# Um mecanismo para recomendação de algoritmos de anonimização de dados baseado no perfil dos dados para ambientes IoT

**Flávio S. Neves**[1] **(Doutorando), Vinicius Cardoso Garcia**[1] **(orientador)**
**Michel Sales Bonfim**[2] **(coorientador)**

[1]Doutorado Acadêmico em Ciência da Computação
Programa de Pós-Graduação em Ciência da Computação
Centro de Informática - Universidade Federal de Pernambuco (UFPE)
Av. Jornalista Anibal Fernandes, s/n – CEP 50740-560 – Recife – PE –Brasil
Ingresso: 03/2018 – Previsão de Defesa 08/2022
Data da aprovação da proposta de tese: 10/12/2020

[2]Universidade Federal do Ceará (UFC) Quixadá – CE – Brasil

fsn2@cin.ufpe.br, vcg@cin.ufpe.br, michelsb@gmail.com

***Resumo.*** *Apesar dos grandes desafios relacionados à privacidade dos dados, a Internet das Coisas (IoT) continua em franca ascensão. Existem inúmeros dispositivos espalhados por vários locais, tais como, casas inteligentes, carros inteligentes, locais públicos, bem como, dispositivos que as pessoas usam em seu corpo, por exemplo, smartwatches. Parte dessas pessoas usam esses dispositivos sem saber das suas reais capacidades e potencialidades. Assim sendo, o problema que permeia esta pesquisa é: não foi identificado na literatura uma solução para privacidade de dados baseada em anonimização que seja adaptável para vários ambientes de uso da IoT. Diante disto, objetivou-se com esta pesquisa a proposição de uma solução que possa recomendar qual o algoritmo de anonimização de dados é mais adequado para um conjunto de dados de acordo com suas características, e que consiga aprender conforme analisa os dados. Para a condução e a execução desta pesquisa foi escolhido como método principal o Design Science Research (DSR) que é uma abordagem que tem duplo objetivo: (i) desenvolver um artefato para resolver um problema prático num contexto específico e (ii) gerar novos conhecimentos técnicos e científicos. As principais contribuições desta pesquisa serão: (i) a solução proposta; (ii) criação dos critérios para escolha de algoritmos de anonimização baseado nas características dos dados; (iii) uma ontologia para dar suporte a recomendação baseada na lógica de descrição; (iv) modelo de aprendizagem para atualizar a base de conhecimento da ontologia à medida que analisa novos dados; e (v) o método para a avaliação da solução proposta. Os resultados da Revisão Sistemática da Literatura (RSL) podem ser considerados contribuições para a comunidade científica, pois nela são apresentadas as principais técnicas de anonimização usadas atualmente para fornecer privacidade em IoT, bem como os pontos positivos e negativos de cada uma.*

***Keywords.*** *Anonimização, segurança, privacidade, Internet da Coisas, Dados Pessoais.*

**Eventos Relacionados:** SBES

## 1. Introdução e Caracterização do Problema

A Internet das Coisas (*Internet of Things* - IoT) está em ascensão, conectando os objetos à Internet ou a uma rede local diariamente, interagindo com humanos, animais e até consigo mesmo. A IoT consiste, essencialmente, em sensores responsáveis por captar os mais variados tipos de dados sobre o meio ambiente e atuadores que executam tarefas de acordo com o que foi captado pelos sensores. Portanto, a IoT é capaz de conectar dispositivos e incorporá-los ao sistema de comunicação, de modo a processar inteligentemente suas informações específicas e tomar decisões autônomas [Ullah and Shah 2016].

