UNIVERSIDADE FEDERAL DE SÃO CARLOS

CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

INSTRUMENTO PARA MENSURAR PRIVACIDADE EM AMBIENTES IOT

BRUNO LOPES

ORIENTADOR: PROF. DR. SERGIO DONIZETTI ZORZO

São Carlos – SP

9 de dezembro de 2019

UNIVERSIDADE FEDERAL DE SÃO CARLOS

CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

INSTRUMENTO PARA MENSURAR PRIVACIDADE EM AMBIENTES IOT

BRUNO LOPES

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

9 de dezembro de 2019

UNIVERSIDADE FEDERAL DE SÃO CARLOS

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

Folha de Aprovação

Assinaturas dos membros da comissão examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato Bruno Lopes, realizada em 11/07/2019:

Prof. Dr. Sergio Donizetti Zorzo
UFSCar

Profa. Dra. Vânia Paula de Almeida Neris
UFSCar

Prof. Dr. Filipe Nunes Ribeiro
UFOP

Certifico que a defesa realizou-se com a participação à distância do(s) membro(s) Filipe Nunes Ribeiro 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

RESUMO

A Internet das Coisas (Internet of Things - IoT) interliga dispositivos usados, normalmente, no dia a dia das pessoas – como celulares, televisores, cafeteiras, geladeiras, camas, sensores, entre outros – de forma que se comuniquem automaticamente por uma rede. A troca de informações entre dispositivos, realizada de forma genérica e impessoal, pode, ocasionalmente, gerar problemas de privacidade, como por exemplo a disponibilização de informações pessoais para aplicativos ao utiliza-los. Visto que esta retém um conceito que envolve várias dimensões dos dados considerados privados, como corporal, comportamental, de comunicação e pessoal. Para mensurar a privacidade em ambientes IoT, este trabalho apresenta a concepção de um instrumento, denominado Internet of Things Privacy Concerns (IoTPC), que é capaz de refletir as preocupações dos usuários quanto à privacidade em ambiente de IoT. O instrumento IoTPC é composto por 17 itens obtidos por meio de uma análise feita dos instrumentos de mensuração de privacidade disponíveis na literatura atual, e que contemplam a opinião dos usuários sobre como os dispositivos coletam, processam e disponibilizam suas informações pessoais em cenários específicos de IoT. A validação do IoTPC foi realizada a partir da análise do resultado de uma amostra de 61 participantes, considerando as dimensões de requisições IoT, poder de decisão e cautela, mediante análise fatorial exploratória. IoTPC subsidiou a construção de um módulo de inferência em um mecanismo de negociação de privacidade para sistemas IoT. Esse módulo realiza uma inferência baseada nos itens do IoTPC e nos cenários IoT por meio de algoritmos de aprendizado de máquina, que foram treinados e testados com as preferências de privacidade advindas do instrumento IoTPC. Os resultados do processo de aprendizado do módulo de inferência obtiveram uma acurácia de 79,20%, concluindo-se que o instrumento pode ser empregado por um mecanismo de negociação de privacidade.

Palavras-chave: Internet das Coisas; Privacidade; Preocupações de Privacidade, Análise Fatorial;

ABSTRACT

The Internet of Things (IoT) connects devices that are commonly used in people's daily lives - such as cell phones, televisions, coffee makers, refrigerators, beds, sensors, and more - so that they automatically communicate over a network. Generic, impersonal information exchange between devices can occasionally lead to privacy issues, such as making personal information available to applications when using them. Since it retains a concept that involves various dimensions of data considered private, such as body, behavioral, communication and personal. To measure privacy in IoT environments, this paper presents the design of an instrument, called the Internet of Things Privacy Concerns (IoTPC), which is capable of reflecting users' concerns about privacy in an IoT environment. The IoTPC instrument consists of 17 items obtained through an analysis of the privacy measurement instruments available in the current literature, which include users' opinion on how devices collect, process and make their personal information available in specific IoT scenarios. . The validation of the IoTPC was performed from the analysis of the results of a sample of 61 participants, considering the dimensions of IoT requests, decision power and caution, through exploratory factor analysis. IoTPC subsidized the construction of an inference module in a privacy negotiation mechanism for IoT systems. This module performs an inference based on IoTPC items and IoT scenarios through machine learning algorithms, which have been trained and tested with the privacy preferences derived from the IoTPC instrument. The results of the learning process of the inference module obtained an accuracy of 79.20 %, concluding that the instrument can be employed by a privacy negotiation mechanism.

Keywords: Internet of Things; Privacy; Privacy Concerns, Factorial Analysis;

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

Capítulo 1

INTRODUÇÃO

1.1 Contextualização

A abrangência da Internet das Coisas (IoT) tem crescido nos últimos anos, com isso, permitindo que máquinas e objetos comuniquem-se de maneira inteligente. Esse crescimento viabilizou a evolução da IoT como plataforma global capaz de processar e autogerenciar as informações (BALTE; KASHID; PATIL, 2015).

A variedade de dispositivos presentes na IoT pode ser muito ampla, assim, permitindo a inclusão de uma diversidade de elementos físicos, desde objetos do dia a dia – como telefones inteligentes, tablets, câmeras digitais, entre outros – até elementos do ambiente – como casas, veículos, trabalho, etc (RAZZAQUE et al., 2016).

A autonomia desses dispositivos de IoT, conectada a outras aplicações, permite a criação de ambientes inteligentes (ALABA et al., 2017). Com isso, as preocupações com a privacidade do usuário são agravadas, pois nesses ambientes inteligentes todos os dispositivos e objetos serão conectados a uma só rede (GUO; TANG; ZHANG, 2017).

Uma das diferenças observadas sobre a Internet tradicional e a IoT é a quantidade de dados coletada dos usuários. Esses dados são recolhidos pelos dispositivos que compõem o sistema IoT e podem ser usados para construir um perfil invasivo do usuário de IoT, por conseguinte, sendo capaz de violar suas preferências de privacidade (LU, 2014).

Os problemas de privacidade são especialmente difíceis de serem discutidos porque, por sua natureza, a privacidade é considerada subjetiva (COVERT, 2014). Isso exige a investigação de novas abordagens a fim de garantir que a privacidade possa ser devidamente representada no contexto de IoT.

1.2 Motivação

A onipresença da IoT permite a coleta constante de informações pessoais, viabilizando o cruzamento de dados e as descobertas de novas informações, tais como números de celulares, documentos, endereços, etc. No entanto as regulamentações necessárias para auxiliar os usuários no âmbito de privacidade não se desenvolveram da mesma maneira que evoluiu a Internet das Coisas (LU, 2014). Com isso, práticas agressivas de acesso e transmissão de dados são adotadas por aplicativos, sistemas operacionais móveis e outros objetos que agravaram essas preocupações (XU et al., 2012).

Para obter uma melhor compreensão da atitude e do comportamento dos indivíduos é necessário examinar a natureza contextual da privacidade (BUCK; BURSTER, 2017). De forma complementar é fundamental entender com precisão quais são as preocupações quanto à privacidade dos usuários (MALHOTRA; KIM; AGARWAL, 2004). No entanto faltam instrumentos capazes de mensurar essa privacidade (SMITH; MILBERG; BURKE, 1996), especificamente para IoT.

Apesar da existência de vários instrumentos capazes de mensurar privacidade em determinado contexto, nenhum deles explora o cenário de Internet das Coisas, ficando restritos apenas a dispositivos móveis, ao comércio eletrônico ou até mesmo a um contexto mais genérico e fora da computação.

Consequentemente, existe a necessidade de construir um instrumento capaz de mensurar a privacidade por meio de uma nova escala de preocupações com privacidade para ambientes IoT. Esse instrumento irá promover esforços de pesquisa cooperativa, permitindo que outros pesquisadores possam utilizá-lo para a realização de testes e ajustes em suas pesquisas, bem como mais clareza para a formulação e interpretação de questões de pesquisa.

1.3 Objetivo da Pesquisa

Este trabalho visa visou a à construção de um instrumento capaz de mensurar a privacidade por meio de uma nova escala de preocupações com privacidade para ambientes IoT. Tal instrumento, deve ser capaz de refletir como os usuários de IoT se sentem-se em relação à sua privacidade em ambientes IoT.

O trabalho proposto também objetiva objetivou apresentar a aplicabilidade do instrumento proposto pela implementação de um módulo de inferência de privacidade para mecanismos de negociação de privacidade em ambientes IoT. Esse módulo apresenta descreve um caso de uso

utilizando o instrumento proposto em uma aplicação especifica específica para o cenário de IoT.

Além da aplicabilidade do instrumento, este trabalho procurou validar o instrumento por meio da análise fatorial exploratória, verificando o nível de correlação dos itens do instrumento, além de verificar sua confiabilidade.

Neste contexto, os sistemas são caracterizados por dispositivos inteligentes, onde a comunicação na maioria das vezes é realizada de forma *wireless*, e dessa forma a privacidade é altamente violável, não existindo assim instrumentos que contenham essas especifidades.

1.4 Estrutura e Organização do Trabalho

O restante deste trabalho está organizado da seguinte forma. O Capítulo 2 apresenta os conceitos de privacidade e de IoT. No Capítulo 3 são relacionados os principais estudos que versam sobre o tema em tela e que serviram como base para o desenvolvimento deste trabalho. No Capítulo 4 são discriminadas, em detalhe, a construção e avaliação do instrumento proposto. No Capítulo 5, são enunciados os resultados obtidos com o instrumento proposto. Já no Capítulo 6 são descritos a construção e os resultados do módulo de inferência de privacidade. Por fim, no Capítulo 7, constam as conclusões e indicam-se trabalhos futuros que enriqueçam os achados desta dissertação.

Capítulo 2

INTERNET DAS COISAS E PRIVACIDADE

2.1 Considerações Iniciais

Com o objetivo de conhecer melhor as tecnologias e os conceitos aqui utilizados, neste capítulo, apresenta-se os conceitos a fim de exemplificar o cenário de construção desta pesquisa.

Este capítulo encontra-se organizado da seguinte maneira: na Seção 2.2 é apresentada a Internet das Coisas, bem como sua evolução, arquitetura e o modelo de referência utilizado. Na Seção 2.3 são descritos alguns conceitos teóricos sobre privacidade, bem como sua história e algumas questões legais.

2.2 Internet das Coisas

Definir o termo Internet das Coisas pode ser considerada uma tarefa confusa, pois o conceito sofre várias mudanças de acordo com a abordagem adotada.

Em termos gerais, a Internet das Coisas pode ser definida como uma abordagem nova em relação à interconexão de tecnologias e objetos por meio de redes de computadores, proporcionando a definição do conceito de rede global de dispositivos (KORESHOFF; ROBERTSON; LEONG, 2013). No entanto a Internet das Coisas depende do processo tecnológico para sua evolução contínua, dessa forma, a IoT não pode ser tratada como uma nova tecnologia disruptiva, mas sim como um paradigma da computação que está em constante evolução (ZIEGELDORF; MORCHON; WEHRLE, 2014).

Alguns autores consideram que o termo “Coisas” não se refere apenas a objetos físicos, mas, também, a entidades vivas ou representações virtuais. Dessa maneira, qualquer ”Coisa”que esteja conectada à Internet e que tenha capacidade de transmitir informações pode ser considerada

um dispositivo IoT (ORIWOH; CONRAD, 2015). A Figura 2.1, a seguir, exemplifica o conceito de IoT, onde qualquer coisa, dispositivo ou pessoa, pode estar conectado a qualquer rede – de qualquer lugar – para utilizar qualquer serviço em determinado contexto ou momento. Como por exemplo, um professor (Qualquer Pessoa) com seu *SmartWatch* (Qualquer Dispositivo), pode enviar um e-mail (Qualquer Serviço) de sua sala de aula (Qualquer Lugar), via Internet móvel (Qualquer Rede), sobre bolsas de pesquisa (Qualquer Contexto).

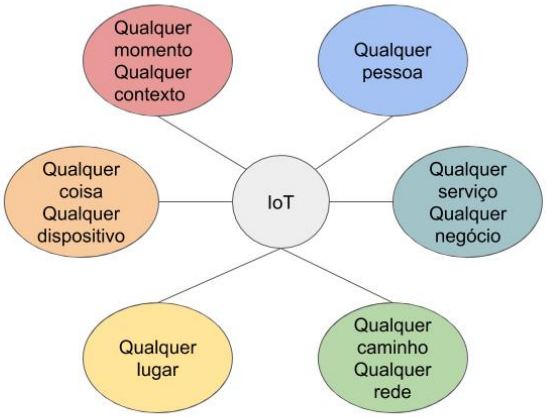

Figura 2.1: Definição de IoT (Adaptado de Perera et al. (2014))

Do ponto de vista conceitual, a Internet das Coisas baseia-se em três pilares relacionados à capacidade de objetos inteligentes: (1) capacidade de se identificar (qualquer objeto pode autoidentificar-se), (2) capacidade de comunicação (qualquer objeto pode comunicar-se) e (3) capacidade de interação (qualquer objeto pode interagir). Por meio desses três pilares é possível construir redes com: objetos interligados, usuários finais e entre outros (MIORANDI et al., 2012)

2.2.1 Evolução

A Internet evoluiu em vários aspectos nos últimos anos, então, tornando-se capaz de conectar bilhões de dispositivos em todo o mundo. Esses dispositivos são de diversos tamanhos e contêm capacidade de processamento computacional diferente uns dos outros, além de oferecerem suporte a distintos tipos de aplicações (HUANG; LI, 2010).

Ao longo das últimas décadas, a Internet progrediu de um simples repositório estático de documentos de hipertexto interligados para um universo dinâmico de interações de humanos, máquinas e aplicativos em rede (JADOUL, 2015). A Figura 2.2 exemplifica essa evolução.

De acordo com Lemos (2013), o termo "*Internet of Things*" foi utilizado pela primeira

vez em uma conferência em Procter Gamble (P&G), em 1999, por Kevin Ashton, em uma palestra a respeito ao uso de dispositivos *Radio-Frequency Identification* (RFIDs) com o intuito de explicar que as "*Things*" poderiam ser qualquer tipo de objeto com capacidade de obter informações por meios próprios.

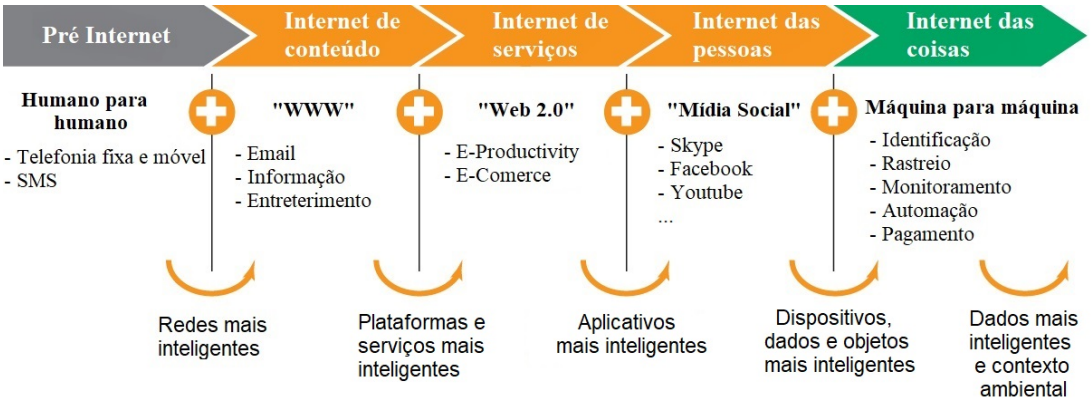

Figura 2.2: Evolução da Internet (Adaptado de Jadoul (2015))

No entanto, apesar do termo "*Internet of Things*" ter sido utilizado pela primeira vez em 1999, segundo Evans (2011), a Cisco *Internet Business Solutions Group* (IBSG) considera que o surgimento da IoT ocorreu de fato entre 2008 a 2009, quando os números de dispositivos ultrapassaram o número de pessoas no mundo.

O relatório apresentado pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) definiu um plano de ação econômica em relação ao crescimento da Internet das Coisas no Brasil. De acordo com esse estudo, em 2025, quatro áreas principais terão destaque na utilização da IoT, sendo elas: saúde, agronegócio, cidades inteligentes e indústrias. Estima-se que o impacto econômico possa gerar entre US$ 50 bilhões a US$ 200 bilhões no Brasil (NETO et al., 2017).

Mediante uma visão mais geral, o relatório global de perspectivas de mercado da Internet das Coisas aponta que a IoT é um dos três principais avanços tecnológicos da próxima década, sendo que o mercado global de sensores de IoT representou cerca de US$ 9,46 bilhões em 2018 e estima-se que haverá uma taxa de crescimento de 23,9% ao longo do período de 2019 a 2027, totalizando US$65,79 bilhões em 2027 (WOOD, 2019).

2.2.2 Arquitetura

A Internet das Coisas consiste em uma arquitetura de três camadas, sendo estas de percepção, rede e aplicação, porém alguns pesquisadores não consideram que essas camadas expliquem

totalmente a arquitetura IoT e acabam adicionando mais duas camadas a essa arquitetura, as camadas de *middlewares* e de negócio (WU et al., 2010; AAZAM; HUH, 2014; KHAN et al., 2012; ZHANG; SUN; CHENG, 2012).

- **Camada de Percepção**: é a camada de mais baixo nível na arquitetura IoT, nesta, encontram-se dispositivos que realizam a coleta de informações, tais como leitores de código de barras, dispositivos de identificação por radiofrequência (RFID), câmeras, sistema de posicionamento global (Global Positioning System - GPS), sensores, entre outros (WU et al., 2010).

- **Camada de Rede**: esta é responsável por transmitir e processar todas as informações, a camada de rede transfere e processa as informações vindas da camada de percepção. A comunicação é feita por redes cabeadas ou sem fio, utilizando tecnologias como *blueto-oth*, infravermelho, *ZigBee*, entre outras(KHAN et al., 2012; WU et al., 2010).

- **Camada de Middleware**: esta é responsável por receber os dados da camada de rede objetivando o gerenciamento de serviços e armazenamento de informações (KHAN et al., 2012; AAZAM; HUH, 2014).

- **Camada de Aplicação**: esta é responsável por executar a apresentação final dos dados. A camada de aplicação recebe informações processadas pela camada de *middlewares* ou de rede e fornece um gerenciamento global do aplicativo apresentado (AAZAM; HUH, 2014)

- **Camada de Negócios**: esta é a camada de mais alto nível na arquitetura IoT, sendo responsável pelo gerenciamento de aplicativos e serviços. Ela gera gráficos, modelos de negócios, fluxogramas, etc., a partir dos dados recebidos pela camada de aplicação. Com base na análise dos dados, esta camada ajudará a determinar ações futuras e estratégias de negócio (KHAN et al., 2012).

A fim de exemplificar melhor as camadas da arquitetura IoT, nota-se, pela Figura 2.3, as camadas descritas de acordo com o nível mais baixo (Camada de Percepção) para a camada de mais alto nível dentro da IoT (Camada de Negócio), além de apresentar os agrupamentos das arquiteturas de 3 e 5 camadas.

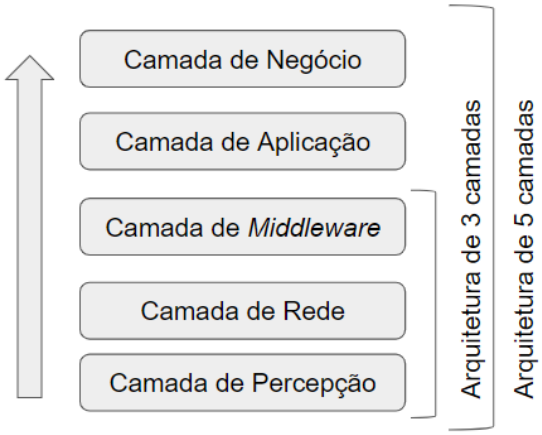

Figura 2.3: Arquiteturas IoT

2.2.3 Modelo de Referência IoT

A grande heterogeneidade de dispositivos proporcionados pela IoT permite a criação de diversos cenários para ambientes inteligentes. E esses cenários podem ser descritos pelas entidades e pelos fluxos de informações que ocorrem nesses ambientes. O modelo de referência IoT considerado neste trabalho foi proposto por (ZIEGELDORF; MORCHON; WEHRLE, 2014), que se basearam nas visões de IoT da União Internacional de Telecomunicações (IUT) e do Conselho Europeu de Investigação da IoT (IERC). Esse modelo de referência considera que qualquer coisa ou pessoa é interconectada em qualquer lugar, a qualquer hora, por uma rede participante de qualquer tipo de serviço.

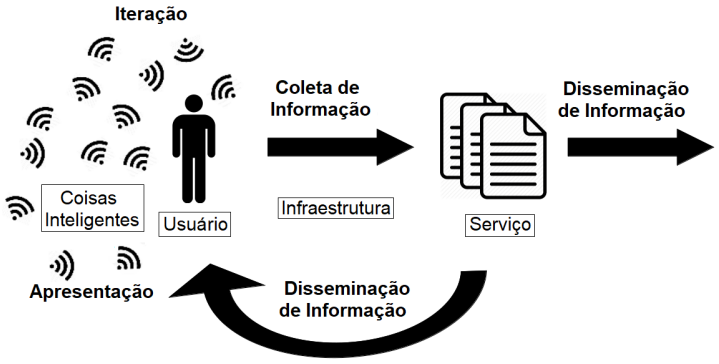

Figura 2.4: Modelo de Referência IoT (Adaptado de Ziegeldorf, Morchon e Wehrle (2014))

A Figura 2.4 apresenta esse modelo, indicando que as coisas inteligentes podem ser qualquer dispositivo do dia a dia capaz de coletar, processar e transmitir dados em determinado ambiente. Esses dispositivos coletam informações sobre os usuários que utilizam a infraestrutura de IoT, obtendo como produto final a disseminação de informações para usuários, bem como para outros sistemas ou dispositivos IoT. (ZIEGELDORF; MORCHON; WEHRLE, 2014). A

utilização desse modelo serviu como base para investigar as preocupações com privacidade em diferentes cenários IoT.

2.3 Privacidade

O compartilhamento de informações pessoais de maneira descontrolada pode, eventualmente, levar a violações de privacidade. Quanto maior for o número de informações disponibilizadas, mais difícil será controlar a privacidade sobre essas informações (GHANI; SIDEK, 2008).

Warren e Brandeis (1890) definiram o conceito de privacidade como o direito de ser deixado sozinho, porém essa definição não foi considerada suficiente para descrever o que é privacidade, surgindo, no decorrer dos anos, novos pesquisadores tentando definir da melhor maneira esse conceito. Westin (1968) define privacidade como o direito do indivíduo, dos grupos ou das instituições de determinar para si mesmo quando, como e quais informações sobre eles serão disponibilizadas para terceiros.

De acordo com Hong e Landay (2004), privacidade pode ser definida como o privilégio dos usuários de determinar por si mesmos quando, como e em que medida as informações sobre eles são disponibilizadas para terceiros. De maneira similar, Rodotà (2008) descreve o conceito de privacidade como a possibilidade do indivíduo ter à sua disposição mecanismos que sejam capazes de controlar o uso de suas informações.

Clarke (1999) define privacidade como o interesse que o indivíduo tem em sustentar um espaço pessoal, sem interferência de outra pessoa ou organização. Além de afirmar que a privacidade possui várias outras dimensões como:

- **Privacidade Pessoal**: Ttambém referenciada como privacidade corporal, refere-se à integridade do estado físico do indivíduo envolvendo procedimentos que incluem imunização compulsória, transfusão de sangue, provisão compulsória de amostras de fluidos corporais e tecido corporal, esterilização compulsória, entre outros, que não devem ser realizados sem o consentimento do interessado.
- **Privacidade do Comportamento Pessoal**: relaciona-se diretamente com todos os aspectos do comportamento, em especial, com questões mais sensíveis como preferências, hábitos sexuais, atividades políticas, religiosas, etc.
- **Privacidade das Comunicações Pessoais**: Oo sujeito estabelece uma troca de informações utilizando diversas ferramentas de comunicação, de maneira que ele não seja monitorado.

