o usuário com os dispositivos IoT. Para testar a aplicação denominado *PrivacyApplication* foi feito um experimento com os usuários para avaliar as suas funcionalidade, assim como, as suas interfaces. Nesta avaliação, os usuários foram submetidos a vários cenários para simular um ambiente inteligente.

Os resultados indicaram que os usuários se sentem confortáveis com as informações apresentadas pelo *PrivacyApplication* e que as funcionalidades disponibilizadas são relevantes e os deixam mais seguros na disponibilização de seus dados.

O processo de aprendizagem, disponibilizado pelo mecanismo e implementado pelo aplicativo obteve uma média de acerto de 88,62% dos cenários previstos. A adição de mais cenários nos testes pode aumentar a acurácia desse processo de aprendizagem.

6.2 Sugestões para trabalhos futuros

Em trabalhos futuros pretendemos adicionar a sensibilidade ao contexto das informações, pois conforme evidenciado por Schaub et al. (2012), a mudança de contexto pode alterar uma decisão do usuário.

Pretendemos também por meio de novas pesquisas ampliar o conjunto de variáveis influentes para proporcionar aos usuários um melhor entendimento sobre a divulgação de seus dados. Buscaremos novas abordagens para o processo de aprendizagem, visando a aumentar a acurácia das respostas fornecidas automáticas pelo mecanismo.

Por meio de novas pesquisas, pretendemos também verificar se o nível de confiança definido como um parâmetro no mecanismo é suficiente para fornecer as respostas no nome do usuário.

6.3 Trabalhos Publicados

Durante o desenvolvimento deste trabalho o seguinte artigo foi publicado:

1. Couto, F. R., Zorzo, S. D. "*Privacy Negotiation Mechanism in Internet of Things Environments*", The 24th Americas Conference on Information Systens(AMCIS), 16 a 18 de Agosto de 2018 em Nova Orleans, Louisiana.

Referências

ALABA, F. A. et al. Internet of things security: A survey. *Journal of Network and Computer Applications*, v. 88, p. 10–28, 2017. ISSN 1084-8045. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1084804517301455>.

ANTUNES, J. B. et al. Maniot: Uma plataforma para gerenciamento de dispositivos da internet das coisas. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, 2016. Disponível em: <https://goo.gl/dijmYo>.

ASHTON, K. That "internet of things"thing: In the real world things matter more than ideas. *RFID Journal*, 2009. Disponível em: <http://www.rfidjournal.com/articles/view?4986>.

ATZORI, L.; IERA, A.; MORABITO, G. The internet of things: A survey. *Comput. Netw.*, Elsevier North- Holland, Inc., New York, NY, USA, v. 54, n. 15, p. 2787–2805, out. 2010. ISSN 1389-1286. Disponível em: <http://dx.doi.org/10.1016/j.comnet.2010.05.010>.

BARNAGHI, P.; SHETH, A. *The Internet of Things: The Story So Far*. 2014. Disponível em: <https://goo.gl/ir4AQw>.

BARUA, D.; KAY, J.; PARIS, C. Viewing and controlling personal sensor data: What do users want? In: BERKOVSKY, S.; FREYNE, J. (Ed.). *Persuasive Technology*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. p. 15–26. ISBN 978-3-642-37157-8.

BOJANOVA, I.; HURLBURT, G.; VOAS, J. Imagineering an internet of anything. *Computer*, v. 47, n. 6, p. 72–77, 2014. ISSN 0018-9162.

BONEH, D.; BOYEN, X.; SHACHAM, H. Short group signatures. In: _____. *24th Annual International Cryptology Conference*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004. p. 41–55. ISBN 978-3-540-28628-8. Disponível em: <https://goo.gl/KSuawh>.

BUJARI, A.; PALAZZI, C. E. Opportunistic communication for the internet of everything. In: *2014 IEEE 11th Consumer Communications and Networking Conference*. [S.l.: s.n.], 2014. p. 502–507. ISSN 2331-9852.

CLARKE, W. *Introduction to Dataveillance and Information Privacy, and Definitions and Terms*. [s.n.], 1999. Disponível em: <https://goo.gl/ZGT901>.

COMMISSION, E. Internet of things in 2020: A road map for the future. *RFID Working Group of the European Technology*, 2008. Acesso em: 20/04/2017. Disponível em: <https://goo.gl/q51UpK>.

COPIGNEAUX, B. Semi-autonomous, context-aware, agent using behaviour modelling and reputation systems to authorize data operation in the internet of things. *CoRR*, abs/1505.07239, 2015. Disponível em: <http://arxiv.org/abs/1505.07239>.

DELERABLÉE, C.; POINTCHEVAL, D. Dynamic fully anonymous short group signatures. In: _____. *First International Conference on Cryptology in Vietnam*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006. p. 193–210. ISBN 978-3-540-68800-6. Disponível em: <https://goo.gl/twnrsQ>.

DRISS, S. B. et al. *A comparison study between MLP and convolutional neural network models for character recognition*. 2017. 10223–10223 p. Disponível em: <https://doi.org/10.1117/12.2262589>.

ETZION, O.; FOURNIER, F.; ARCUSHIN, S. Tutorial on the internet of everything. In: *Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems*. New York, NY, USA: ACM, 2014. (DEBS '14), p. 236–237. ISBN 978-1-4503-2737-4. Disponível em: <http://doi.acm.org/10.1145/2611286.2611308>.

EVANS, D. *The Internet of Things How the Next Evolution of the Internet Is Changing Everything*. 2011. Acesso em: 20/04/2017. Disponível em: <https://goo.gl/9wmOLM>.

FISCHER, H. A history of the central limit theorem: from classical to modern probability theory. In: . [S.l.]: Springer-Verlag New York, 2011. p. 402. ISBN 978-0-387-87856-0.

