Preservando a Utilidade de Dados Urbanos via Alocação Adaptativa de Ruído em Privacidade Diferencial

Ivo A. Pimenta[1],**Marcelo H. Lee**[1], **Evellin S. Moura** [1],
Erick S. Nascimento[1], **Geraldo R. Filho**[2], **Rafael L. Gomes**[1]

[1]Universidade Estadual do Ceará (UECE)

{aguiar.pimenta, marcelo.lee, evellin.moura,

erick.nascimento}@aluno.uece.br, rafa.lopes@uece.br

[2]Universidade Estadual do Sudoeste da Bahia (UESB)

geraldo.rocha@uesb.edu.br

Abstract. *Distributed intelligent systems require privacy-preserving mechanisms that balance data utility and computational efficiency. Conventional approaches often degrade machine learning performance by injecting uniform noise across all features. This paper introduces Adaptive Differential Privacy via Mutual Information (APDIM), an adaptive strategy that allocates noise based on feature relevance and applies correlation-aware perturbations to preserve key statistical dependencies. Experimental results show that APDIM sustains high machine learning accuracy while remaining lightweight for deployment in resource-constrained distributed environments.*

Resumo. *No cenário das cidades inteligentes, os sistemas distribuídos demandam mecanismos de preservação de privacidade que equilibrem utilidade dos dados e eficiência computacional. Abordagens tradicionais degradam o desempenho de aprendizado de máquina ao aplicar ruído uniforme sobre todas as características. Este trabalho apresenta o Adaptive Differential Privacy via Mutual Information (APDIM), uma estratégia adaptativa que aloca ruído conforme a relevância das características e preserva dependências estatísticas por meio de perturbação sensível à correlação. Os resultados mostram que o APDIM mantém elevada acurácia com baixo custo computacional, sendo adequado a ambientes distribuídos com recursos limitados.*

1. Introdução

No cenário das cidades inteligentes, há uma crescente adoção de arquiteturas de computação em borda integradas à nuvem que têm possibilitado o desenvolvimento de aplicações que demandam baixa latência, processamento distribuído e análise contínua de dados, como sistemas de Internet das Coisas (IoT), cidades inteligentes e aplicações industriais. Nesse contexto, o processamento é deslocado para nós próximos às fontes de dados, reduzindo atrasos e consumo de banda, porém ampliando os desafios relacionados à segurança e à privacidade das informações, especialmente quando dados sensíveis são utilizados em tarefas de aprendizado de máquina [Wang et al. 2024, Yao et al. 2023, Souza et al. 2024, Pimenta et al. 2024].

A Privacidade Diferencial (DP) tem se consolidado como um dos principais mecanismos para a proteção de dados sensíveis, ao oferecer garantias matemáticas formais contra a reidentificação de indivíduos [Dwork et al. 2014]. Abordagens tradicionais de DP, como a aplicação uniforme do mecanismo de Laplace, adicionam ruído de forma indiscriminada a todas as características dos dados. Embora eficazes do ponto de vista da privacidade, essas estratégias tendem a degradar significativamente a utilidade dos dados, impactando negativamente o desempenho de modelos de aprendizado de máquina, especialmente em ambientes de computação em borda, nos quais os recursos computacionais e energéticos são restritos [Fernandes et al. 2021]. Ademais, legislações de proteção de dados, como o GDPR na Europa e a LGPD no Brasil, impõem requisitos rigorosos para a proteção de informações sensíveis contra acesso não autorizado, reforçando a necessidade de mecanismos de privacidade que conciliem garantias formais com preservação da utilidade dos dados [Pimenta et al. 2025].

Além disso, estudos anteriores demonstram que a Privacidade Diferencial tradicional pode apresentar limitações significativas quando aplicada a conjuntos de dados com correlações estatísticas entre atributos. Yang et al. [Yang et al. 2015] mostram que, em cenários com dados correlacionados, o vazamento de informação pode ser amplificado, especialmente quando o adversário possui conhecimento parcial. Esses resultados evidenciam que mecanismos de privacidade que tratam atributos como independentes podem oferecer garantias insuficientes, reforçando a necessidade de abordagens que considerem explicitamente a relevância e a correlação estatística entre características ao aplicar perturbações.

Com o intuito de reduzir esses impactos, pesquisas recentes têm explorado mecanismos adaptativos de privacidade diferencial, nos quais o orçamento de privacidade é distribuído de maneira não uniforme, levando em consideração a relevância das características para a tarefa analítica [Zhang et al. 2023, Chen et al. 2024b]. Nesse contexto, a Informação Mútua (IM) destaca-se como uma métrica estatística eficaz para quantificar a dependência entre uma característica e a variável alvo, permitindo identificar atributos mais informativos para o processo de aprendizado de máquina [Hall 1999]. Essa abordagem possibilita direcionar a aplicação de ruído, preservando características essenciais e aplicando maiores perturbações naquelas de menor impacto analítico.

Com base nesse cenário de necessidade de privacidade em cidades inteligentes, este trabalho apresenta o *Adaptive Differential Privacy via Mutual Information* (APDIM) como uma solução chave para a computação urbana. O APDIM executa uma estratégia adaptativa que aloca ruído conforme a relevância das características e preserva dependências estatísticas por meio de perturbação sensível à correlação, aplicando a abordagem de informação mútua como critério para orientar a alocação de ruído coordenada e, consequentemente, buscando preservar relações estatísticas relevantes entre características.

A proposta é avaliada em diferentes conjuntos de dados (com características distintas), níveis de privacidade e arquiteturas de classificação, considerando aspectos de utilidade analítica, custo computacional e preservação de privacidade em cenários de sistemas inteligentes distribuídos. Os resultados obtidos indicam que o APDIM pode oferecer desempenho superior em comparação a mecanismos tradicionais, especialmente em ambientes distribuídos nos quais a preservação da relevância das características e das

relações estatísticas é fundamental.