- **Privacidade dos Dados Pessoais**: os indivíduos afirmam que suas informações pessoais não devem estar disponíveis automaticamente para terceiros, mesmo que outro indivíduo ou organização tenha acesso a elas. O interessado deve ter ao menos um controle substancial sobre suas informações pessoais.

A definição de privacidade adotada para este trabalho é a colocada por Westin (1968), apresentando o direito do indivíduo, dos grupos ou das instituições de determinar para si mesmos quando, como e quais informações sobre eles serão disponibilizadas para terceiros.

2.3.1 História da Privacidade

As discussões sobre privacidade já se estendem por muitos anos. Vários eventos históricos provocaram mudanças sobre a perspectiva de preocupações de privacidade (LANGHEINRICH, 2001). Michael (1994) relata que assuntos sobre privacidade podem ser encontrados a partir do ano de 1361, quando um juiz, na Inglaterra, estabeleceu medidas preventivas quanto a atos de intromissão e curiosidade nas comunicações.

No século 19, Warren e Brandeis (1890) definiram o conceito de privacidade como ”o direito de ser deixado sozinho”, motivados em grande parte pelos repórteres da época, que tiravam fotografias das pessoas sem o seu consentimento.

A privacidade voltou a ser discutida na década de 1960, quando foi descoberto que o governo utilizava o processamento automatizado de dados para catalogar de maneira mais efetiva seus cidadãos. Durante a Segunda Guerra Mundial, já com a prática do nazismo, era possível o detalhamento de registros públicos sobre toda a população das cidades invadidas, assim, permitindo aos nazistas que encontrassem facilmente todo o povo judeu. Diante desse cenário, muitas nações europeias passaram a preocupar-se em ter leis sobre a proteção de dados, com o intuito de evitar qualquer uso incorreto ou abusivo de informações armazenadas (LANGHEINRICH, 2001).

No decorrer dos anos, vários esforços foram realizados para se criar legislações que fossem capazes de garantir as preferências de privacidade dos cidadãos. Pode-se destacar como um desses esforços a lei americana criada na década de 70[1], responsável por apresentar práticas justas de uso de informação (*Fair Information Practice Principles* - FIPPs) (CATE, 2006). A princípio, a criação das FIPPs foram baseadas no trabalho de (WESTIN, 1968), que originalmente definiu sete princípios descritos da seguinte forma:

[1] https://www.justice.gov/opcl/privacy-act-1974

No decorrer dos anos, vários esforços foram realizados para criar legislações que fossem capazes de garantir as preferências de privacidade dos cidadãos. Pode-se destacar como um desses esforços a lei americana, criada na década de 1970[2], responsável por apresentar práticas justas de uso de informação (*Fair Information Practice Principles* - FIPPs) (CATE, 2006). A princípio, a criação das FIPPs foi baseada no trabalho de (WESTIN, 1968), que originalmente definiu sete princípios descritos da seguinte forma:

1. **Abertura e Transparência**: não deverá existir práticas de registros secretos dos indivíduos, ou seja, o usuário deve estar consciente a respeito de todas as informações que estão sendo coletadas sobre ele, bem como do conteúdo dessas informações.

2. **Participação Individual**: este princípio orienta sobre a existência de mecanismos pelos quais os indivíduos possam contestar a validade e requisitar correções de dados.

3. **Limitação de Coleta**: este princípio está relacionado à coleta de dados dos indivíduos, relatando que essa coleta deve ser proporcional ao seu uso, ou seja, devem ser coletadas apenas as informações necessárias, não realizando, assim, a coleta excessiva de informações.

4. **Qualidade dos Dados**: é necessário garantir que os dados reunidos sejam considerados relevantes para os determinados fins aos quais foram coletados, além de verificar, sempre que possível, por atualizações dessas informações, garantindo assim que as informações estarão sempre completas e precisas.

5. **Limitação de Uso**: após os dados serem devidamente coletados e validados pelos passos anteriores, é necessário garantir que essas informações sejam utilizadas da maneira correta, logo, esse princípio visa verificar se os dados estão sendo utilizados conforme o propósito específico para o qual foram coletados, e se as pessoas que estão manipulando essas informações têm autorização para essa tarefa.

6. **Segurança Razoável**: garantias de segurança consideradas adequadas devem ser implementadas de acordo com a sensibilidade dos dados coletados, com o intuito de garantir a segurança das informações disponibilizadas.

7. **Responsabilidade**: o último princípio diz respeito ao fato de que os portadores de informação devem ser responsáveis pelo cumprimento dos demais princípios, ou seja, uma vez que a informação pessoal de um indivíduo está em posse de terceiros, estes devem garantir a aplicação de todos os princípios apresentados.

[2]https://www.justice.gov/opcl/privacy-act-1974

Esses princípios foram um ponto inicial na história para a criação de legislações sobre a privacidade pessoal, resultado na criação de novas leis ao decorrer dos anos, de acordo com o contexto, a cultura e outros fatores que podem influenciar na privacidade

2.3.2 Legislação de Proteção de Dados

Ao analisar as questões legais em uma época mais atual, pode-se citar alguns países que começaram a preocupar-se com essas regulamentações. A privacidade na Europa obteve uma pauta legal com a regulamentação geral de proteção de dados *(General Data Protection Regulation – GDPR*[3]*)*. Essa regulamentação é constituída de um conjunto de regras sobre privacidade e proteção de dados visando proteger os cidadãos europeus contra violações de privacidade.

Organizações que mantêm sob seu controle dados pessoais de usuários europeus devem implementar medidas técnicas e organizacionais para se ajustarem à regulamentação de privacidade, tais como manterem o maior nível de privacidade no tratamento de dados por padrão, não permitirem o tratamento de quaisquer tipos de dados fora do contexto legal especificado, divulgarem claramente qualquer tipo de coleta de dados, sua finalidade, tempo de armazenamento e se vão ser compartilhados com terceiros, entre outras medidas.

Inspirado na lei de proteção de dados europeia, o estado da Califórnia aprovou, em 2018, a *California Consumer Privacy (CCPA*[4]). A lei objetiva aumentar os direitos dos cidadãos em relação à sua privacidade digital, dando aos usuários alguns direitos, como, por exemplo:

- Direito de conhecer todos os dados coletados pelas organizações.
- Direito de se negar a vender suas informações pessoais.
- Direito de apagar dados pessoais já publicados.
- Direito de conhecer o objetivo comercial da coleta de dados.

Em linhas gerais, assim como na regulamentação de proteção de dados europeia, a CCPA preocupa-se em garantir que os cidadãos possam controlar suas informações pessoais sem se sentirem intimidados por grandes empresas de tecnologia. A lei de privacidade do consumidor da Califórnia começará a ter validade a partir de 2020.

[3] https://eugdpr.org/
[4] https://www.caprivacy.org/about

2.3.3 Lei de Proteção de Dados Brasileira

A lei de proteção de dados brasileira (Lei n.º 13.709, de 14 de agosto de 2018, do Código Civil)[5], também, foi inspirada na legislação da União Europeia e objetiva a criação de regras para coleta, armazenamento, processamento e uso de informações pessoais. A lei dispõe sobre o tratamento de dados pessoais, inclusive, quanto a meios digitais, tanto para pessoa jurídica quanto para pessoa física, objetivando proteger os direitos fundamentais de liberdade e privacidade.

Dentre os vários itens dessa nova legislação, alguns pontos são destacados:

1. **Tratamento de Dados:** de acordo com a regulamentação, o tratamento de informações pessoais somente poderá ser realizado com o consentimento do seu titular ou para fins específicos, tais como cumprimento de obrigações legais, administração pública, realização de estudos por órgãos de pesquisa, entre outros.

2. **Segurança e Boas Práticas:** a lei indica que os agentes responsáveis pela coleta e pelo tratamento de dados privados devem atentar-se às políticas de segurança técnica e administrativa com a finalidade de garantir a proteção desses dados privados contra o uso por pessoas não autorizadas e uso em situações acidentais.

3. **Autoridade Nacional de Proteção de dados:** essa autoridade trata-se de um órgão competente integrado à administração pública federal indireta, tendo como atribuições cuidar da proteção de dados pessoais nos termos da legislação, elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, fiscalizar e aplicar punições em casos de descumprimento da lei, entre outras.

4. **Conselho Nacional de Proteção de Dados Pessoais e da Privacidade:** o conselho objetiva propor diretrizes estratégicas, além de fornecer recursos para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade. Também, fica sobre sua responsabilidade sugerir ações às autoridades fiscalizadoras, bem como realização de estudos sobre o tema. O conselho é composto por 23 representantes titulares e seus suplentes das mais diversas áreas do Poder Público, tais como Poder Executivo, Senado Federal, Câmera dos Deputados, Conselho Nacional de Justiça, Ministério Público, entre outros.

A lei obriga que empresas e organizações adaptem-se em relação aos seus princípios em um

[5]https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156212-pl.html

prazo máximo de até 18 meses a partir da lei sancionada, garantindo assim que toda informação pessoal coletada, processada e disponibilizada respeite as diretrizes impostas.

2.4 Considerações Finais

Neste capítulo foram apresentados conceitos considerados fundamentais para este trabalho. Buscou-se, nesse sentido, absorver um conhecimento aprofundado sobre privacidade, além de adquirir um conhecimento geral a respeito do cenário estudado, Internet das Coisas. Vale destacar que os conceitos apresentados neste capítulo agregaram a possibilidade de identificar e explorar com clareza os problemas de privacidade em ambientes IoT.

Capítulo 3

HISTÓRICO DE INSTRUMENTOS DE MENSURAÇÃO DE PRIVACIDADE

3.1 Considerações Iniciais

Com o aumento da preocupação quanto à privacidade do usuário, alguns autores propuseram, na literatura, instrumentos capazes de mensurar a privacidade em determinado contexto. Tais pesquisas contribuíram para o desenvolvimento deste trabalho, relacionando as metodologias de pesquisa dos trabalhos existentes no contexto de IoT para produzir um novo instrumento de privacidade.

Neste contexto, foram selecionados os trabalhos relacionados que tinham como objetivo a construção de instrumentos capazes de mensurar privacidade em um determinado contexto, dando prioridade para os instrumentos que trabalharam com o contexto de computação em geral.

Neste capítulo são abordados alguns dos principais trabalhos que contribuíram para o desenvolvimento desta dissertação. Inicialmente, na Seção 3.2, são individuados estudos que centraram sua atenção a preocupações gerais de privacidade. Na Seção 3.3 são abordados os trabalhos relacionados a preocupações com a privacidade na Internet. Por fim, na Seção 3.4 são apresentadas pesquisas com preocupações relativas à privacidade em dispositivos móveis.

3.2 Preocupações de Privacidade

Com o decorrer dos anos, as preocupações de privacidade aumentaram de acordo com o surgimento de novas tecnologias, com isso, alguns autores propuseram instrumentos capazes de

mensurar privacidade empiricamente.

Smith, Milberg e Burke (1996) propuseram o desenvolvimento de um instrumento capaz de mensurar a privacidade dos indivíduos em práticas organizacionais, que foi denominado *Concern for Information Privacy (CFIP)*. O objetivo desse instrumento é que ele possa capturar as preocupações dos indivíduos em relação à privacidade organizacional empiricamente.

O CFIP é composto por uma escala de 15 itens, refletindo quatro dimensões de preocupações com privacidade, sendo elas: coleta, uso secundário não autorizado, acesso impróprio e erros. Após seu desenvolvimento, o CFIP passou por um rigoroso processo de avaliação envolvendo três estágios, então, utilizando-se de técnicas de análise fatorial, confirmando e reafirmando a validade da sua escala. O fato de ter passado por um processo de validação e ter sido aplicado a várias populações heterogêneas, proporcionou ao CFIP um alto grau de confiança na validade, confiabilidade e generalização da sua escala (SMITH; MILBERG; BURKE, 1996).

É possível apontar duas contribuições importantes para a literatura de privacidade obtidas pelos autores: (1) uma estrutura que descreve as principais dimensões de preocupações de privacidade dos indivíduos sobre as práticas organizacionais e (2) um instrumento validado e apto a medir essas preocupações de privacidade (SMITH; MILBERG; BURKE, 1996).

Stewart e Segars (2002) conduziram um estudo empírico com 355 participantes a fim de examinar a estrutura dos fatores do CFIP e confirmaram as propriedades psicométricas desse instrumento. Os autores utilizaram técnicas de análise fatorial para a avaliação do instrumento, obtendo, com resultados, a confirmação de que o CFIP é considerado um instrumento confiável para a mensuração de privacidade, o CFIP pode ser combinado e aplicado a um contexto mais específico, como, por exemplo, a IoT, mas não garante que o instrumento refletirá realmente as preocupações de privacidade dos usuários de IoT.

3.3 Preocupações de Privacidade na Internet

Ao detectar a falta de confiança dos consumidores em relação à privacidade no comércio eletrônico, Malhotra, Kim e Agarwal (2004) realizaram um estudo sobre a magnitude das preocupações de privacidade dos usuários na Internet, resultando na construção de um instrumento capaz de refletir as preocupações de privacidade dos usuários de comércio eletrônico, denominado *Internet Users' Information Privacy Concerns* (IUIPC). O objetivo desse instrumento é conseguir mensurar empiricamente o que é considerado privado para os usuários de comércio eletrônico.

O IUIPC é composto por uma escala de dez itens, distribuídos em três dimensões, sendo elas: coleta, controle e consciência de práticas de privacidade. A construção do instrumento foi baseada no CFIP (SMITH; MILBERG; BURKE, 1996), agregando dimensões como a de coleta e adaptando itens para o contexto da Internet.

Malhotra, Kim e Agarwal (2004) conduziram dois estudos empíricos na sua pesquisa para desenvolver e testar o IUIPC. O primeiro estudo foi conduzido com o objetivo de levantar novas dimensões para a escala de IUIPC (por exemplo, controle e conscientização), visto que elas não estavam disponíveis em escalas existentes. O segundo estudo foi projetado com o intuito de levantar fatores de segunda ordem do IUIPC com base em escalas existentes, além de testar a pesquisa formalmente no modelo de hipóteses.

Durante essa pesquisa foram coletados dados de 742 participantes por meio de entrevistas presenciais, em que os itens do IUIPC foram aplicados aos participantes, a fim de se medir privacidade no contexto de comércio eletrônico (MALHOTRA; KIM; AGARWAL, 2004).

Os autores aplicaram técnicas de análise fatorial para realizar a validação do seu instrumento, entre elas a análise fatorial exploratória e a análise fatorial confirmatória (MALHOTRA; KIM; AGARWAL, 2004).

Malhotra, Kim e Agarwal (2004) apontam como resultados o fato de que o modelo estrutural e o IUIPC ajustam os dados de forma satisfatória, com isso, explicando a existência de uma grande quantidade de variância na intenção comportamental do usuário. De forma geral, as descobertas dos autores sugeriram que a construção do IUIPC servirá como ferramenta útil para analisar as preocupações de privacidade na Internet.

Também inquietos com as questões de privacidade na Internet, Child, Pearson e Petronio (2009) conduziram um estudo sobre as preocupações de privacidade dos blogueiros em relação ao conteúdo que eles disponibilizavam em seus blogs, gerando uma medida validada, baseada na teoria de gerenciamento de privacidade de blogs, o *The Blogging Privacy Management Measure* (BPMM). O BPMM tem como objetivo avaliar como os estudantes universitários gerenciam seus limites de privacidade *on-line*.

O BPMM é composto por uma escala de 18 itens, distribuídos em três dimensões, sendo elas: permeabilidade dos limites, propriedades de limites e ligações de limite. Além de se basear em instrumentos anteriores como o CFIP e IUIPC, o BPMM aplicou a teoria do *Communication Privacy Management* (CPM) no contexto de blogs para o seu desenvolvimento (CHILD; PEARSON; PETRONIO, 2009).

O estudo foi conduzido com 823 blogueiros em forma de pesquisa on-line, sendo segmen-

tado em três estudos nos quais foram aplicadas as técnicas de análise fatorial a fim de avaliar o instrumento desenvolvido. Child, Pearson e Petronio (2009) comprovaram, através da análise fatorial, que o BPMM é considerado um instrumento válido para mensurar as preferências de privacidade dos usuários de blogs, além de confirmar que as dimensões descobertas durante a pesquisa refletem corretamente essas preocupações de privacidade.

3.4 Preocupações de Privacidade em Dispositivos Móveis

Outra área afetada pelas preocupações de privacidade foi a dos dispositivos móveis, pois, nesse contexto, os desenvolvedores de aplicativos podem ter acesso a um grande volume de informações pessoais do usuário, ocasionando, eventualmente, violações de privacidade.

Inspirado em trabalhos como o CFIP e o IUIPC (SMITH; MILBERG; BURKE, 1996; MALHOTRA; KIM; AGARWAL, 2004), Xu et al. (2012) desenvolveram uma escala com o intuito de representar as preferências de privacidade dos usuários de dispositivos móveis. O *Measuring Mobile Users' Concerns for Information Privacy* (MUIPC) é composto por uma escala de nove itens, distribuídos em três dimensões, sendo elas: vigilância percebida, intrusão percebida e uso secundário não autorizado.

Os autores conduziram uma pesquisa *on-line* com 310 participantes, aplicando os itens do MUIPC dentro de uma escala Likert de 7 pontos, variando de "Concordo Completamente" a "Discordo Completamente", contendo um ponto neutro "Não Sei Opinar".

Assim, seguindo a literatura existente, Xu et al. (2012), também, utilizaram-se da análise fatorial para validar o MUIPC. Os autores aplicaram a análise fatorial exploratória para validar os itens do MUIPC, garantindo que eles se relacionassem, além de utilizar a análise fatorial confirmatória para confirmar a estrutura de fator derivada, gerada pela análise fatorial exploratória.

Xu et al. (2012) discutiram qual era a necessidade de desenvolver outro instrumento de mensuração de privacidade quando já existiam outros na literatura, como o CFIP e o IUIPC. Segundo (XU et al., 2012), as preocupações dos consumidores com a privacidade não são apenas diferentes, mas também mais preocupantes nos ambientes de dispositivos móveis, resultando na construção de um instrumento específico para dispositivos móveis (MUIPC). Os autores apontam como resultados de sua pesquisa o fato de a análise fatorial confirmar que o MUIPC pode ser utilizado como um instrumento capaz de mensurar privacidade em ambientes de dispositivos móveis

Apesar da construção de um instrumento capaz de mensurar as preocupações de privaci-

dade dos usuários de dispositivos móveis (XU et al., 2012), o MUIPC não reflete todas as características relevantes ao contexto de preocupações de privacidade existentes na literatura, como, por exemplo, dimensões de controle e coleta (BUCK; BURSTER, 2017).

Com o intuito de obter um instrumento mais completo referente a dispositivos móveis, Buck e Burster (2017) propuseram um instrumento similar ao MUIPC, porém esse novo instrumento não é voltado apenas ao uso de dispositivos móveis, mas sim para todos os dispositivos inteligentes que usam aplicativos como uma interface tecnológica.

Nesse contexto, os autores desenvolveram o *App Information Privacy Concern* (AIPC), um instrumento capaz de mensurar as preferências de privacidade dos usuários de *smart mobile devices*. O AIPC foi desenvolvido baseado nos instrumentos apresentados anteriormente CFIP, IUIPC e MUIPC (SMITH; MILBERG; BURKE, 1996; MALHOTRA; KIM; AGARWAL, 2004; XU et al., 2012), sendo ele uma das principais referências para este trabalho.

O AIPC é composto por 17 itens, distribuídos em cinco dimensões, sendo elas: coleta, controle percebido, consciência, uso secundário não autorizado e preocupações gerais de privacidade. A construção desse instrumento herdou dimensões das escalas existentes, como, por exemplo, as dimensões de uso secundário não autorizado e coleta (BUCK; BURSTER, 2017).

Buck e Burster (2017) onduziram uma pesquisa on-line na qual aplicaram os itens do AIPC em uma escala Likert de 7 pontos, similar à escala utilizada no MUIPC, a um conjunto de 269 participantes.

Similar aos outros instrumentos, Buck e Burster (2017) utilizaram técnicas de análise fatorial para validar seu instrumento, entre elas a análise fatorial exploratória a fim de validar os itens do AIPC, utilizando também a fatoração de eixo principal com a finalidade de extrair as variáveis latentes.

Os autores apresentam como resultados da sua pesquisa o fato de que o AIPC permite que pesquisadores possam investigar melhor o campo de preocupações de privacidade baseados em itens específicos do contexto, nesse caso, *smart mobile devices*. Ademais, foi possível extrair três fatores da amostra com o auxílio da análise fatorial, sendo eles: ansiedade, atitude pessoal e requisição de dados, então, concluindo que esses três fatores podem ser resumidos como dimensões do AIPC (BUCK; BURSTER, 2017).

Mesmo que sejam medidas para a mensuração da privacidade em diferentes contextos, todos os instrumentos obtiveram um propósito semelhante, em que os autores objetivaram refletir as preocupações de privacidade dos usuários em seu contexto estudado. Uma visão geral dos trabalhos apresentados pode ser observada na Tabela 3.1, onde é descrito um resumo sobre cada

instrumento apresentado, destacando a sua quantidade de itens, seu propósito, seu foco e suas dimensões. Como, por exemplo, o MUIPC, que tem como propósito refletir as preocupações dos usuários de dispositivos móveis sobre a privacidade e tem como foco saber como os usuários se sentem sabendo que terceiros utilizam suas informações pessoais sem seu consentimento.

Tabela 3.1: Quadro Comparativa (adaptado from Xu et al. 2012)

	Propósito	**Foco**	**Dimensões**
CFIP (15-itens)	Refletir as preocupações dos indivíduos com relação as práticas de privacidade organizacional	Responsabilidades das organizações pelo tratamento adequado das informações do cliente	- Coleta - Uso Secundário não Autorizado - Erro - Acesso Improprio
IUIPC (10-itens)	Refletir as preocupações dos usuários da Internet sobre privacidade da informação	Opiniões subjetivas dos indivíduos sobre justiça no contexto de privacidade da informação	- Coleta - Controle - Consciência de práticas de Privacidade
BPMM (18-itens)	Refletir as preocupações dos usuários de blogs na Internet sobre privacidade da informação	Avaliar como os estudantes universitários gerenciam limites de privacidade online	- Permeabilidade dos Limites - Propriedades de Limite - Ligações de Limite
MUIPC (9-itens)	Refletir as preocupações dos usuários de dispositivos móveis sobre privacidade da informação	Como os usuários se sentem sabendo que terceiros possuem suas informações privadas	- Vigilância Percebida - Intrusão Percebida - Uso Secundário não Autorizado
AIPC (17-itens)	Refletir as preocupações dos usuários de dispositivos inteligentes sobre privacidade da informação	O grau em que os indivíduos estão preocupados com suas informações em aplicativos de dispositivos móveis	- Coleta - Controle Percebido - Consciência - Uso Secundário não Autorizado - Preocupações Gerais de Privacidade

3.5 Considerações Finais

Mediante os referenciais teóricos apresentados neste capítulo, buscou-se absorver o máximo de conhecimento possível para o desenvolvimento da proposta do trabalho em tela; com tal perspectiva, analisando as técnicas utilizadas, metodologias, embasamento teórico e qual foi a abordagem de cada autor de acordo com contexto trabalhado.

Uma observação importante a fazer no tocante aos estudos apresentados aqui é a forma como seus autores trabalharam na construção de suas escalas, sempre, observando instrumentos

anteriores, aproveitando dimensões, adaptando itens das escalas de acordo com o seu contexto, bem como a avaliação e a validação dos instrumentos foram realizadas utilizando as mesmas técnicas. De maneira similar, este trabalho, por sua vez, considerou as abordagens dos estudos precedentes e ponderou-as de acordo com a sua necessidade.

