به نام خدا

پاسخ تمرین ۸

علی عدالت ۸۱۰۱۹۹۳۴۸

۱) اصول GDPR : اصول مربوط به پردازش داده های شخصی، قانونی بودن پردازش، شرایط رضایت، شرایط مربوط به رضایت کودک در رابطه با خدمات جامعه اطلاعاتی، پردازش دسته های خاص از داده های شخصی، پردازش داده های شخصی مربوط به محکومیت ها و جرایم جنایی، پردازشی که نیازی به شناسایی ندارد

GDPR	the 1998 Act	
در مقابل، GDPR یک مقررات الزام آور است که به محض اجرایی شدن در 25 ماه مه، از نظر قانونی قابل اجرا خواهد بود و برای همه کشورهای اتحادیه اروپا و هر شرکتی که اطلاعات شهروندان اتحادیه اروپا را در اختیار دارد، اعمال خواهد شد.	دستورالعمل قبلی حفاظت از داده‌های اروپا از رویکرد ساده‌تری نسبت به GDPR استفاده می‌کرد و اهداف و الزامات استانداردهای حفاظت از داده‌ها را تعیین می‌کرد که سپس از طریق قوانین ملی، مانند قانون حفاظت از داده‌های بریتانیا، اجرا شدند.	گستره جغرافیایی
GDPR تعریف "داده های شخصی" را گسترش می دهد تا طیف وسیع تری از اطلاعات مصرف کننده را در برگیرد.	در حالی که قانون حفاظت از داده‌ها فقط به اطلاعاتی مربوط می‌شود که برای شناسایی یک فرد یا اطلاعات شخصی آنها استفاده می‌شود، GDPR این دامنه را گسترش می‌دهد تا نشانگرهای شناسایی آنلاین، داده‌های مکان،	تعریف داده های شخصی

	اطلاعات ژنتیکی و موارد دیگر را در برگیرد.	
طبق GDPR باید اخطارهای حریم خصوصی واضحی برای مصرف‌کنندگان ارائه شود که به آنها اجازه می‌دهد تصمیم آگاهانه‌ای در مورد رضایت آنها برای ذخیره و استفاده از داده‌هایشان اتخاذ کنند. پس از آن می توان این رضایت را در هر زمانی پس گرفت.	این یکی از تفاوت های تعیین کننده بین GDPR و قانون حفاظت از داده ها است. بر اساس قوانین قدیمی، جمع‌آوری داده‌ها لزوماً نیازی به مشارکت کردن افراد و رضایت آنها ندارد	سیاست های رضایت
این امر با آمدن GDPR تغییر کرد و هر گونه نقض باید ظرف 72 ساعت پس از حادثه به مقامات مربوطه گزارش شود.	در قوانین قبلی، کسب‌وکارها هیچ تعهدی برای گزارش دادن در صورت وقوع نقض داده‌ها ندارند، اگرچه آنها تشویق به انجام این کار می‌شوند.	سیاست های نقض عهد درباره داده ها
GDPR تمرکز بسیار بیشتری بر مسئولیت‌پذیری صریح برای حفاظت از داده‌ها دارد و مسئولیت مستقیمی را برعهده شرکت‌ها قرار می‌دهد تا ثابت کنند که با اصول مقررات مطابقت دارند. این بدان معناست که اگر شرکت‌ها بخواهند از نقض قوانین GDPR جلوگیری کنند، باید به فعالیت‌های اجباری مانند	قانون حفاظت از داده‌ها رویکرد عدم دخالت عمدی در این زمینه استفاده می‌شود.	جوابگویی

آموزش کارکنان، ممیزی داده‌های داخلی و نگهداری اسناد دقیق متعهد شوند.		
GDPR این را تغییر داد، زیرا هر شرکتی که بیش از 250 نفر را استخدام می کند موظف است یک افسر اختصاصی حفاظت از داده ها را منصوب کند، همانطور که هر شرکتی که سالانه بیش از 5000 پروفایل موضوع را پردازش می کند.	قانون حفاظت از داده ها نحوه تخصیص عملکردهای امنیت داده را مشخص نمی کند و تنها به تعهد اولیه مدیریت به مفهوم نیاز دارد.	حاکمیت حفاظت از داده ها
تحت GDPR، این محدودیت ها به طور قابل توجهی به 20 میلیون یورو یا چهار درصد از گردش مالی سالانه افزایش می یابد، هر کدام که بیشتر باشد. همچنین لازم به یادآوری است که GDPR به افراد اجازه می دهد تا برای خسارت مادی و غیر مادی ناشی از نقص امنیت داده ها غرامت مطالبه کنند، در حالی که قوانین فعلی فقط خسارت مادی را پوشش می دهد.	در قدیم، عدم انطباق با قانون حفاظت از داده ها می تواند شرکت ها را تا 500000 پوند یا یک درصد از گردش مالی سالانه جریمه کند.	جریمه و غرامت

۲) انجام و تکمیل مراحل ثبت نام در نماوا پس از مطالعه قوانین و مقررات به منزله پذیرش و موافقت کاربر با این قوانین و امضا توافقنامه‌ای بین سایت نماوا و کاربر است و رعایت یکایک مفاد آن الزامی است. لازم به ذکر است در صورت نقض هر یک از مفاد این توافقنامه توسط کاربر، نماوا مجاز است دسترسی کاربر را مسدود نماید. لازم به توضیح و یادآوری است که نماوا حق دارد بنا به ضرورت و یا صلاحدید، تغییراتی در مفاد توافقنامه خود با کاربران ایجاد کند. این تغییرات می‌تواند در هر زمان و بدون اطلاع‌رسانی به کاربران صورت گیرد. بنابراین کاربران می‌بایست