O restante deste artigo está organizado da seguinte forma. A Seção 2 apresenta os trabalhos relacionados à privacidade diferencial adaptativa e à preservação de privacidade em ambientes de computação em borda. A Seção 3 descreve a proposta metodológica baseada em informação mútua para a alocação adaptativa do orçamento de privacidade. A Seção 4 detalha o ambiente experimental, os conjuntos de dados e os modelos de aprendizado de máquina utilizados, enquanto que a Seção 5 discute os resultados obtidos. Por fim, a Seção 6 conclui o artigo e apresenta direções para trabalhos futuros.

2. Trabalhos Relacionados

A preservação da privacidade em dados sensíveis tem sido amplamente investigada na literatura, especialmente diante do crescimento de aplicações baseadas em aprendizado de máquina, computação distribuída e ambientes de nuvem e borda. As abordagens existentes podem ser agrupadas, de forma geral, em mecanismos baseados em privacidade diferencial, técnicas criptográficas e métodos de anonimização clássicos.

Yang et al. [Yang et al. 2015] investigam as vulnerabilidades da Privacidade Diferencial (DP) clássica em dados correlacionados, demonstrando que a suposição de independência entre registros é falha em cenários reais. Os autores provam teoricamente que a correlação estatística, combinada com conhecimento auxiliar do adversário, amplifica o vazamento de informações. No entanto, o estudo limita-se à análise teórica bayesiana, não explorando a aplicação prática dessas descobertas em modelos de aprendizado de máquina ou em arquiteturas distribuídas com restrições computacionais.

Diversos trabalhos exploram a preservação de privacidade em aprendizado distribuído e colaborativo. Aminifar et al. [Aminifar et al. 2022] propõem um modelo baseado em *Extremely Randomized Trees* para dados estruturados de saúde em ambientes distribuídos, utilizando técnicas criptográficas e computação segura multiparte para proteger os dados durante o treinamento. Embora a abordagem ofereça proteção robusta, ela depende de operações criptográficas complexas e comunicação intensiva entre as partes, o que pode limitar sua aplicabilidade em cenários de computação em borda com restrições de latência e recursos computacionais. Além disso, o foco da proteção recai principalmente sobre o modelo, e não sobre a adaptação do ruído aos dados de entrada.

Ainda no contexto de aprendizado de máquina com suporte de computação em borda, Mao et al. [Mao et al. 2018] propõem uma arquitetura para treinamento de redes neurais profundas com preservação de privacidade, na qual o modelo é particionado entre o dispositivo do usuário e um servidor de borda. A abordagem aplica mecanismos de privacidade diferencial às ativações intermediárias, evitando o envio de dados brutos ao servidor. Apesar de apresentar bons resultados em termos de proteção da privacidade e viabilidade computacional, a aplicação de ruído ocorre de forma uniforme, sem considerar a relevância das características ou a correlação estatística entre atributos, o que pode impactar a utilidade analítica em cenários mais gerais.

Outras soluções concentram-se no uso de criptografia e anonimização em ambientes de nuvem. Silveira et al . [Silveira et al. 2023] apresentam um sistema para proteção de dados em bancos de dados legados, combinando criptografia simétrica pesquisável e técnicas de anonimização com preservação de propriedades estatísticas. A

proposta demonstra viabilidade prática em ambientes de nuvem e evita modificações em sistemas existentes. No entanto, tais abordagens são voltadas principalmente à proteção de dados em repouso e durante consultas, não considerando explicitamente o impacto das transformações na utilidade dos dados para tarefas analíticas, como aprendizado de máquina.

No campo das técnicas de anonimização, métodos baseados em k-anonymity continuam sendo amplamente utilizados. Coelho et al. [Coelho et al. 2024] propõem o método *Generalization First k-Member Clustering*, que busca reduzir a perda de informação e o custo computacional por meio de generalização antecipada e clusterização eficiente, preservando parcialmente o desempenho de modelos de aprendizado de máquina. Apesar dos avanços, técnicas baseadas em k-anonimato não oferecem garantias formais contra adversários com conhecimento auxiliar e permanecem vulneráveis a ataques de inferência de atributos, o que limita sua adequação em cenários que exigem garantias probabilísticas rigorosas de privacidade.

Em resumo, embora as abordagens existentes avancem na proteção de dados sensíveis sob diferentes perspectivas, elas frequentemente enfrentam limitações relacionadas à preservação da utilidade analítica, ao tratamento explícito de correlações estatísticas ou à viabilidade em ambientes distribuídos e sensíveis a recursos. Nesse contexto, abordagens baseadas em privacidade diferencial adaptativa, sensíveis à relevância e à correlação entre características, surgem como uma alternativa promissora para equilibrar privacidade, utilidade e eficiência computacional em cenários de computação de sistemas inteligentes distribuídos.

3. Proposta

O **APDIM**, ilustrado na Figura 1, aborda os desafios de privacidade na computação de borda ao equilibrar privacidade, utilidade e eficiência computacional por meio de quatro fases coordenadas que reduzem o esforço de processamento local e a comunicação com a nuvem. Na primeira fase, a análise de importância de características emprega informação mútua para identificar os atributos mais relevantes para a tarefa de aprendizado, permitindo concentrar o orçamento de privacidade onde ele é mais necessário. Adotamos neste trabalho a definição de ε-Privacidade Diferencial (ε-DP), na qual ε controla a magnitude do ruído aplicado aos dados. A segunda fase realiza a descoberta de correlação, agrupando características com fortes dependências estatísticas. Em seguida, o valor do ruído é alocado de forma adaptativa, atribuindo maiores níveis de ruído a características de baixa importância para preservar a utilidade das mais relevantes. Por fim, a aplicação de ruído coordenada injeta ruído considerando os grupos formados, preservando correlações internas e reduzindo a necessidade de transmitir dados de alta resolução à nuvem.

O conjunto de dados (*dataset*) original é inicialmente submetido a uma análise de informação mútua para computar a importância das características e identificar estruturas de correlação entre elas. Subsequentemente, a alocação de ruído é realizada de forma adaptativa com base na relevância de cada característica, de modo que aquelas menos importantes absorvem maior nível de ruído para preservar informações cruciais. Por fim, mecanismos de privacidade diferencial sensíveis à correlação são aplicados para manter relações estatísticas, assegurando simultaneamente as garantias formais de ε-privacidade diferencial.

