Aplicação de *Differential Privacy* em dados de *smart building* seguindo modelo SITA

João V. Gularte[1], **Charles V. Neu**[1]

[1] Departamento de Engenharias, Arquitetura e Computação
Universidade de Santa Cruz do Sul (UNISC)

gularte65@gmail.com, charlesneu@gmail.com

Abstract. *The nature of technologies applied to enable the development of smart buildings introduces new user privacy challenges, such as the potential misuse of data from sensors and IoT devices. Techniques like Differential Privacy (DP) can be used to address these issues. However, there are few studies that assess the actual impact of implementing DP in smart building data. Therefore, this study aims to examine the application and impacts of DP, following the SITA model, on the operation of smart building services. To achieve this, an experimental scenario for the prediction of CO_2 was developed and executed. The findings show that the DP technique can enhance privacy for smart building data without substantially compromising the accuracy of the prediction of CO_2.*

Resumo. *A natureza das tecnologias aplicadas para viabilizar o desenvolvimento dos smart buildings gerou novos desafios relacionadas à privacidade dos usuários, como o possível o uso indevido dos dados capturados por sensores e dispositivos de IoT. Técnicas, como Differential Privacy (DP), podem ser utilizadas para endereçar esses desafios. Entretanto, há poucos estudos que avaliam o verdadeiro impacto da aplicação de DP em dados de smart buildings. Sendo assim, este estudo busca examinar o uso e o impacto que a técnica de Differential Privacy, seguindo o modelo SITA, exerce no funcionamento dos serviços de prédios inteligentes. Para isso, um cenário experimental de predição de CO_2 foi desenvolvido e analisado. Os resultados mostram que a técnica de DP pode ser aplicada para adicionar privacidade aos dados de prédios inteligentes sem comprometer substancialmente a acurácia da predição de CO_2.*

1. Introdução

Os *smart buildings* são ambientes concebidos a partir da popularização das tecnologias de IoT (*Internet of Things*) [Pathmabandu et al. 2023]. Esses edifícios oferecem diversos benefícios aos seus ocupantes, como o conforto e a qualidade dos espaços, garantidos especialmente pela manutenção da qualidade do ar. Por isso, é necessário que esses ambientes monitorem a ocupação dos espaços e os níveis de concentração de CO_2, uma vez que esses fatores influenciam diretamente a qualidade do ar [Chaudhari et al. 2024]. Esses locais empregam sensores que coletam dados sobre temperatura, umidade, luminosidade, concentração de CO_2 e ocupação das salas e demais ambientes [Pathmabandu et al. 2023]. Os dados coletados são armazenados em estruturas adequadas, que permitem a geração de conjuntos de dados específicos (*datasets*). Posteriormente, esses *datasets* são utilizados no treinamento de algoritmos de *machine learning* para a criação de sistemas responsáveis pela predição dos níveis de CO_2 [da Silva et al. 2023].

Contudo, a coleta e a análise desses dados podem representar uma violação de privacidade, especialmente se agentes maliciosos tiverem acesso a essas informações e as utilizarem para fins não autorizados [Liu et al. 2025]. Por exemplo, um invasor com acesso a *datasets* que contenham leituras de CO_2 poderia infringir a privacidade de um indivíduo ao realizar ataques de vinculação, combinando essas informações com outros dados para identificar qual pessoa está em determinado ambiente de um *smart building* [da Silva et al. 2023]. Além disso, existem crescentes pressões sociais e regulatórias, por meio de legislações como a *General Data Protection Regulation*(GDPR)[1], na Europa, e a Lei Geral de Proteção de Dados (LGPD)[2], no Brasil, que buscam regular a coleta, a distribuição e o uso de dados pessoais.

Para resolver esses desafios, técnicas de privacidade, como *Differential Privacy* (DP) [Dwork and Roth 2014] e o modelo conceitual SITA (*Spatial*, *Identity*, *Temporal*, *and Activity*) [Andersen et al. 2013], podem ser utilizadas em conjunto para adicionar proteção aos *datasets* gerados por prédios inteligentes. Porém, é conhecido que os sistemas que utilizam métodos de privacidade podem enfrentar o *trade-off* entre privacidade e utilidade. No contexto deste estudo, essa relação pode influenciar diretamente o funcionamento dos serviços presentes nos *smart buildings*, uma vez que o aumento da privacidade pode comprometer a utilidade dos dados. Diante desse cenário, este trabalho tem como objetivo analisar o uso e o impacto que a técnica de *DP*, seguindo o modelo SITA, exerce sobre o funcionamento dos serviços de prédios inteligentes.