هر چند وقت یکبار مروری بر شرایط و قوانین نماوا در این توافقنامه داشته باشند تا از تغییرات احتمالی آن آگاه شوند. قوانین مربوط به اطلاع رسانی به کاربر برای استفاده و جمع آوری کردن و نکردن داده‌ها مطابق GDPR رعایت نمی‌شود. تنها یک توافق اولیه بر روی قوانین انجام می‌شود و بعد از آن نماوا هر کاری بخواهد با داده‌های کاربر انجام می‌دهد و فقط قول می‌دهد که اطلاعات را فاش نکند. یعنی قوانین GDPR اکثرا رعایت نمی‌شود. تمام اطلاعات افراد بدون توافق می‌تواند مورد پردازش قرار گیرد و محدودیت خاصی توسط کاربر قابل اجرا نیست. برای تغییر اطلاعات کاربر تنها می‌تواند اطلاعات پروفایل خود را تغییر دهد. اطلاع رسانی تغییرات قوانین نیز صورت نمی‌گیرد (خسته نباشید!) چنانچه در قوانین مندرج، تغییراتی ایجاد شود، در صفحه قوانین سایت نماوا منتشر و به‌روزرسانی می‌گردد. از آنجایی که این تغییرات می‌تواند تغییرات جزیی در برخی از قوانین تا تغییر کل محتوای توافقنامه را در برگیرد، به کاربران گرامی توصیه می‌شود در فواصل زمانی مناسب، بخش قوانین سایت نماوا را مرور نمایند تا در جریان تغییرات احتمالی قرار گیرند. بدیهی است کاربران ملزم به رعایت قوانین این توافقنامه و تمامی تغییرات در مفاد آن بوده و در صورت نقض قوانین هیچگونه عذری از طرف کاربر، منجمله عدم اطلاع از قوانین و یا تغییرات انجام شده، پذیرفته نخواهد بود.

در ابتدا قوانینی برای دانلود فیلم از نما و تبلیغات نما و تغییراتی که نماوا در محتواهای سایت می‌تواند بدهد، وجود دارد. قوانین مربوط به استفاده از سایت است. اولین قانونی که در باره داده‌های کاربران حرف می‌زند در زیر آمده است.

نماوا متعهد می‌شود اطلاعات شخصی کاربران را فقط نزد خود نگه دارد و از افشای آن به هر شخص یا گروه سوم شخص اجتناب ورزد. تنها در مواردی که به موجب قوانین جمهوری اسلامی ایران و بنا به درخواست رسمی ارگان‌ها و سازمان‌های دولتی ذیصلاح نیاز به ارائه اطلاعات شخصی کاربران باشد، نماوا موظف به همکاری طبق قانون خواهد بود و هیچ مسئولیتی متوجه نماوا نخواهد بود.

هنگام ثبت نام و عضویت در سایت نماوا، متقاضی موظف به ارائه مشخصات فردی خود شامل: نام، نام خانوادگی، آدرس ایمیل و شماره تلفن همراه است. پس از انجام مراحل ثبت نام و تایید نهایی عضویت، پروفایلی برای کاربر تشکیل خواهد شد که کلیه فعالیت‌های کاربر در سایت نماوا اعم از خریداری فیلم، فیلم‌های مشاهد شده به صورت آنلاین و غیره در آن ثبت می‌شود. کاربر می‌تواند در هر زمان به پروفایل شخصی خود در سایت مراجعه کرده و اطلاعات خود را به جز ایمیل و شماره تلفن همراه ثبت شده در حساب کاربری ویرایش کند.

در ادامه قوانین مربوط به دسترسی از نظر جغرافیایی و امنیت داده‌ها آمده است. به جز این قوانین، مواردی مربوط به مناسب بودن فیلم ها و خرید در سایت و مجوزهای سایت و شرایط غیر پیش بینی و بلایا وجود دارد که چندان مورد توجه ما نیست.