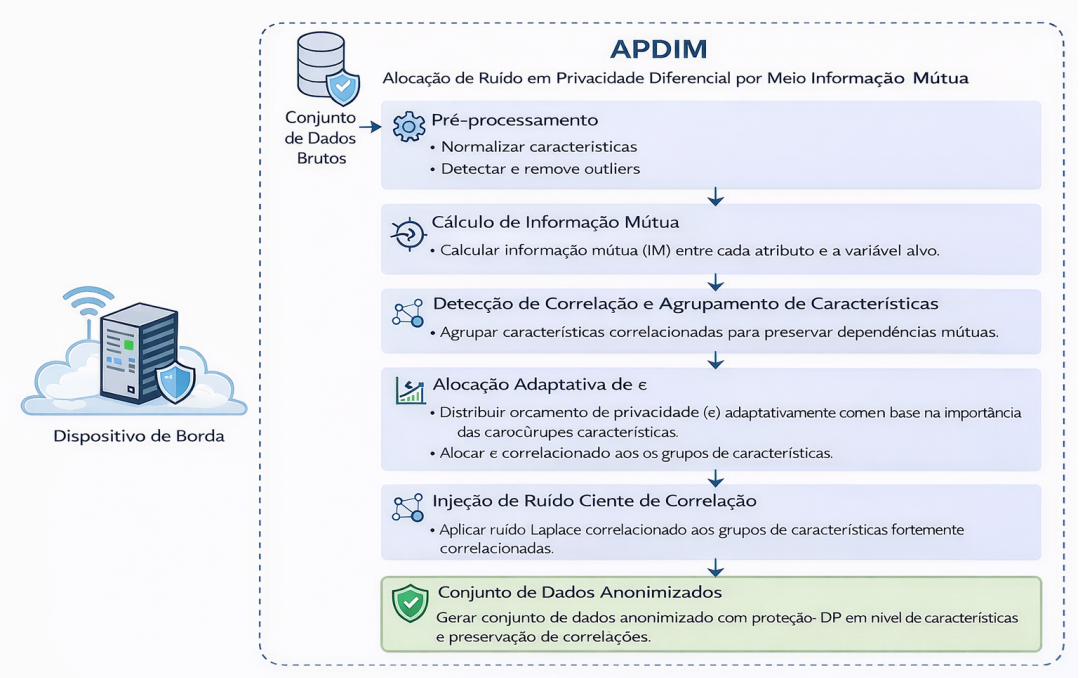

Figura 1. visão geral da proposta.

3.1. Pré-processamento

A etapa de pré-processamento prepara o conjunto de dados para as fases analíticas, assegurando estimativas estatísticas confiáveis. As características são inicialmente normalizadas para eliminar discrepâncias de escala entre atributos heterogêneos, evitando que variáveis com maior magnitude dominem o cálculo da informação mútua e da correlação. Em seguida, procedimentos de detecção e remoção de *outliers*, bem como o tratamento de valores ausentes, são aplicados para mitigar a influência de valores extremos e garantir que os dados estejam em formato adequado para as etapas de análise e alocação adaptativa de ruído.

3.2. Cálculo de Informação Mútua

No APDIM, a relevância de cada característica é quantificada por meio da informação mútua (IM) calculada entre cada atributo X_i e a variável alvo y. Diferentemente de métricas baseadas apenas em correlação linear, a informação mútua é capaz de capturar dependências lineares e não lineares, fornecendo uma medida mais expressiva da contribuição de cada característica para a tarefa de aprendizado.

Formalmente, a informação mútua entre X_i e y é definida como:

$$IM(X_i, y) = \sum_{x_i} \sum_{y} P(x_i, y) \log \left(\frac{P(x_i, y)}{P(x_i)P(y)} \right), \tag{1}$$

onde $P(x_i, y)$ representa a distribuição de probabilidade conjunta entre a característica X_i e a variável alvo y, enquanto $P(x_i)$ e $P(y)$ denotam suas distribuições marginais. Valores elevados de IM indicam que a característica carrega alta quantidade de informação sobre a variável de interesse, sendo, portanto, mais relevante para a predição.

3.3. Detecção de Correlação e Agrupamento de Características

A detecção de correlação tem como objetivo identificar dependências estatísticas entre características, permitindo a aplicação coordenada de ruído em atributos fortemente relacionados. Para isso, é computada uma matriz de correlação baseada no coeficiente de Pearson, definido entre duas características X_i e X_j como:

$$\rho(X_i, X_j) = \frac{\mathrm{cov}(X_i, X_j)}{\sigma_{X_i}\, \sigma_{X_j}}, \tag{2}$$

onde $\mathrm{cov}(\cdot)$ representa a covariância entre as variáveis e σ_{X_i} e σ_{X_j} denotam seus respectivos desvios padrão. Pequenas perturbações numéricas são incorporadas durante o cálculo para evitar instabilidades associadas a características constantes ou quase constantes.

Com base na matriz de correlação, o processo de agrupamento é conduzido de forma iterativa utilizando um limiar θ, que define o nível mínimo de dependência estatística necessário para que duas características sejam consideradas correlacionadas. Formalmente, duas características X_i e X_j são alocadas ao mesmo grupo se:

$$|\rho(X_i, X_j)| \geq \theta. \tag{3}$$

O parâmetro θ controla o equilíbrio entre a preservação de dependências estatísticas e a complexidade do agrupamento, de modo que valores mais altos produzem grupos menores e mais fortemente correlacionados, enquanto valores mais baixos resultam em grupos maiores com dependências mais fracas. O algoritmo assegura que cada característica pertença a exatamente um grupo, evitando sobreposição e garantindo a coordenação da injeção de ruído nas etapas subsequentes.