Capítulo 4

INSTRUMENTO DE MENSURAÇÃO DE PRIVACIDADE EM AMBIENTES IOT

4.1 Considerações Iniciais

Neste capítulo é abordado o processo de desenvolvimento do instrumento produzido neste trabalho. Na seção 4.2 é apresentado o cenário de aplicação do instrumento. Na seção 4.3, a descrição do instrumento proposto é exemplificada. Já na seção 4.4 é definida a percepção de privacidade dos usuários de IoT de acordo com o instrumento IoTPC (Internet of Things Privacy Concerns) proposto. Por fim, na seção 4.5, descreve-se como foi realizada a avaliação do instrumento proposto.

Este trabalho visou delinear a construção de um instrumento capaz de mensurar a privacidade por meio de uma nova escala de preocupações com privacidade para ambientes IoT. Esse instrumento irá promover esforços de pesquisa cooperativa, permitindo que outros pesquisadores possam utilizá-lo para a realização de testes e ajustes em suas pesquisas, bem como mais clareza para a formulação e interpretação de questões de pesquisa. Este trabalho, também, descreve a elaboração de um módulo de inferência de privacidade para mecanismos de negociação de privacidade em ambientes IoT que exemplifica uma das possíveis aplicações do instrumento.

4.2 Cenário de Aplicação do Instrumento

O fato de que vários cenários são possíveis no contexto da IoT torna quase impraticável criar um instrumento capaz de cobrir todas as situações prováveis. Para construir um cenário de concepção e aplicação do instrumento proposto foram observados alguns estudos relacionados na literatura atual. Entre eles, Lee e Kobsa (2016) realizaram um estudo sobre os fatores que

influenciam a privacidade dos usuários de IoT. Nesse estudo, vários cenários foram criados para tentar exemplificar e coletar esses fatores. Dos cenários propostos, cinco parâmetros foram utilizados de forma diferenciada: ”Onde”, ”O que”, ”Quem”, ”Razão” e ”Persistência”. ”Onde” refere-se ao lugar onde a informação é coletada; ”O que” é o tipo de informação coletada; ”Quem” é o agente responsável por coletar a informação; ”Razão”é o objetivo de coletar tal informação; e a ”Persistência” é a frequência com a qual essa informação é coletada.

Em consideração a tais parâmetros propostos por Lee e Kobsa (2016), o escopo de atuação do instrumento neste trabalho foi delimitado para que houvesse melhor precisão. Foram, para tanto, analisados 64 microcenários de IoT considerando a pesquisa de (LEE; KOBSA, 2016), e 25 cenários foram selecionados, considerando os aspectos de abrangência de contexto e heterogeneidade de dispositivos para compor um cenário geral futurista sobre IoT, ao qual serviram como base para a construção dos itens do instrumento. O cenário futurístico apresentado, a seguir, exemplifica a rotina de um estudante universitário interagindo com a internet das coisas no seu dia a dia.

”Seu despertador tocou e as cortinas do seu quarto se abriram para que a luz entrasse lhe ajudando a acordar. Ao se levantar, sua cama notifica que você se mexeu muito durante a noite, não tendo um sono adequado e, por isso, talvez, possa ter a sensação de cansaço e sonolência durante o dia. Ao chegar na cozinha, seu café já está pronto da forma que você gosta, extraforte, sua campainha toca e é a entrega do supermercado da compra realizada pela sua geladeira.

Após seu café da manhã, você se dirige à academia que fica a poucas quadras da sua casa, no caminho, uma loja de esportes exibe promoções sobre luvas e suplementos para você no seu smartphone. Você é notificado que já faz certo tempo que não consulta seu médico pessoal, sendo que a secretária do seu médico já agendou uma consulta, e ele já tem dados prévios sobre sua saúde coletados por dispositivos inteligentes na sua casa, como sua cama, por exemplo. Ao chegar à academia, um painel digital que faz autenticação por biometria informa todos os seus dados desde quando você entrou na academia, exibindo informações como peso, altura, medidas, exercícios, entre outros, apresentando um acompanhamento completo da sua evolução nos treinos.

Após o treino, seu smartphone começa a tocar a música do Start Wars, logo, você percebe que é seu amigo lhe ligando para perguntar se você vai comparecer à aula mais tarde. Parece que hoje o clima vai mudar, você acaba de receber um aviso de um temporal à tarde e que é bom estar preparado. Ao arrumar-se para sair de casa e ir para mais um dia de faculdade, sua mochila avisa que você está esquecendo seu notebook, então, rapidamente, você o pega

e entra no carro. Ao sair de casa, dispositivos inteligentes detectam que a casa está vazia, seu termostato ajusta a temperatura e dispositivos considerados desnecessários são desligados para economia de energia.

Ao inferir que você está indo para a faculdade, seu carro aconselha ir a um posto de combustível abastecer, pois ele estima que não tem autonomia suficiente para realizar esse percurso. No posto, a bomba de combustível, que já tem o seu histórico de abastecimento, informa que seu carro está consumindo mais do que outros veículos do mesmo modelo, uma notificação, então, é enviada para seu mecânico, agendando uma vistoria a fim de evitar problemas maiores. Você aproveita para calibrar os pneus do seu carro, como o compressor já tem dados do seu veículo, ele ajusta a pressão automaticamente para você. No caminho para a faculdade, seu sistema de entretenimento informa que o filme que você aguardava já está disponível nos cinemas e reserva um horário na sua agenda para o próximo final de semana.

Ao chegar à faculdade, o restaurante universitário informa que hoje será servido um dos seus pratos favoritos. Chegando ao seu departamento, você é avisado que tem uma prova e três trabalhos para serem entregues até semana que vem. Antes de entrar na sala de aula, o bebedouro notifica que você não está consumindo o necessário de água, logo, você enche sua garrafa e entra na sala de aula. Ao sentar-se no seu lugar, sua cadeira ajusta-se de acordo com seu peso e altura e ainda exibe que você perdeu 300 gramas em uma semana. A temperatura do ar-condicionado também é ajustada. Ao sair da aula, a sala de aula detecta que você não compreendeu muito bem o conteúdo dessa matéria e agenda um horário com os monitores, tudo já está devidamente marcado na sua agenda eletrônica."

Esse cenário foi empregado na concepção do instrumento descrito na próxima seção. Logo, o IoTPC foi construído para atuar no cenário apresentado, garantindo melhor precisão do instrumento, mas não limitando sua atuação restritamente ao cenário proposto.

4.3 Descrição do Instrumento

O instrumento *Internet of Things Privacy Concerns* (IoTPC) é capaz de medir empiricamente a privacidade dos usuários no cenário futurístico de IoT narrado. O IoTPC é composto por 17 itens distribuídos dentro de cinco dimensões e foi desenvolvido com base em instrumentos de privacidade já existentes como o IUIPC, MUIPC e AIPC, todos tendo como base o CFIP, como apresentado pela Figura 4.1.

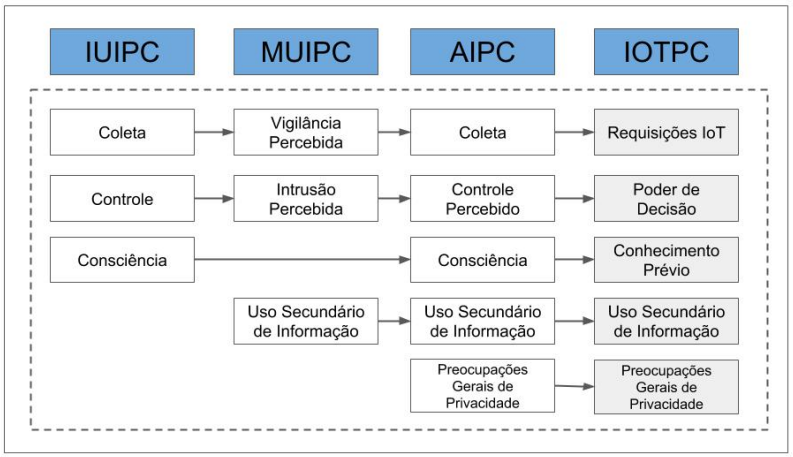

Figura 4.1: Desenvolvimento do IoTPC

Para a construção do instrumento foi necessário, primeiramente, analisar e definir com clareza suas dimensões para que, posteriormente, seus itens fossem bem organizados. Durante seu processo de desenvolvimento, as dimensões do IUIPC, MUIPC e AIPC foram selecionadas como pontos de partida, a Figura 4.2 ilustra essas agregações.

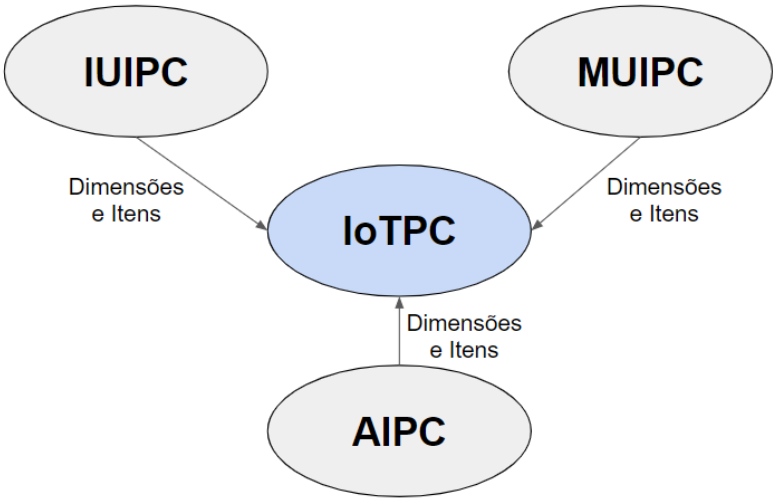

Figura 4.2: Agregações dos Instrumentos Selecionados

4.3.1 Dimensões do IoTPC

As dimensões do IUIPC, MUIPC e AIPC foram analisadas a fim de verificar se refletiam alguma característica de privacidade nos ambientes IoT, como a dimensão de uso secundário de informação, agregada do MUIPC. Esta dimensão revela que, normalmente, os usuários sentem

sua privacidade violada quando terceiros utilizam suas informações sem o seu consentimento. Ela, também, pode refletir questões de privacidade em ambientes IoT, visto que dispositivos coletam várias informações e podem eventualmente disponibilizá-las para terceiros.

As dimensões adotadas pelo IoTPC são descritas, a seguir, e foram concebidas baseadas nas dimensões do IUIPC, MUIPC e AIPC.

1. **Requisições IoT**: esta dimensão do instrumento é definida pelas requisições realizadas por dispositivos IoT aos seus usuários, ou seja, a coleta de dados pessoais realizada pelos dispositivos. Malhotra, Kim e Agarwal (2004) definem que o conceito de coleta está atrelado ao grau que determinado indivíduo está preocupado com a quantidade de dados pessoais em posse de terceiros. No entanto a heterogeneidade de dispositivos possíveis dentro de um cenário de IoT e o fato de que a grande maioria desses dispositivos coleta informações de seus usuários de maneira onipresente destacam o conceito de vigilância que também é incorporado a essa dimensão

   Peissl et al. (2017) definem vigilância como o ato de observar a escuta ou a gravação do indivíduo. Em um ambiente futurista de IoT, os dispositivos podem eventualmente utilizar as informações coletadas para rastrear e vigiar seus usuários.

2. **Poder de Decisão**: Poder de Decisão: esta dimensão é definida como o interesse dos usuários em controlar seus dados pessoais em ambientes IoT. De acordo com Malhotra, Kim e Agarwal (2004), o conceito de controle pode ser definido como o fato de o indivíduo ter o interesse em controlar ou, ao menos, influenciar significativamente o uso de seus dados pessoais. Muitas vezes, em um ambiente IoT, os usuários não se sentem confortáveis com o fato de não terem cem por cento de controle sobre seus dados privados, além de uma sensação de violação de suas preferências de privacidade.

   Segundo Peissl et al. (2017), intrusão percebida pode ser definida como o ato invasivo que perturbe a tranquilidade ou a solidão. O conceito de intrusão percebida, também, aplica-se ao cenário de IoT, uma vez que seus dispositivos podem solicitar informações aos seus usuários, eventualmente, perturbando-os ou, até mesmo, retirando-os de sua tranquilidade.

3. **Conhecimento Prévio**: esta dimensão está relacionada a todo conhecimento sobre práticas de privacidade que o usuário de IoT já carrega consigo. Podendo-se, aqui, utilizar o conceito de consciência para definir essa dimensão, em que consciência é o grau com o qual um indivíduo está preocupado com seu conhecimento em práticas de privacidade relacionadas a informações organizacionais (MALHOTRA; KIM; AGARWAL, 2004).

4. **Uso Secundário de Informações**: algumas vezes, os dados fornecidos pelos usuários para determinado fim são utilizados de maneira diferente sem o seu consentimento, por exemplo, traçando perfis dos indivíduos e enviando mensagens de *marketing* a eles, sem sua autorização (SMITH; MILBERG; BURKE, 1996). Essa prática reflete as preocupações de privacidade em ambientes de IoT e também foi levada em consideração para construção das dimensões do IoTPC. O uso secundário de informações é uma dimensão de privacidade que foge do escopo de poder de decisão do usuário, portanto não podem ser confundidas essas duas dimensões.

5. **Preocupações Gerais de Privacidade**: responsável por representar itens como "Estou preocupado com as ameaças à minha privacidade pessoal hoje" e "Comparado com outros, sou mais sensível sobre o modo como os dispositivos IoT lidam com minha informação pessoal", esta dimensão tem como objetivo capturar preocupações gerais de privacidade do indivíduo em um cenário de IoT (BUCK; BURSTER, 2017).

4.3.2 Itens do IoTPC

A partir do utilizo da mesma estratégia para a criação das dimensões do IoTPC, os itens relacionados a cada dimensão, também, foram gerados com base nos instrumentos citados, sofrendo alterações para o contexto da IoT.

A definição de tais itens é considerada a metodologia de concepção do instrumento, que passaram pela avaliação de especialistas, no caso, os integrantes do grupo de pesquisa em privacidade do departamento de computação da Universidade Federal de São Carlos - UFSCAR, com o intuito de verificar se refletiam alguma característica de privacidade em ambientes IoT.

Os itens do IoTPC foram descritos por um código, dessa forma, objetivando dar uma identificação única para cada um. O código foi composto por três informações, sendo elas: (I) Instrumento de Origem, (II) Dimensão de Origem e (III) Numeração do Item. Para exemplificar qual instrumento contribuiu para a construção daquele item, os três primeiros caracteres do código representam o (I) Instrumento de Origem, por exemplo, se o instrumento que deu origem àquele item foi extraído do MUIPC, os três primeiros caracteres do código desse item formavam-se como "MUI". A segunda parte da identificação do código é referente à (II) Dimensão de Origem, sendo representada por: Co (Controle - *"Control"*), Aw (Consciência - "Awareness"), Coll (Coleta - *"Collection"*), Ps (Vigilância Percebida - *"Perceived Surveillance"*), Pi (Intrusão Percebida - *"Perceived Intrusion"*), Sui (Uso Secundário de Informações - *"Secondary Use of Information"*), Gen (Preocupações Gerais de Privacidade da Informação

- General Information Privacy Concern). Por fim, na última parte do código, é atribuído um número de 1 a 17, para melhor ordenação dos itens dentro da escala. A Tabela 4.1 apresenta os itens concebidos para esse instrumento.

Tabela 4.1: Itens do IoTPC

Item	Cenário
IUICo1	A privacidade em ambientes IoT é realmente uma questão de direito dos consumidores de exercerem controle e autonomia sobre as decisões de como suas informações são coletadas, usadas e compartilhadas.
IUIAw2	Dispositivos IoT que buscam informações devem divulgar a forma como os dados são coletados, processados e usados.
IUIAw3	É muito importante para mim que eu esteja ciente e conhecedor sobre como minhas informações pessoais serão usadas.
IUIColl4	Normalmente me incomoda quando dispositivos IoT me pedem informações pessoais.
IUIColl5	Quando dispositivos IoT me pedem informações pessoais, às vezes penso duas vezes antes de fornecer.
IUIColl6	Incomoda-me fornecer informações pessoais a tantos dispositivos IoT.
MUIPs7	Eu acredito que a localização do meu dispositivo móvel é monitorada pelo menos parte do tempo.
MUIPs8	Estou preocupado que os dispositivos IoT estejam coletando muita informação sobre mim.
MUIPs9	Estou preocupado que os dispositivos IoT possam monitorar minhas atividades através do meu dispositivo móvel.
MUIPi10	Eu sinto que, como resultado do uso de dispositivos IoT, outros sabem sobre mim mais do que eu gostaria, causando-me desconforto.
MUIPi11	Eu acredito que, como resultado do uso de dispositivos IoT, as informações sobre mim que considero privadas são agora acessíveis para outros mais do que eu gostaria.
MUISui12	Estou preocupado que os dispositivos IoT possam usar minhas informações pessoais para outros fins sem me notificar ou obter minha autorização.
MUISui13	Quando forneço informações pessoais para usar ambientes IoT, estou preocupado que os dispositivos IoT possam usar minhas informações para outros fins.
MUISui14	Estou preocupado que os dispositivos IoT possam compartilhar minhas informações pessoais com outras entidades sem minha autorização.
AIPGen15	Comparado com outras pessoas, sou mais sensível sobre o modo como os dispositivos IoT lidam com minha informação pessoal.
AIPGen16	Para mim, a coisa mais importante é manter minha privacidade intacta ao usar os dispositivos IoT.
AIPGen17	Estou preocupado com as ameaças à minha privacidade pessoal hoje.

A organização dos itens em relação às dimensões do IoTPC ficaram da seguinte maneira: a dimensão Poder de Decisão engloba os itens IUICo1, MUIPi10 e MUIPi11. Na dimensão de Conhecimento Prévio, os itens contidos nela são IUIAw2 e IUIAw3. A dimensão de Requisições IoT contém os itens IUIColl4, IUIColl5, IUIColl6, MUIPs7, MUIPs8 e MUIPs9. Já o Uso Secundário contém os itens MUISui12, MUISui13 e MUISui14. Por fim, a dimensão Preocupações

Gerais contém os itens AIPGen15, AIPGen16 e AIPGen17. A Tabela 4.2 ilustra essa organização.

Tabela 4.2: Organização dos Itens do IoTPC por Dimensões

Dimensões	Itens
Requisições IoT	IUIColl(4,5 e 6), MUIPs7, MUIPs8 e MUIPs9
Poder de Decisão	IUICo1, MUIPi10 e MUIPi11
Conhecimento Prévio	IUIAw2 e IUIAw3
Uso Secundário de Informações	MUISui12, MUISui13 e MUISui14
Preocupações Gerais de Privacidade	AIPGen15, AIPGen16 e AIPGen17

4.4 Percepção da Privacidade Pelos Usuários de IoT

Para obter as preferências de privacidade dos usuários de dispositivos IoT, foi aplicado um questionário eletrônico contendo o cenário futurista apresentado na seção 4.2, pelo qual os usuários responderam a questões de privacidade relacionadas a ele. A coleta dos dados teve o intuito de aplicar o IoTPC aos usuários de IoT e confirmar se seus itens realmente refletem suas preocupações de privacidade.

O questionário eletrônico foi composto por cinco seções, sendo elas: (I) Introdução, (II) Caracterização do Participante, (III) Introdução ao Cenário de Aplicação do Instrumento, (IV) Cenário de Aplicação do Instrumento e (V) Itens do IoTPC.

Ao iniciar o questionário, o participante é direcionado para a (I) Introdução, que tem por finalidade apresentar-lhe o conceito de IoT e a importância do participante na contribuição com essa pesquisa. No próximo passo, o participante avança para a seção (II) Caracterização do participante, onde ele deve fornecer informações de idade, sexo e escolaridade. Após a caracterização do participante, ele é direcionado para a (III) Introdução ao Cenário de Aplicação do Instrumento, tendo como objetivo apresentar ao participante o tempo estimado para concluir o questionário e as orientações de como prosseguir nas próximas seções. Na próxima seção é apresentado o (IV) Cenário de Aplicação do Instrumento, que foi exemplificado na seção 4.2 desse documento. Por fim, na última etapa (V), Itens do IoTPC, são exibidos os 17 itens do IoTPC em uma escala *Likert* de 5 pontos, variando de ”Concordo Completamente”a ”Discordo Completamente”e contendo um ponto neutro ”Não sei Opinar”. Os participantes informaram nessa seção o grau de concordância com cada item do IoTPC baseados em suas preferências de privacidade.

Para que a privacidade e o conforto dos participantes fossem preservados durante a pesquisa, foi submetido um projeto ao comitê de ética da UFSCar com o intuito de exemplificar

todo o processo de coleta de dados dos participantes. Junto ao projeto do Comitê de Ética, também, foram anexados o questionário aplicado e o Termo de Consentimento Livre e Esclarecido (TCLE). O projeto e anexos aprovados pelo comitê de ética podem ser observados no Apêndice B

4.5 Avaliação do Instrumento

Com os resultados obtidos a partir da aplicação dos questionários, foi possível utilizar as respostas dadas pelos participantes para avaliar a construção do IoTPC.

A avaliação do instrumento foi realizada com objetivo de validar os itens do IoTPC e verificar se ele poderia ser considerado um instrumento confiável. Existe um grande número de técnicas estatísticas na literatura capaz de avaliar a construção de instrumentos para a mensuração de um dado fator. Assim como nos trabalhos relacionados no capítulo 3, a análise fatorial foi conduzida, neste estudo, como forma de validação do IoTPC.

Segundo Field (2017), a análise fatorial é uma técnica usada para identificar grupos ou *clusters* de variáveis que podem ter três usos principais: (a) entender a estrutura de um conjunto de variáveis; (b) construir um questionário capaz de medir uma variável subjacente e (c) reduzir um conjunto de dados para um tamanho mais gerenciável, mantendo a maior parte da informação original possível.

De acordo com Basilevsky (2009), análise fatorial é geralmente entendida como um conjunto de modelos estreitamente relacionados e destinados a explorar ou estabelecer a estrutura de correlação entre as variáveis aleatórias observadas.

A análise fatorial é útil para estudos que envolvem algumas centenas de variáveis, itens de questionários ou uma série de testes que podem ser reduzidos a um conjunto menor, com isso, obtendo um conceito subjacente para facilitar as interpretações (RUMMEL, 1988). Segundo Yong e Pearce (), conjuntos de dados grandes que consistem em diversas variáveis podem ser reduzidos em grupos de variáveis, chamados fatores, ou seja, a análise fatorial reúne variáveis comuns em categorias descritivas.

Na análise fatorial, duas técnicas destacam-se, sendo elas a análise fatorial exploratória e a análise fatorial confirmatória. A análise fatorial confirmatória objetiva confirmar hipóteses utilizando diagramas de análise de caminho para representar variáveis e fatores, enquanto que a análise fatorial exploratória objetiva descobrir padrões complexos explorando o conjunto de dados e as previsões de teste (CHILD, 2006).

Com o intuito de avaliar se o instrumento proposto era capaz de refletir as preferências de privacidade dos usuários de IoT, utilizou-se a Análise Fatorial Exploratória (*Exploratory Factory Analysis* - EFA) para validar os 17 itens do IoTPC, com o auxílio do software de análise estatística SPSS Statistics[1] em sua versão *trial*.

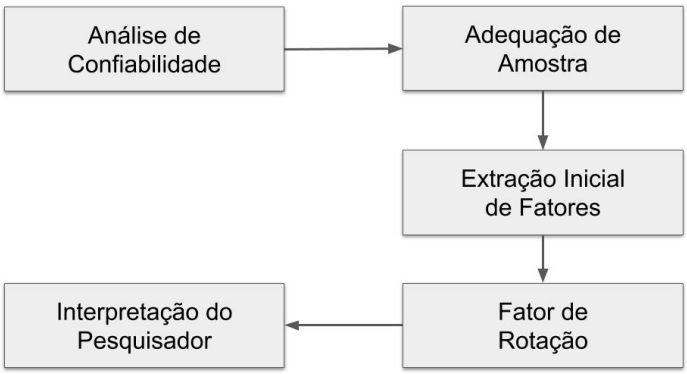

Figura 4.3: Fluxo de Avaliação do IoTPC

Para uma interpretação melhor de como foi realizada a avaliação do IoTPC, na Figura 4.2, exemplifica-se um fluxo de passos que foram dados para avaliar o instrumento. Pode-se observar que as preocupações para essa análise já iniciam verificando a confiabilidade do instrumento desenvolvido, um passo que foi dado antes de iniciar a EFA de fato. Após essa análise, várias verificações foram realizadas para garantir a integridade da EFA, assim como cuidado com o tamanho da amostra, extração inicial dos fatores, fatores de rotação e a interpretação final do pesquisador.