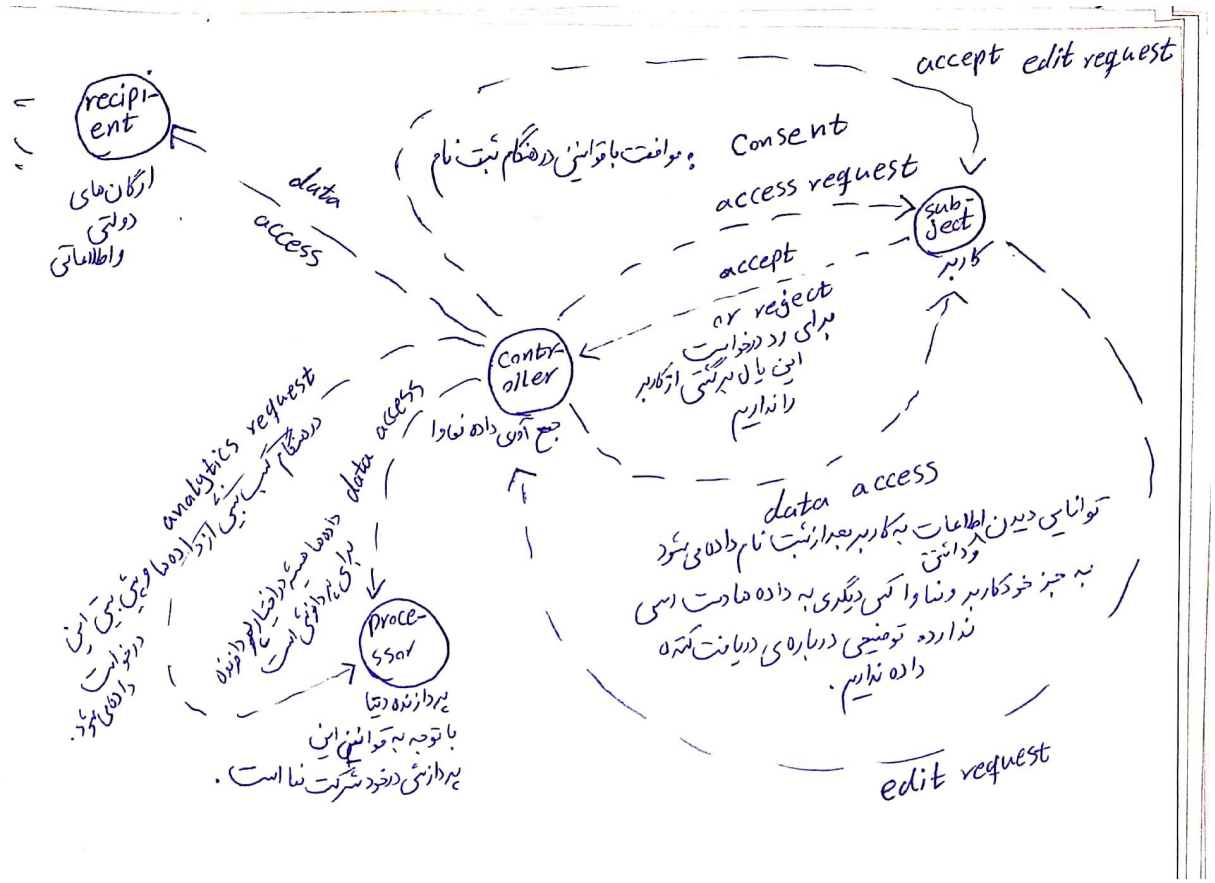
بدیهی است محیط وب از امنیت کامل برخوردار نیست بنابراین اگر در حین انتقال اطلاعات هر گونه دسترسی توسط افراد یا گروه‌های سوم شخص به اطلاعات کاربر ممکن گردد، هیچ مسئولیتی متوجه نماوا نخواهد بود.

کاربر مجاز نیست اطلاعات کاربری خود را در اختیار دیگران قرار دهد. در صورتی که کاربر اطلاعات کاربری خود را در اختیار دیگران قرار دهد، مسئولیت هر گونه مشکلی که به واسطه این امر رخ دهد به عهده کاربر است.

مشاهده تمامی محتوای موجود در سایت نماوا تنها از طریق IP های داخل ایران امکان پذیر خواهد بود و در صورتی که کاربر خارج از ایران هستید و یا اینکه از انواع VPN استفاده می‌کنید، تنها می‌توانید فیلم‌ها و سریال‌های ایرانی را تماشا نمایید. ممکن است در موارد خاص، برخی فیلم‌های ایرانی بخاطر اکران بین المللی، تا مدتی برای کاربران خارج از ایران قابل تماشا نباشند که بر حسب مورد در صفحه مختص به همان فیلم اطلاع رسانی خواهد شد.

بر اساس قوانین روابط عامل ها به شکل زیر است. کنترلر در اینجا نماوا است که وظیفه جمع آوری و نگهداری داده‌ها را دارد. یک پردازنده هم داریم که وظیفه پردازش داده‌ها و استخراج بینش از آنها را دارد. با توجه به قوانین و سیستم نماوا، پردازنده هم خود نماوا است. اطلاعات به جای دیگری ارسال نمی‌شود. پردازنده و کنترل کننده دو زیر مجموعه از نماوا هستند. یک موضوع برای توافق بین نماوا و کاربر وجود دارد. آن پذیرش قوانین نماوا توسط کاربر

است. این موضوع به عنوان درخواست دسترسی (access request) به کاربر در فرم ثبت نام فرستاده میشود. اگر کاربر ثبت نام کند با این قوانین موافق است. یال accept در صورت توافق برقرار می‌شود. این دو مورد به ترتیب انجام می‌شود و اگر accept برقرار نشود، دیگر موارد هم برقرار نمی‌شود. بعد از پذیرش کاربر، بلافاصله دسترسی به داده‌های کاربر در پروفایل به او داده می‌شود. بر اساس قوانین نماوا بعد از پذیرش اولیه، نماوا هر کاری در زمینه جمع آوری و پردازش داده می‌تواند انجام دهد. یعنی بدون گرفتن موافقت و درخواست کاربر هر زمان که بخواهد داده های او را جمع آوری می‌کند. کاربر نمی‌تواند درخواست محدودیت در جمع آوری داده و پردازش به نماوا داشته باشد. کاربر فقط می‌تواند درخواست ویرایش اطلاعات پروفایل را به نماوا بدهد که بلافاصله مورد پذیرش قرار خواهد گرفت. نماوا دسترسی به داده‌های جمع آوری شده را به پردازنده خود می‌دهد. هر وقت که نماوا بخواهد می‌تواند درخواست پردازش داده‌های کل یا یک کاربر را به پردازنده بدهد.