Para [Borgia 2014], a aplicação da IoT vem sendo utilizada em três grandes domínios: (i) domínio industrial, (ii) domínio de cidades inteligentes, e (iii) domínio da saúde e bem-estar. A IoT pode ser subdividida, a partir destes três domínios, em mais nove subdomínios. [Borgia 2014], são eles: (i) Gerenciamento de logística e vida útil do produto; (ii) Agricultura e criação de animais; (iii) Processamento industrial; (iv) Mobilidade inteligente e Turismo inteligente; (v) Smart Grid; (vi) Casa / edifício inteligente; (vii) Monitor de segurança pública e meio ambiente; (viii) Vida independente; e (ix) Medicina e saúde. Na literatura, ainda é possível encontrar mais um subdomínio, que é o (x) Campus inteligente [Hossain et al. 2019, Sastra and Wiharta 2016, Du et al. 2016, Alghamdi and Shetty 2016].

Atrelada a um grande número de dispositivos e o enorme volume de dados que são gerados por esses dispositivos que fazem parte da IoT, existe uma preocupação sobre a privacidade dos dados dos usuários destes dispositivos IoT. A maioria dos usuários não está disposta a compartilhar seus dados pessoais diretamente com terceiros, seja para pesquisa acadêmica ou análise comercial, porque os dados pessoais contêm informações privadas ou confidenciais, como situação econômica ou hábitos de vida [Liu et al. 2019]. Diante disso, a coleta autônoma dos dados pessoais torna a privacidade uma das principais preocupações éticas e/ou tecnológicas com relação à IoT na atualidade [Berrehili and Belmekki 2016, Haradat et al. 2018].

Face ao exposto é possível observar que a IoT têm vantagens para o cotidiano das pessoas. No entanto, o uso de dispositivos inteligentes (coisas inteligentes) na vida pessoal apresenta alguns pontos fracos, por exemplo, a divulgação de dados pessoais, e estes podem facilitar a violação da privacidade. Logo, se por um lado esses dispositivos inteligentes ajudam a melhorar a qualidade de vida, a autonomia e o meio ambiente, por outro lado, esses mesmos dispositivos inteligentes e suas aplicações reúnem uma enorme quantidade de dados pessoais que podem ser usados de maneira maliciosa. Em vista disso, os consumidores de dispositivos IoT, estão usando esses dispositivos inteligentes conectados extensivamente, e eles (as coisas inteligentes) estão usando os dados pessoais das pessoas [Berrehili and Belmekki 2016].

Dentre as várias soluções existentes para tratar privacidade em IoT, a anonimização de dados tem se apresentado como uma solução bem aceita na comunidade científica [Elkhodr et al. 2012, Samani et al. 2015, Berrehili and Belmekki 2016, Davoli et al. 2017, Takbiri et al. 2018]. A anonimização utiliza várias técnicas, tais como pertubação e ofuscação, e essas técnicas podem ser utilizadas em vários contextos de aplicação da IoT, contudo, ainda não se tem uma técnica considerada ampla o suficiente para atender a todas as áreas da IoT.

Diante deste contexto e também de acordo com uma Revisão Sistemática da Literatura (RSL) conduzida nesta pesquisa que analisou trabalhos entre o período de 2009 a 2021, nenhum outro trabalho na literatura forneceu uma solução que possa ser aplicada nos vários campos de aplicação da IoT. Portanto, esta proposta de tese, pretende lidar com esse problema. Diante do exposto, o problema que permeia esta pesquisa é: **Não foi identificado uma solução para privacidade de dados, baseada em anonimização, que seja adaptável para vários ambientes de uso da IoT.** Fruto deste problema, cinco (5) questões de pesquisa (*research questions* - RQ) serão respondidas no decorrer do trabalho:

- **RQ1:** como anonimização de dados pode fornecer privacidade de dados aos usuários considerando o contexto e os vários ambientes de uso da IoT?
- **RQ2:** quais critérios devem ser considerados para recomendar algoritmos de anonimização para diferentes tipos de dados?
- **RQ3:** como Lógica de Descrição (DL) pode contribuir para que o mecanismo proposto possa definir qual algoritmo de anonimização recomendar de acordo com as características dos dados no contexto de ambientes IoT?
- **RQ4:** como o aprendizado supervisionado pode contribuir para que o mecanismo proposto seja capaz de aprender conforme analisa os dados?
- **RQ5:** como medir e analisar a qualidade da recomendação baseada no perfil dos dados?