3.4. Alocação Adaptativa de ε

Nesta fase, a magnitude total de ruído controlada por ε é distribuída de forma adaptativa. Inicialmente define-se uma parcela base:

$$\varepsilon_{\text{base}} = \varepsilon_{\text{total}} \times \text{razão\_mínima} \tag{4}$$

O restante da alocação é calculado por:

$$\varepsilon_{\text{restante}} = \varepsilon_{\text{total}} - (\varepsilon_{\text{base}} \times n_{\text{características}}) \tag{5}$$

A alocação adaptativa por característica é dada por:

$$\varepsilon_{\text{adaptiva}}[i] = \varepsilon_{\text{restante}} \times (1 - \text{Taxa\_de\_Importancia}[i] \times \alpha) \tag{6}$$

e a alocação final:

$$\varepsilon_{\text{final}}[i] = \varepsilon_{\text{base}} + \varepsilon_{\text{adaptiva}}[i] \tag{7}$$

Esse mecanismo de alocação adaptativa permite que características com baixa relevância preditiva absorvam maior intensidade de ruído, enquanto atributos críticos para a tarefa de aprendizado são preservados com níveis reduzidos de perturbação. Como resultado, o APDIM maximiza a utilidade analítica do conjunto de dados anonimizado sem violar as garantias formais de ε-privacidade diferencial, promovendo um equilíbrio controlado entre privacidade e desempenho do modelo, particularmente adequado para ambientes de computação de borda com restrições severas de recursos e latência.

3.5. Injeção de Ruído Ciente de Correlação

Após a definição das intensidades individuais de ruído, o APDIM executa a etapa de injeção de ruído ciente de correlação, cujo objetivo é preservar dependências estatísticas relevantes entre características fortemente correlacionadas. Para isso, características pertencentes a um mesmo grupo de correlação $G = \{i_1, \ldots, i_k\}$ recebem uma alocação coordenada de ruído, calculada como a média das intensidades individuais:

$$\varepsilon_{\text{grupo}} = \frac{1}{|G|} \sum_{j \in G} \varepsilon_{\text{final}}[j]. \tag{8}$$

Essa coordenação evita perturbações desbalanceadas em características fortemente correlacionadas, preservando relações estruturais relevantes para modelos de aprendizado de máquina. A injeção de ruído laplaciano é realizada de forma conjunta sobre cada grupo, utilizando a mesma intensidade $\varepsilon_{\text{grupo}}$, o que mantém as proporções relativas entre atributos correlacionados.

Além disso, o tratamento coordenado reduz redundâncias no processo de perturbação e diminui o risco de sobrecarregar características críticas com ruído excessivo, contribuindo para a estabilidade dos modelos treinados sobre dados anonimizados, especialmente em cenários de computação de borda.

3.6. Geração do Conjunto de Dados Anonimizado

Por fim, o APDIM gera o conjunto de dados anonimizado aplicando ruído Laplace de acordo com as alocações coordenadas de ε. O resultado é um conjunto de dados protegido por ε-privacidade diferencial em nível de característica, mantendo correlações relevantes e reduzindo a perda de utilidade analítica.

4. Experimentos

Esta seção detalha a configuração experimental projetada para avaliar o desempenho da estratégia de anonimização proposta, tanto em ambientes de computação borda-nuvem quanto em contextos de aprendizado de máquina. Os experimentos visam demonstrar o equilíbrio entre a preservação de utilidade de dados, as garantias de privacidade, e a eficiência computacional em diversos conjuntos de dados e modelos de aprendizado de máquina, enquanto também avaliam a adequação do APDIM para implantação na computação de borda. Por fim, é válido ressaltar que com o objetivo de garantir a reprodutibilidade científica, o código-fonte da solução proposta, bem como o conjunto de dados utilizado nos experimentos, estão publicamente disponíveis em um repositório online[1].

[1] `https://github.com/IvoAP/sbrc_2026_adpim`

4.1. Ambiente e Datasets

Para avaliar a adequação do APDIM para cenários de computação de borda, conduzimos experimentos de desempenho em uma máquina equipada com um Intel(R) Core(TM) i9-14900 CPU (2.00 GHz) e 64 GB de RAM, focando em tempo de processamento, tendo em vista que é de suma importância em ambientes com recursos limitados e capacidade de resposta em tempo real [Yao et al. 2023, Chen et al. 2024a]. Assim, comparou-se o desempenho do APDIM com a abordagem Laplace, que é um componente central da privacidade diferencial, o qual adiciona ruído de uma distribuição de Laplace à saída [Fernandes et al. 2021].

Diversos conjuntos de dados públicos amplamente utilizados em pesquisas de preservação de privacidade em Aprendizado de Máquina foram empregados nesta avaliação, incluindo o *Adult*[2], composto por 45.222 instâncias e 14 atributos do censo dos Estados Unidos; o *MGM*[3], contendo 830 instâncias e 5 atributos referentes a dados de mamografia; o *CMC*[4], formado por 1.473 instâncias e 9 atributos oriundos da Pesquisa de Prevalência de Contraceptivos da Indonésia; e o *Heart*[5], que reúne 920 instâncias e 14 atributos combinando dados de quatro localizações distintas.

4.2. Modelos e Parametrização

Avaliamos a abordagem APDIM utilizando múltiplos classificadores, incluindo *K-Nearest Neighbors* (KNN), *Gaussian Naive Bayes* (GNB), *Random Forest* (RF), *Multilayer Perceptron* (MLP), e *AdaBoost* (ADB), sob diferentes níveis de privacidade ($\epsilon \in 0.01, 0.05, 0.1, 0.5, 1.0, 5.0$) utilizando o mecanismo de Laplace. Para efeitos de comparação, o baseline Laplace DP uniforme é reportado como o intervalo $[F1_{\min}, F1_{\max}]$ obtido entre todos os classificadores avaliados para cada valor de ε. Ajuste de hiperparâmetros foi feito utilizando a otimização Bayesiana (20 testes), a seleção de características Chi-quadrado foi aplicada para redução de dimensionalidade, e os parâmetros foram $\alpha = 0.8$ e $\theta = 0.7$. O valor limite $\theta = 0.7$ foi selecionado seguindo diretrizes estabelecidas na literatura, que sugerem que valores acima de 0.7 refletem forte correlação e ajudam a balancear relevância de agrupamento sem agrupar excessivamente as características não relacionadas [Hall 1999]. Ademais, a alocação de 5% do orçamento de privacidade total para a fase de análise de correlação se alinha com trabalhos passados sobre estratégias de particionamento de orçamento em sistemas diferencialmente privados [Dwork et al. 2014], garantindo acurácia suficiente enquanto mantém garantias de privacidade.