به جز کاربر و پردازنده، دسترسی به داده‌ها به ارگان‌های دولتی و نظارتی داده می‌شود که دریافت کننده اطلاعات هستند و به سیستم کمکی نمی‌کنند.

۳) در سیستم ما یک پیشنهاد دهنده فیلم به افراد وجود دارد که با یادگیری، تعدادی از فیلم‌های مناسب کاربر را به او پیشنهاد می‌دهد. کاربر می‌تواند دیدن این فیلم‌های پیشنهادی را درخواست کند. سامانه دیگری در صورت قانونی بودن تماشای فیلم توسط کاربر درخواست او را می‌پذیرد یا رد می‌کند. سامانه رد و پذیرش یک قانون دارد که مربوط به محل جغرافیایی کاربر است. اگر کاربر در ایران باشد محدودیتی در تماشای فیلم ها ندارد. اگر کاربر در خارج از کشور باشد یا IP مربوط به خارج کشور را داشته باشد، با محدودیت هایی در تماشا مواجه است. برخی درخواست‌های تماشای فیلم کاربر خارجی رد می‌شود. با توجه به این توصیف ما دوست داریم که سیستم پیشنهاد دهنده نزدیک ترین فیلم‌ها به کاربرها را پیشنهاد دهد به طوری که نرخ رد شدن کمینه شود. مسئله اینگونه ساده می‌کنیم که پیشنهاد گر یک فیلم به کاربر پیشنهاد می‌دهد اگر مکان جغرافیایی کاربر و مکان مجاز فیلم یکسان بود، تماشا پذیرفته می‌شود و در غیر درخواست تماشا رد می‌شود. در کل دو مکان جغرافیای داخل ایران و خارج ایران را هم داریم. همانطور که دیده می‌شود، ما یک تبعیض برای کاربران خارجی قایل می‌شویم و مدل پیشنهاد دهنده نسبت به مکان جغرافیای کاربر بایاس دارد.

۴) پیشنهاد دهنده عملا دارد مکان جغرافیای کاربر در لحظه را بر اساس تاریخچه پیش بینی می‌کند. مکان کنونی کاربر لیبل واقعی است و مکان جغرافیای فیلم پیشنهادی، پیش بینی مدل از مکان کاربر است. زمانی مدل با دقت خوب داریم که مکان فیلم‌های با تناسب بالای با کاربر زیادی با کاربر مورد نظر یکسان باشد. عملا زمانی دقت مدل خوب است که نرخ رد تماشای فیلم کمینه باشد. با این کار عملا داریم عدالت را زیر پا می‌گذاریم و به کاربران خارج امکانات کمتری می‌دهیم. عدالت زمانی رخ می‌دهد که امکانات برای همه یکسان باشد. یعنی پیشنهاد فیلم

مدل به کاربران مستقل از مکان باشد. امکانات یعنی بیشترین تناسب بین فیلم پیشنهادی و ویژگی ها و تاریخچه فرد وجود داشته باد. باید محدودیتی متناسب با این استقلال مربوط به عدالت در تابع هزینه قرار دهیم. تابع هزینه را می توان به شکل زیر بیان کرد.

$$minimize\ BCELoss(Y,\ h(X))$$

$$s.t.\ \ h(X)\ \perp\ Y$$

در اینجا h مدل پیشنهاد دهنده ما است. X سابقه کاربر است و Y مکان‌های واقعی کاربران است. برای کم کردن نرخ رد شدن درخواست تماشا باید مکان جغرافیایی فیلم پیشنهادی $h(X_i)$ و Y_i مکان واقعی در موارد زیادی مشابه باشد. برای رعایت و دادن خدمات برابر به افراد باید شرط استقلال بیان شده در محدودیت تا حد ممکن برقرار شود. یعنی فیلم‌های پیشنهادی به افراد مستقل از مکان آنها و فقط بر اساس سابقه و عملکرد باشد. هر چه بخواهیم عدالت را بیشتر برقرار کنیم، فیلم‌ها بیشتر بر اساس ویژگی‌های فرد و امتیازات قبلی او به فیلم‌ها است و مکان در پیشنهاد کم اهمیت تر است. این موضوع موارد عدم تشابه مکان فیلم و کاربر را بیشتر می‌کند و باعث کاهش دقت مدل و افزایش نرخ رد درخواست تماشا می‌شود. اگر بخواهیم نرخ رد را کاهش دهیم، استقلال پیش بینی از مکان کمتر می‌شود و تبعیض پر رنگ تر می‌شود. راه دیگر انجام دو بهینه سازی است. به این شکل که می‌خواهیم BCELoss و خطای ناشی از استقلال را کمینه کنیم. خطای ناشی از استقلال این است که می خواهیم $p(h(X_i)|Y_i = 0) = p(h(X_i)|Y_i = 1)$ به ازای تمام کاربران i برقرار باشد. یعنی احتمال پیش بینی به ازای هر کار به شرط داخل و خارج بودن یکسان باشد. پیش بینی می تواند داخل یا خارج باشد ولی در این تساوی در دو طرف پیش بینی یکسان است. یعنی می خواهیم مجموع قدرمطلق اختلاف دو طرف تساوی را برای تمام کاربران کمینه کنیم و به صفر برسانیم. در اینجا p مشخص کننده احتمال است. محدودیت حرکت در بهینه سازی روش قبل را به صورت یک loss در کنار loss اصلی تعریف کریم. برای بهینه کردن همزمان هر دو می توان از ترکیب خطی آنها استفاده کرد. ضریب هر loss اهمیت آن است. در این شکل ما با توجه به مسئله و انتظارات و