FOOTE, K. D. *A Brief History of the Internet of Things*. 2016. Acesso em: 20/04/2017. Disponível em: <https://goo.gl/nvudPG>.

GARCíA, C. G. et al. A review about smart objects, sensors, and actuators. *International Journal of Interactive Multimedia and Artificial Intelligence*, v. 4, n. 3, p. 7–10, 03/2017 2017. ISSN 1989-1660.

GHANI, N. A.; SIDEK, Z. M. Controlling your personal information disclosure. In: *Proceedings of the 7th WSEAS International Conference on Information Security and Privacy*. Stevens Point, Wisconsin, USA: World Scientific and Engineering Academy and Society, 2008. (ISP'08), p. 23–27. ISBN 978-960-474-048-2. Disponível em: <https://goo.gl/gxYQFM>.

GOYAL, V. et al. Attribute-based encryption for fine-grained access control of encrypted data. In: *Proceedings of the 13th ACM Conference on Computer and Communications Security*. New York, NY, USA: ACM, 2006. (CCS '06), p. 89–98. ISBN 1-59593-518-5. Disponível em: <https://goo.gl/Q0kDz1>.

GUO, K.; TANG, Y.; ZHANG, P. Csf: Crowdsourcing semantic fusion for heterogeneous media big data in the internet of things. *Information Fusion*, v. 37, p. 77–85, 2017. ISSN 1566-2535. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1566253517300702>.

GURSES, S. F.; BERENDT, B.; SANTEN, T. Multilateral security requirements analysis for preserving privacy in ubiquitous environments. *ECML/PKDD location:Berlin, Germany date:September, 2006*, 2006. Disponível em: <https://goo.gl/41pBnk>.

HAJNY JANAND MALINA, L. Unlinkable attribute-based credentials with practical revocation on smart-cards. In: _____. *Smart Card Research and Advanced Applications: 11th International Conference*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. p. 62–76. ISBN 978-3-642-37288-9. Disponível em: <https://goo.gl/IPwm7N>.

HERNáNDEZ-RAMOS, J. L. et al. Safir: Secure access framework for iot-enabled services on smart buildings. *Journal of Computer and System Sciences*, v. 81, n. 8, p. 1452–1463, 2015. ISSN 0022-0000. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0022000014001858>.

KARKOUCH, A. et al. Data quality enhancement in internet of things environment. In: *2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA)*. [S.l.: s.n.], 2015. p. 1–8.

KERR, I. R. The internet of people? reflections on the future regulation of human-implantable radio frequency identification. Feb 2013. Disponível em: <https://ssrn.com/abstract=2225565>.

KLASNJA, P. et al. Exploring privacy concerns about personal sensing. In: TOKUDA, H. et al. (Ed.). *Pervasive Computing*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. p. 176–183. ISBN 978-3-642-01516-8.

LARMAN, C. *Utilizando UML e padrões: uma introdução à análise e ao projeto orientados a objetos e ao processo unificado*. [S.l.]: Porto Alegre: Bookman, 2006.

LEDERER, S.; MANKOFF, J.; DEY, A. K. Who wants to know what when? privacy preference determinants in ubiquitous computing. In: *CHI '03 Extended Abstracts on Human Factors in Computing Systems*. New York, NY, USA: ACM, 2003. (CHI EA '03), p. 724–725. ISBN 1-58113-637-4. Disponível em: <http://doi.acm.org/10.1145/765891.765952>.

LEE, H.; KOBSA, A. Understanding user privacy in internet of things environments. In: *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*. [S.l.: s.n.], 2016. p. 407–412.

LEE, H.; KOBSA, A. Privacy preference modeling and prediction in a simulated campuswide iot environment. In: *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. [S.l.: s.n.], 2017. p. 276–285.

LEON, P. G. et al. What matters to users?: factors that affect users' willingness to share information with online advertisers. In: BERKOVSKY, S.; FREYNE, J. (Ed.). *In Proceedings of the ninth symposium on usable privacy and security*. Newcastle, UK: Springer Berlin Heidelberg, 2013.

LI, F.; ZHENG, Z.; JIN, C. Secure and efficient data transmission in the internet of things. *Telecommunication Systems*, v. 62, n. 1, p. 111–122, 2016. ISSN 1572-9451. Disponível em: <https://goo.gl/fX6qec>.

MALINA, L. et al. On perspective of security and privacy-preserving solutions in the internet of things. *Computer Networks*, v. 102, p. 83–95, 2016. ISSN 1389-1286. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1389128616300779>.

MINERVA, R.; BIRU, A.; ROTONDI, D. Towards a definition of the internet of things (iot). In: *IEEE Internet of Things*. [s.n.], 2015. Disponível em: <https://goo.gl/myhPD2>.

MIORANDI, D. et al. Internet of things. *Ad Hoc Netw.*, Elsevier Science Publishers B. V., Amsterdam, The Netherlands, The Netherlands, v. 10, n. 7, p. 1497–1516, set. 2012. ISSN 1570-8705. Disponível em: <http://dx.doi.org/10.1016/j.adhoc.2012.02.016>.

MOHAMED, H. et al. *Assessment of Artificial Neural Network for bathymetry estimation using High Resolution Satellite imagery in Shallow Lakes: Case Study El Burullus Lake*. March 2015. 1–11 p.

MQTT. *MQTT.ORG*. 2018. Acesso em: 2018-05-01. Disponível em: <http://mqtt.org/>.

NAEINI, P. E. et al. Privacy expectations and preferences in an iot world. In: *in Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. [s.n.], 2017. Disponível em: <https://www.usenix.org/system/files/conference/soups2017/soups2017-naeini.pdf>.