Esta proposta de tese tem por objetivo geral propor uma solução que recomende qual o algoritmo de anonimização de dados é o mais adequado para o conjunto de dados de acordo com suas características, e consiga aprender conforme analisa os dados.

## 2. Fundamentação Téorica

### 2.1. Internet das Coisas

É possível encontrar na literatura várias definições para o termo Internet das Coisas (*Internet of Things* - IoT), contudo, ainda não existe um consenso geral a respeito deste conceito. Neste trabalho, será usada como referência a definição apresentada por [Santos et al. 2016], assim os autores afirmam que a Internet das Coisas "nada mais é que uma extensão da Internet atual", para proporcionar que objetos do dia a dia (quaisquer que sejam), se conectem a Internet e permitam que os próprios objetos, sejam acessados como provedores de serviços.

### 2.2. Anonimização de Dados

Uma das principais técnicas para tratar a privacidade de dados, é a anonimização. Ela remove ou substitui as informações que podem ser exploradas por um invasor, para comprometer a privacidade de um usuário. Portanto, a anonimização permite que os indivíduos permaneçam ocultos de ameaças em potencial quando seus dados são publicados para fins analíticos ou comerciais. Informações confidenciais ou identificadoras de indivíduos, que não devem ser publicadas ao domínio público, são chamadas de informações confidenciais [Li and Palanisamy 2019].

### 2.3. Ontologias

Para [BORST 2006]: "Uma ontologia é uma especificação formal e explícita de uma conceitualização compartilhada". Já [Almeida and Bax 2003] afirma que essa definição,

"formal" significa legível para computadores; "especificação explícita" diz respeito a conceitos, propriedades, relações, funções, restrições, axiomas que são explicitamente definidos; "compartilhado" quer dizer conhecimento consensual; e, "conceitualização" diz respeito a um modelo abstrato de algum fenômeno do mundo real.

## 3. Metodologia

Para a condução e execução desta pesquisa foi escolhido como método principal o *Design Science Research* (DSR) que tem duplo objetivo: (1) desenvolver um artefato para resolver um problema prático num contexto específico e (2) gerar novos conhecimentos técnicos e científicos [Pimentel et al. 2020], inicialmente nesta pesquisa foram feitos estudos para entender os problemas abordados (etapa 1 e etapa 2), para então propor um artefato para solucioná-los (etapa 3 e etapa 4), é também proposta uma avaliação experimental (etapa 5), que foi desenvolvida e modelada específicamente para avaliar o artefato proposto . Além da DSR, uma Revisão Sistemática da Literatura (RSL) é utilizada como metodologia de apoio para condução dessa pesquisa. Finalmente, a avaliação experimental se dará por meio de um *Benchmark* do mecanismo de recomendação proposto, para medir sua eficácia no processo de recomendação dos algoritmos de anonimização, as métricas a serem avaliadas são, a acurácia e a precisão. Esta pesquisa foi dividida em cinco etapas descritas a seguir:

- **Etapa 1:** realizar um estudo exploratório *ad hoc* da literatura para compreender os principais problemas relacionados à segurança e à privacidade de dados no contexto de IoT e as tecnologias mais promissoras para solucionar os problemas de privacidade; (RQ1);
- **Etapa 2:** condução de uma Revisão Sistemática da Literatura (RSL) que possibilitou conhecer as principais técnicas de anonimização para resolver problemas de privacidade de dados em IoT; (RQ1);
- **Etapa 3:** classificação dos tipos de dados presentes nos subdomínios da IoT. Após a classificação foi proposto o mecanismo de recomendação que é usado para analisar as características de um conjunto de dados, e a partir desta análise, identificar a qual subdomínio da IoT ele pertence; (RQ2,RQ3);
- **Etapa 4:** desenvolvimento do Mecanismo de Recomendação proposto, seguindo os fundamentos descritos na Etapa 3; (RQ4) e
- **Etapa 5:** avaliação experimental, em que será feita a comparação dos resultados após a execução do mecanismo com os resultados esperados de acordo com as características dos dados. As métricas para a avaliação são descritas na seção 4.1 (RQ5).