Com o objetivo de exemplificar como foi realizada a análise fatorial neste trabalho, expõe-se, a seguir, o detalhamento de cada passo realizado durante o processo de avaliação do instrumento.

No primeiro passo, são abordadas as preocupações em relação à confiabilidade do instrumento, apresentando a técnica utilizada para validar esse passo. Já no segundo passo são apresentadas as preocupações quanto às medições confiáveis, dessa forma, exemplificando conceitos e técnicas que foram utilizados para realizar a EFA neste trabalho. No terceiro passo são colocados conceitos e estratégias tomados sobre o número inicial de fatores que foram extraídos durante a EFA. No quarto passo são exibidos os tipos de fatores de rotação, bem como qual foi adotado neste trabalho. Por fim, no quinto e último passo são estabelecidos os critérios de interpretação dos fatores realizados pelo pesquisador.

1. **Análise de Confiabilidade**: a análise de confiabilidade foi realizada por meio do coefici-

[1]https://www.ibm.com/br-pt/analytics/spss-statistics-software

ente alfa de Cronbach (CRONBACH, 1951), que tem por objetivo estimar a confiabilidade de um questionário através das respostas dadas pelos participantes, apresentando uma correlação média entre as perguntas. A fórmula para calcular o alfa de Cronbach pode ser observada a seguir:

$$\alpha = \left(\frac{k}{k-1}\right) \cdot \left(1 - \frac{\Sigma_{i=1}^{k} s_i^2}{S_t^2}\right)$$

onde:

- k = Número de itens do instrumento.
- s_i^2 = Variância de cada item do instrumento.
- s_t^2 = Variância total do instrumento.

A importância dessa avaliação dá-se ao fato de provar que o instrumento desenvolvido é fidedigno. Os critérios de avaliação definidos por (STREINER, 2003) foram utilizados para validar o valor do alfa de Cronbach obtido, cujos valores abaixo de 0.700 são considerados insuficientes e valores acima de 0.800 são considerados suficientes, enquanto valores acima de 0.300 são considerados bons para a correlação total do item corrigido.

2. **Adequação de Amostra**: o teste esférico de Bartlett (BARTLETT, 1954) foi realizado para verificar se existia a geração de uma matriz de identidade, além de observar se as variáveis do instrumento estavam significativamente correlacionadas para a aplicação da EFA. A fórmula do teste de Bartlett é dada por:

$$T^2 = -\left[(n-1) - \frac{2k+5}{6}\right] In|R|$$

onde:

- n = Tamanho da amostra.
- k = Número de itens do instrumento.
- $|R|$ = Determinante da matriz de correlação.

Após essa análise, o tamanho da amostra também passou por uma avaliação. A medida de Kaiser-Meyer-Olkin (KMO) (KAISER, 1970) foi utilizada para validar o tamanho da amostra. A estatística KMO varia entre 0 e 1, onde o valor 0 indica que a soma das

correlações parciais é grande em relação à soma das correlações, indicando a difusão no padrão de correlações, e portanto, a análise dos fatores provavelmente não será apropriada (KAISER, 1974; FIELD, 2017). Um valor próximo a 1 indica que os padrões de correlações são relativamente compactos e, logo, a análise fatorial deve produzir fatores distintos e confiáveis, comprovando que a amostra é suficiente para o estudo (KAISER, 1974). O valor da amostra é dado pela seguinte equação:

$$KMO = \frac{\Sigma\Sigma_{j\neq k} r_{jk}^2}{\Sigma\Sigma_{j\neq k} r_{jk}^2 + \Sigma\Sigma_{j\neq k} p_{jk}^2}$$

onde:

- r_{jk} = Coeficiente de correlação entre os itens do instrumento X_j e X_k
- p_{jk} = Coeficiente de correlação parcial

Para este trabalho, foram utilizados os valores recomendados pelos autores R, onde o KMO deve retornar um valor acima de 0,5 para ser considerada uma boa amostra.

3. **Extração Inicial de Fatores**: a extração de fatores dentro de uma EFA está relacionada ao número de fatores a serem extraídos, sendo que existem basicamente quatro técnicas para realizar essa extração inicial.

   (a) **Regra de Kaiser:** devem ser extraídos fatores com autovalores maiores do que 1 (um) (KAISER, 1960; LATTIN; CARROLL; GREEN, 2011);

   (b) **Critério a Priori:** o pesquisador define quantos fatores ele quer extrair;

   (c) **Variância Acumulada:** o pesquisador deve continuar com a extração de fatores até atingir um nível mínimo de 60% de variância acumulada, o que é considerado aceitável (HAIR et al., 2006);

   (d) **Scree Test:** deve ser analisado graficamente a disseminação do número de fatores até que a curva de variância de cada fator sofra uma queda bruta ou se torne horizontal (FILHO; JÚNIOR, 2010).

Todas as técnicas foram utilizadas para o processo de avaliação do instrumento – Variância Acumulada, Regra de Kaiser, critério a priori e Scree Test – em que todos realizaram a extração das variáveis latentes por meio da Fatoração de Eixo Principal (*Principal axis Factoring* - PAF). Esse tipo de extração objetiva o menor número de fatores que podem explicar a correlação de um conjunto de variáveis.

4. **Fator de Rotação**: o fator de rotação é essencial em uma análise fatorial porque ele melhora significativamente a interpretação dos fatores. O fator de rotação potencializa o carregamento de cada variável em um dos fatores extraídos, reduzindo o carregamento em todos os outros fatores, dessa forma, esse processo torna mais clara a visualização de quais variáveis se relacionam com quais fatores (FIELD, 2017).

   De acordo com Field (2017), existem dois tipos de rotações que podem ser realizadas, a rotação ortogonal, na qual não há correlação dos fatores extraídos, e a rotação oblíqua, onde existe correlação dos fatores extraídos. A Figura 4.3 exemplifica os dois fatores de rotação apresentados, nos quais as variáveis são carregadas em eixos de um gráfico, sendo que quando esses eixos são rotacionados é possível realizar o agrupamento de variáveis.

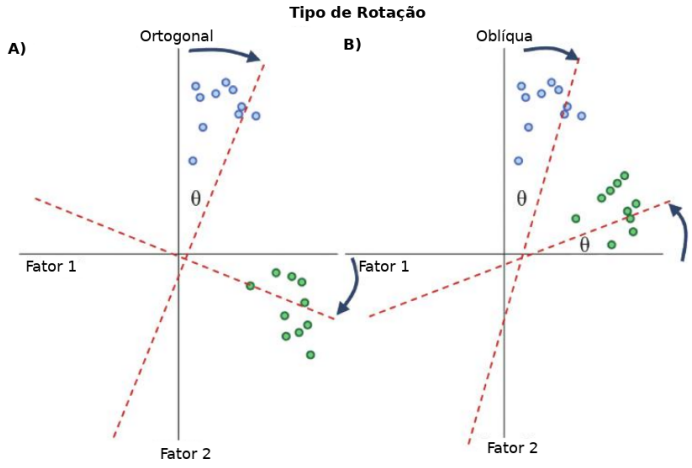

Figura 4.4: (A) Representação gráfica do Fator de Rotação Ortogonal; (B) Representação Gráfica do Fator de Rotação Oblíqua (Adaptado de (FIELD, 2017))

   Não é considerada uma tarefa fácil decidir qual rotação utilizar, por isso, Field (2017) sugere que se aplique as duas rotações; dessa forma, caso a rotação oblíqua demonstre uma correlação insignificante entre os fatores extraídos, então, é razoável usar a solução com rotação ortogonal. Os autores sugerem que correlações mais significantes sejam adotadas, com isso, simplificando a interpretação dos fatores.

5. **Interpretação do Pesquisador**: um passo considerado importante é a verificação dos fatores extraídos através da EFA e decidir quais fatores devem ser mantidos. Neste trabalho, os critérios de (FIELD, 2017) foram utilizados, onde fatores com menos de quatro variáveis carregadas foram considerados insuficientes; e fatores que representavam de 70 a 80% da variância foram mantidos.

   Após terem sido devidamente extraídos os fatores finais, foi realizada a análise dos fatores extraídos com relação à IoT para que fosse possível nomeá-los de acordo com a

característica apresentada em cada fator.

O fluxo de avaliação do IoTPC no *software SPSS* é realizado em duas etapas:

1. **Análise de Confiabilidade**: esta é encontrada no menu *"Analisar"—"Escala"—"Análise de Confiabilidade"*, nesse passo é necessário selecionar os itens do instrumento que serão avaliados e em seguida no campo *"Modelo"* selecionar a opção *"Alfa"*. No botão "Estatísticas" selecione as descritivas de *"Item"*, *"Escala"* e *"Escala se o Item foi Excluído"*. Na seção de resumos selecione as opções de *"Médias"* e *"Variâncias"*, como demonstrado na Figura 4.4.

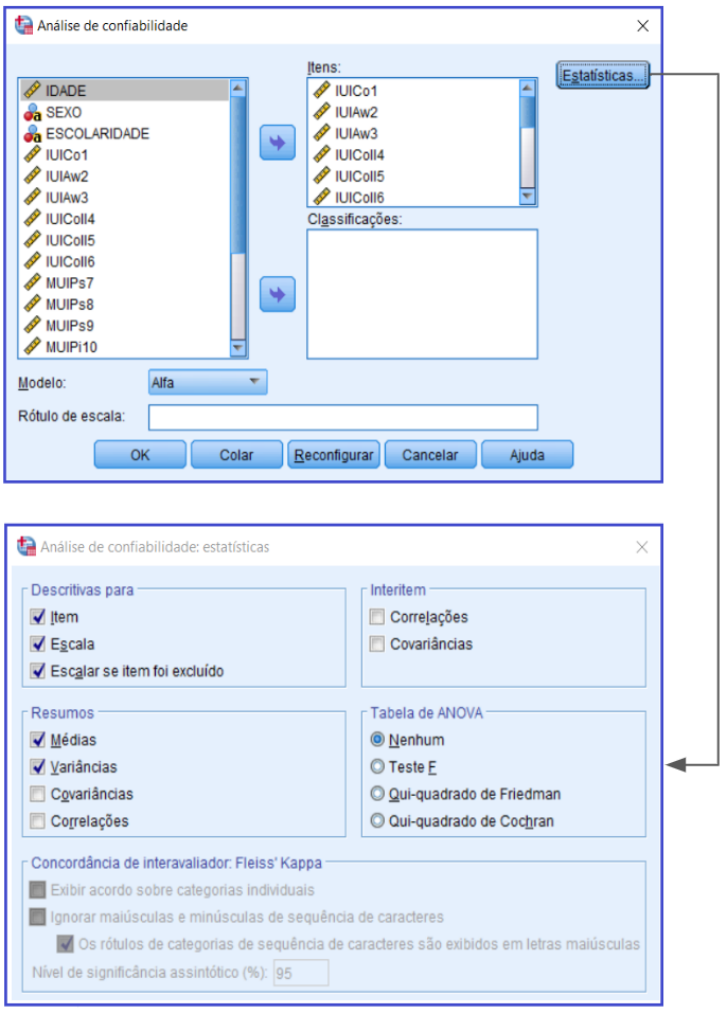

Figura 4.5: Alfa de Cronbach no *software SPSS*

2. **Análise Fatorial Exploratória**: esta é encontrada no menu *"Analisar"—"Redução de Dimensão"—"Fator"*, nesse passo é necessário selecionar os itens do instrumento que serão avaliados e, em seguida, no botão *"Descritivos"*, selecionar a opção *"Teste de esfericidade de Bartlett e KMO"*. Já no botão *"Extração"*, selecione o método *Fatoração*

pelo eixo principal e, na seção *"Exibir"*, selecione a opção *"Gráfico de escarpa"*, por fim, fixe o número de fatores a serem extraídos em três. No botão *"Rotação"*, selecione o método *"Varimax"* e a *"Solução Rotacionada"*. Por fim, no botão *"Opções"*, selecione para ordenar os dados por tamanho. Todas essas configurações no *SPSS* podem ser observadas pela Figura 4.5

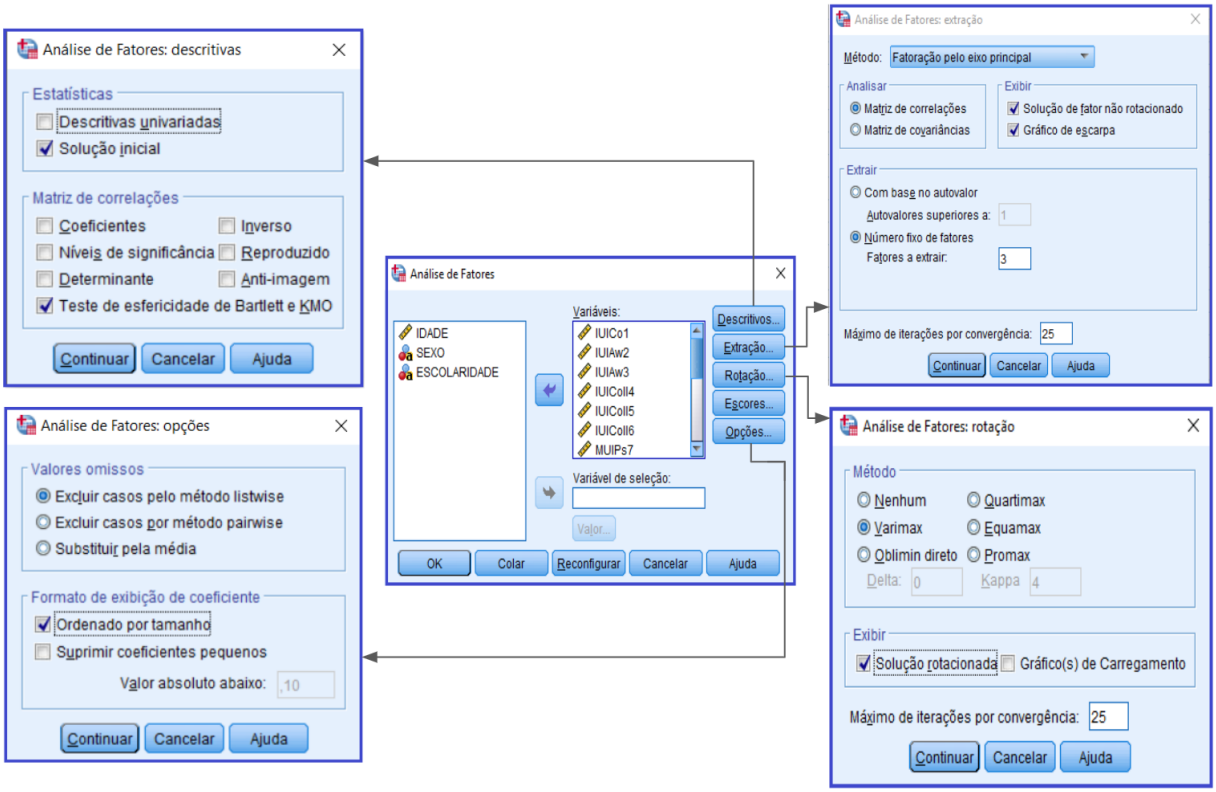

Figura 4.6: Análise Fatorial Exploratória no *software SPSS*

4.6 Considerações Finais

Neste capítulo foi abordado o processo de construção e avaliação do instrumento proposto. A elaboração de um instrumento que seja capaz de identificar com clareza o que é considerado uma informação privada ou não dentro do contexto de IoT é de grande importância, pois a privacidade não pode ser tratada como uma ciência exata. Por conseguinte, o processo de validação do instrumento proposto é de suma importância para este trabalho em razão de objetivar a garantia de confiabilidade do IoTPC.

Capítulo 5

RESULTADOS DE AVALIAÇÃO DO IOTPC

5.1 Considerações Iniciais

Neste capítulo, detalhadamente, são descritos os resultados obtidos com a avaliação do instrumento proposto. Na seção 5.2 são apresentados os resultados da avaliação do IoTPC relacionados ao estudo I e, por fim, na seção 5.3, discriminam-se os resultados da avaliação do IoTPC pertinentes ao estudo II.

Os instrumentos encontrados na literatura que serviram de base para este trabalho utilizaram itens genéricos em suas construções, não contendo nenhum instrumento que relacionasse diretamente o contexto estudado com os itens de sua escala. Em razão dessa característica em comum entre os instrumentos estudados foram desenvolvidas e avaliadas duas versões do IoTPC, desse modo, objetivando verificar qual das duas versões geraria melhores resultados – uma que produzisse itens genéricos em sua construção ou a versão do instrumento que abordasse o contexto estudado diretamente em seus itens.

5.2 Estudo I

Neste primeiro estudo[1], os itens do IoTPC mantiveram-se genéricos, conforme enunciado na seção 4.3.2, objetivando observar se os resultados de avaliação obtidos com a construção de um instrumento genérico obteriam melhores resultados se comparado a um instrumento com itens mais específicos

[1] https://github.com/brunolp15/Internet-of-Things-Privacy-Concerns/blob/master/IoTPC/Estudo-1.csv

5.2.1 Dados da População

O local escolhido para a execução deste estudo foi os Laboratórios de Informática pertencentes à Pontifícia Universidade Católica (PUC), campus de Poços de Caldas – MG. Foi tomado como amostra, pelo pesquisador responsável, um conjunto de 61 alunos, sendo estes de graduação e pós-graduação. A idade dos participantes que realizaram a pesquisa variou de 18 anos (4,9%) a 37 anos (3,3%), tendo a maior parte da amostra a idade de 20 anos (18%) e as demais 32 e 33 anos, representado 1,6% do total da idade. A Figura 5.1 exemplifica essas informações.

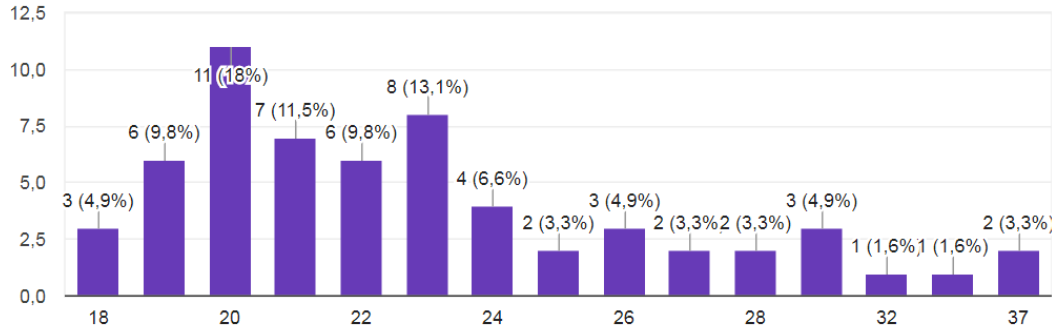

Figura 5.1: Idade dos Participantes

A população masculina foi de 52 participantes (85,2%) contra 9 participantes (14,8%) da população feminina. A escolaridade dos participantes teve pontuações de 51 (83,6%) para graduandos, 5 (8,2%) para graduados, 1 (1,6%) para pós-graduandos e 4 (6,6%) para pós-graduados. Essas informações são exemplificadas pela Tabela 5.1.

Tabela 5.1: Dados Demográficos

Sexo	**Participantes**	**Porcentagem (%)**
Masculino	52	85,2
Feminino	9	14,8
Escolaridade		
Graduando	51	83,6
Graduado	5	8,2
Pós Graduando	1	1,6
Pós Graduado	4	6,6

5.2.2 Avaliação do Instrumento

A) Análise de Confiabilidade: AAo testar a confiabilidade do IoTPC, a medida do Alfa de Cronbach retornou a um valor de (α=0,911), garantido a confiança do instrumento de acordo com as métricas de (STREINER, 2003).

A análise do Alfa de Cronbach, tão significativo, foi avaliada em quanto cada item do IoTPC contribui para o resultado, apresentando sua média e seu desvio padrão. Os detalhes estatísticos de cada item contribuindo para o Alfa de Cronbach podem ser observados pela Tabela 5.2, tais como média, desvio padrão, correlação total do item corrigida e a alteração do Alfa de Cronbach se um item do instrumento foi excluído.

Tabela 5.2: Análise do Alfa de Cronbach

Item	Média	Desvio Padrão	Correlação do Item Total Corrigida	Alfa de Cronbach se o Item for Excluído
IUICo1	4,44	0,958	0,498	0,909
IUIAw2	4,41	1,131	0,330	0,913
IUIAw3	4,74	0,705	0,502	0,909
IUIColl4	3,82	1,232	0,620	0,905
IUIColl5	4,11	1,212	0,562	0,907
IUIColl6	3,87	1,245	0,634	0,905
MUIPs7	4,28	1,280	0,332	0,914
MUIPs8	3,85	1,352	0,790	0,900
MUIPs9	3,87	1,372	0,644	0,905
MUIPi10	3,80	1,364	0,624	0,905
MUIPi11	3,97	1,211	0,536	0,908
MUISui12	4,30	1,022	0,702	0,904
MUISui13	4,21	1,112	0,697	0,903
MUISui14	4,34	1,031	0,559	0,907
AIPGen15	3,34	1,569	0,757	0,901
AIPGen16	3,59	1,383	0,444	0,911
AIPGen17	3,89	1,380	0,773	0,900

Pode-se observar que as pontuações médias dos itens individuais variaram de 3,34 para o item AIPGen15 – ”Comparado com outras pessoas, sou mais sensível sobre o modo como os dispositivos IoT lidam com minha informação pessoal” – a 4,74 para o item IUIAw3 – ”É muito importante para mim que eu esteja ciente e conhecedor sobre como minhas informações pessoais serão usadas”.

Na Correlação do Item Total Corrigida, responsável por exemplificar quanto cada item influencia para o valor total do Alfa de Cronbach, os resultados respeitaram o valor mínimo de 0,300, variando suas pontuações de 0,330 para o item IUIAw2 – ”Dispositivos IoT que buscam informações devem divulgar a forma como os dados são coletados, processados e usados” – a 0,790 para o item MUIPs8 – ”Estou preocupado que os dispositivos IoT estejam coletando muita informação sobre mim”.

B) Adequação de Amostra: a medida de adequação KMO apresentou um resultado de (KMO = 0,774), considerado um valor válido para a realização da EFA. Já o teste esférico de Bartlett apresentou um resultado de ($T<0,001$), concluindo que as variáveis estão significativamente correlacionadas para a realização da EFA.

Outro ponto importante a observar durante a EFA são as comunalidades. Durante a aplicação da EFA, as variáveis podem ser definidas como uma combinação linear de fatores comuns que irão explicar uma parcela da variância de cada variável, porém uma pequena parcela que resume essa variância total não pode ser explicada (REZENDE et al., 2007). De acordo com Hair et al. (1998), a parcela explicada pelos fatores comuns é denominada de comunalidades. As comunalidades são responsáveis por mostrar quanto cada item herda da variância total, ou seja, quanto da variância total está sendo carregada em cada item. A Tabela 5.3 apresenta o detalhamento do carregamento de cada item em relação à variância total.