NELSON, G. S. *Practical Implications of Sharing Data: A Primer on Data Privacy, Anonymization, and De-Identification*. Abril 2015. 1–23 p. Disponível em: <https://support.sas.com/resources/papers/proceedings15/1884-2015.pdf>.

O'LEARY, D. E. 'big data', the 'internet of things' and the 'internet of signs'. *Intelligent Systems in Accounting, Finance and Management*, v. 20, n. 1, p. 53–65, 2013. ISSN 1099-1174. Disponível em: <http://dx.doi.org/10.1002/isaf.1336>.

ORIWOH, E.; CONRAD, M. 'things' in the internet of things: Towards a definition. *International Journal of Internet of Things*, v. 4, p. 1–5, 2015. ISSN 1566-2535. Disponível em: <https://goo.gl/VF8bDT>.

ORTMANN, S.; LANGENDöRFER, P.; MAASER, M. A self-configuring privacy management architecture for pervasive systems. In: *Proceedings of the 5th ACM International Workshop on Mobility Management and Wireless Access*. New York, NY, USA: ACM, 2007. (MobiWac '07), p. 184–187. ISBN 978-1-59593-809-1. Disponível em: <http://doi.acm.org/10.1145/1298091.1298125>.

PAILLIER, P. Public-key cryptosystems based on composite degree residuosity classes. In: _____. *International Conference on the Theory and Application of Cryptographic Techniques Prague*. Berlin, Heidelberg: Springer Berlin

Heidelberg, 1999. p. 223–238. ISBN 978-3-540-48910 -8. Disponível em: <https://goo.gl/lmzgGe>.

PALLAPA, G.; KUMAR, M.; DAS, S. K. Privacy infusion in ubiquitous computing. In: *2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking Services (MobiQuitous)*. [S.l.: s.n.], 2007. p. 1–8.

PERERA, C. et al. Context aware computing for the internet of things: A survey. *IEEE Communications Surveys Tutorials*, v. 16, n. 1, p. 414–454, First 2014. ISSN 1553-877X.

PöHLS, H. C. Json sensor signatures (jss): End-to-end integrity protection from constrained device to iot application. In: *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. [S.l.: s.n.], 2015. p. 306–312.

RAZZAQUE, M. A. et al. Middleware for internet of things: A survey. *IEEE Internet of Things Journal*, v. 3, n. 1, p. 70–95, Feb 2016. ISSN 2327-4662.

ROGERS, Y. Moving on from weiser's vision of calm computing: Engaging ubicomp experiences. In: *Proceedings of the 8th International Conference on Ubiquitous Computing*. Berlin, Heidelberg: Springer-Verlag, 2006. (UbiComp'06), p. 404–421. ISBN 978-3-540-39634-5. Disponível em: <https://goo.gl/9GDNqY>.

ROSA, T. A. *Modelo de compartilhamento de localização em redes sociais móveis com garantias de privacidade*. Dissertao (Mestrado) — Universidade Federal de São Carlos, 2015. Disponível em: <https://repositorio.ufscar.br/handle/ufscar/7058>.

ROSE, K.; ELDRIDGE, S.; CHAPIN, L. The internet of things (iot): An overview. 2015. Disponível em: <https://goo.gl/wTR5FA>.

ROUSE, M. *Definition IoT device*. 2017. Acesso em: 20/04/2017. Disponível em: <https://goo.gl/jMH8zz>.

SCHAUB, F. et al. Privacy context model for dynamic privacy adaptation in ubiquitous computing. In: *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. New York, NY, USA: ACM, 2012. (UbiComp '12), p. 752–757. ISBN 978-1-4503-1224-0. Disponível em: <https://goo.gl/ZpWypO>.

SFAR, A. R. et al. A roadmap for security challenges in internet of things. *Digital Communications and Networks*, 2017. ISSN 2352-8648. Disponível em: <http://www.sciencedirect.com/science/article/pii/S2352864817300214>.

TAN, L.; WANG, N. Future internet: The internet of things. In: *2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)*. [S.l.: s.n.], 2010. v. 5, p. 376–380. ISSN 2154-7491.

UKIL, A. et al. Negotiation-based privacy preservation scheme in internet of things platform. In: *Proceedings of the First International Conference on Security of Internet of Things*. New York, NY, USA: ACM, 2012. (SecurIT '12), p. 75–84. ISBN 978-1-4503-1822-8. Disponível em: <http://doi.acm.org/10.1145/2490428.2490439>.

WARREN, S. D.; BRANDEIS, L. D. The right to privacy. *Harvard Law Review*, The Harvard Law Review Association, v. 4, n. 5, p. 193–220, 1890. ISSN 0017811X. Disponível em: <http://www.jstor.org/stable/1321160>.

WEBER, R. H. Internet of things: Privacy issues revisited. *Computer Law & Security Review*, v. 31, n. 5, p. 618–627, 2015. ISSN 0267-3649. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0267364915001156>.

WEISER, M. The computer for the 21st century. *SIGMOBILE Mob. Comput. Commun. Rev.*, ACM, New York, NY, USA, v. 3, n. 3, p. 3–11, jul. 1999. ISSN 1559-1662. Disponível em: <http://doi.acm.org/10.1145/329124.329126>.

WESTIN, A. *Privacy and Freedom*. Atheneum, 1967. Disponível em: <https://goo.gl/Ycuj8d>.

YAN, Z.; ZHANG, P.; VASILAKOS, A. V. A survey on trust management for internet of things. *Journal of Network and Computer Applications*, v. 42, p. 120–134, 2014. ISSN 1084-8045. Disponível em: <http://www.sciencedirect.com/science/article/pii/S1084804514000575>.