## 4. Método para Avaliar Resultados

Conforme descrito na seção 5, o mecanismo de recomendação proposto é dividido em módulos, e cada módulo tem suas funcionalidades específicas. Para avaliar a eficácia de todos os módulos do mecanismo, a avaliação se dará por meio de alguns estudos de caso divididos em 4 etapas, listadas a seguir:

- **Avaliação 1:** avaliar qual algoritmo de aprendizado supervisionado se adapta melhor ao objetivo desta proposta de tese;

- **Avaliação 2:** avaliação da classificação dos conjuntos de dados recebidos, para medir o desempenho do modelo de classificação lógica;
- **Avaliação 3:** avaliação da recomendação para medir o desempenho do modelo de recomendação personalizada; e
- **Avaliação 4:** avaliar o mecanismo completo com diferentes bases de dados de origens diferentes e com características distintas, para verificar a eficácia da recomendação.

Para executar todas as avaliações experimentais, será usado o conceito de teste A/B [Anderson 2015], onde serão comparadas versões dos módulos do artefato proposto, bem como versões completas do artefato, utilizando as métricas descritas na seção 4.1. De acordo com [Deng and Shi 2016] testes A/B são experimentos em que são criados duas versões de uma mesma peça/sistema. [Kompella 2015] define teste A/B como: "um processo no qual você escolhe a versão de melhor desempenho de uma página da *web*, exibindo aleatoriamente diferentes versões de seu *site* aos visitantes e avaliando o desempenho de cada variante em relação a uma métrica desejada".

### 4.1. Métricas de Avaliação

As métricas usadas nesta avaliação são baseadas nos trabalhos de [Espíndola and Ebecken 2005, Martins 2016], que fizeram um mapeamento sistemático sobre sistemas de recomendação e identificaram que normalmente para fazer avaliações desse tipo de sistema são usadas as métricas descritas a seguir:

Em que TP são valores verdadeiros positivos (True Positives), FP falso positivo (False Positive), TN verdadeiro negativo (True Negative) e FN falso negativo (False Negative).

**Acurácia:** é a proporção entre o número de previsões corretas e o número total de amostras de entrada:

$$\text{Acurácia} = \frac{TP + TN}{TP + FP + FN + TN}$$

**Sensibilidade:** também chamada de taxa de acerto ou recall, mede o quanto um classificador pode reconhecer exemplos positivos:

$$\text{Sensibilidade} = \frac{TP}{TP + FN}$$

**Especificidade:** mede o quanto um classificador pode reconhecer exemplos negativos:

$$\text{Especificidade} = \frac{TN}{TN + FP}$$

**Precisão:** é a proporção de exemplos positivos previstos que realmente são positivos:

$$\text{Precisão} = \frac{TP}{TP + FP}$$

**G-mean 1:** é a média geométrica de sensibilidade e precisão:

$$\text{GSP} = \sqrt{Sensibilidade\ X\ Precisão}$$

**G-mean 2:** é a média geométrica de sensibilidade e especificidade:

$$\text{GSE} = \sqrt{Sensibilidade\ X\ Especificidade}$$

## 5. Estado Atual do Trabalho

O mecanismo de recomendação proposto tem por objetivo recomendar qual o algoritmo de anonimização de dados é o mais adequado para o conjunto de dados de acordo com suas características, e consiga aprender conforme analisa os dados. São usados como critérios para fazer a recomendação as principais características dos dados. Para a recomendação é necessário que seja feita uma análise dos dados levando em consideração a origem deles, o tipo e a heterogeneidade, essa classificação é feita por meio do formalismo das ontologias e da Lógica de Descrição. De acordo com essas características, é recomendado o algoritmo de anonimização mais eficaz para proteger os dados privados dos usuários e, ao mesmo tempo possibilitar que os dados sejam úteis para análises futuras.