Para a avaliação de preservação de privacidade, um ataque de inferência foi conduzido para examinar o quão efetivamente atributos sensíveis podem ser reconstruídos depois da anonimização com APDIM e aplicação de ruído Laplace padrão. Neste cenário, foram gerados datasets anonimizados sob diferentes orçamentos de privacidade (ε), e um classificador treinado por atacante para prever os atributos sensíveis escondidos. A

[2]*Adult Dataset*. Disponível em: `https://archive.ics.uci.edu/dataset/2/adult`

[3]*Mammographic Mass Dataset*. Disponível em: `https://archive.ics.uci.edu/dataset/161/mammographic+mass`

[4]*Contraceptive Method Choice Dataset*. Disponível em: `https://archive.ics.uci.edu/dataset/30/contraceptive+method+choice`

[5]*Heart Disease Dataset*. Disponível em: `https://www.kaggle.com/datasets/johnsmith88/heart-disease-dataset`

métrica utilizada foi acurácia, que diretamente reflete o sucesso do atacante: valores altos indicam proteção fraca, enquanto valores menores indicam garantias de privacidade mais fortes.

5. Resultados

Nesta seção, apresentamos a análise dos resultados obtidos a partir da configuração experimental descrita anteriormente.

5.1. Desempenho para Computação de Borda

A Figura 2 apresenta os resultados dos experimentos que comparam o tempo de processamento por lote no dataset *Adult* (tamanhos de lotes variando de 10k a 40k) e orçamentos de privacidade ($\varepsilon \in \{0.01, 0.1, 1.0\}$).

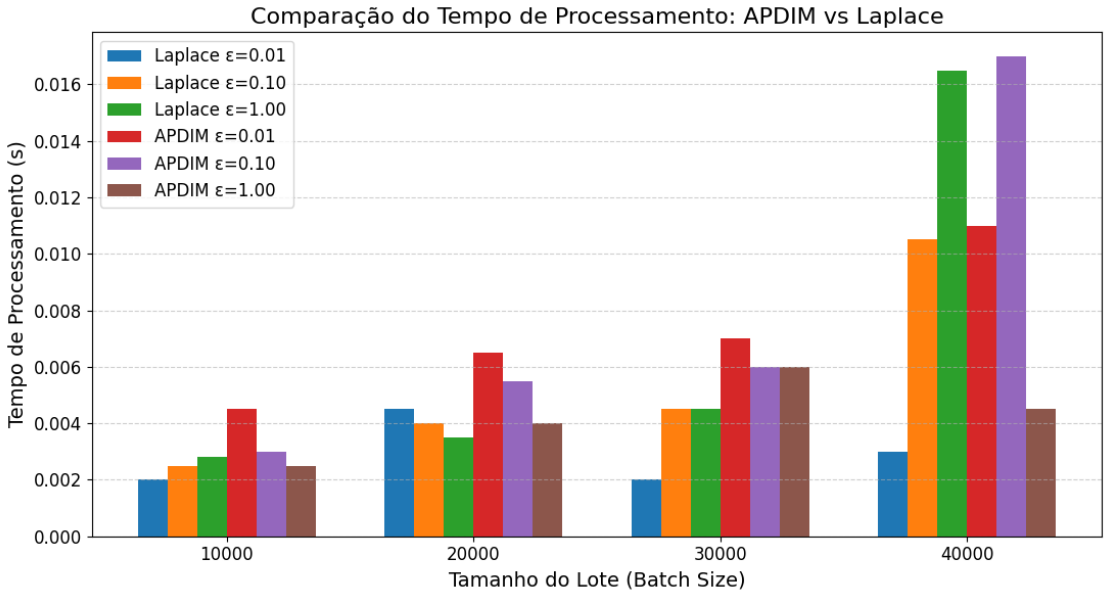

Figura 2. Avaliação de Tempo de Processamento.

De acordo com os resultados, o tempo de processamento aumenta com o tamanho do lote para ambos os mecanismos. O Laplace exibe um crescimento mais suave e quase monotônico para todo ε, refletindo sua perturbação. O APDIM é mais sensível ao ε: para orçamentos baixos e moderados ($\varepsilon = 0.01$ e 0.1), as curvas sobem bem mais acentuadamente em lotes maiores (refletindo o custo da estimativa da informação mútua, triagem de correlação e alocação adaptativa), enquanto em um orçamento mais alto ($\varepsilon = 1.0$) a curva se achata e se torna mais comparável, e às vezes ligeiramente menor que o Laplace para lotes médios a grandes.

Ademais, os resultados indicam que o método do APDIM mantém um comportamento previsível e estável ao longo das execuções, uma característica crucial para sistemas com recursos limitados onde a variabilidade no tempo de processamento pode afetar o escalonamento e o gerenciamento de energia. A consistência do perfil de execução do APDIM respalda seu uso em cargas de trabalho de borda sensíveis a latência, onde o desempenho determinístico é frequentemente necessário.

5.2. Desempenho dos Modelos de Aprendizado de Máquina

Para avaliar o impacto do parâmetro de limite de correlação (θ) no desempenho do APDIM, conduzimos experimentos utilizando o conjunto de dados *Adult*. Os resultados apresentados na Figura 3 mostram que $\theta = 0.7$ consistentemente alcançou a melhor troca entre privacidade e utilidade, com o *F1-score* de até 0,85, particularmente quando combinado com valores α na faixa de 0,5 a 0,8. Valores menores de θ (por exemplo, 0,5) resultaram em um agrupamento muito amplo de características, reduzindo a habilidade de preservar correlações críticas, enquanto valores maiores (por exemplo, 0,9) resultaram em um agrupamento esparso e alocação de orçamento ineficiente. Estas descobertas demonstram que $\theta = 0.7$ oferece o equilíbrio ótimo ao capturar correlações significativas sem comprometer a robustez do modelo, servindo assim como um valor padrão justificado para as configurações do APDIM.