Glossário

ACL – *Acess Control List*

IoE – *Internet of Everything*

IoT – *Internet of Things*

JSON – *JavaScript Object Notation*

M2M – *Machine-to-Machine*

MLP – *Multilayer Perceptron*

QoS – *Quality of Service*

RAM – *Random Access Memory*

RFID – *Radio-Frequency Identification*

TLS – *Transport Layer Security*

UML – *Unified Modeling Language*

URI – *Uniform Resource Identifier*

WSANs – *Wireless Sensor and Actor Networks*

Apendice A

Questionário do levantamento da abordagem

1) Qual a sua nacionalidade?
( ) Brasil Outros:_____

2) Sexo:
( ) Masculino ( ) Feminino

3) Nível de escolaridade:
( ) Graduado ( ) Graduando ( ) Pós Graduado ( ) Pós Graduando

4) Qual é a sua faixa etária?
( ) Abaixo de 18 anos ( ) Entre 21 a 29 anos ( ) 60 ou mais
( ) Entre 18 e 20 anos ( ) Entre 40 a 49 anos
( ) Entre 30 a 39 anos ( ) Entre 50 a 59 anos

5) Aproximadamente, quantas horas você passa utilizando computadores ou outros dispositivos?
( ) Nenhuma ( ) 4 a 6 horas ( ) 13 a 17 horas
( ) 1 a 2 horas ( ) 6 a 9 horas ( ) Mais de 17 horas
( ) 2 a 4 horas ( ) 9 a 13 horas

6) **Qual é o nível de conhecimento que você se considera em relação ao uso da internet em geral?**

( ) Especialista ( ) Experiente ( ) Intermediário ( ) Amador ( )Iniciante

7) Indique se as seguintes afirmações te influenciaria em um processo de tomada de decisão. **Eu estaria mais disposto a permitir a coleta de informações pessoais(ou seja, informações que podem ser usadas para me identificar e me contatar) se de alguma forma..**.

a) **...me permitisse escolher antecipadamente o que as empresas podem aprender sobre mim.**
( ) Influenciaria ( ) Não sei ou não tenho opinião ( ) Não influenciaria

b) **...me permitisse controlar quais empresas podem coletar e usar essas informações.**
( ) Influenciaria ( ) Não sei ou não tenho opinião ( ) Não influenciaria

c) **...me permitisse visualizar o que as empresas já conhecem sobre mim.**
( ) Influenciaria ( ) Não sei ou não tenho opinião ( ) Não influenciaria

d) **...me permitisse controlar quais dados serão coletados.**

( ) Influenciaria ( ) Não sei ou não tenho opinião ( ) Não influenciaria

8) Quanto você concorda ou discorda das seguintes afirmações:

a) **Quando algum dispositivo IoT me solicita informações pessoais, costumo pensar duas vezes em fornecer isso.**

( )	( )	( )	( )	( )
Concordo fortemente	Concordo	Nem concordo nem discordo	Discordo	Discordo fortemente

b) **Você acha que tendo um mecanismo que responda em seu nome, você perde o controle sobre as suas informações.**

( )	( )	( )	( )	( )
Concordo fortemente	Concordo	Nem concordo nem discordo	Discordo	Discordo fortemente

c) **Eu sinto que os sites que eu visito sabem mais sobre mim do que eu estou confortável.**

( )	( )	( )	( )	( )
Concordo fortemente	Concordo	Nem concordo nem discordo	Discordo	Discordo fortemente

d) **A maioria dos sites/dispositivos lidam com informações pessoais coletadas de forma correta e confidencial.**

( )	( )	( )	( )	( )
Concordo fortemente	Concordo	Nem concordo nem discordo	Discordo	Discordo fortemente

9) A tabela abaixo apresenta as variáveis que foram utilizadas no processo de tomada de decisão do aplicativo.

consumidor de dados	É quem está solicitando a informação.
atributo	Informação que está sendo solicitada.
motivo	Motivo da solicitação.
benefício	Quem se beneficia da solicitação (usuário, consumidor ou ambos).
retenção	Tempo de a informação ficará armazenada.
localização	É o local onde está sendo solicitada a informação.
compartilhar	Se a informação será compartilhada com terceiros.
inferência	Se pode ser inferido alguma outra informação a partir da informação solicitada.

Além das variáveis apresentadas no mecanismo, existe alguma outra variável que te influenciaria no processo de tomada decisão? Descreva.

_____

_____

10) Ao definir um nível de privacidade, o mecanismo te deixa mais confiante nas respostas fornecidas em seu nome?

( ) Sim ( ) Acredito que sim ( ) Não sei ( ) Acredito que não ( ) Não

11) A possibilidade de disponibilizar uma informação de forma anônima, influência no seu processo de decisão ?

( ) Sim ( ) Acredito que sim ( ) Não sei ( ) Acredito que não ( ) Não

12) O mascaramento hierárquico é uma técnica de generalizar uma informação no formato de hierarquia. Por exemplo:
Os bairros (Vila Nery, Faga e Vila Prado) podem ser generalizados para cidade de São Carlos. Já a cidade de São Carlos pode ser generalizada para o estado de São paulo e assim por diante.

Em um hipotético cenário IoT, um consumidor de dados pode solicitar o seu bairro para realizar uma determinada tarefa. Neste contexto, você se sente confortável em disponibilizar seu bairro utilizando a técnica de mascaramento hierárquico?

( ) Sim ( ) Acredito que sim ( ) Não sei ( ) Acredito que não ( ) Não

13) A generalização é uma técnica na qual permite especificar um intervalo de um número. Por exemplo: O número 26 poderia ser generalizado para 22 - 29.

Neste contexto, você se sente confortável em disponibilizar a sua Idade utilizando a técnica de generalização?