Tabela 5.3: Comunalidades

	Variância Comum	**Variância Total Herdada por Cada Item**
IUICo1	0,422	0,418
IUIAw2	0,403	0,371
IUIAw3	0,558	0,355
IUIColl4	0,681	0,703
IUIColl5	0,752	0,424
IUIColl6	0,687	0,619
MUIPs7	0,457	0,183
MUIPs8	0,742	0,716
MUIPs9	0,675	0,514
MUIPi10	0,548	0,422
MUIPi11	0,632	0,645
MUISui12	0,848	0,612
MUISui13	0,756	0,611
MUISui14	0,632	0,477
AIPGen15	0,803	0,780
AIPGen16	0,553	0,275
AIPGen17	0,732	0,709

C) Extração Inicial de Fatores: ao realizar a extração inicial de fatores, a primeira técnica utilizada foi a da variância acumulada, que pode ser observada pela Tabela 5.4. Nota-se que, com a extração de 3 fatores para os 17 itens do instrumento, a variância acumulada chega a 60,138%, o que já é considerado suficiente. A regra de Kaiser resultou na extração de cinco fatores dentre os 17 itens que obtiveram um autovalor acima de 1.

A análise gráfica do *Scree Test* também foi realizada indicando que, a partir da extração de três fatores para os 17 itens do instrumento, a variância acumulada não era tão significante. A Figura 5.2 exibe essa queda abrupta de autovalores.

Tabela 5.4: Variância Total Explicada

Número de Fatores	Total	% Variância	% Cumulativa
1	7,334	43,140	43,140
2	1,532	9,014	52,154
3	1,357	7,984	60,138
4	1,234	7,261	67,398
5	1,014	5,967	73,366
6	0,759	4,466	77,832
7	0,633	3,725	81,557
8	0,603	3,549	85,106
9	0,561	3,298	88,404
10	0,439	2,584	90,987
11	0,365	2,150	93,137
12	0,299	1,762	94,899
13	0,275	1,619	96,518
14	0,221	1,301	97,819
15	0,193	1,134	98,953
16	0,101	0,593	99,545
17	0,077	0,455	100,000

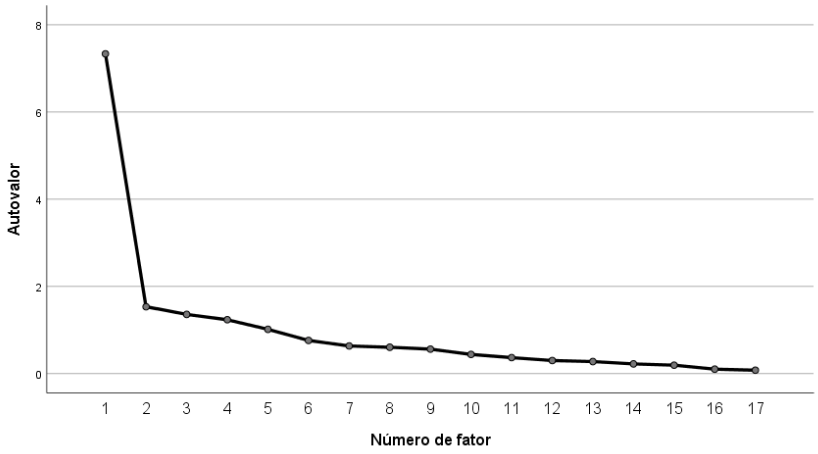

Figura 5.2: Scree Test

De acordo com essas análises, os resultados obtidos pelas técnicas de variância acumulada e *Scree Test* apontaram que o número ideal de fatores a serem extraídos do IoTPC era três. Com essas informações, foi gerada a primeira matriz de fatores extraindo três fatores. Pode-se notar, pela Tabela 5.5, que nesta primeira matriz gerada a maioria dos itens do IoTPC foi carregada no Fator 1, obtendo uma carga baixa de carregamento nos demais fatores.

D) Fator de Rotação: com a aplicação do fator de rotação *Varimax* a essa mesma matriz, pode-se observar, pela Tabela 5.6, que ocorre uma distribuição mais uniforme dos itens do IoTPC dentro dos fatores obtidos. Observa-se que o fator 1 está relacionado à di-

Tabela 5.5: Matriz de Fatores

Item	Fator 1	Fator 2	Fator 3
MUIPs8	**0,830**	-0,093	-0,135
AIPGen15	**0,804**	-0,323	0,169
AIPGen17	**0,796**	-0,202	0,185
MUISui12	**0,743**	0,245	0,028
MUISui13	**0,739**	0,229	-0,111
IUIColl6	**0,693**	-0,063	-0,367
MUIPs9	**0,692**	-0,182	-0,044
IUIColl4	**0,678**	-0,314	-0,381
MUIPi10	**0,647**	-0,007	0,060
IUIColl5	**0,585**	-0,071	-0,276
MUISui14	**0,584**	0,337	0,150
MUIPi11	**0,568**	-0,288	0,489
IUICo1	**0,519**	0,355	0,149
IUIAw3	**0,518**	0,268	-0,125
AIPGen16	0,460	0,053	0,245
MUIPs7	0,339	0,052	0,255
IUIAw2	0,367	0,482	-0,058

mensão de Requisições IoT, visto que os itens carregados neste fator pertencem a essa dimensão. O fator 2 obteve variáveis carregadas originárias das dimensões de Requisições IoT, Poder de Decisão e Preocupações Gerais de Privacidade. Por fim, o fator 3 obteve itens carregados pertencentes às dimensões de Conhecimento Prévio, Uso Secundário de Informações e Poder de Decisão.

Tabela 5.6: Matriz de Fatores Rotativa

Item	Fator 1	Fator 2	Fator 3
IUIColl4	**0,817**	0,177	0,066
IUIColl6	**0,722**	0,116	0,291
MUIPs8	**0,677**	0,379	0,336
IUIColl5	**0,595**	0,130	0,230
MUIPs9	**0,562**	0,403	0,190
MUIPi11	0,181	**0,781**	0,041
AIPGen15	0,556	**0,674**	0,127
AIPGen17	0,493	**0,643**	0,227
AIPGen16	0,133	**0,423**	0,280
MUIPi10	0,398	**0,402**	0,320
MUIPs7	0,045	**0,366**	0,218
IUIAw2	0,098	-0,001	**0,601**
MUISui14	0,167	0,325	**0,586**
MUISui12	0,386	0,347	**0,585**
IUICo1	0,117	0,283	**0,569**
MUISui13	0,478	0,244	**0,568**
IUIAw3	0,324	0,099	**0,491**

E) Interpretação do Pesquisador: o fator 1 consiste nos itens IUIColl4, IUIColl6, MUIps8, IUIColl5 e MUIps9. Essa nova dimensão do IoTPC reflete claramente a preocupação dos usuários de IoT em relação aos dados coletados por dispositivos IoT e a forma como esses dispositivos os vigiam. Devido ao fato de todos os itens carregados nesse fator pertencerem à dimensão de Requisições IoT, o fator 1, também, foi denominado Requisições IoT.

O fator 2 consta nos itens MUIPi11, AIPGen15, AIPGen17, AIPGen16, MUIPi10 e MUIPs7. Essa nova dimensão relaciona-se fortemente com dois aspectos principais, o primeiro é o fato de que os usuários IoT estão preocupados em controlar suas informações pessoais em relação aos dispositivos IoT; e o segundo fato relaciona-se com as questões gerais de privacidade, pois todos os itens que abordavam essa dimensão foram carregados nesse fator. Dado isso, o segundo fator extraído do IoTPC também foi denominado de Poder de Decisão.

O fator 3 consta nos itens IUIAw2, MUISui14, MUISui12, IUICo1, MUISui13 e IUIAw3. Essa nova dimensão reflete a preocupação dos usuários de IoT com relação a dispositivos IoT fornecerem informações coletadas por eles a terceiros, sem a autorização de seus usuários, além de se preocuparem em obter um conhecimento prévio em relação a boas práticas de privacidade. Com isso, o terceiro fator extraído do IoTPC foi denominado de Cautela. A Tabela 5.7 ilustra a organização de todos os itens dos IoTPC nos fatores extraídos.

Tabela 5.7: Organização dos Itens do IoTPC por Fatores Extraídos

Fatores	Itens
Requisições IoT	IUIColl4, IUIColl6, MUIps8, UIUColl5 e MUIps9
Poder de Decisão	MUIPi11, APIGen15, AIPGen16, AIPGen17, MUIPi10 e MUIPs7
Cautela	IUIAw2, MUISui14, MUISui12, IUICo1, MUISui13 e IUIAw3

5.3 Estudo II

Neste segundo estudo[2], os itens do IoTPC sofreram algumas alterações com a finalidade de torná-los mais específicos para o cenário de IoT. Itens como o IUIAw2 ”Dispositivos IoT que buscam informações devem divulgar a forma como os dados são coletados, processados e usados” foram alterados para ”Dispositivos domésticos como cortinas inteligentes, que buscam informações, devem divulgar a forma como os dados são coletados, processados e usados”.

[2]https://github.com/brunolp15/Internet-of-Things-Privacy-Concerns/blob/master/IoTPC/Estudo-2.csv

Dessa maneira cada um dos 25 micro cenários utilizados para a construção do IoTPC foram vinculados diretamente aos itens do instrumento. Alguns itens como IUICo1, IUIAw3, MUIPs7, AIPGen15, AIPGen16, AIPGen17 não sofreram alterações, por se tratarem de itens que refletem questões gerais de privacidade. Os novos itens do IoTPC utilizados neste segundo estudo podem ser observados na Tabela 5.8.

Tabela 5.8: Itens do IoTPC

Item	Cenário
IUICo1	A privacidade em ambientes IoT é realmente uma questão de direito dos usuários exercer controle e autonomia sobre as decisões de como suas informações são coletadas, usadas e compartilhadas.
IUIAw2	Dispositivos domésticos como cortinas inteligentes, que buscam informações, devem divulgar a forma como os dados são coletados, processados e usados.
IUIAw3	É muito importante para mim que eu esteja ciente e conhecedor sobre como minhas informações pessoais serão usadas.
IUIColl4	Normalmente me incomoda quando minha cama solicita informações sobre meu sono.
IUIColl5	Quando dispositivos como minha geladeira solicitam minhas informações bancarias, normalmente penso duas vezes antes de fornece-las.
IUIColl6	Incomoda-me fornecer informações pessoais à dispositivos como máquinas de café, ares-condicionados, termostatos entre outros.
MUIPs7	Eu acredito que a localização do meu dispositivo móvel é monitorada pelo menos parte do tempo.
MUIPs8	Estou preocupado que minha academia esteja coletando muita informação sobre mim.
MUIPs9	Estou preocupado que lojas de esportes possam estar monitorando minhas atividades através do meu dispositivo móvel.
MUIPi10	Eu sinto que, como resultado do uso de dispositivos de entretenimento, hospitalares e comerciais, outros possam saber sobre mim mais do que eu estou confortável.
MUIPi11	Eu acredito que, como resultado do uso de dispositivos de consumo veicular, autonomia veicular e pressão dos pneus, as informações sobre mim que considero privadas são agora mais acessíveis para outros mais do que eu gostaria.
MUISui12	Estou preocupado que minha faculdade possa usar minhas informações pessoais para outros fins sem me notificar ou obter minha autorização.
MUISui13	Quando forneço informações pessoais para usar ambientes IoT, estou preocupado que os dispositivos como minha cadeira ou o bebedouro possam usar minhas informações para outros fins.
MUISui14	Estou preocupado que os dispositivos, como meu departamento ou o restaurante universitário, possam compartilhar minhas informações pessoais com outras entidades sem obter minha autorização.

AIPGen15	Comparado com outros, sou mais sensível sobre o modo como os dispositivos IoT lidam com minha informação pessoal.
AIPGen16	Para mim, a coisa mais importante é manter minha privacidade intacta dos dispositivos IoT.
AIPGen17	Estou preocupado com as ameaças à minha privacidade pessoal hoje.

5.3.1 Dados da População

O local escolhido para a execução do segundo estudo foi os Laboratórios de Informática pertencentes ao Instituto Federal de São Paulo (IFSP), campus de Presidente Epitácio – SP. Foi tomado como amostra, pelo pesquisador responsável, um conjunto de 65 alunos, sendo esses alunos de graduação. A idade dos participantes que realizaram a pesquisa variou de 17 anos (7,7%) a 54 anos (1,5%), tendo a maior parte da amostra a idade de 20 anos (16,9%) e as menores 45 anos (3,1%) e 54 anos (1,5%). Essas informações são exemplificadas na Figura 5.3.

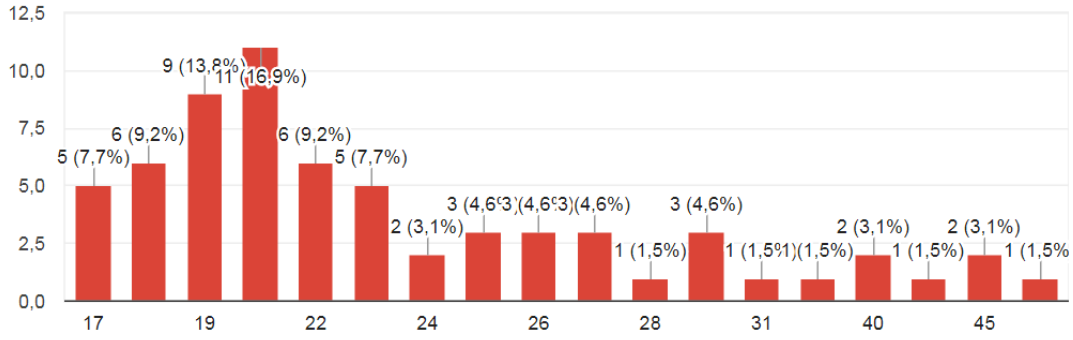

Figura 5.3: Idade dos Participantes

A população masculina do segundo estudo foi de 47 participantes (72,3%) contra 18 participantes (27,7%) da população feminina. Os cursos dos participantes obtiveram pontuações de 46 (70,8%) para Análise e Desenvolvimento de Sistemas e 19 (29,2%) para Bacharelado em Ciência da Computação. Essas informações são apresentadas na Tabela 5.9.

Tabela 5.9: Dados Demográficos

Sexo	**Participantes**	**Porcentagem (%)**
Masculino	47	72,3
Feminino	18	27,7
Curso		
Análise e Desenvolvimento de Sistemas	46	70,8
Bacharelado em Ciência da Computação	19	29,2

5.3.2 Avaliação do Instrumento

A) Análise de Confiabilidade: ao testar a confiabilidade da versão mais específica do IoTPC a medida do Alfa de Cronbach retornou um valor de (α=0,849). Esse valor é considerado relativamente alto, demonstrando que esta versão do instrumento avaliado também apresenta um alto grau de confiabilidade (STREINER, 2003).

Para atingir um valor de Alfa de Cronbach tão significativo, também, foi analisado quanto cada item do IoTPC específico contribui para esse resultado, apresentando sua média e seu desvio padrão. Os detalhes estatísticos de cada item contribuindo para o Alfa de Cronbach podem ser observados na Tabela 5.10.

Tabela 5.10: Análise do Alfa de Cronbach

Item	Média	Desvio Padrão	Correlação do Item Total Corrigida	Alfa de Cronbach se o Item for Excluído
IUICo1	4,43	0,809	-0,004	0,857
IUIAw2	4,11	1,214	0,113	0,857
IUIAw3	4,89	0,437	-0,033	0,854
IUIColl4	3,06	1,424	0,294	0,850
IUIColl5	4,20	1,148	0,385	0,844
IUIColl6	3,35	1,462	0,496	0,839
MUIPs7	4,37	1,193	0,201	0,853
MUIPs8	3,06	1,499	0,605	0,833
MUIPs9	3,85	1,337	0,650	0,831
MUIPi10	4,28	1,008	0,396	0,844
MUIPi11	3,65	1,374	0,557	0,836
MUISui12	3,42	1,550	0,745	0,824
MUISui13	3,40	1,618	0,692	0,827
MUISui14	3,88	1,341	0,697	0,828
AIPGen15	3,77	1,170	0,629	0,833
AIPGen16	3,62	1,307	0,533	0,837
AIPGen17	4,02	1,269	0,464	0,841

Pode-se verificar que as pontuações médias dos itens individuais variam de 3,06 para os itens IUIColl4 ”Normalmente me incomoda quando minha cama solicita informações sobre meu sono” e MUIPs8 ”Estou preocupado que minha academia esteja coletando muita informação sobre mim” a 4,89 para o item IUIAw3 ”É muito importante para mim que eu esteja ciente e conhecedor sobre como minhas informações pessoais serão usadas”.

A correlação do item total corrigida neste segundo estudo violou o valor crítico de 0,300 em alguns itens, como, por exemplo, os itens IUICo1 com -0,004, IUIAw2 com 0,113, IUIAw3 com -0,033, IUIColl4 com 0,294 e MUIPs7 com 0,201, mostrando que os itens dessa versão do IoTPC contêm uma baixa correlação.

B) Adequação da Amostra: a medida de adequação de amostra KMO gerou um resultado de (KMO=0,718), também, acima do valor mínimo de 0,5, sendo considerada um valor válido para a realização da análise fatorial. O teste esférico de Bartlett apresentou um resultado de (T<0,001), dessa forma, confirmando que não houve a geração de uma matriz de identidade.

As comunalidades do segundo estudo obtiveram valores de extração variando entre 0,123 para o item MUIPs7 "Eu acredito que a localização do meu dispositivo móvel é monitorada pelo menos parte do tempo"a 0,873 para o item IUIAw3 "É muito importante para mim que eu esteja ciente e conhecedor sobre como minhas informações pessoais serão usadas". A Tabela 5.11 elenca o detalhamento do carregamento de cada item em relação à variância total.

Tabela 5.11: Comunalidades

Item	Variância Comum	Variância Total Herdada por Cada Item
IUICo1	0,182	0,159
IUIAw2	0,294	0,259
IUIAw3	0,385	0,873
IUIColl4	0,554	0,522
IUIColl5	0,273	0,251
IUIColl6	0,608	0,704
MUIPs7	0,275	0,123
MUIPs8	0,514	0,480
MUIPs9	0,626	0,636
MUIPi10	0,486	0,343
MUIPi11	0,535	0,439
MUISui12	0,769	0,818
MUISui13	0,716	0,631
MUISui14	0,741	0,738
AIPGen15	0,615	0,696
AIPGen16	0,522	0,672
AIPGen17	0,550	0,562

C) Extração Inicial de Fatores: para o segundo estudo, os resultados com a extração inicial de fatores com a regra de Kaiser assinalaram a extração de cinco fatores para os 17 itens do instrumento, que obtiveram um autovalor acima de 1. A técnica de variância acumulada indica que, com a extração de cinco fatores para os 17 itens do instrumento, a variância cumulativa chegou a 65,307%, o que já atenderia a esse critério. A variância acumulada pode ser observada pela Tabela 5.12.

A técnica *Scree Test* foi aplicada indicando que, a partir da extração de cinco fatores para os 17 itens do instrumento, a variância acumulada não era tão significante. A Figura 5.4 exibe essa queda abrupta de autovalores.

Tabela 5.12: Variância Total Explicada

Número de Fatores	Total	% Variância	% Cumulativa
1	5,496	32,329	32,329
2	1,691	9,949	42,278
3	1,406	8,272	50,550
4	1,321	7,770	58,319
5	1,188	6,988	65,307
6	0,951	5,593	70,900
7	0,865	5,086	75,986
8	0,779	4,583	80,569
9	0,724	4,258	84,827
10	0,535	3,147	87,974
11	0,478	2,814	90,788
12	0,429	2,524	93,312
13	0,323	1,899	95,211
14	0,314	1,847	97,058
15	0,195	1,149	98,207
16	0,181	1,065	99,271
17	0,124	0,729	100,000

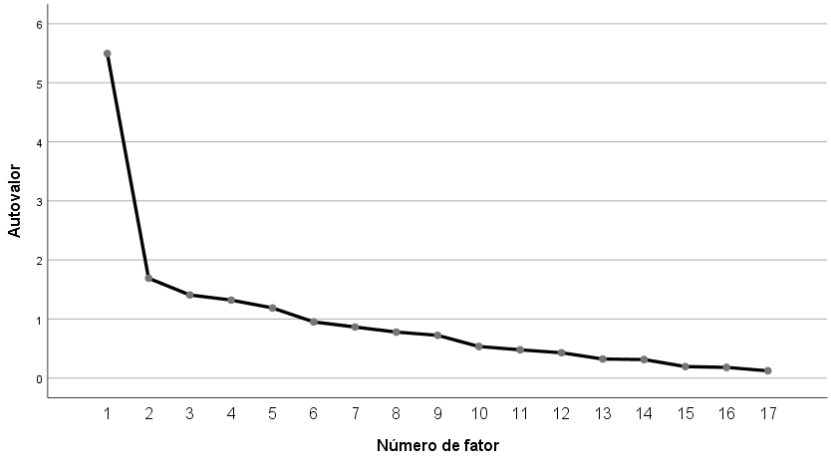

Figura 5.4: Gráfico de Scree

Com essas avaliações, os resultados obtidos pelas técnicas de variância acumulativa, regra de Kaiser e *Scree Test* foram consideradas para a extração inicial de fatores da nova versão do IoTPC. Pode-se observar na Tabela 5.13 que, nesta primeira matriz gerada, assim como no estudo I, a maioria dos itens do IoTPC foi carregada no fator 1, obtendo uma carga baixa nos demais fatores.

Tabela 5.13: Matriz de Fatores

Item	Fator 1	Fator 2	Fator 3	Fator 4	Fator 5
MUISui12	**0,849**	-0,227	0,022	0,058	-0,207
MUISui14	**0,775**	-0,269	0,059	0,180	-0,171
MUISui13	**0,771**	-0,067	-0,005	0,083	-0,160
MUIPs9	**0,709**	-0,179	-0,122	0,292	0,035
AIPGen15	**0,675**	-0,057	0,215	-0,314	0,305
MUIPs8	**0,663**	-0,147	-0,013	-0,118	0,066
MUIPi11	**0,600**	0,172	-0,135	0,057	0,167
AIPGen16	**0,581**	0,227	0,162	-0,504	0,043
IUIColl6	**0,554**	0,531	-0,222	0,187	0,175
AIPGen17	**0,546**	0,011	-0,008	-0,391	-0,332
MUIPi10	**0,412**	-0,109	0,203	0,345	0,034
IUIColl5	**0,406**	0,183	0-,161	0,144	0,074
IUIColl4	0,328	**0,641**	-0,037	0,029	-0,039
IUIAw3	-0,058	0,306	**0,835**	0,262	-0,097
IUIAw2	0,121	-0,197	**0,346**	-0,139	0,259
IUICo1	-0,002	-0,252	-0,009	0,041	**0,306**
MUIPs7	0,198	-0,099	0,014	0,106	**0,250**

D) Fator de Rotação: assim como no estudo I, a rotação *Varimax* foi utilizada para potencializar o carregamento dos itens nos fatores. Pode-se observar na Tabela 5.14 que, com a aplicação de um fator de rotação, a matriz obteve um carregamento mais distribuído dos itens dentro dos fatores.

Notou-se que o fator 1 se relacionou às dimensões de Uso Secundário de Informações, Requisições IoT e Poder de Decisão, visto que os itens carregados neste fator pertencem a essas dimensões. O fator 2 obteve variáveis carregadas originárias da dimensão de Preocupações Gerais de Privacidade. O fator 3 obteve itens carregados pertencentes às dimensões de Requisições IoT e Poder de Decisão. No fator 4, apenas, a dimensão de Conhecimento Prévio foi carregada. Por fim, no fator 5, as dimensões relacionadas a esse fator foram as dimensões de Requisições IoT e Conhecimento Prévio.