Os dados são gerados pelos dispositivos IoT, que podem ser de 10 subdomínios distintos, dispostos na categoria (subdomínios) da Figura 1. Esses dados normalmente são enviados para serem armazenados em alguma plataforma na nuvem (por exemplo: Amazon Web Services - AWS e Microsoft Azure), representada na Figura 1 como Dados Brutos, local onde os dados são armazenados depois que são gerados. Essa base de dados pode ser atualizada constantemente pelos dispositivos ou podem ser dados que já foram armazenados.

O mecanismo de recomendação proposto está dividido em 3 módulos, são eles: (i) **Módulo de Dados**, responsável por receber os dados brutos e convertê-los em um formato padronizado e enviá-los para o modelo de recomendação lógica, que fará a classificação por meio do formalismo das ontolotogias e da Lógica de Descrição; (ii) **Módulo de Recomendação**, responsável por fazer a classificação dos dados de acordo com suas características, e recomendar o algoritmo de anonimização mais adequado; (iii) **Módulo Anonimizador**, responsável por anonimizar os dados de acordo com a recomendação.

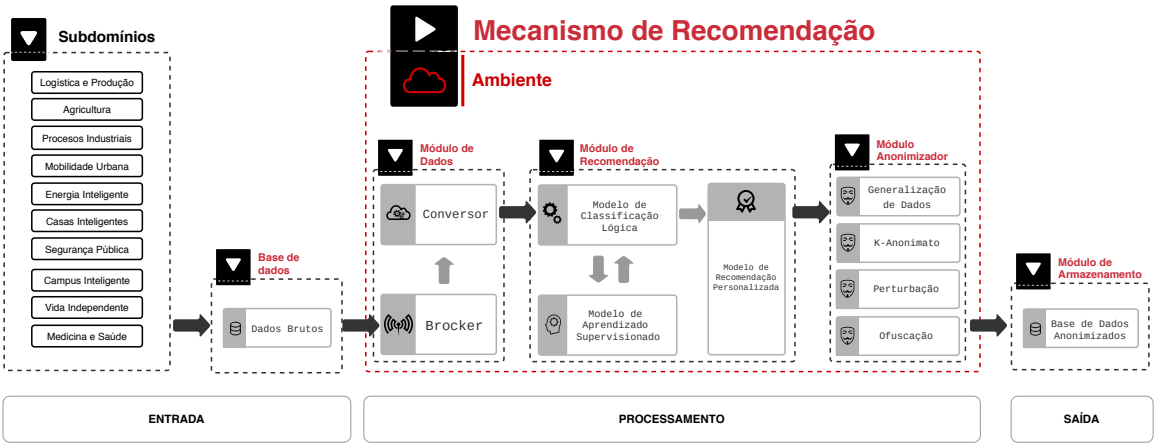


**Figura 1. Arquitetura do mecanismo de recomendação proposto**

Até o momento de escrita deste documento já foram concluídas as três primeiras das cinco etapas descritas na seção 3. O desenvolvimento do mecanismo está em fase de implementação até o momento de escrita deste documento (etapa 4). A etapa de

avaliação já foi projetada como descrito na seção 4.1, e será executa após a finalização da implementação do mecanismo.

## 6. Contribuições esperadas

Com o desenvolvimento desta pesquisa, espera-se responder as questões de pesquisa listadas na seção 1, e alcançar as seguintes contribuições:

- O desenvolvimento de uma RSL para mapear as principais técnicas de anonimização de dados em IoT e os pontos positivos e negativos de cada técnica;
- Uma proposta de solução que recomenda qual o algoritmo de anonimização de dados é mais adequado para o conjunto de dados de acordo com suas características, e consiga aprender conforme analisa novos dados;
- A criação dos critérios para escolha de algoritmos de anonimização baseado nas características dos dados;
- Uma ontologia para dar suporte a recomendação baseada na lógica de descrição;
- O modelo de aprendizagem supervisionado para atualizar a base de conhecimento da ontologia a medida que analisa novos dados; e
- A metodologia para avaliação da solução proposta.