اهمیت عدالت می توانیم برای loss مربوط به آن ارزش قائل شویم. در اینجا محدودیت را به صورت loss در آوردیم. روش‌های دیگری برای تعیین loss عدالت وجود دارد. مانند استفاده توان ۲ به جای قدر مطلق در روش قبل یا استفاده از sigmoid اختلاف بیان شده به جای قدر مطلق. همچنین می‌توان عدالت را بر اساس FPR, FNR, TPR, TNR و Bias Parity Score Based Loss[1] مبتنی بر این معیارها تعریف کرد. از ترکیب خطی این نوع loss ها استفاده می‌کنیم. برای بررسی اینکه کدام روش بهتر است، باید مجموعه داده مربوط به نماوا را داشته باشیم. در کنار صورت پروژه این داده وجود ندارد. همچنین دسترسی به این مجموعه داده ممکن نیست و نماوا تا کنون به نظر می‌رسد که چنین مجموعه داده‌ای را منتشر نکرده است. اما مواردی که از قدر مطلق و sigmoid استفاده می‌شود به دلیل مشکل در مشتق گیری و پیچیدگی فرآیند محاسبات چندان مناسب به نظر نمی‌رسد. در مورد Bias Parity Score Based Loss نسبت به دیگر موارد ما بخش‌های مختلف خطای سازنده خطای عدالت را متفاوت مورد توجه قرار می‌دهیم و اهمیت می‌دهیم. به نظر می‌رسد چنین روش‌هایی در زمان کمتر و با کیفیت بیشتر پاسخ می‌دهند. وزن متفاوت بخش‌های مختلف loss باعث ایجاد توانایی در تعریف دقیق تر و نرم تر عدالت می‌شود.

۵) اگر راه حلی وجود داشته باشد که همه اهداف (loss همه) را به طور همزمان به حداقل برساند، این راه حل برای جمع وزنی loss مربوط به اهداف نیز بهینه خواهد بود. پس انتخاب تابع هدف برای تجمیع سه هدف در یک تابع هدف به صورت مجموع وزن دار loss های اهداف مختلف، رضایت بخش است البته باید نکاتی رعایت شود. برای این که پاسخ تابع هدف تجمیعی پاسخی برای اهداف باشد، باید loss های اهداف با هم سازگار باشند. یعنی باید واحدهای هر واحد تغییر این loss ها یکسان با هم باشد. هدف دوم ما کمینه کردن اختلاف دو نرخ است. این در حالی است که هدف اول به دنبال کاهش تعداد رد شدن و هدف سوم به دنبال کاهش زمان تعامل عاملها است. نیاز داریم که برای هدف های اول و سوم نیز معیار نرخی را معرفی کنیم که کمینه کردن آن معادل کمینه کردن متغیر اصلی باشد. در هدف اول از نرخ رد شدن استفاده می‌کنیم. نرخ رد شدن یعنی تعداد رد شدن تقسیم بر تعداد کل

[1] https://arxiv.org/pdf/2111.03638.pdf

درخواست ها در کل از ابتدا تا آخرین زمان اجرا و بهینه سازی است. مخرج همیشه ثابت است و تاثیری کمینه کردن تعداد درخواست های رد شده ندارد. برای هدف سوم از نسبت زمان تعامل به کل زمان بهینه سازی و اجرا استفاده می‌کنیم. به این شکل ما برای سه هدف، loss به صورت سه نرخ داریم که با ترکیب خطی وزن دار می‌توان با هم ترکیب کرد. وزن‌ها اهمیت یک واحد تغییر loss اهداف نسبت به هم را نشان می‌دهد.

۶) در اینجا ما سه عامل مشابه با هدف مخصوص خود داریم که می‌خواهیم هر سه را در یک مسئله راضی کنیم. هدف هر یک بیشینه کردن پاداش است. می‌توانیم مانند قبل عمل کنیم و ترکیب خطی سه هدف را به عنوان هدف نهایی تعیین کنیم. تفاوت نسبت به قبل این است که ما یک MDP برای محیط داریم. هر بار وضعیت توسط محیط به عامل‌ها گفته می‌شود و عامل ها تصمیم می‌گیرند. تغییرات وضعیت محیط هر بار بر اساس فعالیت یک سری از عامل ها است. هرچه محیط عادلانه تر به سه عامل نگاه کند و تغییرات آنها را در تعین وضعیت و پاداشها لحاظ کند پاداش دریافت می‌کند. هرچه تعیین پاداش‌ها و شرایط محیط دقیق تر باشد و بیشتر به سمت یادگیری سریع باشد نیز پاداش دریافت می‌کند. عملا محیط یک یادگیری برای کار خود دارد. هر چه پیش بینی وضعیت آینده و پاداشها بهتر و بیشتر به سمت یادگیری سریع باشد، دقت بیشتر است. هر چه در پیش بینی‌ها به مساوات بیشتری به عامل‌ها نگاه شود، پیش بینی عادلانه تر است. به جای تعیین loss برای این یادگیری از پاداش استفاده می‌کنیم که می‌خواهیم بیشینه کنیم. یعنی ما پنج پاداش داریم. سه تا برای رفتن عامل به وضعیت مناسب داریم و یک پاداش برای پیش بینی دقیق پاداش‌ها و وضعیت محیط و یک پاداش برای عادلانه بودن پیش بینی داریم. این پنج پاداش را طوری تعریف می‌کنیم که ارزش هر واحد آنها یکی باشد. بعد مانند قبل به صورت ترکیب خطی این پاداش‌ها را به یک پاداش تبدیل می‌کنیم و یک مسئله بهینه سازی برای بیشینه کردن این پاداش ساخته شده داریم.