( ) Sim ( ) Acredito que sim ( ) Não sei ( ) Acredito que não ( ) Não

14) A Pseudonimização por máscara de carácter é uma técnica que consiste substituir caracteres de uma informação por outros caracteres aleatórios.
Por exemplo:
A frase "Eu gosto das minhas informações anonimizadas" poderia ser peseudonimizada para "Yu cohte tel jihniv alwahriçõyj owojepytupot".

Neste contexto, você se sente confortável em disponibilizar uma informação utilizando a técnica pseudonimização?

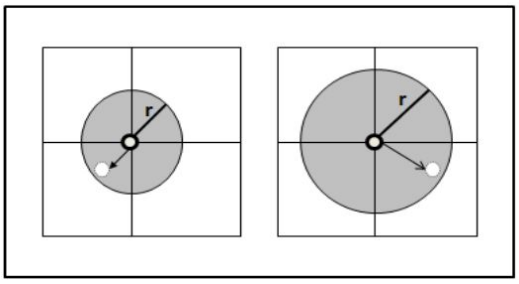
( ) Sim ( ) Acredito que sim ( ) Não sei ( ) Acredito que não ( ) Não

15) A Pseudonimizado também permite substituir os caracteres de uma informação por uma cadeia de caracteres fixo.
Por exemplo:
O sexo Masculino/Feminino pode ser pseudonimizado para "indefinido".

Neste contexto, você se sente confortável em disponibilizar seu sexo pseudonimizado para "indefinido"?

( ) Sim ( ) Acredito que sim ( ) Não sei ( ) Acredito que não ( ) Não

16) As informações de sua localização permite que outras pessoas te localizem. Em determinadas ocasiões você pode querer disponibilizar a sua localização de forma anonimizada.
A técnica implementada no App é uma técnica de ajuste de precisão na qual é feito um deslocamento da localização original para qualquer direção dentro de uma raio, conforme apresentado na imagem abaixo.



Neste contexto, você se sente confortável em disponibilizar sua localização, desde que o seu anonimato esteja assegurado?

( ) Sim ( ) Acredito que sim ( ) Não sei ( ) Acredito que não ( ) Não

Apendice B

Questões referente a demografia dos participantes

1) Qual a sua nacionalidade?
( ) Brasil Outros:_____

2) Sexo:
( ) Masculino ( ) Feminino

3) Nível de escolaridade:
( ) Graduado ( ) Graduando ( ) Pós Graduado ( ) Pós Graduando

4) Qual é a sua faixa etária?
( ) Abaixo de 18 anos ( ) Entre 21 a 29 anos ( ) 60 ou mais
( ) Entre 18 e 20 anos ( ) Entre 40 a 49 anos
( ) Entre 30 a 39 anos ( ) Entre 50 a 59 anos

5) Aproximadamente, quantas horas você passa utilizando computadores ou outros dispositivos?
( ) Nenhuma ( ) 4 a 6 horas ( ) 13 a 17 horas
( ) 1 a 2 horas ( ) 6 a 9 horas ( ) Mais de 17 horas
( ) 2 a 4 horas ( ) 9 a 13 horas

Apendice C

Cenários para tomadas de decisão

O Posto de gasolina do Serjão quer saber o modelo do seu carro para cadastrar essas informações em seu sistema com o intuito de manter um registro de seus abastecimentos. Essas informações serão mantidas para sempre pelo posto e poderão ser compartilhadas com outros postos de gasolina.
O Posto de gasolina do Serjão quer saber o ano do seu carro para cadastrar essas informações em seu sistema com o intuito de manter um registro de seus abastecimentos. Essas informações serão mantidas para sempre pelo posto e poderão ser compartilhadas com outros postos de gasolina.
O Posto de gasolina do Serjão quer saber a placa do seu carro para cadastrar essas informações em seu sistema com o intuito de manter um registro de seus abastecimentos. Essas informações serão mantidas para sempre pelo posto e poderão ser compartilhadas com outros postos de gasolina.
O Posto de gasolina do Serjão quer saber a data da última troca de óleo de seu carro para cadastrar essa informação em seu sistema com o intuito de manter um registro das suas trocas de óleo. Esta informação será mantida para sempre pelo posto e poderá ser compartilhada com outros postos de gasolina.
O Posto de gasolina do Serjão quer saber a quantidade de quilômetros rodados pelo seu carro para calcular o seu consumo de combustível com o intuito de informar a você possiveis problemas de consumo excessivo . Essas informações serão mantidas para sempre pelo posto e poderão ser compartilhadas com outros postos de gasolina.
O Posto de gasolina do Serjão quer saber se você tem interesse em lavar o seu carro enquanto abastece com intuito de coletar essas informações para avaliar a viabilidade de investimentos futuros. Essas informações serão mantidas até o seu propósito ser concluído pelo posto e não serão compartilhadas com outros postos de gasolina.
O Posto de gasolina do Serjão quer saber se deseja agendar uma troca de óleo para o seu carro pois ele identificou que com base em seus abastecimentos seu carro está próximo de trocar o óleo. Esta informação será mantidas até o seu propósito ser concluído e não será compartilhada com outros postos de gasolina.

