Aplicação de *local differential privacy* para preservar a privacidade em dados de rotas

Renan Ricoldi Fróis Pedro[1], **Bruno Bogaz Zarpelão**[1]

[1]Departamento de Computação – Universidade Estadual de Londrina (UEL)
Caixa Postal 10.011 – CEP 86057-970 – Londrina – PR – Brasil

renan.ricoldi@uel.br, brunozarpelao@uel.br

Abstract. *The progress of internet has shown the failure of many companies on securing data. Sensitive information, such as routes, frequently get accessible, allowing devastating actions to their owners. Thus, a way of granting user privacy is necessary. With local differential privacy, data security is possible as well as using the information. On this work, we shall compare the analysis on two different uses of the quoted technique, upon route data, together with the pure one.*

Resumo. *O avanço no número de usuários na internet nos mostrou que muitas empresas não conseguem assegurar seus dados. Informações sensíveis, como rotas, frequentemente ficam acessíveis permitindo ações devastadoras aos seus donos. Frente a essa ameaça, faz se necessário encontrar maneiras de garantir a privacidade dos usuários. Através de local differential privacy faz-se possível a segurança dos dados, bem como a utilidade das informações. Neste trabalho, será comparado o resultado de análises, feitas em duas aplicações distintas da técnica em cima de dados de rotas, e também nos dados puros.*

1. Introdução

Com o avanço da internet nos últimos anos, atualmente quase tudo o que fazemos gera dados compartilhados através da rede. Em algumas situações empresas não definem um bom uso para esses dados, e da mesma forma não providenciam a devida atenção para como os armazenam, gerando grandes vazamentos de dados pessoais privados que podem identificar as pessoas as quais eles pertencem, como o caso do vazamento de dados de 57 milhões de usuários da Uber[1].

Dados de rotas e localização se tornam um risco enorme, permitindo ações como o controle de tráfego de uma região, bem como a identificação da residência e o local onde uma pessoa se encontra[1][7].

Observando como os dados que deveriam ser privados podem estar no acesso de pessoas sem permissão, entende-se a necessidade de técnicas que garantam a privacidade das informações colhidas e enviadas pela rede. Uma maneira de garantir, e ainda quantificar, a privacidade em uma base de dados, se encontra na *differential privacy* a qual permite através de um fator de privacidade, aumentar ou diminuir o ruído aplicado em um dado. Quanto mais ruído é aplicado, mais privado e menos preciso um dado é.

[1]uber.com/en-CA/newsroom/2016-data-incident/

No entanto, mesmo que aplicado uma grande quantia de ruído nos dados de um banco, ainda precisamos extrair informações deles, para isso faz-se necessário manter um certo nível de fidelidade, ou então aumentar o número de dados da base, visto que se trata de uma técnica gulosa, que se torna muito confiável como uma larga quantia de informações.

Considerando tudo isso ainda temos o fato de enviar nossas informações via internet até o servidor que vai armazenar, e talvez, aplicar privacidade diferencial para obter as informações necessárias. Durante todo o processo existem muitas brechas que permitem o acesso ao conteúdo antes mesmo da execução da técnica, com intenção de evitar essas formas de vazamento a *local differential privacy* deve ser utilizada, posto que aplica a técnica antes apresentado direto no dispositivo onde o dado é gerado[5][7].

Por sumo, percebe-se a possibilidade de atingir a privacidade dos usuários em relação aos seus dados de rota, onde foram coletados, e ainda assim conseguir obter informações úteis com o estudo deles. Neste trabalho será discutido dois métodos de *local differential privacy* em um conjunto de dados de rotas, que ao serem implementados e aplicados seja possível verificar a partir de análises estatísticas um resultado satisfatório em dois pontos, privacidade e utilidade, comparando ainda com os dados sem ruídos, onde as informações estão todas acessíveis, bem como as análises são precisas.

Este documento esta organizado na seguinte estrutura: A Seção 2 apresenta a fundamentação teórica necessária para a compreensão do trabalho; a Seção 3 apresenta o objetivo proposto; a Seção 4 contém informações sobre a metodologia e técnicas; a Seção 5 apresenta o cronograma para o desenvolvimento e a 6 os resultados esperados.

2. Fundamentação Teórico-Metodológica e Estado da Arte

2.1. Privacidade Diferencial (*Differential Privacy*)

A privacidade diferencial, proposta por Dwork et al.[3], define como impedir que as informações de um indivíduo sejam identificadas em uma análise de uma população, garantindo que independente do indivíduo compor ou não a base de dados, o resultado não deve ser alterado. Desta forma, se possuirmos dois bancos de dados, onde a diferença entre eles existe em apenas um registro, então tudo que aprendemos do primeiro banco também será aprendido com o segundo.