Tabela 5.14: Matriz de Fatores Rotativa

Item	Fator 1	Fator 2	Fator 3	Fator 4	Fator 5
MUISui12	**0,828**	0,336	0,132	-0,043	0,006
MUISui14	**0,825**	0,209	0,098	0,015	0,069
MUIPs9	**0,710**	0,056	0,279	-0,095	0,204
MUISui13	**0,697**	0,285	0,249	-0,015	-0,024
MUIPs8	**0,496**	0,408	0,164	-0,111	0,170
MUIPi10	**0,481**	-0,038	0,124	0,245	0,189
AIPGen16	0,144	**0,760**	0,266	0,042	-0,044
AIPGen15	0,316	**0,660**	0,195	0,056	0,346
AIPGen17	0,371	**0,562**	0,050	-0,126	-0,299
IUIColl6	0,217	0,100	**0,804**	-0,018	0,001
IUIColl4	0,013	0,165	**0,637**	0,148	-0,259
MUIPi11	0,351	0,228	**0,490**	-0,080	0,135
IUIColl5	0,263	0,050	**0,416**	-0,066	0,036
IUIAw3	-0,026	-0,005	0,000	**0,930**	-0,083
IUICo1	0,014	-0,033	-0,091	-0,078	**0,378**
IUIAw2	0,036	0,271	-0,157	0,205	**0,343**
MUIPs7	0,147	0,022	0,104	0,002	**0,300**

E) Interpretação do Pesquisador: como apresentado na seção 4.5, foram conservados apenas os fatores com quatro ou mais variáveis carregadas, com isso, os fatores 2, 4 e 5 foram excluídos. O primeiro fator (fator 1) consiste nos itens MUISui12, MUISui14, MUIps9, MUISui13, MUIps8 e MUIPi10. Essa nova dimensão do IoTPC, na versão com itens específicos, apresenta as preocupações dos usuários em relação aos dados coletados por dispositivos IoT e a forma como esses dispositivos tratam essas informações. Os usuários se questionaram se as informações coletadas pelos dispositivos são usadas apenas para o fim proposto ou se essas informações também são compartilhadas com terceiros, ferindo assim o poder de controle dos usuários IoT.

O segundo fator (fator 3) consiste nos itens IUIColl6, IUIColl4, MUIPi11 e IUIColl5. Essa nova dimensão do IoTPC, na versão com itens específicos, também, está atrelada à coleta de dados realizada por dispositivos IoT de forma imprudente, não permitindo que seus usuários tenham controle sobre suas informações.

5.3.3 Comparando a Análise de Confiabilidade

Apesar de ambos os instrumentos terem obtido um alto valor de confiabilidade, o IoTPC genérico mostrou-se mais fidedigno, obtendo um Alfa de Cronbach de 0,911 contra 0,849 do

IoTPC específico. Outro ponto a observar no estudo II é que, em alguns itens, os valores para a correlação do item total corrigida atingiram níveis críticos inferiores a 0,300, em alguns casos, chegando a valores negativos, como, por exemplo, os itens IUICo1 e IUIAw3. Por sua vez, o IoTPC genérico não violou em nenhum dos seus itens esse valor crítico, obtendo como menores valores os itens IUIAw2 com 0,330 e MUIPs7 com 0,332, afirmando que os itens dessa versão do instrumento contêm uma alta correlação.

5.3.4 Comparando a Análise Fatorial Exploratória

O teste esférico de Barlett apresentou resultado igual em ambos os estudos ($T<0{,}001$), porém o teste de amostragem KMO revelou-se mais eficaz com a amostra do estudo I, com o valor de 0,774 contra 0,718 do segundo estudo.

As comparações com relação ao número de fatores a serem extraídos dos instrumentos de ambos os estudos podem ser observadas de maneira clara. No estudo I, o percentual de variância cumulativa atingiu o valor mínimo de 60% com o carregamento de três fatores, contra cinco do segundo estudo, obtendo o mesmo número de fatores extraídos pelo *Scree Test*.

Com a aplicação da rotação *Varimax*, o IoTPC genérico obteve seus itens distribuídos igualitariamente nos três fatores extraídos inicialmente, tendo como menor valor o item MUIPs7 com uma carga fatorial de 0,366. No segundo estudo, os cinco fatores foram reduzidos de acordo com a regra a priori, apresentada na seção 4.5, gerando apenas a extração de dois fatores, representando cerca de 42% da variância acumulada não sendo considerado válido.

5.4 Considerações Finais - IoTPC

Como observado no decorrer deste capítulo, foi relatado todo o processo de avaliação das duas versões do instrumento proposto, bem como seus respectivos resultados. Detectou-se que a versão do IoTPC genérica apresentada pelo estudo I se mostrou superior à versão do IoTPC mais específico. O instrumento do estudo I obteve avaliações superiores em quase todos os quesitos comparados com o instrumento do segundo estudo, tais como confiabilidade, tamanho da amostra, correlação dos itens e menor número de fatores extraídos. Com essa avaliação de ambas as versões do IoTPC, foi adotado para este trabalho a versão genérica do IoTPC apresentada no estudo I, constituída de 17 itens distribuídos em três dimensões (Requisições IoT, Poder de Decisão e Cautela), como a versão final deste instrumento.

Capítulo 6

CRIAÇÃO DO MÓDULO DE INFERÊNCIA *IoTPC Learning*

6.1 Considerações Iniciais

Neste capítulo, apresenta-se a construção do módulo de inferência *IoTPC Learning* e os resultados obtidos com sua avaliação. Na seção 6.2, é descrito o módulo de inferência *IoTPC Learning*, bem como suas regras de conversão e técnicas aplicadas. Por fim, na seção 6.3, os resultados alcançados com o modelo de aprendizagem do *IoTPC Learning* são exemplificados.

6.2 Módulo de Inferência *IoTPC Learning*

Com a finalidade de utilizar o IoTPC para auxiliar em um mecanismo de preservação de privacidade em ambientes IoT foi construído um módulo de inferência de cenários IoT denominado de *IoTPC Learning*. A seguir é descrito o processo de construção desse módulo, relatando seu desenvolvimento, bem como as técnicas utilizadas.

6.2.1 Regras de Conversão

No contexto de módulos de inferência foram criadas regras de conversão objetivando transpor as respostas dadas pelos participantes da pesquisa em respostas binárias, com isso, foi possível realizar a inferência de cenários IoT por meio do IoTPC. As informações e os serviços solicitados pelos cenários utilizados na construção do IoTPC foram classificados da seguinte maneira: (I) Informação Crítica - IC, (II) Informação Simples - IS, (III) Serviço Crítico - SC e (IV) Serviço Simples - SS. Uma visão geral sobre as regras de conversão pode ser observada na

Tabela 6.1.

Tabela 6.1: Regras de Conversão

	Informação Critica - IC	**Informação Simples - I.S**	**Serviço Critico - S.C**	**Serviço Simples - S.S**
Concordo Completamente	Não	Não	Não	Não
Concordo Parcialmente	Não	Não	Não	Não
Não sei Opinar	Não	Sim	Sim	Não
Discordo Parcialmente	Sim	Sim	Sim	Sim
Discordo Completamente	Sim	Sim	Sim	Sim

A Informação Crítica - IC diz respeito a cenários que desejam coletar dados sensíveis; – documentos, registros bancários entre outros –, como em: ”A geladeira deseja ter acesso aos seus dados bancários para poder comprar alimentos assim que estiverem fora de estoque”.

A Informação Simples - IS refere-se à coleta de informações menos sensíveis, tais como preferências musicais, preferências de alimentos, entre outras, como o cenário ”O ar-condicionado do seu escritório quer saber suas preferências de temperatura para ajustar a temperatura”.

De maneira similar à classificação de informações, alguns dos cenários IoT, além de informar o tipo de informação coletada, indicam também a finalidade dessa coleta, com isso o Serviço Crítico - SC aborda cenários cuja finalidade gera economia de recursos, como combustível, energia, entre outros, por exemplo: ”O termostato da sua casa quer saber o seu cronograma do dia para ajustar a temperatura de acordo e economizar energia”.

Já o Serviço Simples - SS refere-se a serviços menos sensíveis, relacionando-se a cenários que utilizam as informações dos usuários para tarefas menos importantes, como ”A academia deseja suas preferências musicais para tocar apenas músicas de sua preferência”.

As respostas dadas pelos usuários foram associadas a uma saída ”Sim”ou ”Não”, disponibilizando ou não a informação solicitada, determinando os resultados de inferência para o cenário vinculado àquele item do instrumento.

Em alguns casos, um só item do IoTPC pode refletir a resposta de inferência para mais de um cenário IoT, sendo possível obter mais de uma classificação de serviço ou informação para esses cenários. Alguns dos itens do instrumento refletem características gerais de privacidade, por isso, foram associados a todos os 25 cenários IoT utilizados na construção do IoTPC. Uma visão geral sobre a classificação de cenários de acordo com o tipo de serviço ou informação pode ser observada pela Tabela 6.2.

Tabela 6.2: Classificação de Cenários de Acordo com o Tipo de Serviço ou Informação

Item	Dimensões De Construção	Fatores Extraídos	Cenário	Tipo de Informação ou Serviço
1*	Poder de Decisão	Cautela	1 a 25	I.S, I.C, S.S, S.C
2	Conhecimento Prévio	Cautela	1	S.S
3*	Conhecimento Prévio	Cautela	1 a 25	I.S, I.C, S.S, S.C
4	Requisições IoT	Requisições IoT	2	I.S
5	Requisições IoT	Requisições IoT	4	I.C
6	Requisições IoT	Requisições IoT	3, 11, 12, 13, 24	S.S, S.C
7*	Requisições IoT	Poder de Decisão	1 a 25	I.S, I.C, S.S, S.C
8	Requisições IoT	Requisições IoT	8, 9	S.S
9	Requisições IoT	Requisições IoT	5, 10	S.S
10	Poder de Decisão	Poder de Decisão	6, 7, 18	S.S, SC
11	Poder de Decisão	Poder de Decisão	14, 15, 16, 17	S.S, SC
12	Uso Secundário	Cautela	25	S.S
13	Uso Secundário	Cautela	21, 22, 23	I.S
14	Uso Secundário	Cautela	19, 20	I.S
15*	Preocupações Gerais	Poder de Decisão	1 a 25	I.S, I.C, S.S, S.C
16*	Preocupações Gerais	Poder de Decisão	1 a 25	I.S, I.C, S.S, S.C
17*	Preocupações Gerais	Poder de Decisão	1 a 25	I.S, I.C, S.S, S.C

6.2.2 Técnicas Aplicadas

A primeira etapa na construção do *IoTPC Learning* foi gerar uma base de dados com os resultados de inferência obtidos a partir das regras de conversão, o que levou à escolha de um algoritmo de aprendizado de máquina que fosse capaz de inferir as respostas para esses cenários de acordo com as preferências de privacidade dadas pelo IoTPC.

A árvore de decisão foi selecionada neste trabalho como modelo de aprendizagem devido ao tamanho pequeno da base de dados e pelo fato de a maioria dos atributos ser descritiva, contendo apenas duas saídas possíveis, sim ou não.

Uma árvore de decisão é definida como um procedimento de classificação que visa particionar repetitivamente um conjunto de dados em subdivisões menores, baseando-se em um conjunto de testes definidos em cada ramificação da árvore (FRIEDL; BRODLEY, 1997).

Um exemplo gráfico de árvore de decisão pode ser observado pela Figura 6.1, onde é exemplificado quando um jogador de tênis deve sair para jogar de acordo com o clima. Observa-se que, na ramificação à esquerda da árvore, quando estiver ensolarado e houver umidade elevada, ele não deverá sair para jogar, porém, quando estiver ensolarado e a umidade for normal, ele poderá praticar seu esporte normalmente. E da mesma maneira as regras estendem-se para o clima nublado e chuvoso, como apresentado pelas ramificações centrais e mais à direita da figura.

O software de aprendizado de máquina Weka[1] foi utilizado para gerar os modelos de apren-

[1] https://www.cs.waikato.ac.nz/ml/index.html

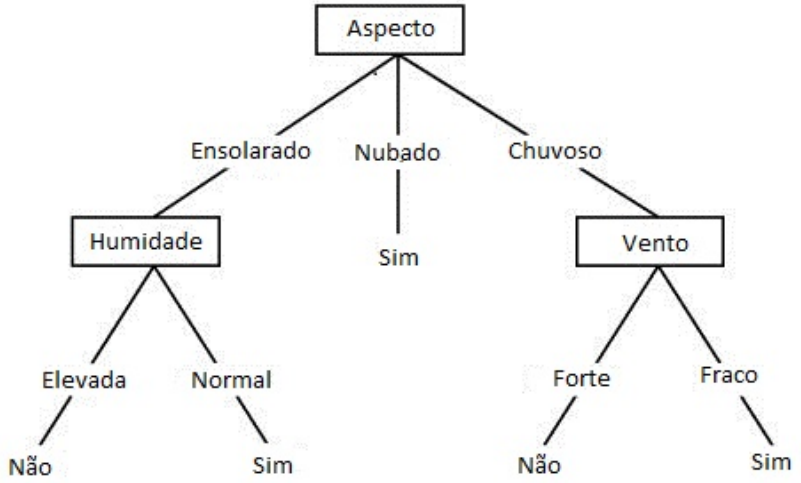

Figura 6.1: Árvore de Decisão para Jogar Tênis (Adaptado de (HV, 2017))

dizagem, porém para isso algumas precauções e adaptações foram realizadas antes de gerar as árvores de decisão. Foi aplicada a técnica de poda objetivando evitar o *overfitting* (AGGARWAL, 2014), além de um filtro de reamostragem *(Resample)*, com a finalidade de realizar o balanceamento das classes. Por fim, o cross-validation com dez folds foi utilizado para o treinamento e teste da base de dados (AGGARWAL, 2014)

Para cada um dos 25 cenários foi gerada uma árvore de decisão correspondente, cuja inferência foi baseada apenas nos atributos pessoais dos usuários, sem permitir que os outros 24 cenários influenciassem na tomada de decisão.

6.3 Resultados de Avaliação do *IoTPC Learning*

6.3.1 Análise de Resultados

Os resultados[2] das 25 árvores de decisão geradas para inferir os cenários do IoTPC são apresentados de forma agrupada a seguir. Como pode ser observado na Figura 6.2, dos 61 dados de treinamento utilizados para o modelo de aprendizagem, aproximadamente 79.21% foram previstos corretamente, representando 48,32 respostas. Já para as predições erradas, foi gerado um percentual de cerca de 20.45%, o que equivale a 12.48 respostas. Em termos gerais, a média do nível de acurácia dos 25 modelos gerados foi de 79.20%.

Alguns pontos interessantes são individuados mediante a análise de cada um desses modelos. Na Figura 6.3, pode-se observar claramente que o nível de predições corretas é superior ao

[2]https://github.com/brunolp15/Internet-of-Things-Privacy-Concerns/blob/master/IoTPC-Learning/dataset.arff

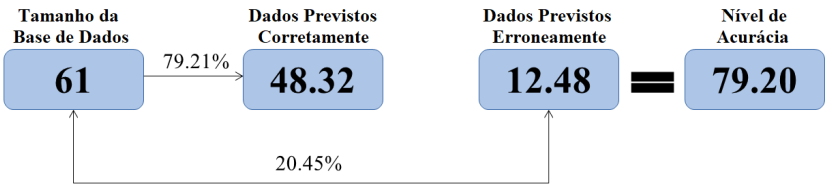

Figura 6.2: Nível de acurácia do processo de aprendizagem

nível de predições incorretas e que, em casos específicos, alguns cenários obtiveram o mesmo valor de inferências corretas e erradas, assim como o mesmo valor de acurácia, o que pode ser exemplificado pelos cenários 14 e 15. Essa semelhança de valores deu-se pelo fato de que, entre os 25 cenários utilizados, alguns tratam de situações parecidas. Nesse exemplo, o cenário 14 – "Seu carro quer acesso ao seu destino para calcular a rota mais econômica"– e o cenário 15 – "Seu carro quer informações sobre seu itinerário para determinar se tem autonomia para o percurso"– tratam de maneira geral sobre a economia de combustível em veículos; logo, já era esperado que os modelos para esses dois cenários fossem similares.

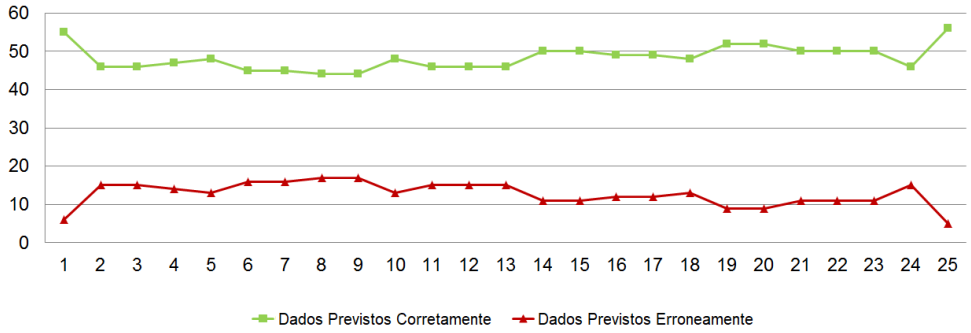

Figura 6.3: Relação individual do número de dados previstos corretamente em cada cenário

Entre as árvores de decisão geradas, além do percentual de instâncias classificadas corretamente, foi observada a precisão dessas classificações. Os resultados detalhados de cada modelo gerado podem ser observados pela Tabela 6.3.

A estrutura do *IoTPC Learning* é dividida nos três fatores de privacidade extraídos da análise fatorial exploratória: requisições IoT, poder de decisão e cautela. Dessa forma, as 25 árvores de decisão desenvolvidas foram distribuídas entre esses três fatores, tornando possível obter um controle sobre qual dimensão pertence às requisições realizadas ao módulo de inferência.

Os resultados obtidos com o *IoTPC Learning* podem apresentar um nível de acurácia menor em relação a módulos existentes em alguns mecanismos de negociação de privacidade, como o PrivacyApplication (COUTO; ZORZO, 2018); porém alguns pontos devem ser destacados.

Tabela 6.3: Detalhes de inferência de cada modelo gerado

Árvore de Decisão	Inferidos Corretamente	Inferidos Erroneamente	Precisão	Instâncias Classificadas Corretamente (%)
1	55	6	0,94	90,16
2	46	15	0,75	75,4
3	46	15	0,74	75,4
4	47	14	0,79	77,04
5	48	13	0,79	78,68
6	45	16	0,73	73,77
7	45	16	0,73	73,77
8	44	17	0,72	72,13
9	44	17	0,72	72,13
10	48	13	0,79	78,68
11	46	15	0,74	75,4
12	46	15	0,74	75,4
13	46	15	0,74	75,4
14	50	11	0,81	81,96
15	50	11	0,81	81,96
16	49	12	0,82	80,32
17	49	12	0,82	80,32
18	48	13	0,78	78,68
19	52	9	0,85	85,24
20	52	9	0,85	85,24
21	50	11	0,82	81,96
22	50	11	0,82	81,96
23	50	11	0,82	81,96
24	46	15	0,74	75,4
25	56	5	0,91	91,8

No *PrivacyApplication* e em outros mecanismos de negociação de privacidade, o processo de aprendizado dos seus módulos de inferência é dado pelo uso contínuo do mecanismo, tendo o usuário de responder a uma série de perguntas de inferência até que o mecanismo tenha capacidade de começar a inferir corretamente. Com a integração do *IoTPC Learning* a esses mecanismos, essa calibração inicial não seria necessária, uma vez que juntos – o instrumento desenvolvido e o modelo de aprendizagem – já são capazes de indicar quais informações são consideradas privadas ou não naquele ambiente. Outro ponto a observar é que as validações utilizadas na construção do *IoTPC Learning*, tais como técnica de poda e balanceamento de classes, garantem um maior grau de confiabilidade do módulo. Uma vez que o *IoTPC Learning* está atuando em um mecanismo de negociação de privacidade, sua capacidade de aprendizado torna-se contínua. Conforme o *IoTPC Learning* é utilizado, ele agrega a capacidade de aprender com novos usuários, assim, melhorando gradativamente suas predições.

6.4 Considerações Finais

Neste capítulo foi abordado o processo de construção do módulo de inferência *IoTPC Learning*. Alguns pontos importantes valem a pena serem destacados quanto a esse processo, tais como o fato de que as regras de conversão para definir se o usuário disponibilizaria ou não uma informação em determinado cenário terem sido criadas por um especialista em privacidade em ambientes IoT, neste caso, o pesquisador responsável pelo presente trabalho. Uma limitação evidente deu-se em relação ao modelo de aprendizagem, apesar de ter-se obtido resultados de acurácia satisfatórios, seria interessante uma base de dados maior para realizar o treinamento do modelo, assim, gerando resultados mais precisos, da mesma forma, mais atributos pessoais sobre os usuários, como, por exemplo, posição política, condição financeira, região onde reside, entre outros, o que ajudaria a traçar um perfil melhor desses usuários, além de contribuir para maior precisão do modelo de aprendizagem.

Capítulo 7

CONCLUSÕES E TRABALHOS FUTUROS

7.1 Conclusões

Este trabalho apresentou o processo de construção de um instrumento capaz de mensurar a preocupação com a privacidade dos usuários dentro de cenários IoT; o desenvolvimento de um módulo de inferência de cenários IoT e seus resultados. Oferece, desse modo, como contribuição a construção de um instrumento novo, devidamente validado, capaz de mensurar tais preocupações, além de uma opção de módulo de inferência de cenários IoT para auxiliar mecanismos de negociação de privacidade.

As análises do instrumento evidenciaram a classificação dos itens avaliados em três fatores, além de verificar o grau de confiabilidade do instrumento. Os três fatores permitiram estratificar as preocupações de privacidade em três grandes grupos, o primeiro grupo é representado pelos usuários que se preocupam com a forma que os dispositivos IoT coletam suas informações pessoais e como podem utilizar essa coleta para vigiá-los. O segundo grupo é representado por usuários que se preocupam em controlar suas informações pessoais e que, por conta dessa preocupação, consideram-se mais sensíveis no que tange à sua privacidade pessoal. Por fim, o terceiro grupo é representado pelos usuários que se preocupam com o fato de dispositivos IoT estarem compartilhando suas informações pessoais com terceiros sem sua autorização. Essa ação indevida acaba levando os usuários a aprenderem boas práticas sobre como manter uma privacidade maior dos seus dados pessoais.

Já as análises do *IoTPC Learning* apresentaram a construção de 25 modelos de aprendizagem, sendo que cada modelo representa o resultado de inferência correspondente a um cenário IoT. O módulo também indica uma solução inicial de inferência para mecanismos de negociação de privacidade, podendo gerar um *feedback* sobre as dimensões de privacidade mais solicitadas

pelos dispositivos IoT. Este caso de uso de utilização do instrumento evidenciou que o módulo pode ser útil em outros mecanismos de negociação de privacidade, disponibilizando opções de integração do *IoTPC Learning* com esses mecanismos, assim, resultando em melhorias significativas e até mesmo em novas funcionalidades.

Conquanto os esforços empregados, este trabalho enfrentou algumas limitações. O fato de que o contexto da privacidade estudado neste trabalho é o de IoT acabou levando o desenvolvimento do instrumento a um cenário específico, portanto, não contemplando todas as possibilidades de violação de privacidade possíveis em um ambiente de IoT. O tamanho pequeno da base de dados e a quantidade de *features* relativamente baixa, contando apenas com idade, sexo e escolaridade, também, influenciaram na construção e validação do módulo de inferência.

7.2 Trabalhos Futuros

Trabalhos futuros poderiam visar à aplicação da Análise Fatorial Confirmatória *(Confirmatory Factor Analysis - CFA)* a fim de confirmar os dados obtidos por meio da EFA; além de verificar se o módulo de inferência desenvolvido obtém um nível de acurácia maior quando comparado a módulos de outros mecanismos de negociação de privacidade com o decorrer da sua utilização.

Outra abordagem possível seria utilizar o aprendizado de máquina para verificar se os algoritmos de classificação agrupam os perfis de usuários do IoTPC de acordo com os fatores extraídos pela EFA.

7.3 Trabalhos Publicados

Durante o desenvolvimento deste trabalho o seguinte artigo foi publicado.

1. Lopes, B. Zorzo, S. D. Pontes, D. R. G. D. ”An Instrument for Measuring Privacy in IoT Environments”, 16th International Conference on Information Technology : New Generations, 1 a 3 de Abril de 2019 em Las Vegas, Nevada.