## 7. Comparação com Trabalhos Relacionados

[Davoli et al. 2017] criaram um protocolo de anonimato, projetado especificamente para a comunicação Máquina a Máquina IoT e SIoT (*Social Internet of Things*). O sistema de anonimato proposto é baseado no conceito de roteamento do Tor. Já em [Haradat et al. 2018], é proposto um método para anonimizar dados de demanda de energia.

Em sua pesquisa [Lim et al. 2018], apresentam a implementação e avaliação de uma estrutura de anonimização de dados escalável e leve para a implantação flexível da função de anonimização que eles propõem. [Nayahi and Kavitha 2017] propõem um algoritmo de anonimização baseado em *cluster* e resiliente a ataques de similaridade e ataques de inferência probabilística. Os dados anonimizados são distribuídos no *Hadoop Distributed File System*.

O trabalho de [Liao et al. 2017], tem como foco principal a solução de dois problemas: (i) preservação da privacidade da localização para uma única consulta; (ii) preservação da privacidade da trajetória para consultas contínuas. Eles propõem um algoritmo eficiente baseado na técnica de *k-anonymity* para proteger a privacidade da trajetória do usuário em serviços baseados em localização. Em sua pesquisa, [Otgonbayar et al. 2016] apresentam um novo algoritmo de anonimato que publica fluxos de dados da IoT gerados a partir de vários dispositivos sob o modelo de privacidade do *k-anonymity*. Já [Rodriguez-Garcia et al. 2020] apresentam um novo mecanismo de comunicação anônima colaborativa voltada para ambientes multiusuário.

Com está pesquisa, foi possível verificar que na literatura, até o presente momento não há a identificação de uma solução para privacidade de dados baseada em anonimização que seja adaptável para vários ambientes de uso da IoT. Neste sentido esta pesquisa visa o desenvolver um mecanismo que possa recomendar algoritmos de anonimização para conjuntos de dados no contexto de IoT levando em consideração suas

características. Está proposta visa desenvolver uma solução seja robusta para tratar dados provenientes dos diferentes subdomínios da IoT, e que tenha a capacidade de aprender conforme analisa novos dados.

## Referências


Alghamdi, A. and Shetty, S. (2016). Survey toward a smart campus using the internet of things. In *2016 IEEE 4th international conference on future internet of things and cloud (FiCloud)*, pages 235–239. IEEE.

Almeida, M. B. and Bax, M. P. (2003). An overview about ontologies: survey about definitions, types, applications, evaluation and building methods. *Ciência da Informação*, 32(3):7–20.

Anderson, C. (2015). *Creating a data-driven organization: Practical advice from the trenches*. "O'Reilly Media, Inc.".

Berrehili, F. Z. and Belmekki, A. (2016). Privacy preservation in the internet of things. In *International Symposium on Ubiquitous Networking*, pages 163–175. Springer.

Borgia, E. (2014). The internet of things vision: Key features, applications and open issues. *Computer Communications*, 54:1–31.

BORST, W. N. (2006). *Construction of engineering ontologies. 1997. 243 f.* PhD thesis, Tese (Doutorado).–University of Twente, Enschede, 1997. Disponível em:¡ http ....

Davoli, L., Protskaya, Y., and Veltri, L. (2017). An anonymization protocol for the internet of things. In *2017 International Symposium on Wireless Communication Systems (ISWCS)*, pages 459–464. IEEE.

Deng, A. and Shi, X. (2016). Data-driven metric development for online controlled experiments: Seven lessons learned. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 77–86.

Du, S., Meng, F., and Gao, B. (2016). Research on the application system of smart campus in the context of smart city. In *2016 8th International Conference on Information Technology in Medicine and Education (ITME)*, pages 714–718. IEEE.