O Posto de gasolina do Serjão quer acesso a sua agenda para agendar uma troca de óleo. A informação de acesso será mantida até o seu propósito ser concluído e não será compartilhada outros postos de gasolina.
O Posto de gasolina do Serjão quer saber se está indo viajar para informar possíveis rotas e dicas de trânsito. Esta informação será mantida até o seu propósito ser concluído e não será compartilhada com outros postos de gasolina.
O Posto de gasolina do Serjão quer os dados de sua carteira eletrônica para debitar o valor de seu abastecimento. Esta informação será mantida até o seu propósito ser concluído e não será compartilhada com ninguém.
O Posto de gasolina do Serjão quer saber o seu nome para cadastrar em seu sistema interno. Esta informação será mantida para sempre e não será compartilhada.
O estacionamento do shopping eldorado quer saber a placa do seu carro para cadastrar em seu sistema interno. Essas informações serão mantidas para sempre pelo estacionamento e não serão compartilhadas.
O estacionamento do shopping eldorado quer saber o seu nome para cadastrar em seu sistema interno. Essas informações serão mantidas para sempre pelo estacionamento e não serão compartilhadas.
O estacionamento do shopping eldorado quer saber o numero do seu celular para caso haja algum problema com seu carro entrar em contato contigo. Essas informações serão mantidas para sempre pelo estacionamento e não serão compartilhadas.
O estacionamento do shopping eldorado quer saber se seu carro possui seguro para questões de registro. Esta informação será mantida até o seu propósito ser concluído e será compartilhado com seguradoras de carro.
O estacionamento do shopping eldorado quer os dados de sua carteira eletrônica para debitar o valor do estacionamento. Esta informação será mantida até o seu propósito ser concluído e não será compartilhada com ninguém.
O Shopping eldorado quer saber a sua renda anual para fins internos. Esta informação será mantida até o seu propósito ser concluído e não será compartilhada com ninguém.
O Shopping eldorado quer saber as suas preferências de compra para montar um perfil dos seus consumidores. Esta informação será mantida até o seu propósito ser concluído e será compartilhada com terceiros.
O Shopping eldorado quer saber o seu email para enviar notificações quando as lojas do shopping tiver em promoções. Esta informação será mantida para sempre e será compartilhada com terceiros.
A Seguradora de carro Genebra quer saber se tem interesse em adquirir um seguro para seu carro com o objetivo de apresentar uma proposta de seguro. Esta informação será mantida até o seu propósito ser concluído e não será compartilhada com ninguém.
A Seguradora de carro Genebra quer acesso a sua agenda para agendar uma reunião com intuito de apresentar uma proposta de seguro. A informação de acesso será mantida até o seu propósito ser concluído e não será compartilhada com ninguém.

A Seguradora de carro Genebra quer saber o modelo do seu carro para realizar o orçamento. Essas informações serão mantidas até o seu propósito ser concluído e não será compartilhada com terceiros.
O Seguradora de carro Genebra quer saber sua idade para realizar o orçamento. Esta informação será mantida até seu propósito ser concluído e não será compartilhada com terceiros.
A Seguradora de carro Genebra quer saber o ano do seu carro para realizar o orçamento. Essas informações serão mantidas até o seu propósito ser concluído e não será compartilhada com terceiros.
A Seguradora de carro Genebra quer seus histórico médico para avaliar as suas condições físicas. A informação será mantida para sempre e não será compartilhada com terceiros.
A Seguradora de carro Genebra quer saber o valor da sua renda anual para manter em seu cadastro. A informação será mantida para sempre e não será compartilhada com terceiros.
O Seguradora de carro Genebra quer saber o seu email para enviar notificações quando os documentos estiverem pronto. Esta informação será mantida para sempre e não será compartilhada com terceiros.
A sua Cafeteira quer saber como foi a sua noite de sono para ajustar o nível de cafeína de seu café. A informação será mantida até o seu propósito ser concluído e poderá ser compartilhada com terceiros.
A sua Geladeira quer acesso a sua agenda para verificar se alguns de seus compromissos necessita de suplemento especial. A informação será mantida para sempre e não será compartilhada com terceiros.
A sua Geladeira quer acesso aos dados de sua carteira eletrônica para efetuar pagamentos das compras. A informação será mantida para sempre e não será compartilhada com terceiros.
A sua Geladeira quer saber seus preferências de comida para montar uma lista de compra baseado nas suas preferências. A informação será mantida para sempre e não será compartilhada com terceiros.
A sua Geladeira quer saber se você toma bebidas alcoólicas para registrar em seu banco de dados. A informação será mantida para sempre e não será compartilhada com terceiros.
A sua Geladeira quer saber suas preferências de bebidas alcoólicas para comprar bebidas de acordo com seu gosto. A informação será mantida para sempre e não será compartilhada com terceiros.
A sua Geladeira quer saber o time que você torce para manter a geladeira cheia em dias de jogos. A informação será mantida para sempre e não será compartilhada com terceiros.
O Bar do alemão quer saber suas preferências de bebidas alcoólicas para oferecer bebidas de acordo com seu gosto. A informação será mantida para sempre e não será compartilhada com terceiros.
O Bar do alemão quer saber o time que você torce para montar um perfil de seus clientes. A informação será mantida para sempre e não será compartilhada com terceiros.

O Bar do alemão quer saber o seu nome para cadastrar em seu sistema interno. Essas informações serão mantidas para sempre e não serão compartilhadas.
O Bar do alemão quer saber o seu email para enviar notificações em dias de jogos. Esta informação será mantida para sempre e será compartilhada com terceiros.
O Bar do alemão quer saber se a temperatura do ambiente está agradável para te deixar mais confortável . A informação será mantida até seu propósito ser concluído e não será compartilhada com terceiros.
O Bar do alemão quer saber as suas preferências musicais para tocar as músicas de sua preferências. Esta informação será mantida para sempre e poderá ser compartilhada com terceiros.
O Bar do alemão quer saber sua idade para verificar se pode vender bebida alcoólica. Esta informação será mantida até seu propósito ser concluído e não será compartilhada com terceiros.
O seu Médico quer seus histórico médico para realizar a sua avaliação . A informação será mantida para sempre e não será compartilhada com terceiros.
O seu Médico quer acesso as suas informações vitais para manter uma constante análise de sua saúde. A informação será mantida para sempre e não será compartilhada com terceiros.
O seu Médico quer acesso a sua agenda para agendar uma consulta. A informação será mantida até seu propósito ser concluído e não será compartilhada com terceiros.
O seu Médico quer saber se você toma bebidas alcoólicas para registrar em seu banco de dados. A informação será mantida para sempre e não será compartilhada com terceiros.
A sua Nutricionista quer acesso ao histórico das suas compras de comida para fazer uma avaliação nutricional. A informação será mantida até seu propósito ser concluído e não será compartilhada com terceiros.
A sua Nutricionista quer acesso a sua agenda para marcar uma consulta. A informação será mantida até seu propósito ser concluído e não será compartilhada com terceiros.
A sua Nutricionista quer saber o seu sexo para informações de cadastro. A informação será mantida para sempre e não será compartilhada com terceiros
A sua Nutricionista quer saber a data de seu nascimento para informações de cadastro. A informação será mantida para sempre e não será compartilhada com terceiros.
A sua Nutricionista quer saber o numero do seu celular para informações de cadastro. A informação será mantida para sempre e não será compartilhada com terceiros.
O seu Nutricionista quer saber se você toma bebidas alcoólicas para informações de cadastro. A informação será mantida para sempre e não será compartilhada com terceiros.
O seu local de trabalho quer acesso a sua agenda para marcar uma reunião. A informação será mantida até seu propósito ser concluído e não será compartilhada com terceiros.