REFERÊNCIAS

AAZAM, M.; HUH, E.-N. Fog computing and smart gateway based communication for cloud of things. In: IEEE. *Future Internet of Things and Cloud (FiCloud), 2014 International Conference on*. Barcelona, 2014. p. 464–470. ISBN 978-1-4799-4357-9.

AGGARWAL, C. C. Data classification: algorithms and applications. CRC Press, 2014.

ALABA, F. A. et al. Internet of things security: A survey. *Journal of Network and Computer Applications*, Elsevier, v. 88, p. 10–28, 2017. ISSN 1084-8045.

BALTE, A.; KASHID, A.; PATIL, B. Security issues in internet of things (iot): A survey. *International Journal of Advanced Research in Computer Science and Software Engineering*, v. 5, n. 4, 2015. ISSN 2277-6451.

BARTLETT, M. S. A note on the multiplying factors for various χ 2 approximations. *Journal of the Royal Statistical Society. Series B (Methodological)*, JSTOR, p. 296–298, 1954. ISSN 2517-6161.

BASILEVSKY, A. T. Statistical factor analysis and related methods: theory and applications. John Wiley & Sons, v. 418, 2009.

BUCK, C.; BURSTER, S. App information privacy concerns. *AMCIS – The Americas Conference on Information Systems*, Boston, p. 1–10, 2017.

CATE, F. H. The failure of fair information practice principles. *Consumer Protection in the Age of the "Information Economy - Ashgate Publishing*, p. 341–349, 2006.

CHILD, D. The essentials of factor analysis. A&C Black, 2006.

CHILD, J. T.; PEARSON, J. C.; PETRONIO, S. Blogging, communication, and privacy management: Development of the blogging privacy management measure. *Journal of the Association for Information Science and Technology*, v. 60, n. 10, p. 2079–2094, 2009. ISSN 2330-1635.

CLARKE, R. Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, ACM, v. 42, n. 2, p. 60–67, 1999. ISSN 0001-0782.

COUTO, F. R. P.; ZORZO, S. Privacy negotiation mechanism in internet of things environments. *AMCIS – The Americas Conference on Information Systems*, New Orleans, p. 1–10, 2018.

COVERT, A. O. E. *Ethical Challenges of the Internet of Things*. 2014. Disponível em: <https://www.scmagazine.com/ethical-challenges-of-the-internet-of-things/article/538993/1/>.

CRONBACH, L. J. Coefficient alpha and the internal structure of tests. *psychometrika*, Springer, v. 16, n. 3, p. 297–334, 1951. ISSN 1860-0980.

EVANS, D. *The internet of things: How the next evolution of the internet is changing everything*. 2011. Disponível em: <https://tinyurl.com/ydytlqm7>.

FIELD, A. Discovering statistics using ibm spss statistics: North american edition. SAGE, 2017.

FILHO, D. B. F.; JÚNIOR, J. A. d. S. Visão além do alcance: uma introdução à análise fatorial. *Opinião pública*, v. 16, n. 1, p. 160–185, 2010. ISSN 1993-9999.

FRIEDL, M. A.; BRODLEY, C. E. Decision tree classification of land cover from remotely sensed data. *Remote sensing of environment*, v. 61, n. 3, p. 399–409, 1997. ISSN 1879-0704.

GHANI, N. A.; SIDEK, Z. M. Controlling your personal information disclosure. In: WORLD SCIENTIFIC AND ENGINEERING ACADEMY AND SOCIETY (WSEAS). *Proceedings of the 7th WSEAS international conference on Information security and privacy*. Istanbul, 2008. p. 23–27.

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 1872-6305.

HAIR, J. et al. Multivariate data analysis (6ª edição). new jersey: Pear-son educational. Inc, 2006.

HAIR, J. F. et al. Multivariate data analysis . uppersaddle river. *Multivariate Data Analysis (5th ed) Upper Saddle River*, Prentice-Hall International, 1998.

HONG, J. I.; LANDAY, J. A. An architecture for privacy-sensitive ubiquitous computing. In: ACM. *Proceedings of the 2nd international conference on Mobile systems, applications, and services*. Boston, 2004. p. 177–189. ISBN 1-58113-793-1.

HUANG, Y.; LI, G. A semantic analysis for internet of things. In: IEEE. *Intelligent computation technology and automation (icicta), 2010 international conference on*. Changsha, 2010. v. 1, p. 336–339. ISBN 978-1-4244-7280-2.

HV. *A Tutorial to Understand Decision Tree ID3 Learning Algorithm*. 2017. Disponível em: <https://nullpointerexception1.wordpress.com/2017/12/16/a-tutorial-to-understand-decision-tree-id3-learning-algorithm/>.

JADOUL, M. *The IoT: The next step in internet evolution*. 2015. Disponível em: <https://insight.nokia.com/iot-next-step-internet-evolution>.

KAISER, H. F. The application of electronic computers to factor analysis. *Educational and psychological measurement*, Sage Publications Sage CA: Thousand Oaks, CA, v. 20, n. 1, p. 141–151, 1960. ISSN 1552-3888.

KAISER, H. F. A second generation little jiffy. *Psychometrika*, Springer, v. 35, n. 4, p. 401–415, 1970. ISSN 1860-0980.

KAISER, H. F. An index of factorial simplicity. *Psychometrika*, Springer, v. 39, n. 1, p. 31–36, 1974. ISSN 1860-0980.

KHAN, R. et al. Future internet: the internet of things architecture, possible applications and key challenges. In: IEEE. *Frontiers of Information Technology (FIT), 2012 10th International Conference on*. Islamabad, 2012. p. 257–260. ISBN 978-0-7695-4927-9.

KORESHOFF, T. L.; ROBERTSON, T.; LEONG, T. W. Internet of things: a review of literature and products. In: ACM. *Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration*. Adelaide, 2013. p. 335–344. ISBN 978-1-4503-2525-7.

LANGHEINRICH, M. Privacy by design—principles of privacy-aware ubiquitous systems. In: *Ubicomp 2001: Ubiquitous Computing*. [S.l.: s.n.], 2001. p. 273–291.

LATTIN, J.; CARROLL, J. D.; GREEN, P. E. Análise de dados multivariados. *São Paulo: Cengage Learning*, v. 475, 2011.

LEE, H.; KOBSA, A. Understanding user privacy in internet of things environments. In: IEEE. *Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on*. Reston, 2016. p. 407–412. ISBN 978-1-5090-4130-5.

LEMOS, A. A comunicação das coisas: teoria ator-rede e cibercultura. *São Paulo: Annablume*, v. 310, p. 18–47, 2013.

LU, C. Overview of security and privacy issues in the internet of things. *Internet of Things (IoT): A vision, Architectural Elements, and Future Directions*, p. 1–11, 2014.

MALHOTRA, N. K.; KIM, S. S.; AGARWAL, J. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information systems research*, v. 15, n. 4, p. 336–355, 2004. ISSN 1526-5536.

MICHAEL, J. Privacy and human rights: an international and comparative study, with special reference to developments in information technology. Dartmouth Pub Co, 1994.

MIORANDI, D. et al. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, v. 10, n. 7, p. 1497–1516, 2012. ISSN 1570-8713.

NETO, P. et al. *Produto 8: Relatório do Plano de Ação: Iniciativas e Projetos Mobilizadores*. 2017. Disponível em: <http://www.abinee.org.br/informac/arquivos/pniot.pdf>.

ORIWOH, E.; CONRAD, M. 'things' in the internet of things: towards a definition. *International Journal of Internet of Things*, Scientific & Academic Publishing, v. 4, n. 1, p. 1–5, 2015. ISSN 2332-8347.

PEISSL, W. et al. Introduction: Surveillance, privacy and security. In: *Surveillance, Privacy and Security*. [S.l.]: Routledge, 2017. p. 1–12.

PERERA, C. et al. Context aware computing for the internet of things: A survey. *IEEE communications surveys & tutorials*, IEEE, v. 16, n. 1, p. 414–454, 2014. ISSN 1553-877x.

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

REZENDE, M. L. et al. Utilização da análise fatorial para determinar o potencial de crescimento econonômico em uma região do sudeste do brasil. *Economia e Desenvolvimento*, n. 19, p. 1–18, 2007. ISSN 2595-833X.

RODOTÀ, S. *A vida na sociedade da vigilância: a privacidade hoje*. [S.l.]: Renovar, 2008.

RUMMEL, R. J. *Applied factor analysis*. [S.l.]: Northwestern University Press, 1988.

SMITH, H. J.; MILBERG, S. J.; BURKE, S. J. Information privacy: measuring individuals' concerns about organizational practices. *MIS quarterly*, p. 167–196, 1996. ISSN 1540-1979.

STEWART, K. A.; SEGARS, A. H. An empirical examination of the concern for information privacy instrument. *Information Systems Research*, v. 13, n. 1, p. 36–49, 2002. ISSN 1526-5536.

STREINER, D. L. Being inconsistent about consistency: When coefficient alpha does and doesn't matter. *Journal of personality assessment*, Taylor & Francis, v. 80, n. 3, p. 217–222, 2003. ISSN 0022-3891.

WARREN, S. D.; BRANDEIS, L. D. The right to privacy. *Harvard law review*, JSTOR, p. 193–220, 1890. ISSN 2161-976X.

WESTIN, A. F. Privacy and freedom. *Washington and Lee Law Review*, v. 25, n. 1, p. 166, 1968. ISSN 0043-0463.

WOOD, L. Iot sensor market to 2027 - global analysis and forecasts by type; connectivity type; and application. Research and Makets: The world's Largest Market Research Store, 2019.

WU, M. et al. Research on the architecture of internet of things. In: IEEE. *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*. Chengdu, 2010. v. 5, p. V5–484. ISBN 978-1-4244-6542-2.

XU, H. et al. Measuring mobile users' concerns for information privacy. *Thirty Third International Conference on Information Systems*, Orlando, p. 167–196, 2012.

YONG, A. G.; PEARCE, S. A beginner's guide to factor analysis: Focusing on exploratory factor analysis. *Tutorials in quantitative methods for psychology*, v. 9, n. 2, p. 79–94. ISSN 1913-4126.

ZHANG, M.; SUN, F.; CHENG, X. Architecture of internet of things and its key technology integration based-on rfid. In: IEEE. *Computational Intelligence and Design (ISCID), 2012 Fifth International Symposium on*. Hangzhou, 2012. v. 1, p. 294–297. ISBN 978-1-4673-2646-9.

ZIEGELDORF, J. H.; MORCHON, O. G.; WEHRLE, K. Privacy in the internet of things: threats and challenges. *Security and Communication Networks*, Wiley Online Library, v. 7, n. 12, p. 2728–2742, 2014. ISSN 1939-0122.

GLOSSÁRIO

AIPC – *App Information Privacy Concern*

BPMM – *The Blogging Privacy Management Measure*

CFA – *Confirmatory Factor Analysis*

CFIP – *Concern for Information Privacy*

EFA – *Exploratory Factor Analysis*

FIPPs – *Fair Information Practice Principles*

GPS – *Global Positioning System*

IC – *Informação Crítica*

IP – *Internet Protocol*

IS – *Informação Simples*

IUIPC – *Internet Users' Information Privacy Concerns*

IoTPC – *Internet of Things Privacy Concerns*

IoT – *Internet of Things*

KMO – *Kaiser Meyer Olki*

MUIPC – *Measuring Mobile Users' Concerns for Information Privacy*

PFA – *Principais Factor Analysis*

RFID – *Radio-Frequency Identification*

SC – *Serviço Crítico*

SS – *Serviço Simples*

TCP – *Transmission Control Protocol*

Apendice A

Micro Cenários IoT Utilizados

Os micro cenários apresentados a seguir foram utilizados com o intuito de compor o cenário geral futurista apresentado na seção 4.2 deste trabalho.

Tabela A.1: Micro cenários utilizados para a criação do cenário geral futurista

Código	Cenário
1	As cortinas do seu quarto querem acesso aos horários do seu despertador para abrirem ao seu despertar.
2	Sua cama deseja coletar informações sobre seu sono.
3	A cafeteria solicita dados do seu celular para preparar o café de acordo com as suas preferencias de sabor.
4	A geladeira deseja ter acesso aos seus dados bancários para poder comprar alimentos assim que não tiverem mais em estoque.
5	Uma loja de esportes deseja ter acesso ao seus esportes favoritos, para realizar propaganda de produtos para você.
6	Seu celular quer informações sobre a ultima vez que visitou seu médico.
7	O seu médico quer acesso aos seus dados de saúde para acompanhar a sua saúde.
8	A academia deseja coletar informações sobre suas medidas e peso;.
9	A academia deseja suas preferencias musicais para tocar apenas musicas de sua preferencia.
10	O seu telefone quer acesso à sua agenda para ajustar o nível do toque de acordo com as suas tarefas.
11	Sua cidade quer acesso ao seu celular para lhe notificar sobre mudanças no tempo.
12	Sua mochila pede acesso aos itens que você carrega dentro dela diariamente, para que possa te avisa quando esquecer de algo.
13	O termostato da sua casa quer saber o seu cronograma do dia para ajustar a temperatura de acordo e economizar energia.
14	Seu carro quer acesso ao seu destino para calcular a rota mais econômica.

15	Seu carro quer informações sobre seu itinerário para determinar se tem autonomia para o percurso.
16	Um posto de gasolina quer informações sobre o consumo do seu carro.
17	O compressor de ar do posto de gasolina quer informações sobre o modelo do seu carro para determinar a pressão adequada do calibrador.
18	O seu sistema de entretenimento quer acesso às suas buscas mais recentes de notícias para selecionar uma programação relevante.
19	O restaurante universitário quer informações sobre suas preferencias de alimentos.
20	O seu departamento deseja informações sobre datas de trabalhos e provas.
21	O bebedouro de água deseja coletar informações sobre a quantidade de vezes que você o utiliza.
22	Sua cadeira deseja saber qual a sua altura e peso, para um melhor ajuste e acordo com suas condições físicas.
23	Sua cadeira no escritório quer saber sua identidade para manter histórico sobre seu peso.
24	O ar condicionado do seu escritório quer saber suas preferencias de temperatura para ajustar a temperatura.
25	Sua sala de aula deseja coletar expressões faciais sua durante as aulas.

Apendice B

CAAE

Termo de Consentimento Livre e Esclarecido

1. Você está sendo convidado para participar da pesquisa intitulada “Negociação de Privacidade em Ambientes IoT”.

2. Você foi selecionado pela sua formação acadêmica e pelo fato de ser um entusiasta em novas tecnologias, no entanto sua participação não é obrigatória.

3. A qualquer momento você pode desistir de participar e retirar seu consentimento.

4. Sua recusa não trará nenhum prejuízo em sua relação com o pesquisador ou com a instituição onde esse estudo é aplicado.

5. O objetivo deste estudo é a construção de um instrumento que atenda as preocupações em se determinar o que é considerado uma informação privada ou não para os usuários de Internet of Things - IoT. Além de sua construção será verificado se o instrumento de pesquisa IoTPC (Internet of Things Privacy Concerns) proposto é capaz de auxiliar nas tomadas de decisões de mecanismos de negociação de privacidade me ambientes IoT.

6. Sua participação nesta pesquisa consistirá em responder um questionário eletrônico, contendo um cenário geral futurístico sobre IoT onde os usuários responderão a questões de privacidade relacionadas ao cenário apresentado, objetivando coletar informações sobre as preferências de privacidade dos participantes.

7. Está pesquisa pode causar algum desconforto em relação ao tempo dedicado a leitura e interpretação do cenário apresentado, além do preenchimento do questionário apresentado, sendo que faremos o possível para minimizar tais desconfortos.

8. A sua contribuição visa validar o instrumento de pesquisa IoTPC que tem fins estritamente acadêmicos. Sua colaboração é voluntária e será realizada de forma anônima.

9. As informações obtidas através dessa pesquisa serão confidencias e asseguramos o sigilo sobre sua participação.

10. Os dados não serão divulgados de forma a possibilitar sua identificação. As informações coletadas não estarão vinculadas à sua identidade.

11. Caso desejar, você poderá receber uma cópia deste termo onde consta o telefone e o endereço do pesquisador principal, podendo tirar suas dúvidas sobre o projeto e sua participação, agora ou a qualquer momento.

Bruno Lopes

Universidade Federal de São Carlos – Departamento de Computação
Rodovia Washington Luis, km 235, Cep: 13565-905 São Carlos – SP
Tel: (16) 3351-8626
Endereço e Telefone do Pesquisador
Rua José de Alencar, 980
13556-000 – São Carlos – SP
Tel: (18) 98108-3554

Declaro que entendi os objetivos, riscos e benefícios de minha participação na pesquisa e concordo em participar. O pesquisador me informou que o projeto foi aprovado pelo Comitê de Ética em Pesquisa em Seres Humanos da UFSCar que funciona na Pró-Reitoria de Pós-Graduação e Pesquisa da Universidade Federal de São Carlos, localizada na Rodovia Washington Luiz, Km. 235 - Caixa Postal 676 - CEP 13.565-905 - São Carlos - SP – Brasil. Fone (16) 3351-8110. Endereço eletrônico: cephumanos@power.ufscar.br.

Participante da Pesquisa

PROJEDO DETALHADO

PLANEJAMENTO DE PESQUISA ENVOLVENDO SERES HUMANOS

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

“Negociação de Privacidade em Ambientes IoT”

Responsáveis:

Aluno: Bruno Lopes
Orientador: Prof. Dr. Sérgio Donizetti Zorzo

Abril 2018

Sumário

Resumo

Considerando que as preocupações de privacidade dos usuários de Internet of Things (IoT) são de grande importância e devem ser respeitadas, entende-se que é necessário a construção de instrumentos que visem mensurar as preocupações de privacidade dos usuários de IoT.

A partir disso, apresenta-se neste documento, o planejamento e as diretivas a serem seguidas para a realização de um estudo, envolvendo seres humanos, objetivando atender sua satisfação e validar o instrumento desenvolvido.

Para se obter as preferências de privacidade dos usuários de dispositivos IoT, será aplicado um questionário eletrônico, contendo um cenário geral futurístico onde os participantes responderão a questões de privacidade relacionadas ao cenário apresentado.

1. Introdução

Cada vez mais, o número de usuários utilizando a Internet vem crescendo progressivamente. Com esse crescimento é possível o surgimento de outras áreas englobando a Internet, dentre elas uma área se destaca tendo como finalidade utilizar a Internet como uma plataforma global, permitindo que máquinas e objetos inteligentes possam se comunicar, processar informações e se auto gerenciarem (Balte et al. 2015). Atualmente essa área é denominada de "Internet das Coisas" (Internet of Things - IoT).

O termo "Coisas" pode ser muito amplo, permitindo a inclusão de uma variedade de elementos físicos, desde objetos do nosso dia a dia, como telefones inteligentes, *tablets*, câmeras digitais entre outros até elementos em nossos ambientes, como casas, veículos, trabalho, etc. (Duce. 2008; Razzaque et al. 2016).

Alguns dispositivos IoT não utilizam *tags* em seus objetos, permitindo que eles possam ficar anônimos para seus usuários, podendo não existir sinais acústicos ou visuais afim de chamar a atenção do usuário de IoT. Desta maneira, o usuário pode ser monitorado por esses dispositivos de forma que ele não tenha conhecimento sobre essa prática (JUELS, 2006). Nesse contexto, não é possível que o usuário aplique conceitos de privacidade sobre suas informações pessoais, o impossibilitando de incluir a ocultação de suas informações pessoais, bem como a capacidade de controlar essas informações (GURSES; BERENDT; SANTEN, 2006).

Uma das diferenças observadas sobre a Internet tradicional e a IoT é a quantidade de dados coletados sobre seus usuários. Na IoT uma grande quantidade de dados são coletados sobre seus usuários. Esses dados são recolhidos de forma universal e podem ser usados para construir um perfil invasivo do usuário de IoT, sendo capaz de violar suas preferências de privacidade (LU, 2014).

Os problemas de privacidade são especialmente difíceis de serem discutidos já que, por sua natureza a privacidade é considerada subjetiva (COVERT, 2014). Isso exige a investigação de novas abordagens, a fim de garantir que a privacidade possa ser devidamente representada dentro do contexto de IoT.

Com o decorrer dos anos as preocupações de privacidade aumentaram de acordo com o surgimento de novas tecnologias, com isso alguns autores propuseram na literatura instrumentos capazes de mensurar privacidade empiricamente.

Smith, Milberg e Burke (1996) propuseram o desenvolvimento de um instrumento capaz de mensurar a privacidade dos indivíduos em praticas organizacionais, denominado *Concern for Information Privacy* - CFIP. O objetivo desse instrumento é que ele possa capturar as preocupações dos indivíduos em relação à privacidade organizacional empiricamente.

O CFIP é composto por uma escala de 15 itens, refletindo quatro dimensões de preocupações com privacidade sendo elas: coleta, uso secundário não autorizado, acesso impróprio e erros. Após seu desenvolvimento o CFIP passou por um rigoroso processo de avaliação envolvendo três estágios de avaliação, utilizando-se de técnicas de análise fatorial e validade nomológica, confirmando e reafirmando a validade da sua escala. O fato de ter passado por um rigoroso processo de avaliação e ter sido aplicado a varias populações heterogenias, proporcionou ao CFIP um alto grau de confiança na validade, confiabilidade e generalização da sua escala (SMITH;MILBERG; BURKE, 1996).

É possível apontar duas contribuições importantes para a literatura de privacidade obtidas pelos autores: (1) uma estrutura que descreve as principais dimensões de preocupações de privacidade dos indivíduos sobre as práticas organizacionais e (2) um instrumento validado e apto à se medir essas preocupações de privacidade (SMITH;MILBERG; BURKE, 1996).

Stewart e Segars (2002) conduziram um estudo empírico com cerca de 355 participantes, afim de examinar a estrutura dos fatores do CFIP, confirmando as propriedades psicométricas desse instrumento. Os autores utilizaram técnicas de análise fatorial para a avaliação do instrumento, obtendo como resultados a confirmação de que o CFIP é considerado um instrumento confiável para a mensuração de privacidade, além de apontar que o uso do CFIP deve ser cuidadosamente combinado com o contexto da pesquisa (STEWART; SEGARS, 2002).

Observando a falta de confiança dos consumidores em relação à privacidade no comercio eletrônico, Malhotra, Kim e Agarwal (2004) realizaram um estudo sobre a magnitude das preocupações de privacidade dos usuários na Internet, resultando na construção de um instrumento capaz de refletir as preocupações de privacidade dos usuários de comércio eletrônico, denominado Internet Users' Information Privacy Concerns - IUIPC. O objetivo desse instrumento é conseguir mensurar empiricamente o que é considerado privado para os usuários de comercio eletrônico.

O IUIPC é composto por uma escala de 10 itens, distribuídos em três dimensões, sendo elas: coleta, controle e consciência de práticas de privacidade. A construção do

instrumento foi baseada no CFIP (SMITH;MILBERG; BURKE, 1996), agregando dimensões como a de coleta e adaptando itens para o contexto da internet.

Outra área afetada pelas preocupações de privacidade foram os dispositivos móveis, já que nesse contexto os desenvolvedores de aplicativos podem ter acesso a um grande volume de informações pessoais do usuário, ocasionando eventualmente em violações de privacidade.

Inspirado em trabalhos como o CFIP e o IUIPC (SMITH; MILBERG; BURKE, 1996; MA-LHOTRA; KIM; AGARWAL, 2004), Xu et al. (2012) desenvolveram uma escala com o intuito de representar as preferêcias de privacidade dos usuários de dispositivos móveis. O MUIPC - *Measuring Mobile Users' Concerns for Information Privacy* é composto por uma escala de 9 itens, distribuídos em três dimensões como na escala anterior (IUIPC), sendo elas: vigilância percebida, intrusão percebida e uso secundário não autorizado.

Os autores conduziram uma pesquisa online com cerca de 310 participantes, aplicando os itens do MUIPC dentro de uma escala Likert de 7 pontos, variando de "Concordo Completamente" a "Discordo Completamente", contendo um ponto neutro "Não Sei Opinar".