Elkhodr, M., Shahrestani, S., and Cheung, H. (2012). A review of mobile location privacy in the internet of things. In *2012 Tenth International Conference on ICT and Knowledge Engineering*, pages 266–272. IEEE.

Espíndola, R. and Ebecken, N. (2005). On extending f-measure and g-mean metrics to multi-class problems. *WIT Transactions on Information and Communication Technologies*, 35.

Haradat, K., Ohnot, Y., Nakamurat, Y., and Nishit, H. (2018). Anonymization method based on sparse coding for power usage data. In *2018 IEEE 16th International Conference on Industrial Informatics (INDIN)*, pages 571–576. IEEE.

Hossain, I., Das, D., and Rashed, M. G. (2019). Internet of things based model for smart campus: Challenges and limitations. In *2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2)*, pages 1–4. IEEE.

Kompella, K. (2015). A guide to a/b testing tools.

Li, C. and Palanisamy, B. (2019). Reversible spatio-temporal perturbation for protecting location privacy. *Computer Communications*, 135:16–27.

Liao, D., Sun, G., Li, H., Yu, H., and Chang, V. (2017). The framework and algorithm for preserving user trajectory while using location-based services in iot-cloud systems. *Cluster Computing*, 20(3):2283–2297.

Lim, Y.-s., Srivatsa, M., Chakraborty, S., and Taylor, I. (2018). Learning light-weight edge-deployable privacy models. In *2018 IEEE International Conference on Big Data (Big Data)*, pages 1290–1295. IEEE.

Liu, Y.-N., Wang, Y.-P., Wang, X.-F., Xia, Z., and Xu, J.-F. (2019). Privacy-preserving raw data collection without a trusted authority for iot. *Computer Networks*, 148:340–348.

Martins, R. F. d. V. (2016). *Sistema de Recomendação de Tutoriais*. PhD thesis.

Nayahi, J. J. V. and Kavitha, V. (2017). Privacy and utility preserving data clustering for data anonymization and distribution on hadoop. *Future Generation Computer Systems*, 74:393–408.

Otgonbayar, A., Pervez, Z., and Dahal, K. (2016). Toward anonymizing iot data streams via partitioning. In *2016 IEEE 13th International conference on mobile ad hoc and sensor systems (MASS)*, pages 331–336. IEEE.

Pimentel, M., Filippo, D., and Santos, T. M. (2020). Design science research: pesquisa científica atrelada ao design de artefatos. *RE@ D-Revista de Educação a Distância e Elearning*, 3(1):37–61.

Rodriguez-Garcia, M., Cifredo-Chacón, M.-á., and Quirós-Olozábal, Á. (2020). Cooperative privacy-preserving data collection protocol based on delocalized-record chains. *IEEE Access*, 8:180738–180749.

Samani, A., Ghenniwa, H. H., and Wahaishi, A. (2015). Privacy in internet of things: A model and protection framework. In *ANT/SEIT*, pages 606–613.

Santos, B. P., Silva, L., Celes, C., Borges, J. B., Neto, B. S. P., Vieira, M. A. M., Vieira, L. F. M., Goussevskaia, O. N., and Loureiro, A. (2016). Internet das coisas: da teoriaa prática. *Minicursos SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuidos*, 31.

Sastra, N. P. and Wiharta, D. M. (2016). Environmental monitoring as an iot application in building smart campus of universitas udayana. In *2016 International Conference on Smart Green Technology in Electrical and Information Systems (ICSGTEIS)*, pages 85–88. IEEE.

Takbiri, N., Li, K., Pishro-Nik, H., and Goeckel, D. L. (2018). Statistical matching in the presence of anonymization and obfuscation: Non-asymptotic results in the discrete case. In *2018 52nd Annual Conference on Information Sciences and Systems (CISS)*, pages 1–6. IEEE.

Ullah, I. and Shah, M. A. (2016). A novel model for preserving location privacy in internet of things. In *2016 22nd International conference on automation and computing (ICAC)*, pages 542–547. IEEE.