۷و۱۰) ما یک جدول برای اطلاعات شخصی کاربران داریم. در این جدول برای هر فرد نام، نام خانوادگی، آدرس ایمیل، نام کاربری، رمز عبور و شماره تلفن همراه را داریم. یک جدول برای فیلم‌های دیده شده توسط کاربر و امتیازات او به فیلم‌ها داریم. یک جدول هم برای خریدهای کاربر داریم. برای فیلم‌ها یک سری ویژگی داریم که از جمله آنها منطقه جغرافیایی مجاز است. برای کاربر در لحظه نیز این مکان را داریم. برای مکان از IP استفاده می‌کنیم. برای IP ها ما IP را به IP کلی ایران یا IP غیر از آن تبدیل می کنیم که برای خارج از کشور باشد. از روش تعمیم استفاده می‌کنیم. باز می‌توان بیشتر جلو رفت. مثلا اگر فهمیدن لیست فیلم‌های قابل پخش در ایران و خارج مهم باشد. در این صورت می توان از hash نتیجه تعمیم با کلید خصوصی استفاده کرد. کار ساده تر استفاده از 1 مثال برای IP داخل و 2 برای خارج است. یک جدول خودمان داشته باشیم که بعدا بتوانیم این map را انجام دهیم. روش دوم Pseudonymization است. در روش تعمیم ما جزئیات داده را از دست می‌دهیم و فقط می‌دانیم که مربوط به داخل ایران است یا نه. در Pseudonymization معمولا از hash استفاده می شود که تابع متداولی دارد و حمله brute force برای آن ممکن است. تمام IP ها را hash می‌گیریم و مشابه خروجی hash را در جدول پیدا می‌کنیم. نکته این است که بین خروجی hash و محتوای اصلی رابطه‌ای است. در روش عدد دهی ما این ارتباط را فقط خودمان می دانیم و فهمیدن آن از بیرون سخت تر است. چون محاسبه hash روش‌ها و مپ های متداولی دارد. از همه بهتر استفاده از hash با کلید خصوصی است که جلوی حمله بیان شده را هم می‌گیرد. برای حمله یا یافتن ورودی که مقدار hash آن را داریم باید به کلید خصوصی برسیم. برای فیلم ما اطلاعات خود فیلم‌خا مانند نام و نام کارگردان و سال ساخت و ژانر را هم نگه می‌داریم. این اطلاعات، اطلاعی درباره اطلاعات افراد نمی‌دهد. این که دیگران بفهمند یک سامانه چه فیلم‌هایی دارد چندان مهم نیست. اطلاعات فیلم‌ها در یک جدول است و هر فیلم یک id یکتا دارد. افراد به فیلم ها امتیاز می‌دهند. هر رکورد امتیاز دهی به این شکل است که کاربر id فلان به فیلم فلان در فلان تاریخ امتیاز مشخصی از یک تا پنج داده است. تاریخ امتیاز دهی باید از دیگران پنهان شود. چون رفتار فیلم دیدن یک کاربر را مشخص می‌کند. شاید این رفتار به صورت یکتا یک کاربر را معرفی کند که

باعث فاش شدن اطلاعات فرد می‌تواند بشود. نام فیلم هم نباید فاش شود. باز روی نام فیلم‌های امتیاز داده شده افراد می‌توان به علایق و رفتار آنها پی برد. با نام فیلم می‌توان به ژانر آن رسید. استفاده از id به جای نام فیلم مناسب تر است. Id های اختصاصی به فیلم ها باید رندم باشند. همچنین بین هر دو جدول با Id فیلم، باید id فیلم‌ها متفاوت باشد. یعنی با یک مپ رندم id های جدول فیلم ها را به id هایی برای جدول امتیاز دهی تبدیل می کنیم. برای جدول دیگر از یک مپ متفاوت برای این کار استفاده می‌کنیم. جدول مپ‌ها را فقط خودمان نگه می‌داریم. این کار باعث می‌شود اگر id های فیلم در یک جدول فاش شود، نتوان مستقیم به id های اصلی جدول فیلم رسید. برای id کاربران هم این کار را می کنیم. در هر جدول نیز id های کاربران و فیلم‌ها را hash می‌کنیم. باز بهتر است از hash با کلید خصوصی استفاده کنیم. تاریخ امتیاز دهی را نیز باید بپوشانیم. می توانیم از یک مرحله تعمیم استفاده کنیم. مثلا فق سال و ماه را نگه داریم و روز را حذف کنیم. باز این اطلاعات می‌تواند باعث پی بردن به رفتار یک فرد شود و از روی اطلاعات مربوط به افراد واقعی اطلاعت آنها در سامانه را پیدا کرد. راه دیگر این است که از id برای ماه‌های سال‌های مختلف استفاده کنیم. Id ها باید رندم باشد و ترتیب معناداری نسازد. باز می‌توان از hash برای id تاریخ هم استفاده کرد. برای اطلاعات شخصی ما ایمیل را داریم که اطلاعات نام را می‌تواند داشته باشد یک راه برای جلوگیری از فاش این داده، روش Suppression / Wiping است. در این روش قسمت‌های مهم در ایمیل را با حرف x جایگزین می‌کنیم. این طور اطلاعات مهم در ایمیل دیده نمی‌شود ولی داده ایمیل از دست می‌رود. راه حل مناسب باز انجام hash است و بهترین کار hash با کلید خصوصی است. برای شماره تلفن می‌توان مانند ایمیل رفتار کرد. با روش Suppression / Wiping می‌توان تعدادی از ارقام شماره تلفن را x کرد یا کل را به این شکل تبدیل کرد. در حالت پوشاندن کل، کل اطلاعات از دست می‌رود. در حالت پوشاندن تعدادی رقم، اطلاعات مکان سیم کارت می‌تواند فاش شود که از روی آن می‌توان منطقه جغرافیایی رسید. مثلا شروع با 0917 تعین کننده تعداد محدودی استان برای صدور سیم کارت است. البته اکنون افراد با چنین شماره هایی در کشور تا حد خوبی پخش شده اند. اگر شروع را نپوشانیم کد کشور فاش می‌شود و خارج ایران بودن مشخص می‌شود. برای اطلاعات بانکی