Dado alguns dos trabalhos relacionados apresentados, essa proposta medirá de forma empírica o que é considerado uma informação privada ou não para os usuários de IoT em um determinado cenário futurístico. Essa mensuração será realizada por meio do instrumento desenvolvido denominado de Internet of Things Privacy Concers - IoTPC, baseado nos trabalhos relacionados encontrados a literatura.

A coleta da percepção de privacidade dos usuários de IoT por meio de questionários eletrônicos é necessária para avaliar e validar o projeto de mestrado “Negociação de Privacidade em Ambientes IoT” do discente Bruno Lopes, aluno mestrando do Programa de Pós-Graduação em Ciência da Computação, do Departamento de Computação da Universidade Federal de São Carlos (PPG-CC/UFSCar), estando esse projeto de pesquisa está sob orientação do Prof. Dr. Sérgio Donizetti Zorzo, docente do PPG-CC/UFSCar.

2. Hipótese

Considerando o contexto apresentado, pretende-se avaliar se é possível a construção de um instrumento que seja capaz de mensurar as preocupações de privacidade dos usuários de IoT empiricamente. Para isso, vamos aplicar um questionário - objeto deste projeto detalhado - que visa dar subsídios para a pesquisa que esta sendo realizada.

3. Objetivo Primário

Infelizmente, a compreensão sobre as preocupações de privacidade dos usuários, através de abordagens empíricas confirmatórias podem não ser realizadas pela falta de instrumentos validados para realizar essa medição (SMITH; MILBERG; BURKE, 1996).

O objetivo deste trabalho é propor um instrumento que seja capaz de mensurar preocupações de privacidade em ambientes IoT. Este instrumento visa a construção de uma escala para medir empiricamente preocupações de privacidade em ambientes IoT, além de verificar se é possível realizar a extração de fatores deste instrumento.

4. Objetivo Secundário

Esse trabalho também objetiva utilizar os resultados apresentados com a construção do instrumento citado em um mecanismo de negociação de privacidade em ambientes IoT, a fim de verificar se o instrumento é capaz de auxiliar o mecanismo na tomada de decisão, podendo assim melhorar o seu desempenho.

5. Metodologia

O instrumento IoTPC, será capaz de medir empiricamente a privacidade dos usuários em um determinado cenário IoT apresentado no Anexo I. O Instrumento foi desenvolvido com base em instrumentos de privacidade já existentes como o IUIPC, MUIPC e AIPC no qual todos tem como base o CFIP (MALHOTRA; KIM; AGARWAL, 2004; XU et al., 2012; BUCK;BURSTER, 2017; SMITH; MILBERG; BURKE, 1996) . O CFIP foi utilizado como ponto inicial para o desenvolvimento do IoTPC, já que ele já foi devidamente validado pela literatura e é base de desenvolvimento para outros instrumentos. O IoTPC é composto por 17 itens distribuídos dentro de 5 dimensões agregadas dos instrumentos anteriores, já que essas dimensões também refletem questões de privacidade em ambientes IoT.

Assim como a criação das dimensões do IoTPC foi baseada em instrumentos anteriores a mesma estratégia foi adotada para a geração de seus itens, com base nos instrumentos anteriores. Os itens de cada instrumento relacionado à construção do IoTPC passaram por uma avaliação, com o intuito de verificar se esse item reflete alguma característica de privacidade em ambientes IoT com base no cenário proposto nessa pesquisa.

5.1. Local de Estudo

O local escolhido para a execução desta pesquisa foram os Laboratórios de Informática pertencentes ao Instituto Federal de São Paulo, campus de Presidente Epitácio – SP.

Os questionários serão preenchidos com a presença dos participantes juntamente ao pesquisador responsável, onde será apresentado ao participante o termo de consentimento livre e esclarecido e em seguida um link para o preenchimento do questionário eletrônico via Internet, de modo a coletar as preferencias de privacidade dos participantes.

5.2. Planejamento

Faz-se necessário a utilização do estudo com humanos, a fim de comprovar a validade e a confiabilidade do instrumento desenvolvido no projeto de mestrado “Negociação de Privacidade em Ambientes IoT”.

Os questionários serão aplicados presencialmente se utilizando da Internet como uma ferramenta, a fim de apoiar o preenchimento do questionário eletrônico. Durante o preenchimento os participantes e o pesquisador responsável se encontrarão no mesmo local físico (Laboratório de Informática), onde serão explicados os motivos e a importância dos participantes na pesquisa.

Para cada membro da amostra, ou seja, para cada participante, será exemplificado todo o cenário futurístico da pesquisa, objetivando esclarecer possíveis duvidadas dos participantes, em seguida será aplicado um questionário eletrônico, contendo os itens do instrumento desenvolvido, distribuídos em uma escala *Likert* de 5 pontos, variando de "Concordo Completamente" a "Discordo Completamente" contendo um ponto neutro "Não sei Opinar". Os participantes informarão nessa seção o grau de concordância com cada item do IoTPC baseado em suas preferências de privacidade.

5.3. Amostra

Malhotra (2001) discorre que o objetivo principal de uma amostragem de qualidade é aumentar a precisão sem aumentar o custo. De acordo com McDaniel e Gates (2003), a solução para a seleção não é o tamanho da amostra em relação ao tamanho da população e sim se a amostra é realmente capaz de representar a população. Provas empíricas mostram que amostras pequenas, mas representativas podem refletir, com bastante precisão, as características da população (MCDANIEL e GATES, 2003).

Amostragem é definida como o processo de colher amostras de uma população. Sendo a amostra um subconjunto da população total, que inclui todos os objetos dos quais ou sobre os quais pode-se coletar informações para atender os objetivos da pesquisa (Mattar, 2001).

Sendo assim, será tomado como amostra um conjunto de 60 alunos, sendo esses da graduação que tenham acesso permitido ao local e disponibilidade de tempo para participar da pesquisa.

Como forma de comprovar a veracidade dos dados e que os participantes preencheram corretamente os questionários, é apresentado a eles, antes do inicio do estudo, um temo de consentimento livre e esclarecido, onde o participante deverá assina-lo, concordado ou não com as diretivas transcritas.

5.4. Coleta de Dados

Os participantes, após a explicação da pesquisa, deverão responder ao questionário, o qual possibilitará a avaliação do instrumento proposto além de exporem suas ideias, conclusões e sugestões, com vistas a contribuir com o amadurecimento do “IoTPC”, acarretando em um melhoramento da pesquisa.

6. Critérios de inclusão

Para essa pesquisa foi utilizado como critério de inclusão os alunos do ensino superior em computação que estejam familiarizados com novas tecnologias, dentre elas a Internet das Coisas. Além de conterem esse conhecimento prévio os alunos selecionados para a pesquisa também deverão estar preocupados com questões relacionadas à privacidade em ambientes IoT.

7. Riscos e Benefícios

A aplicação do questionário eletrônico aos participantes pode eventualmente causar algum desconforto em relação ao tempo dedicado para seu preenchimento, além de que alguns participantes podem se sentir confusos em relação ao cenário futurístico apresentado, uma vez que não estão habituados com tais tecnologias no seu dia a dia, podendo assim não compreender o contexto de privacidade estudado, no caso Internet das Coisas.

O instrumento auxiliará a promover esforços de pesquisa cooperativa, permitindo que outros pesquisadores possam utiliza-lo para a realização de testes e ajustes em suas pesquisas,

bem como uma maior clareza para a formulação e interpretação de questões de pesquisa (STRAUB, 1989).

8. Metodologia de Análise dos Dados

Os dados coletados serão analisados por meio da análise fatorial. A análise fatorial é uma técnica estatística utilizada amplamente nas ciências sociais. De acordo com (FIELD, 2013) a análise fatorial é uma técnica utilizada para identificar grupos ou *clusters* de variáveis, que pode ter três utilizações principais: (1) compreender a estrutura de um conjunto de variáveis; (2) construir um questionário capaz de medir uma variável subjacente; e (3) reduzir um conjunto de dados para um tamanho mais gerenciável, mantendo a maior parte da informação original possível.

De acordo com (BASILEVSKY, 2009) análise fatorial é geralmente entendida como um conjunto de modelos estreitamente relacionados destinados a explorar ou estabelecer a estrutura de correlação entre as variáveis aleatórias observadas.

Na análise fatorial duas técnicas se destacam, sendo elas a análise fatorial exploratória e a análise fatorial confirmatória. A análise fatorial confirmatória objetiva confirmar hipóteses utilizando diagramas de análise de caminho para representar variáveis e fatores, enquanto que a análise fatorial exploratória objetiva descobrir padrões complexos explorando o conjunto de dados e as previsões de teste (CHILD, 2006).

A análise fatorial é útil para estudos que envolvem algumas centenas de variáveis, itens de questionários ou uma série de testes que podem ser reduzidos a um conjunto menor, para obter um conceito subjacente e para facilitar as interpretações (RUMMEL, 1988). Segundo (YONG; PEARCE, 2013) conjuntos de dados grandes que consistem em várias variáveis podem ser reduzidos em grupos de variáveis, chamados fatores, ou seja, a análise fatorial reúne variáveis comuns em categorias descritivas.

9. Desfecho Primário

Espera-se através desse estudo com seres humanos, confirmar a validade do instrumento desenvolvido, assim como garantir que as preferências de privacidade dos usuários de ambientes IoT possam ser respeitadas, utilizando o instrumento desenvolvido no auxilio de mecanismos de negociação de privacidade em ambientes IoT.

E em consequência desses resultados, espera-se concluir e efetivar o trabalho proposto e desenvolvido como projeto de mestrado, dando-me, Bruno Lopes, o direito a obtenção do

título de Mestre em Ciência da Computação. Ainda espera-se validar tais resultados através da aprovação de artigos científicos, em congressos e revistas da área.

10. Cronograma de Aplicação

A – Apresentar o contexto da pesquisa, bem como introduzir os participantes ao cenário futurístico, aplicação e execução do estudo, o que consequentemente aborta na coleta das respostas;

B – Análise das respostas obtidas;

C – Formalização das conclusões sobre a viabilidade do instrumento e possíveis melhorias no IoTPC, caso as análises retornem quem o instrumento está incompleto ou inválido;

Atividades	**Semanas**		
	1ª	**2ª**	**3ª**
A	X		
B		X	X
C			X

11. Bibliografia

Balte, A. a. (2015). Security Issues in Internet of Things (IoT): A Survey. International Journal of Advanced Research in Computer Science and Software Engineering.

Basilevsky, A. T. (2009). Statistical factor analysis and related methods: theory and applications. John Wiley & Sons.

Buck, C. a. (2017). App Information Privacy Concerns.

Child, D. (2006). The essentials of factor analysis. A&C Black.

Duce, H. (2008). Internet of Things in 2020.

Ed Covert, A. O. (2014). Acesso em 2018, disponível em Ethical Challenges of the Internet of Things: https://www.scmagazine.com/ethical-challenges-of-the-internet-of-things/article/538993/1/

Field, A. (2013). Discovering statistics using IBM SPSS statistics. Sage.

Gurses, S. a. (2016). Multilateral security requirements analysis for preserving privacy in ubiquitous environments. Proceedings of the UKDU Workshop, 51--64.

Juels, A. (2006). RFID security and privacy: A research survey. IEEE journal on selected areas in communications, 381--394.

Lu, C. (2014). Overview of Security and Privacy Issues in the Internet of Things. Internet of Things (IoT): A vision, Architectural Elements, and Future Directions.

Malhotra, N. K. (2012). Pesquisa de marketing: uma orientação aplicada. Bookman Editora.

MATTAR, F. N. Pesquisa de Marketing. 3ª Ed. São Paulo: Atlas. vol.1. 2001. 275 p.

MCDANIEL, D. C. e GATES, R. Pesquisa de Marketing. São Paulo: Thomson. 2003. 562 p.

RAZZAQUE, M. A. et al. Middleware for internet of things: a survey. IEEE Internet of Things Journal , IEEE, v. 3, n. 1, p. 70–95, 2016

RUMMEL, R. J. Applied factor analysis. [S.l.]: Northwestern University Press, 1988.

SMITH, H. J.; MILBERG, S. J.; BURKE, S. J. Information privacy: measuring individuals' concerns about organizational practices. MIS quarterly , JSTOR, p. 167–196, 1996.
STEWART, K. A.; SEGARS, A. H. An empirical examination of the concern for information privacy instrument. Information Systems Research , INFORMS, v. 13, n. 1, p. 36–49, 2002.
STRAUB, D. W. Validating instruments in mis research. MIS quarterly, JSTOR, p. 147–169, 1989.
YIN, R. K. Estudo de Caso: Planejamento e método. 3ª Ed. Porto Alegre: Bookman. 2005.
YONG, A. G.; PEARCE, S. A beginner's guide to factor analysis: Focusing on exploratory factor analysis.
Tutorials in quantitative methods for psychology , v. 9, n. 2, p. 79–94, 2013.

Anexo I

Seu despertador tocou e as cortinas do seu quarto se abriram para que a luz entrasse te ajudando a acordar. Ao se levantar sua cama te notifica que você se mexeu muito durante a noite, não tendo um sono adequado, e talvez possa ter a sensação de cansaço e sonolência durante o dia. Ao chegar na cozinha seu café já esta pronto da forma que você gosta extra forte, sua campainha toca e é a entrega do supermercado da compra realizada pela sua geladeira.

Após seu café da manha você se dirige a academia que fica a poucas quadras da sua casa, no caminho uma loja de esportes exibe promoções sobre luvas e coqueteleiras para você no seu smartphone. Você é notificado que já faz um tempo que não consulta seu médico pessoal, mas a secretária do seu médico já agendou uma consulta e ele já tem dados prévios sobre sua saúde coletados por dispositivos inteligentes na sua casa, como sua cama por exemplo. Ao chegar na academia, um painel digital que faz autenticação por biometria informa todos os seus dados desde quando você entrou na academia, exibindo informações como peso, altura, medidas corporais, exercícios realizados entre outros, apresentando um acompanhamento completo da sua evolução nos treinos.

Após o treino seu smartphone começa a tocar a musica do Start Wars, logo você percebe que é seu amigo te ligando perguntando se você vai comparecer na aula mais tarde. Parece que hoje o clima vai mudar, você acaba de receber um aviso de um temporal a tarde e que é bom estar preparado. Ao se arrumar para sair de casa e ir para mais um dia de faculdade sua mochila te avisa que você esta esquecendo seu notebook, então rapidamente você o pega e entra no carro. Ao sair de casa, dispositivos inteligentes detectam que a casa esta vazia, seu termostato ajusta a temperatura e dispositivos considerados desnecessários são desligados para uma maior economia de energia.

Ao inferir que você esta indo para a faculdade, seu carro te aconselha ir a um posto de combustível abastecer, já que ele estima que não tem autonomia suficiente para realizar esse percurso. No posto a bomba de combustível que já tem o seu histórico de abastecimento, te informa que seu carro esta consumindo mais que outros veículos do mesmo modelo, uma notificação então é enviada para seu mecânico agendando uma vistoria para evitar problemas maiores. Você aproveita para calibrar os pneus do seu carro, como o compressor já tem dados do seu veiculo ele ajusta a pressão automaticamente para você. No caminho de volta para a faculdade seu sistema de entretenimento te informa que o filme que você aguardava já esta disponível nos cinemas e reserva um horário na sua agenda para o próximo final de semana.

Ao chegar na faculdade o restaurante universitário te informa que hoje será servido um dos seus pratos favoritos. Chegando no seu departamento você é avisado que tem uma prova e três trabalhos para ser entregues até semana que vem, antes de entrar na sala de aula o bebedouro te notifica que você não está consumindo o necessário de água, logo você enche sua garrafa e entra na sala de aula. Ao se sentar no seu lugar, sua cadeira se ajusta de acordo com seu peso e altura, e ainda exibe que você perdeu 300 gramas, em uma semana. A temperatura do ar-condicionado também é ajustada. Ao sair da aula, a sala de aula detecta que você não compreendeu muito bem o conteúdo dessa matéria e agenda um horário com os monitores, tudo já esta devidamente marcado na sua agenda eletrônica.

Preocupações de Privacidade em Ambientes IoT (Internet of Things)

Internet das Coisas é uma tradução literal da expressão em inglês Internet of Things, refere-se a uma revolução tecnológica que tem como objetivo interligar dispositivos usados normalmente no seu dia a dia - como celulares, televisores, cafeteiras, geladeiras, camas, sensores entre outros - de forma que se comuniquem automaticamente por uma rede de computadores.
Em um mundo totalmente conectado, os dispositivos IoT tem livre acesso à coleta e à troca de dados sobre seus usuários de maneira automática. No entanto, essa troca constante de informação pode ocasionalmente violar as preferências de privacidade dos usuários.
Focando o problema apresentado acima, esse formulário é um convite para você contribuir com suas preferências de privacidade em um cenário que será apresentado no decorrer dessa pesquisa.
A sua contribuição visa validar o instrumento de pesquisa IOTPC (Internet of Thing Privacy Concerns) que tem fins estritamente acadêmicos. Sua colaboração é voluntária e será realizada de forma anônima.

*Obrigatório

Caracterização do Participante

1. **Idade** *

2. **Sexo** *
   Marcar apenas uma oval.
   - Masculino
   - Feminino

3. **Curso** *
   Marcar apenas uma oval.
   - Análise e Desenvolvimento de Sistemas - ADS
   - Bacharelado em Ciência da Computação - BCC

Vamos Nos Situar!

Vamos apresentar um cenário da rotina de um estudante universitário fictício visando situá-lo em um ambiente IoT. A seguir, serão apresentadas as questões de privacidade relacionadas a esse cenário futurístico.

Vale observar que o cenário descrito é possível de ser criado com a tecnologia que temos hoje.

Tempo estimado
- 5mim para a leitura do cenário
- 10mim para responder as questões de privacidade

Cenário Geral Futurístico

Seu despertador tocou e as cortinas do seu quarto se abriram para que a luz entrasse te ajudando a acordar.
Ao se levantar sua cama te notifica que você se mexeu muito durante a noite, não tendo um sono adequado, e talvez possa ter a sensação de cansaço e sonolência durante o dia.

Ao chegar na cozinha seu café já esta pronto da forma que você gosta extra forte, sua campainha

toca e é a entrega do supermercado da compra realizada pela sua geladeira.

Após seu café da manha você se dirige a academia que fica a poucas quadras da sua casa, no caminho uma loja de esportes exibe promoções sobre luvas e coqueteleiras para você no seu smartphone.

Você é notificado que já faz um tempo que não consulta seu médico pessoal, mas a secretária do seu médico já agendou uma consulta e ele já tem dados prévios sobre sua saúde coletados por dispositivos inteligentes na sua casa, como sua cama por exemplo. Ao chegar na academia, um painel digital que faz autenticação por biometria informa todos os seus dados desde quando você entrou na academia, exibindo informações como peso, altura, medidas corporais, exercícios realizados entre outros, apresentando um acompanhamento completo da sua evolução nos treinos.

Após o treino seu smartphone começa a tocar a musica do Start Wars, logo você percebe que é seu amigo te ligando perguntando se você vai comparecer na aula mais tarde.

Parece que hoje o clima vai mudar, você acaba de receber um aviso de um temporal a tarde e que é bom estar preparado. Ao se arrumar para sair de casa e ir para mais um dia de faculdade sua mochila te avisa que você esta esquecendo seu notebook, então rapidamente você o pega e entra no carro.

Ao sair de casa, dispositivos inteligentes detectam que a casa esta vazia, seu termostato ajusta a temperatura e dispositivos considerados desnecessários são desligados para uma maior economia de energia.
Ao inferir que você esta indo para a faculdade, seu carro te aconselha ir a um posto de combustível abastecer, já que ele estima que não tem autonomia suficiente para realizar esse percurso. No posto a bomba de combustível que já tem o seu histórico de abastecimento, te informa que seu carro esta consumindo mais que outros veículos do mesmo modelo, uma notificação então é enviada para seu mecânico agendando uma vistoria para evitar problemas maiores. Você aproveita para calibrar os pneus do seu carro, como o compressor já tem dados do seu veiculo ele ajusta a pressão automaticamente para você.

No caminho de volta para a faculdade seu sistema de entretenimento te informa que o filme que você aguardava já esta disponível nos cinemas e reserva um horário na sua agenda para o próximo final de semana.

Ao chegar na faculdade o restaurante universitário te informa que hoje será servido um dos seus pratos favoritos.
Chegando no seu departamento você é avisado que tem uma prova e três trabalhos para ser entregues até semana que vem, antes de entrar na sala de aula o bebedouro te notifica que você não está consumindo o necessário de água, logo você enche sua garrafa e entra na sala de aula.

Ao se sentar no seu lugar, sua cadeira se ajusta de acordo com seu peso e altura, e ainda exibe que você perdeu 300 gramas, em uma semana. A temperatura do ar-condicionado também é ajustada.

Ao sair da aula, a sala de aula detecta que você não compreendeu muito bem o conteúdo dessa matéria e agenda um horário com os monitores, tudo já esta devidamente marcado na sua agenda eletrônica.

Privacidade na Internet das Coisas

4. **A privacidade em ambientes IoT é realmente uma questão de direito dos usuários exercer controle e autonomia sobre as decisões de como suas informações são coletadas, usadas e compartilhadas.** *

   Marcar apenas uma oval.

   - ◯ Concordo Completamente
   - ◯ Concordo Parcialmente
   - ◯ Não sei Opinar
   - ◯ Discordo Parcialmente
   - ◯ Discordo Completamente

5. **Dispositivos domésticos como cortinas inteligentes, que buscam informações, devem divulgar a forma como os dados são coletados, processados e usados.** *
Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

6. **É muito importante para mim que eu esteja ciente e conhecedor sobre como minhas informações pessoais serão usadas.** *
Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

7. **Normalmente me incomoda quando minha cama solicita informações sobre meu sono.** *
Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

8. **Quando dispositivos como minha geladeira solicitam minhas informações bancarias, normalmente penso duas vezes antes de fornece-las.** *
Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

9. **Me incomoda fornecer informações pessoais há dispositivos como máquinas de café, ares-condicionados, termostatos entre outros.** *
Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

10. **Eu acredito que a localização do meu dispositivo móvel é monitorada pelo menos parte do tempo.** *
Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

11. **Estou preocupado que minha academia esteja coletando muita informação sobre mim.** *
Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

12. **Estou preocupado que lojas de esportes possam estar monitorando minhas atividades através do meu dispositivo móvel.** *
Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

13. **Eu sinto que, como resultado do uso de dispositivos de entretenimento, hospitalares e comerciais, outros possam saber sobre mim mais do que eu estou confortável.** *
Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

14. **Eu acredito que, como resultado do uso de dispositivos de consumo veicular, autonomia veicular e pressão dos pneus, as informações sobre mim que considero privadas são agora mais acessíveis para outros mais do que eu gostaria.** *
Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

15. **Estou preocupado que minha faculdade possa usar minhas informações pessoais para outros fins sem me notificar ou obter minha autorização.** *

Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

16. **Quando forneço informações pessoais para usar ambientes IoT, estou preocupado que os dispositivos como minha cadeira ou o bebedouro possam usar minhas informações para outros fins.** *

Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

17. **Estou preocupado que os dispositivos, como meu departamento ou o restaurante universitário, possam compartilhar minhas informações pessoais com outras entidades sem obter minha autorização.** *

Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

18. **Comparado com outros, sou mais sensível sobre o modo como os dispositivos IoT lidam com minha informação pessoal.** *

Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

19. **Para mim, a coisa mais importante é manter minha privacidade intacta dos dispositivos IoT.** *

Marcar apenas uma oval.

- Concordo Completamente
- Concordo Parcialmente
- Não sei Opinar
- Discordo Parcialmente
- Discordo Completamente

20. **Estou preocupado com as ameaças à minha privacidade pessoal hoje.** *

Marcar apenas uma oval.

- ◯ Concordo Completamente
- ◯ Concordo Parcialmente
- ◯ Não sei Opinar
- ◯ Discordo Parcialmente
- ◯ Discordo Completamente