Isso se faz necessário, pois com outras formas de se atingir a privacidade como tornar os dados anônimos, ou então retirar os campos identificadores como nome, não garantem a privacidade, visto que junto de dados auxiliares ou mesmo com os dados diretos do banco é possível fazer uma combinação para identificar o usuário[4].

É importante ressaltar que os dados não podem ser totalmente anônimo e continuar útil, bem como, de forma geral, quanto mais informação mais útil será para a análise dos dados[5].

Na definição de privacidade diferencial, também possuímos a noção de $\epsilon - DP$, o qual é usado para controlar o nível de privacidade, assim seu aumento causa aleatoriedade nos dados, bem como seu decréscimo implica em dados mais precisos e menos privados. Para obtermos $\epsilon - DP$ utilizamos a equação (3). Onde uma função randomizada M dá $\epsilon - DP$, se todos os *datasets* xey, assim como dito anteriormente, diferem em apenas um registro, e onde S são todos os eventos possíveis.

$$Pr[M(x) \in S] \leq (1 + \epsilon) \times Pr[M(y) \in S] \quad (1)$$

A privacidade diferencial provê a privacidade através de processos, como a aleatoriedade. Um exemplo consiste na aleatoriedade de respostas, onde a resposta nem sempre depende da vontade de quem responde e sequer da verdade. Para atingir isso, ao fazer uma pergunta, cuja resposta é "sim"ou "não", a alguém esta pessoa fará como a seguir:

1. jogue uma moeda.
2. Caso caia coroa, responda a pergunta com a verdade.
3. Caso caia cara, jogue novamente a moeda e responda "Sim"caso caia cara e "Não"caso caia coroa.

Desta forma, ao aplicar este ruído nas respostas, não como afirmar com certeza que a resposta dada é verdadeira, ainda mais sabendo que pelo menos 1/4 das vezes a resposta será "Sim". Se p é a razão de respostas verdadeiras, temos que o número esperado de respostas "Sim"é dado por (2).

$$P(Yes) = (1/4)(1 - p) + (3/4)p = (1/4) + p/2. \quad (2)$$

2.2. *Local Differential Privacy*

O exemplo acima nos mostra uma categoria de informação onde aplicamos ruído logo na resposta, de uma forma que quando quem perguntou recebe a resposta, já não sabe se a resposta é verdadeira ou falsa.

Esta técnica é chamada *Local Differential Privacy*, onde não precisamos enviar a resposta ao banco de dados, onde será aplicado privacidade diferencial para assegurar as informações, garantindo privacidade já ao apresentar seus dados. Esse é considerado um modelo superior à sua base, dado que apenas o dono tem acesso aos dados originais, permitindo uma proteção muito mais forte[5][7].

Assim como a privacidade diferencial, possuímos um $\epsilon - LDP$, onde um algoritmo M randomizado o satisfaz, se e somente se, para todo x e y, e onde S são todos os eventos possíveis[7], temos:

$$Pr[M(x) \in S] \leq e^{\epsilon} \times Pr[M(y) \in S] \quad (3)$$

A maioria dos mecanismos de *Local Differential Privacy* se baseiam na ideia de respostas randomizadas, como apresentado acima, e normalmente podemos adicionar ruídos através da aplicação de Laplace ou Gaussiano. No entanto, na maioria dos algoritmos, primeiro os dados são codificados, para depois serem perturbados, no fim são agregados para que as análises possam ser feitas. Atingindo assim $\epsilon - LDP$[7].

Dentre as atuais aplicações de LDP podemos citar O *RAPPOR* da *Google*, que utiliza respostas randomizadas, e consegue identificar URLs populares sem revelar hábitos dos usuários, direto no lado do cliente[2][6].

2.3. *Differential Privacy* em dados de rota

Existem muitas maneiras de armazenar rotas em um banco de dados, podendo armazenar apenas latitude e longitude de origem e destino, bem como a localização em certo horário

de um usuário, capturado novamente a cada quantia tempo ou sempre que a localização mudar.

Em [1] verificamos o uso de privacidade diferencial para publicar trajetórias de qualquer tamanho em tempo real, tendo os dados no modelo de privacidade. Para isso primeiro define $l - trajectoryprivacy$ onde se encontram os dados espaçotemporais de todos os usuários u, sendo garantido que todos $l_u - trajectory$ de um específico u está protegido sob $\epsilon - DP$. Neste trabalho, também é feito uma comparação entre diversos algoritmos, e se conclui que o melhor se dá através de um algoritmo guloso a privacidade dentro de $\epsilon - DP$ dos dados de qualquer $l_u - trajectory$, junto de um algoritmo de aproximação privada, que dirá se é benéfico fazer a publicação aproximada ou não, tendo como objetivo o erro médio absoluto.