2. *Differential Privacy* e o modelo conceitual SITA

Differential Privacy (DP) [Dwork and Roth 2014] é uma técnica baseada na inserção controlada de ruído estatístico nos dados. Esta característica permite que a técnica estabeleça um equilíbrio entre a privacidade e a utilidade dos dados [Liu et al. 2025]. Em termos práticos, a quantidade de ruído inserido é controlada por meio do **parâmetro de privacidade**; quanto menor for o seu valor, maior será o ruído adicionado e, portanto, maior será a privacidade da informação. A inserção do ruído é realizada a partir de uma **distribuição estatística**, sendo as mais comuns, nesse contexto, as distribuições de Laplace e a Gaussiana [Liu et al. 2025]. São essas características que permitem a técnica de DP oferecer a proteção das informações sem a necessidade de sua exclusão ou remoção, como ocorre nas abordagens tradicionais de anonimização [Ponomareva et al. 2023].

O modelo conceitual SITA permite aos usuários controlar, de maneira granular, as preferências de privacidade de uma aplicação [da Silva et al. 2023]. Nele, as informações são categorizadas em **quatro dimensões** [Andersen et al. 2013]: espacial (*spatial*), relacionadas aos dados de localização do usuário; identidade (*identity*), ligadas aos dados pessoais do usuário; temporal (*temporal*), para os dados sobre o instante em que o usuário realizou uma atividade na aplicação; e, por último, atividade (*activity*), que corresponde a informações relacionadas ao comportamento do usuário. Para cada dimensão, podem ser atribuídos **cinco níveis de privacidade**, sendo que, para cada nível, pode ser aplicada alguma técnica de privacidade específica [Andersen et al. 2013]. No modelo, os níveis são representados pelos números de 0 a 4, e sugere-se que, no nível 0, nenhuma informação seja compartilhada, enquanto no nível 4, toda a informação é divulgada. Por

[1]https://gdpr.eu/

[2]https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd

fim, a atribuição do nível de privacidade para cada dimensão gera uma **configuração SITA** (Figura 1), que pode ser expressa pela sequência de quatro dígitos, seguindo a ordem das dimensões: *spatial*, *identity*, *temporal* e *activity*.

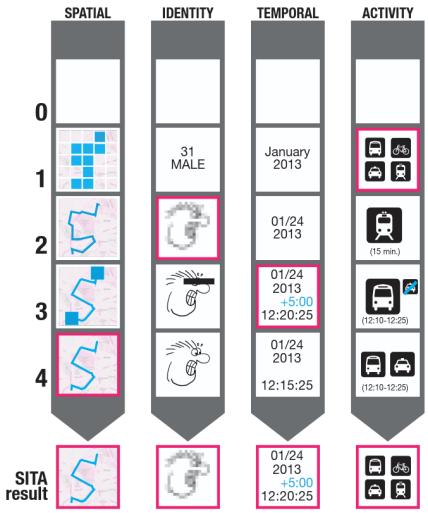

Figura 1. Exemplo de configuração SITA 4231. Fonte: [Andersen et al. 2013]

3. Trabalhos Relacionados

Os desafios relacionados à privacidade de dados em *smart buildings* constituem um campo cada vez mais explorado pela academia. É possível citar como exemplo o trabalho de [Neu et al. 2023] que propõe uma solução para lidar com a gestão das preferências de privacidade dos ocupantes dos prédios inteligentes. A solução consiste em um sistema de *blockchain*, baseado no modelo de privacidade SITA, que permite aos ocupantes de *smart buildings* definir e gerenciar suas preferências de privacidade de forma anônima. Por meio de contratos inteligentes, essa solução controla como as preferências de privacidade são compartilhadas, garantindo aos usuários o controle total. Seguindo uma temática semelhante, [Pathmabandu et al. 2023] propõe uma solução para a gestão do consentimento informado em prédios inteligentes, com o objetivo de ampliar a transparência sobre quais dados são coletados pelos dispositivos IoT. Com essa solução, os autores buscam gerar conscientização nos usuários sobre as implicações da privacidade dos dados coletados e incentivar decisões mais conscientes de consentimento.