می‌توان از تعمیم استفاده کرد. تاریخ پرداخت‌های فرد را به صورت ماهیانه یا سالیانه ثبت کنیم. یعنی برای هر فرد مجموع پرداخت های ماه‌های او را ثبت کنیم. به این شکل جزئیات رفتاری فرد مشخص نمی‌شود. با این کار ممکن است نتوان از روی اطلاعات پرداخت یک فرد یکتا را مشخص کرد. یک کار دیگر انجام تبدیل روی مقادیر پرداخت است. از یک تبدبل خاص استفاده کنیم که روش آن را فقط خود بدانیم. نتایج تبدیل بهتر است به گونه این باشد که همه پرداخت خیلی نزدیک هم باشند. از hash برای پرداخت‌ها هم می‌توان استفاده کرد. دستکاری یک مجموعه داده با تکنیک‌های کلاسیک ناشناس‌سازی منجر به ۲ نقطه ضعف کلیدی می‌شود: تحریف یک مجموعه داده منجر به کاهش کیفیت داده ها می شود. خطر حفظ حریم خصوصی کاهش خواهد یافت، اما همیشه وجود خواهد داشت. نسخه مجموعه داده اصلی را با رابطه 1-1 دستکاری می کنند که این رابطه ها قابل بازیابی خواهند بود. شاید سخت باشد ولی ممکن است. ما در ناشناس سازی یک طیف داریم. یک سر آن کاهش شدید کیفیت داده و حفظ حریم خصوصی بالا است و سر دیگر کیفیت داده بالا و حفظ حریم خصوصی بسیار پایین است. در اولی داده را دور ریختیم و در دومی کاری برای ناشناس کردن انجام نداده ایم. ما در ناشناس سازی به دنبال یه نقطه بهینه هستیم. عملا کیفیت داده و حفظ حریم خصوصی یک trade off می‌سازند. ما به دنبال نقطه بهینه آن هستیم. نکته این است که تکنیک‌های کلاسیک ناشناس‌سازی، نقطه کمتر از حد مطلوب بین کیفیت داده و حفاظت از حریم خصوصی ارائه می‌دهند. Syntho نرم‌افزاری را برای تولید مجموعه‌ای کاملاً جدید از داده‌های اصلی توسعه می‌دهد. اطلاعات برای شناسایی افراد واقعی به سادگی در یک مجموعه داده مصنوعی ساخته شده از دیتاست اصلی وجود ندارد. از آنجایی که مجموعه داده ساخته شده این نرم افزار حاوی داده‌های مصنوعی تولید شده توسط نرم‌افزار هستند، داده‌های شخصی به سادگی وجود ندارند و در نتیجه وضعیتی بدون خطرات حفظ حریم خصوصی ایجاد می‌شود. تفاوت اصلی در Syntho، استفاده از یادگیری ماشین است. در نتیجه، راه‌حل این نرم افزار ساختار و ویژگی‌های مجموعه داده اصلی را در مجموعه داده مصنوعی بازتولید می‌کند که منجر به حداکثر شدن سودمندی داده می‌شود. بر این اساس، می‌توانید نتایج یکسانی را هنگام تجزیه و تحلیل داده‌های مصنوعی در مقایسه با استفاده از

داده‌های اصلی به دست آورید. در نتیجه، داده های مصنوعی راه حل ترجیحی برای غلبه بر پاسخ زیر بهینه بین کیفیت داده و حفاظت از حریم خصوصی است، که تمام تکنیک های کلاسیک ناشناس سازی به شما ارائه می دهند. راه حل‌های بهتری که ما برای راه های کلاسیک اولیه گفتیم، همگی هنوز پاسخ زیر بهینه دارند. در این روش‌ها، ما از تبدیلات روی ویژگی‌ها استفاده می‌کنیم که تضمینی به حفظ توزیع و ویژگی‌های اصلی نمی‌دهند. Hash و map هم نوعی تبدیل به حساب می‌آیند.