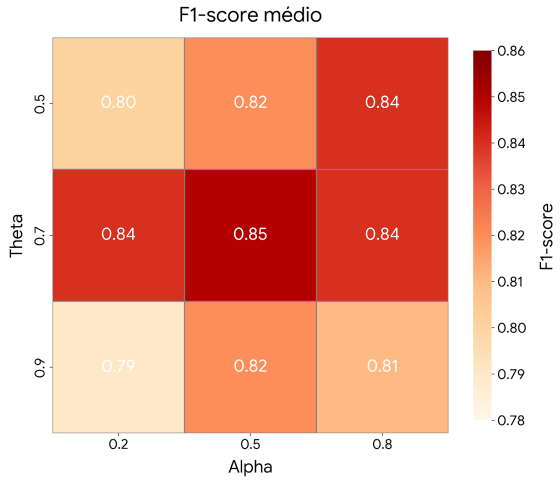

Figura 3. F1-Score para Parâmetros.

Após definir os parâmetros mais adequados, examinamos a métrica *F1-score* em múltiplas arquiteturas de classificadores e níveis de privacidade para demonstrar a eficácia do APDIM em manter a utilidade analítica enquanto assegura as garantias de privacidade.

A avaliação do *F1-score* demonstra que o que a nossa abordagem consistentemente supera privacidade diferencial uniforme tradicional em todos os datasets e níveis de privacidade. Em configurações de privacidade rígidas ($\varepsilon = 0.01$), ele atinge ganhos de 4 a 8 pontos percentuais em ambas as métricas, mantendo o equilíbrio na troca entre precisão e recall. Melhorias notáveis são vistas no *dataset CMC*, onde seu *F1-score* chega a aumentar de 0,33 para 0,96 à medida que a privacidade relaxa. Modelos baseados em árvores como *Random Forest* e *AdaBoost* se sobressaem sob o APDIM, alcançando um *F1-score* de 85% quando $\varepsilon = 5.0$, enquanto até modelos sensíveis a ruído, como o *Gaussian Naive Bayes*, demonstram melhorias na estabilidade. Estes resultados confirmam a habilidade do APDIM de preservar relações estatísticas e entregar classificações robustas e balanceadas sob restrições de privacidade.

A avaliação comparativa demonstra a generalização robusta da nossa abordagem diante diversos conjuntos de dados, com melhorias de desempenho consistentes em relação às abordagens tradicionais. Em conjuntos de dados maiores, como o *Adult* (45,222

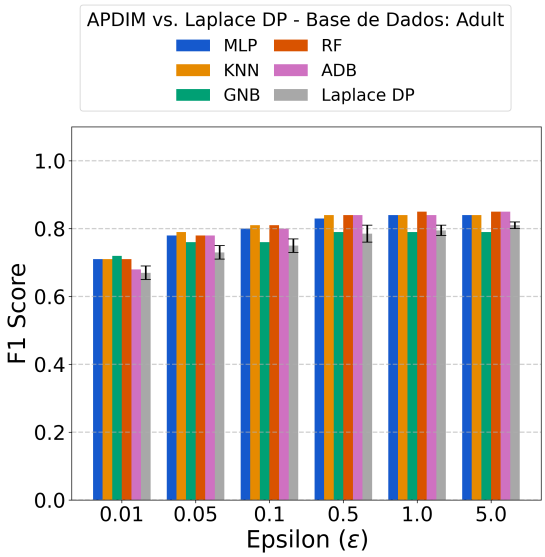

Figura 4. Performance de Classificação (Adult)

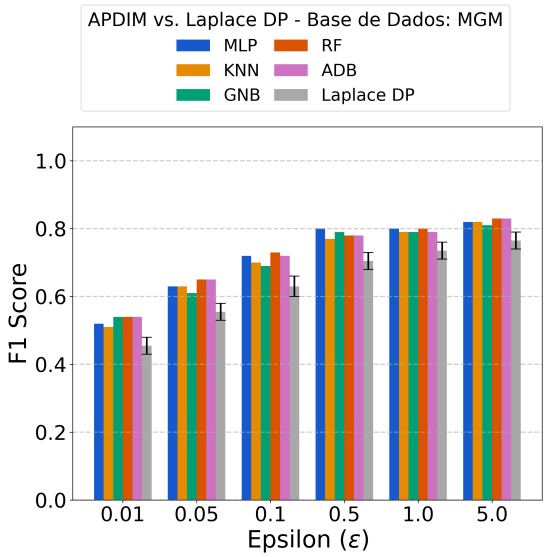

Figura 5. Performance de Classificação (MGM)

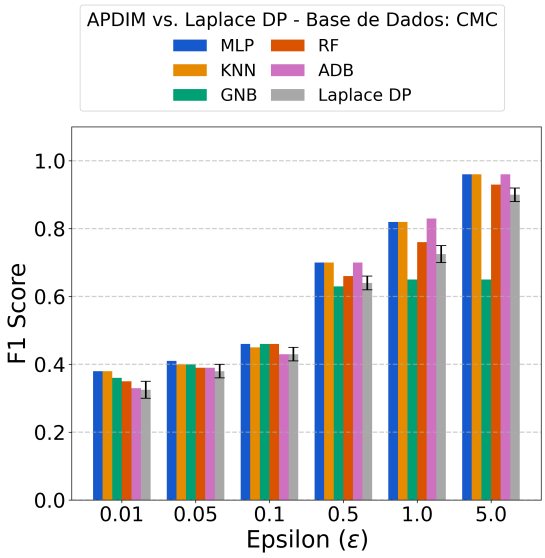

Figura 6. Performance de Classificação (CMC)