Em outro estudo, [da Silva et al. 2023] analisa os impactos gerados pelo uso de técnicas de privacidade nos dados utilizados pelos serviços de *smart buildings*. Para tal, é realizada uma implementação para a proteção de dados, seguindo o modelo SITA, que utiliza as técnicas de generalização e supressão. A avaliação dos impactos gerados pela implementação é feita por meio de um experimento que simula a predição de CO_2 em prédios inteligentes, utilizando dados que foram privados pela implementação. Os resultados indicam a viabilidade do uso de técnicas de privacidade para adicionar proteção aos dados de prédios inteligentes utilizados no modelo de predição. Contudo, os resultados demonstram como as técnicas de privacidade aplicadas no estudo reduzem a utilidade dos dados e, portanto, prejudicam o desempenho da predição de CO_2.

Devido à natureza das tecnologias utilizadas, como sensores e dispositivos IoT, para implementar prédios inteligentes, emergiu uma variedade de desafios na área de privacidade de dados que precisam ser abordados. Os estudos selecionados apresentam uma amostra desses desafios e das soluções aplicadas. Já o estudo apresentado por [da Silva et al. 2023] instigou e motivou a realização deste trabalho.

4. Aplicação de *Differential Privacy* seguindo o modelo SITA

O desenvolvimento deste trabalho aplica a técnica de *DP*, seguindo o modelo SITA, para a proteção de *datasets* de prédios inteligentes (Figura 2). Dado o cenário deste trabalho, a aplicação do modelo SITA pode ser especialmente útil devido a dois fatores: por meio das dimensões SITA, o modelo oferece uma estrutura flexível que permite lidar com diferentes tipos de dados presentes nos *smart buildings*; já os níveis de privacidade, através da configuração SITA, oferecem flexibilidade e facilidade na definição da privacidade aplicada às informações dos prédios inteligentes.

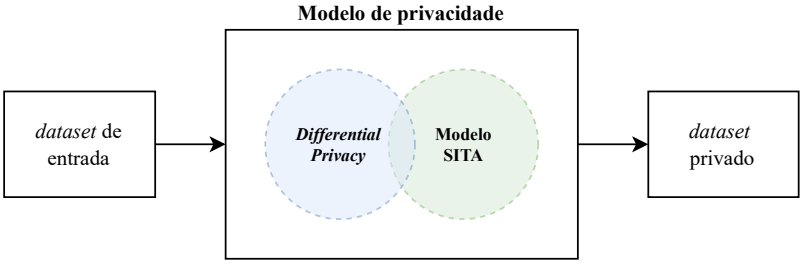

Figura 2. Representação conceitual

Junto a isso, é aplicada a técnica de DP como mecanismo de privacidade da implementação porque, diferentemente de outros métodos — nos quais a privacidade da informação é garantida pela exclusão parcial ou total dos dados —, com DP, a privacidade dos dados é assegurada pela adição controlada de ruído. Essa característica é o que permite alterar os valores dos dados mantendo a estrutura original do *dataset*. Por fim, a união dessas duas abordagens possibilita que os níveis de privacidade do modelo SITA sejam utilizados como referência para a definição dos valores do parâmetro de privacidade do DP.

4.1. Cenário experimental de predição de CO_2 em prédios inteligentes

A fim de compreender os efeitos que a implementação deste trabalho pode gerar nos serviços de prédios inteligentes, foi conduzido um experimento que simula o cenário de predição de CO_2. O objetivo deste experimento é responder à pergunta: qual é o impacto gerado pelo uso da técnica de DP, seguindo o modelo SITA, sobre os serviços de prédios inteligentes? Para responder a esta questão, o experimento foi estruturado nas etapas que estão ilustradas na Figura 3 e descritas brevemente a seguir.

- ***Dataset* de entrada:** os dados utilizados no experimento foram coletados em um ambiente real e disponibilizados pelo trabalho de [da Silva et al. 2023] por meio de um *dataset* composto por 200 mil registros. O *dataset* é composto por dados de sensores de umidade, temperatura, ocupação, luminosidade e CO_2, agrupados por sala, data e horário de leitura dos dados pelos sensores.