O seu local de trabalho quer acesso a sua localização para lhe encontrar mais facilmente durante o expediente. A informação será mantida até seu propósito ser concluído e poderá ser compartilhada com outros colegas de trabalho.
O seu local de trabalho quer o seu itinerário para manter um registro das rotas de seus funcionários. A informação será mantida para sempre e não será compartilhada com terceiros.
O restaurante do Ceara quer saber seus preferências de comida para montar um buffet de acordo com suas preferências. A informação será mantida para sempre e poderá ser compartilhada com terceiros.
O restaurante do Ceara quer acesso aos dados de sua carteira eletrônica para debitar o valor de seu almoço. A informação será mantida até seu propósito ser concluído e não será compartilhada com terceiros.
O restaurante do Ceara quer saber se a temperatura do ambiente está agradável para te deixar mais confortável. A informação será mantida até seu propósito ser concluído e não será compartilhada com terceiros.
A Biblioteca quer acesso às suas preferências literários para aprimorar o seu acervo de livros. Esta informação será mantida para sempre e não será compartilhada com terceiros.
A Biblioteca quer acesso ao seu RA para poder liberar o seu livro. Esta informação será mantida para sempre e não será compartilhada com terceiros.
A livraria Sampaio quer acesso a suas preferências literárias para aprimorar o seu acervo de livros. Esta informação será mantida para sempre e poderá ser compartilhadas com terceiros.
O livraria Sampaio quer saber o seu nome para cadastrar em seu sistema interno. Esta informação será mantida para sempre e poderá ser compartilhadas com terceiros.
O livraria Sampaio quer saber o seu email para enviar notificações de novos lançamento de livros. Esta informação será mantida para sempre e poderá ser compartilhadas com terceiros.
O Taxi quer saber as suas preferências musicais para sintonizar a rádio em músicas de suas preferências. Esta informação será mantida para sempre e poderá ser compartilhada com terceiros.

Apendice D

Avaliação das respostas fornecidas automática pelo processo de aprendizagem do PrivacyApplication

Solicitante:	local de trabalho	Irá Compartilhar:	Não	[ ] Correto
Atributo Solicitado:	**acesso_agenda**	Resultado Inferido:	**Permitir**	[ ] Errado: _____
Tempo de retenção:	até satisfazer o seu propósito	Nível de Confiança:	**95.9964**	
Quem se beneficia:	user_consumer	Inf. Disponibilizada:	**sim**	
Local da solicitação:	Semi público			
Motivo:	Para marcar uma reunião.			

Solicitante:	Bar do alemão	Irá Compartilhar:	Não	[ ] Correto
Atributo Solicitado:	**preferencias_bebidas_alcoó**	Resultado Inferido:	**Permitir**	[ ] Errado: _____
Tempo de retenção:	Para sempre	Nível de Confiança:	**97.7875**	
Quem se beneficia:	user_consumer	Inf. Disponibilizada:	**não**	
Local da solicitação:	Semi público			
Motivo:	Para oferecer bebidas de acordo com seu gosto.			

Solicitante:	Bar do alemão	Irá Compartilhar:	Não	[ ] Correto
Atributo Solicitado:	**idade**	Resultado Inferido:	**Negar**	[ ] Errado: _____
Tempo de retenção:	até satisfazer o seu propósito	Nível de Confiança:	**97.6807**	
Quem se beneficia:	user_consumer	Inf. Disponibilizada:	**sim**	
Local da solicitação:	Semi público			
Motivo:	Para verificar se pode vender bebida alcoólica..			

Solicitante:	Nutricionista	Irá Compartilhar:	Não	[ ] Correto
Atributo Solicitado:	**acesso_agenda**	Resultado Inferido:	**Permitir**	[ ] Errado: _____
Tempo de retenção:	Para sempre	Nível de Confiança:	**99.1624**	
Quem se beneficia:	user_consumer	Inf. Disponibilizada:	**sim**	
Local da solicitação:	Privado			
Motivo:	Para marcar uma consulta.			

Solicitante:	Restaurante do Ceara	Irá Compartilhar:	Não	[ ] Correto
Atributo Solicitado:	**acesso_carteira_eletronica**	Resultado Inferido:	**Negociar**	[ ] Errado: _____
Tempo de retenção:	até satisfazer o seu propósito	Nível de Confiança:	**87.1809**	
Quem se beneficia:	consumer	Inf. Disponibilizada:	sim	
Local da solicitação:	Semi público			
Motivo:	Para debitar o valor de seu almoço.			