3. Objetivos

O principal objetivo desse trabalho é aplicar *local differential privacy* para preservar a privacidade em dados de rotas. Entre os objetivos específicos temos:

1. Revisar duas técnicas de *local differential privacy* que possam ser utilizadas para dados de rotas;
2. Aplicar as técnicas escolhidas em um conjunto de dados de rotas;
3. Analisar os resultados obtidos em comparação aos dados sem privacidade, e definir qual técnica garante o maior nível de privacidade escondendo o menor número de informações;

4. Procedimentos metodológicos/Métodos e técnicas

O primeiro passo será realizar um levantamento bibliográfico de trabalhos que expliquem implementações e algoritmos básicos da ideia de *differential privacy* descrita em [3].

Em seguida será feito uma revisão bibliográfica de artigos definam ou apliquem técnicas de *local differential privacy*, dando preferência àqueles com algoritmos já implementados.

Com os algoritmos definidos, serão pesquisados *datasets* com dados de rotas, onde deverão conter ao menos colunas de local de origem, destino e algo que identifique quem fez o trajeto, permitindo obter análises sobre trajetos feitos por pessoas.

Os artigos escolhidos terão seus códigos alterados, para que consigam trabalhar com os dados de rotas.

Uma vez implantados os algoritmos, serão feitos testes com diversos coeficientes de privacidade. Os resultados serão análises estatísticas em cima dos dados, os quais serão comparados a fim de verificar a fidelidade e a privacidade reproduzida por cada algoritmo.

Por fim, será apresentado a técnica que melhor manteve fidelidade nas análises estatísticas perdendo menos informações, bem como a comparação entre as análises sem a aplicação da técnica.

5. Cronograma de Execução

Atividades:

1. Revisão Bibliográfica;

2. Estudo nos algoritmos que utilizam *local differential privacy*;
3. Escolha dos algoritmos;
4. Escolha do *dataset*;
5. Alteração e implementação dos códigos;
6. Testes;
7. Análise dos resultados obtidos;
8. Redação do TCC;

Tabela 1. Cronograma de Execução

	ago	set	out	nov	dez	jan	fev	mar	abr	mai
Atividade 1	X	X								
Atividade 2		X	X							
Atividade 3			X	X						
Atividade 4				X						
Atividade 5					X	X				
Atividade 6							X	X		
Atividade 7									X	
Atividade 8						X	X	X	X	X

6. Contribuições e/ou Resultados esperados

Com esse TCC, espera-se encontrar quais algoritmos conseguem, através da técnica de *local differential privacy*, garantir análises fiéis aos dados originais, sem comprometer a privacidade dos usuários. Desta forma, sendo de grande importância para outros trabalhos que precisam garantir a privacidade em *datasets* com dados de rotas, uma vez que disponibilizado o código implementado.

7. Espaço para assinaturas

Londrina, *13 de setembro de 2021*.

Renan R.T. Pedro

Aluno

Orientador

Referências

[1] Yang Cao and Masatoshi Yoshikawa. Differentially private real-time data release over infinite trajectory streams. In *2015 16th IEEE International Conference on Mobile Data Management*, volume 2, pages 68–73, 2015.

[2] Graham Cormode, Somesh Jha, Tejas Kulkarni, Ninghui Li, Divesh Srivastava, and Tianhao Wang. Privacy at scale: Local differential privacy in practice. In *Proceedings of the 2018 International Conference on Management of Data*, pages 1655–1658, 2018.

[3] Cynthia Dwork. Differential privacy. In *International Colloquium on Automata, Languages, and Programming*, pages 1–12. Springer, 2006.

[4] Cynthia Dwork. Differential privacy: A survey of results. In *International conference on theory and applications of models of computation*, pages 1–19. Springer, 2008.

[5] Cynthia Dwork, Aaron Roth, et al. The algorithmic foundations of differential privacy. *Found. Trends Theor. Comput. Sci.*, 9(3-4):211–407, 2014.

[6] Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. Rappor: Randomized aggregatable privacy-preserving ordinal response. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security*, pages 1054–1067, 2014.

[7] Mengmeng Yang, Lingjuan Lyu, Jun Zhao, Tianqing Zhu, and Kwok-Yan Lam. Local differential privacy and its applications: A comprehensive survey. *arXiv preprint arXiv:2008.03686*, 2020.