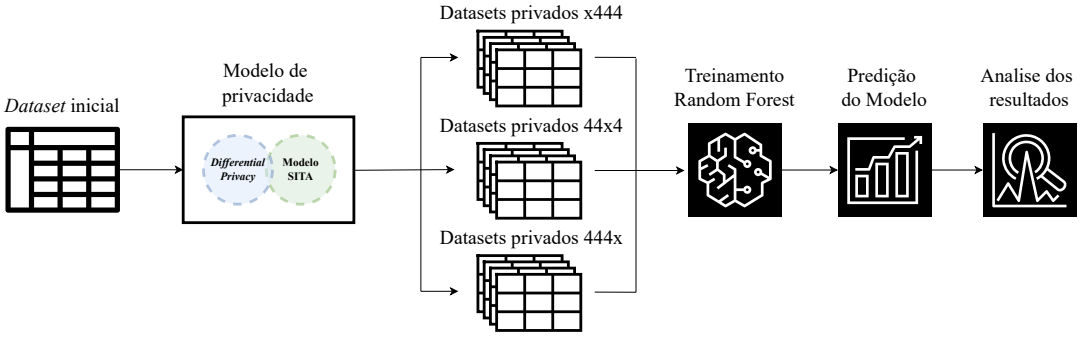

Figura 3. Etapas do experimento

- **Modelo de privacidade:** a implementação utiliza a técnica de DP, seguindo o modelo SITA; por esse motivo, as colunas do *dataset* de entrada foram mapeadas da forma mais apropriada para as dimensões do SITA, e os valores do parâmetro de privacidade da técnica de DP foram atribuídos com base nos níveis de privacidade do SITA. O ruído adicionado pela técnica de DP é gerado por meio da distribuição clássica de Laplace e, para isso, foi empregada a biblioteca Diffprivlib[3].
- **Geração dos *datasets* privados:** Por meio do uso do modelo de privacidade, foram gerados 12 *datasets* privados, um para cada uma das seguintes configurações SITA: 3444, 2444, 1444, 0444, 4434, 4424, 4414, 4404, 4443, 4442, 4441 e 4440. Essas configurações foram escolhidas com base no estudo de [da Silva et al. 2023]. Cada um dos 12 *datasets* privados foi utilizado no treinamento do modelo de predição de CO_2.
- **Treinamento e Predição do modelo:** a predição dos níveis CO_2 foi realizada a partir do uso do algoritmo de *machine learning Random Forest*. Este algoritmo foi escolhido com base nos resultados dos trabalhos de [da Silva et al. 2023]. Para o treinamento, predição e avaliação do desempenho do modelo, foi utilizada a biblioteca Scikit-learn[4].
- **Análise dos resultados:** para avaliar o desempenho do modelo, foram analisadas as médias das métricas de coeficiente de determinação (R^2), erro médio absoluto (MAE) e a raiz do erro quadrático médio (RMSE). O método de avaliação segue o mesmo aplicado por [da Silva et al. 2023], considerando a equivalência do cenário em que ambos os experimentos estão inseridos.

Por fim, os *datasets* e o *notebook*, que contém a implementação do modelo de privacidade e do experimento, seguidos dos resultados, estão disponíveis em um repositório público[5]. Isto permite a reprodutibilidade do estudo e pode servir de base para desdobramentos em trabalhos futuros.

5. Discussões dos resultados

A Tabela 1 resume os resultados obtidos por meio da execução do experimento. Com isso, é possível analisar qual foi o impacto que a implementação deste trabalho gerou

[3]https://diffprivlib.readthedocs.io/
[4]https://scikit-learn.org/
[5]https://github.com/joaogularte/differential-privacy-and-sita-model-for-smart-building-data

sobre o desempenho do modelo de predição de CO_2. É possível notar que os resultados das configurações associadas às dimensões *Spatial* (**x444**) e *Temporal* (**44x4**), mesmo nos níveis mais restritivos de privacidade (0444 e 4404), foram aqueles que causaram a menor degradação da capacidade preditiva do modelo — redução de 3,3% e 2,07% quando comparadas com a configuração 4444 do *dataset* inicial. Estes resultados sugerem que a aplicação de *Differential Privacy* adicionou privacidade ao *dataset* por meio da adição de ruído, sem comprometer negativamente a utilidade dos dados. Isso leva a conclusão de que a técnica de DP pode ser utilizada para adicionar privacidade aos *datasets* de prédios inteligentes, sem gerar perda significativa no desempenho da predição de CO_2. Portanto, essas descobertas podem ser úteis na construção de sistemas baseados em *machine learning* de prédios inteligentes, especialmente para aqueles que estão inseridos em cenários mais desafiadores, onde há uma necessidade simultânea de manter altos níveis de privacidade e garantir o bom funcionamento dos serviços.