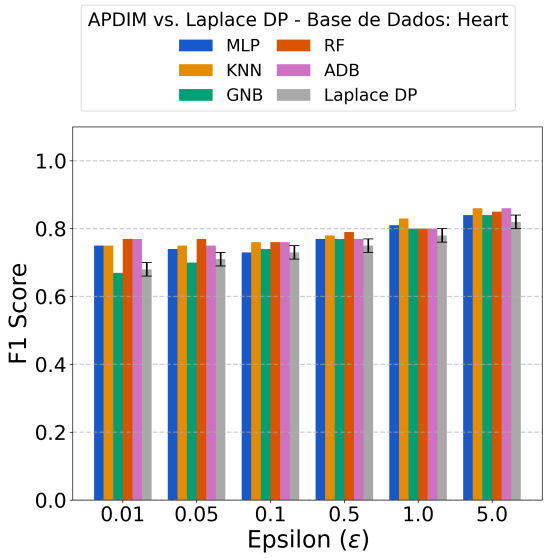

Figura 7. Performance de Classificação (Heart)

amostras), o APDIM alcançou uma progressão em seu *F1-score* de 75-76% para 84-86% ao longo dos níveis de privacidade, enquanto conjuntos de dados menores, como o *MGM* (830 amostras), apresentam melhoras ainda maiores, com uma melhora de 5-11 pontos percentuais em relação ao Laplace DP. Notavelmente, o APDIM atinge níveis de desempenho competitivos com baselines não privadas (86% no *Adult*, 83% no *MGM*) enquanto mantém garantias de privacidade. Dentro do panorama de privacidade diferencial adaptativa, o APDIM oferece uma contribuição complementar a abordagens especializadas como AWDP-FL [Chen et al. 2024b], EnADPP [Zhang et al. 2023], e EDP-PUDL [Chen et al. 2024a]. Ademais, comparado a abordagens recentes de semântica e inteligência de borda [Yang et al. 2022], o APDIM permanece agnóstico ao modelo, operando direta-

mente sobre as distribuições em nível de característica guiado pela informação mútua, e alcança escalabilidade sem exigir treinamento de modelo específico para a tarefa ou perfis de recursos estáticos.

5.3. Avaliação de Preservação de Privacidade

Os resultados dos experimentos de preservação de privacidade são apresentados na Figura 8 e destacam comportamentos distintos entre as duas abordagens. Para orçamentos de privacidade fixos, o Laplace uniforme alcança menor acurácia de ataque (ou seja, privacidade mais forte) em três conjuntos de dados (*Heart* para $\varepsilon \geq 0.1$, *MGM* e *Adult*), enquanto APDIM reduz o sucesso do ataque primariamente no CMC (para todo ε) e marginalmente no *Heart* em $\varepsilon = 0.01$. Este padrão sugere que, na configuração atual, o APDIM preserva mais a estrutura preditiva, enquanto Laplace a perturba de forma mais agressiva.

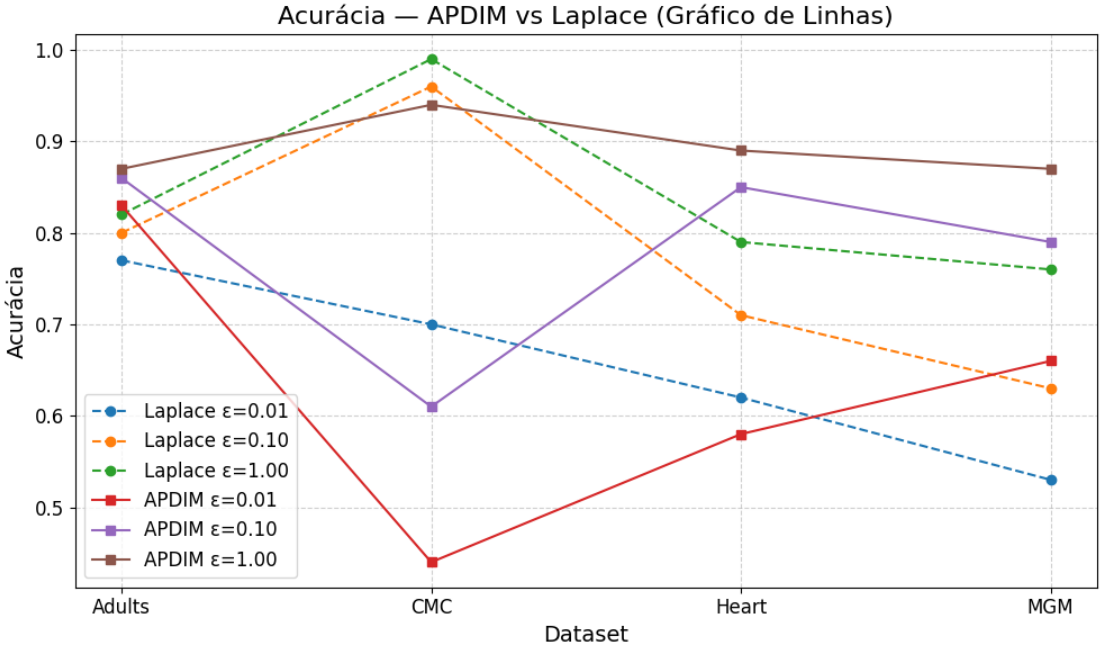

Figura 8. Avaliação de Preservação de Privacidade

O conjunto de dados CMC é uma exceção, pois sua estrutura de correlação se alinha melhor com a perturbação indiscriminada, portanto, o Laplace não protege a privacidade tão efetivamente quanto APDIM. Isso ressalta que a proteção relativa de cada mecanismo pode depender da geometria do conjunto de dados e das correlações entre características, não só do ε.

5.4. Discussão Final

Os resultados experimentais demonstram de forma consistente que o APDIM supera a aplicação uniforme do mecanismo de Laplace ao longo de diferentes conjuntos de dados, arquiteturas de classificação e níveis de privacidade. Em especial, a alocação adaptativa de ruído orientada por informação mútua preserva melhor a utilidade analítica, refletida em ganhos de até 4–11 pontos percentuais no F1-score, principalmente em cenários de privacidade rígida ($\varepsilon \leq 0.1$). A coordenação da injeção de ruído em grupos de características correlacionadas mostrou-se fundamental para manter a estabilidade dos modelos, beneficiando inclusive classificadores mais sensíveis ao ruído, como o *Gaussian Naive Bayes*.

