باسمه تعالی

دانشگاه صنعتی شریف

دانشکده ریاضی و علوم کامپیوتر

مقدمه‌ای بر محرمانگی تفاضلی و کاربردها

an Introduction to Differential Privacy and Applications

گروه مطالعاتی دکتر جواد ابراهیمی بروجنی

نگارنده: دانیال آیتی

(و جمعی از دانشجویان گروه)

تابستان ۱۴۰۳

پیش‌گفتار

با توجه به مطرح شدن حوزه محرمانگی تفاضلی که حوزه‌ای بسیار جدید است و در عین حال داشتن تئوری ریاضی مشخص و فرمول‌بندی شده، به صورت مستقیم در صنعت کاربردهای فراوان دارد.

همجنین دانشجویان این گروه در تهیه و تنظیم و نوشتن این جزوه تلاش بسیاری کرده‌اند که از آنان تشکر ویژه به عمل می‌آوریم:
علی‌رضا توفیقی محمدی - فیروزه ابریشمی - محمدحسین کلانتری - مهشید دهقانی - سارا کرمانی و مهدی عباس‌زاده

امید است این کتابچه برای علاقه‌مندان و پژوهش‌گران مفید واقع شود.

فهرست مطالب

فصل ۱

مقدّمه

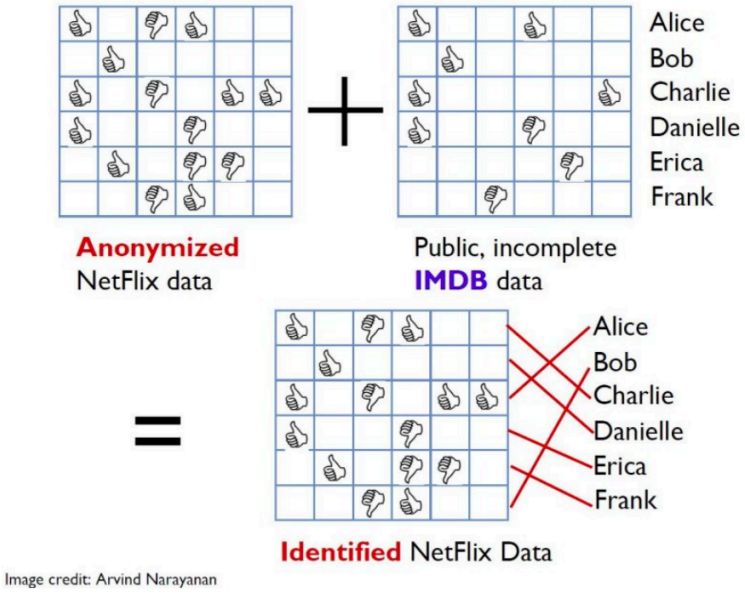
در ابتدا مقدمه‌ای از نیاز به محرمانگی در بسیاری از وقایع روزمره را بررسی می‌کنیم؛ که البته فعلا خالی از مطلب است!

۱.۱ امنیت و حریم خصوصی در زندگی مدرن

در ابتدا عکسی معروف که احتمالا در تمام جزوه‌ها دیدید را این‌جا قرار می‌دهم تا فرمت قرار دادن عکس را هم ببینید:

۱.۱.۱ مثال‌هایی از نیاز به محرمانگی و امنیت

اگر مسئله جایزه نتفلیکس [۱] را به خاطر داشته باشید، که تحول عظیمی در حوزه سیستم‌های پیشنهاددهنده [۲] به وجود آورد، جالب است بدانید که در یک تحقیق معروف که عکس آن در زیر قرار داده شده‌است، به این نتیجه رسیدند که داده‌هایی که برای این مسابقه در اختیار عموم قرار داده شده‌اند (که داده‌های واقعی بودند.)، هنگامی که در کنار داده‌های جمع شده از نظرات سایت معروف IMDb قرار بگیرند، می‌تواند منجر به لو رفتن اطلاعات کاربران شوند. با داشتن نظرات تعداد محدودی کاربر در مورد تعداد مشخصی فیلم، می‌توان جدول یکتایی برای نظر هرکاربر نسبت به هر فیلم ارائه داد، البته توجه کنید این پارگراف را بدون هیچ دلیلی نوشته‌ام و فقط برای آماده کردن تمپلیت بود!



شکل ۱.۱: لطفا برای همه‌ی عکس‌ها کپشن بنویسید!

حال به مقاله‌ی دکتر ابراهیمی در مورد محرمانگی تفاضلی در گراف‌ها [۱] ارجاع می‌زنم تا این راه هم دیده باشید:)

[۱] Netflix prize
[۲] Recommender Systems

کتاب‌نامه

[1] S. Torkamani, J. B. Ebrahimi, P. Sadeghi, R. G. L. D'Oliveira and M. Médard, "Optimal Binary Differential Privacy via Graphs," in IEEE Journal on Selected Areas in Information Theory, vol. 5, pp. 162-174, 2024, doi: 10.1109/JSAIT.2024.3384183.