Configuração SITA		**Métricas**		
		R²	**MAE**	**RMSE**
x444	0444	69,82%	38,90%	66,74%
	1444	69,49%	39,45%	67,05%
	2444	68,87%	40,24%	67,91%
	3444	68,43%	40,78%	68,25%
44x4	4404	69,49%	38,25%	67,14
	4414	70,37%	37,00%	66,17%
	4424	71,06%	36,16%	65,46%
	4434	71,33%	35,61%	65,10%
444x	4440	64,05%	45,91%	73,17%
	4441	64,38%	45,11%	72,70%
	4442	64,58%	44,96%	72,49%
	4443	64,08%	45,51%	72,92%
***Dataset* inicial**	4444	73,13%	32,31%	62,87%

Tabela 1. Métricas do modelo de predição

Outra discussão que pode ser feita ao compararmos os resultados obtidos neste estudo com os de [da Silva et al. 2023], uma vez que ambos abordam a mesma problemática e utilizam o modelo SITA. Apesar dessas igualdades, há uma diferença significativa na implementação que distingue os dois trabalhos: neste estudo, é aplicada a técnica de *Differential Privacy*, enquanto no estudo dos outros autores, são empregadas técnicas de ofuscação. Essa diferença resultou em impactos significativos no cenário avaliado. Por exemplo, é possível observar que às configurações da dimensão Temporal (**44x4**) da implementação deste trabalho permitem níveis de privacidade mais restritivos (4404), sem causar perda significativa no desempenho do modelo de predição. Já na implementação do estudo comparado, esse mesmo cenário resulta em uma redução de 28% no desempenho do modelo de predição. Isso reflete que, dependendo do cenário, a técnica de *Differential Privacy* pode ser menos suscetível aos efeitos do *trade-off* entre privacidade e utilidade quando comparada a técnica de ofuscação.

6. Considerações Finais

Neste trabalho, foi analisado o uso e o impacto que a técnica de *Differential Privacy*, seguindo o modelo SITA, exerce sobre o funcionamento dos serviços de prédios inteligentes. Nesse sentido, foi realizada uma implementação que combina o uso de DP com o modelo SITA. Para compreender o impacto desta implementação sobre os serviços dos *smart buildings*, foi elaborado um cenário experimental que simula a predição de CO_2.

Com base nos resultados do experimento, foi possível analisar o impacto que a implementação deste trabalho gerou na predição de CO_2 de prédios inteligentes. A partir disso, foi possível concluir que DP pode ser utilizada para adicionar privacidade aos dados de prédios inteligentes, sem comprometer sua utilidade e, assim, sem gerar perda significativa no desempenho da predição de CO_2. Essa consideração foi reforçada ao comparar os resultados deste estudo com os disponíveis na literatura. Os achados apresentados neste trabalho podem ser relevantes para o desenvolvimento de serviços de *machine learning* em prédios inteligentes que precisam atender a requisitos rigorosos de privacidade. Por fim, como direcionamento para trabalhos futuros, é importante validar a eficácia da implementação deste trabalho na proteção da privacidade por meio de um cenário que simule um ataque de vinculação, utilizando dados de ocupação de prédios inteligentes.

Referências

[Andersen et al. 2013] Andersen, M. S., Kjargaard, M. B., and Grønbæk, K. (2013). The sita principle for location privacy — conceptual model and architecture. In *2013 International Conference on Privacy and Security in Mobile Systems (PRISMS)*.

[Chaudhari et al. 2024] Chaudhari, P., Xiao, Y., Cheng, M. M.-C., and Li, T. (2024). Fundamentals, algorithms, and technologies of occupancy detection for smart buildings using iot sensors. *Sensors*, 24(7).

[da Silva et al. 2023] da Silva, M. P., Nunes, H. C., Neu, C. V., Thomas, L. T., Zorzo, A. F., and Morisset, C. (2023). Impact of using privacy model on smart buildings data for co2 prediction. In *Data and Applications Security and Privacy XXXVII: 37th Annual IFIP WG 11.3 Conference*.

[Dwork and Roth 2014] Dwork, C. and Roth, A. (2014). The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, 9(3–4):211–407.

[Liu et al. 2025] Liu, Q., Shakya, R., Khalil, M., and Jovanovic, J. (2025). Advancing privacy in learning analytics using differential privacy. In *Proceedings of the 15th International Learning Analytics and Knowledge Conference*, page 181–191.

[Neu et al. 2023] Neu, C. V., Gibson, J., Lunardi, R. C., Leesakul, N., and Morisset, C. (2023). A blockchain-based architecture to manage user privacy preferences on smart shared spaces privately. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*.

[Pathmabandu et al. 2023] Pathmabandu, C., Grundy, J., Chhetri, M. B., and Baig, Z. (2023). Privacy for iot: Informed consent management in smart buildings. *Future Generation Computer Systems*.

[Ponomareva et al. 2023] Ponomareva, N., Vassilvitskii, S., Xu, Z., McMahan, B., Kurakin, A., and Zhang, C. (2023). How to dp-fy ml: A practical tutorial to machine learning with differential privacy.