Embora o APDIM apresente maior custo para baixos valores de ε e grandes tamanhos de lote, seu comportamento torna-se comparável, e por vezes superior ao Laplace em orçamentos moderados, mantendo um perfil de execução previsível, aspecto essencial para ambientes de borda com severas restrições de recursos.

Do ponto de vista da preservação de privacidade, a avaliação por meio de ataques de inferência indica que a eficácia relativa entre APDIM e Laplace depende da geometria e da estrutura de correlação dos dados. Enquanto o Laplace uniforme mostrou-se mais agressivo na redução da acurácia do atacante em alguns conjuntos, o APDIM foi particularmente eficaz no *dataset* CMC, sugerindo que mecanismos sensíveis à correlação oferecem vantagens em cenários com estrutura estatística complexa. Em conjunto, esses resultados reforçam a contribuição central deste trabalho:a proposição de um mecanismo adaptativo de privacidade diferencial, independente do modelo e guiado por propriedades estatísticas dos dados, que busca equilibrar privacidade, utilidade e custo computacional, posicionando o APDIM como uma solução prática e escalável para a proteção de dados em sistemas inteligentes distribuídos.

6. Conclusão

Em conclusão, este trabalho apresentou o APDIM como uma abordagem de preservação de privacidade projetada para lidar com os desafios específicos da computação em borda integrada à nuvem. Ao utilizar a informação mútua para orientar a alocação do orçamento de privacidade e incorporar a aplicação de ruído sensível às correlações estatísticas, o APDIM busca equilibrar a utilidade dos dados e a privacidade. Os resultados indicam que essa estratégia pode oferecer desempenho superior em comparação a mecanismos tradicionais, especialmente em ambientes distribuídos nos quais a preservação da relevância das características e das relações estatísticas é fundamental. Como trabalhos futuros, pretende-se estender essa abordagem para o cenário federado para explorar o desempenho da técnica a nível de modelo.

Agradecimentos

Pesquisa parcialmente financiada pelo CNPq (Processos N^o 305946/2025-0 e N^o 405940/2022-0) e Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 88887.954253/2024-00.

Referências

Aminifar, A., Shaban-Nejad, A., Lavigne, M., and Moghaddam, S. (2022). Extremely randomized trees with privacy preservation for distributed structured health data. *IEEE Journal of Biomedical and Health Informatics*, 26(7):3311–3322.

Chen, Q., Ni, Z., Zhu, X., Lyu, M., Liu, W., and Xia, P. (2024a). Dynamic edge-based high-dimensional data aggregation with differential privacy. *Electronics*, 13(16):3346.

Chen, Z., Zheng, H., and Liu, G. (2024b). Awdp-fl: An adaptive differential privacy federated learning framework. *Electronics*, 13(19):3959.

Coelho, R., Almeida, B., and Costa, D. (2024). A new k-anonymity method based on generalization first k-member clustering for healthcare data. *Journal of Biomedical Informatics*, 149:104579.

Dwork, C., Roth, A., et al. (2014). The algorithmic foundations of differential privacy. *Foundations and trends® in theoretical computer science*, 9(3–4):211–407.

Fernandes, N., McIver, A., and Morgan, C. (2021). The laplace mechanism has optimal utility for differential privacy over continuous queries. In *2021 36th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–12.

Hall, M. A. (1999). *Correlation-based feature selection for machine learning*. PhD thesis, The University of Waikato.

Mao, Y., Chen, X., Zhang, Y., Li, J., and Liu, Y. (2018). A privacy-preserving deep learning approach for face recognition with edge computing. In *Proceedings of the 2018 USENIX Workshop on Hot Topics in Edge Computing (HotEdge)*. USENIX Association.

Pimenta, I., Silva, D., Moura, E., Silveira, M., and Gomes, R. L. (2024). Impact of data anonymization in machine learning models. In *Proceedings of the 13th Latin-American Symposium on Dependable and Secure Computing*, pages 188–191.

Pimenta, I. A., Araújo, R. S., Rodrigues, R. L., Silveira, M. M., and Gomes, R. L. (2025). Anonimização de dados para inteligência artificial usando o algoritmo da tropa dos gorilas. In *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, pages 448–461. SBC.

Silveira, M. M., Portela, A. L., Menezes, R. A., Souza, M. S., Silva, D. S., Mesquita, M. C., and Gomes, R. L. (2023). Data protection based on searchable encryption and anonymization techniques. In *NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium*, pages 1–5. IEEE.

Souza, M. S., Ribeiro, S. E. S. B., Lima, V. C., Cardoso, F. J., and Gomes, R. L. (2024). Combining regular expressions and machine learning for sql injection detection in urban computing. *Journal of Internet Services and Applications*, 15(1):103–111.

Wang, Y., Yang, C., Lan, S., Zhu, L., and Zhang, Y. (2024). End-edge-cloud collaborative computing for deep learning: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 26(4):2647–2683.

Yang, B., Sato, I., and Nakagawa, H. (2015). Bayesian differential privacy on correlated data. In *Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data*, SIGMOD '15, pages 747–762, Melbourne, Australia. ACM.

Yang, W., Liew, Z. Q., Lim, W. Y. B., Xiong, Z., Niyato, D., Chi, X., Cao, X., and Letaief, K. B. (2022). Semantic communication meets edge intelligence. *IEEE wireless communications*, 29(5):28–35.

Yao, A., Li, G., Li, X., Jiang, F., Xu, J., and Liu, X. (2023). Differential privacy in edge computing-based smart city applications: Security issues, solutions and future directions. *Array*, 19:100293.

Zhang, X., Yang, F., Guo, Y., Yu, H., Wang, Z., and Zhang, Q. (2023). Adaptive differential privacy mechanism based on entropy theory for preserving deep neural networks. *Mathematics*, 11(2):330.