Solicitante:	Posto de Gasolina do Serjão	Irá Compartilhar:	Não	[ ] Correto
Atributo Solicitado:	**esta_indo_viajar**	Resultado Inferido:	**Negociar**	[ ] Errado: _____
Tempo de retenção:	até satisfazer o seu propósito	Nível de Confiança:	**82.4800**	
Quem se beneficia:	user_consumer	Inf. Disponibilizada:	**sim**	
Local da solicitação:	Público			
Motivo:	Para informar possíveis rotas e dias de trânsito.			

Solicitante:	Bar do alemão	Irá Compartilhar:	Sim	[ ] Correto
Atributo Solicitado:	**preferencias_musicais**	Resultado Inferido:	**Permitir**	[ ] Errado: _____
Tempo de retenção:	até satisfazer o seu propósito	Nível de Confiança:	**98.9414**	
Quem se beneficia:	user_consumer	Inf. Disponibilizada:	**sim**	
Local da solicitação:	Semi público			
Motivo:	Para tocar as músicas de sua preferência.			

Apendice E

Questionário de Usabilidade e Aceitabilidade

A usabilidade do PrivacyApplication é fácil?

( )	( )	( )	( )	( )
Discordo fortemente	Discordo	Nem concordo nem discordo	Concordo	Concordo fortemente

As informações apresentadas pelo PrivacyApplication é de fácil compreensão?

( )	( )	( )	( )	( )
Discordo fortemente	Discordo	Nem concordo nem discordo	Concordo	Concordo fortemente

É útil utilizar o PrivacyApplication em ambientes inteligentes para responder em seu nome?

( )	( )	( )	( )	( )
Discordo fortemente	Discordo	Nem concordo nem discordo	Concordo	Concordo fortemente

As interações respondidas automaticamente pelo App te traz resultados satisfatório?

( )	( )	( )	( )	( )
Discordo fortemente	Discordo	Nem concordo nem discordo	Concordo	Concordo fortemente

Você considera os métodos de anonimização adequados para anonimizar as suas informações pessoais?

( )	( )	( )	( )	( )
Discordo fortemente	Discordo	Nem concordo nem discordo	Concordo	Concordo fortemente

Utilizar o PrivacyApplication te traz algum benefício relevante?

( )	( )	( )	( )	( )
Discordo fortemente	Discordo	Nem concordo nem discordo	Concordo	Concordo fortemente

Em ambientes nos quais existem muitas interações entre dispositivos IoT, a utilização do PrivacyApplication minimizaria o seu tempo de interação com esses dispositivos?

( )	( )	( )	( )	( )
Discordo fortemente	Discordo	Nem concordo nem discordo	Concordo	Concordo fortemente

O app apresentado é uma boa idéia?

( )	( )	( )	( )	( )
Discordo fortemente	Discordo	Nem concordo nem discordo	Concordo	Concordo fortemente

Apendice F

Termo de Consentimento Livre e Esclarecido

UNIVERSIDADE FEDERAL DE SÃO CARLOS
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO
PROGRAMA DE PÓS GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

ESTUDO: Mecanismo de privacidade em ambientes inteligentes

Eu, Fagner Roger Pereira Couto, estudante do Programa de Pós Graduação em Ciência da Computação da Universidade Federal de São Carlos – UFSCar o(a) convido a participar da pesquisa "Mecanismo de privacidade em ambientes inteligentes" orientada pelo Professor Dr Sergio Zorzo.

Esta pesquisa tem o intuito avaliar um mecanismo de privacidade em ambientes inteligentes. O objetivo desta avaliação é identificar se o modelo de mecanismo proposto satisfaz as necessidades de privacidade impostas pela Internet das Coisas; bem como avaliar se as métricas utilizadas no modelo são suficiente para tomar as decisões em nome do usuário; e também avaliar a aceitação do mecanismo de privacidade.

Você foi selecionado (a) para ser usuário do nosso mecanismo. Primeiramente você será convidado a responder um questionário sobre diversos aspectos que envolvem esse estudo. Após responder ao questionário, você será convidado a utilizar o mecanismo de privacidade.

Este mecanismo é uma aplicação android que você utilizará usando um celular disponibilizado pelo pesquisador. Nesta aplicação você será submetido a vários cenários que podem ocorrer em um ambiente inteligente e responderá a esses cenários de acordo com as suas preferências.

Sua participação nessa pesquisa auxiliará na obtenção de dados que poderão ser utilizados para fins científicos, proporcionando maiores informações e discussões que poderão trazer benefícios para o modelo do mecanismo proposto e para area de privacidade em geral..

A sua participação neste estudo envolve riscos como desconforto pelo uso de ferramentas em desenvolvimento e pelo compartilhamento de suas preferências de privacidade.

Sua participação é voluntária e não haverá compensação em dinheiro pela sua participação. A qualquer momento o (a) senhor (a) pode desistir de participar e retirar seu consentimento. Todas as informações obtidas através da pesquisa serão confidenciais, sendo assegurado o sigilo sobre sua participação em todas as etapas do estudo. Caso haja menção a nomes, a eles serão atribuídas letras, com garantia de anonimato nos resultados e publicações, impossibilitando sua identificação.

Você receberá uma via deste termo, rubricada pelo pesquisador, onde consta o telefone e endereço do pesquisador. A qualquer momento você poderá tirar dúvidas sobre o mecanismo de privacidade ou sobre sua participação neste estudo.

Declaro que entendi os objetivos, riscos e benefícios de minha participação na pesquisa e concordo em participar.

_____

Fagner Roger Pereira Couto

Departamento de Computação (DC) / Universidade Federal de São Carlos (UFSCar) Caixa postal 676 / 13565-905 São Carlos-SP / Tel.: 16-33518513

São Carlos, ___/___/_____

_____

Participante