۸) جمع آوری داده های ناشناس و حذف شناسه ها از پایگاه داده توانایی شما را برای استخراج ارزش و بینش از داده های خود محدود می کند. برای مثال، داده‌های ناشناس را نمی‌توان برای تلاش‌های بازاریابی یا شخصی‌سازی تجربه کاربر استفاده کرد. در زمینه منابع انسانی، ما می‌خواهیم از کارمندان بهترین خروجی را بگیریم با کمترین هزینه اضافه. این زمانی رخ می‌دهد که با توجه به شخصیت کارمندان از آنها در کارها استفاده کنیم. چون در منابع انسانی در مواردی به شخصی سازی نیاز داریم، ناشناس کردن داده‌ها و حذف هویت کاربرد ندارد.

۹) بله. این روش را استفاده نام مستعار می‌نامیم. هدف اصلی از نام مستعار محدود کردن قابلیت پیوند است بین یک مجموعه داده مستعار و دارندگان نام مستعار و در نتیجه محافظت از هویت موضوع داده ها و صاحبان آنها است. این نوع حفاظت معمولاً برای مقابله با تلاش های یک دشمن برای انجام یک حمله شناسایی هویت صورت می‌گیرد. در یک راه معمول برای این کار، می‌توان شناسه فرد صاحب رکورد را hash کنیم و از آن استفاده کنیم. شرایطی را در نظر بگیرید که هویت تنها با این شناسه قابل دسترسی است. در hash با خروجی تقریبا بی معنی مواجه هستیم که برگشت ناپذیر است و نمی توان به هویت رسید. همچنین یک به یک بودن تابع را هم در نظر می‌گیریم. به این hash به صورت دقیق تر هش رمزنگاری گفته می‌شود. در این شرایط باز می‌توان به هویت رسید. شناسه هویت را اسم و فامیل در نظر می‌گیریم. برای رسیدن به هویت می‌توان از حمله brute force استفاده کنیم. مثلا از

جستجوی لغت نامه یا دیگر روش های آن می‌توان استفاده کرد. استفاده از اطلاعات موجود در مورد داده‌های اصلی می‌تواند جستجو را کمتر کند. برای بهبود این روش می‌توان از MAC یا Message authentication code استفاده کرد. این روش مانند قبل است و تنها تفاوت آن این است که در تابع hash از یک کلید مخفی استفاده می‌شود. تابع ورودی و کلید خصوصی را می‌گیرد و hash را محاسبه می‌کند. Hash های حاصل ورودی ویژگی‌های قبلی دارند. تا زمانی که کلید خصوصی فاش نشده است، نمی توان از اسم مستعار به هویت رسید. حمله‌های مشابه مورد گفته شده ممکن نیست. MAC از نقطه نظر حفاظت از داده ها، به طور کلی به عنوان یک تکنیک مستعار سازی قوی در نظر گرفته می شود. از آنجایی که بازگرداندن نام مستعار تا زمانی که کلید به خطر نیفتاده است، غیر ممکن است. نمی‌توانیم هش حالات ممکن را برای حمله بدست آوریم چون کلید خصوصی را نداریم.

۱۱) ما دو نوع تبعیض مستقیم و غیر مستقیم داریم. فرض کنیم متغیر ایجاد کننده تبعیض c و l متغیر هدف باشد. برای عدم تبعیض نیاز است که اثر علی مستقیمی از c به l نداشته باشد (c->l). همچنین نیاز است که هیچ اثر علی غیر مستقیمی از c به l باشد. مدل ما یک مدل علی بین متغیرهای ما است. برای اثرات غیر مستقیم باید اثر علی از c به l با واسته‌ای مثل m نداشته باشیم (c->m->l). برای نداشتن تبعیض باید اثر علی از c به l به صورت مستقیم نداشته باشیم. یعنی استقلال این دو متغیر را داشته باشیم. ممکن است استقلال کامل همیشه ممکن نیست به صورت مشروط باید این استقلال برقرار باشد. گره‌های X و Y در گراف علی G با Z از هم جدا می‌شوند، اگر شرط های زیر برآورده شود (به این جدایی d-separation گویند). گره‌های X و Y با Z از هم جدا می‌شوند اگر و فقط اگر Z هر مسیری را از یک گره در X به یک گره در Y مسدود کند. یک مسیر p به مجموعه‌ای از گره‌های Z مسدود می‌شود اگر و فقط اگر p شامل یک زنجیره $i \rightarrow m \rightarrow j$ یا یک چنگال $i \leftarrow m \rightarrow j$ است به طوری که گره وسط m در Z باشد، یا p شامل یک برخورد دهنده $i \rightarrow m \leftarrow j$ است به طوری که گره وسط m در Z نیست و هیچ فرزندی از m در Z نیست. بنابراین، معنای گرافیکی d-separation را می توان به گونه ای تفسیر کرد که مسیرهای

بین X و Y را مسدود می‌کند به طوری که هیچ تاثیری از هیچ گره ای در X به هیچ گرهی در Y منتقل نمی شود. این مسدود سازی باعث ایجاد عدم تبعیض می‌شود. پس برای عدم تبعیض باید سه حالت مسدود سازی ارتباط دو گره با گره سوم بیان شده در مدل ما برقرار باشد.

۱۲) چندین طرح حریم خصوصی مبتنی بر پارتیشن در افشای داده ها با شرایط اثبات بر روی بلوک های q یک مجموعه داده منتشر شده، تعریف می شوند. k-anonymity مستلزم این است که پشتیبانی از هر بلوک q غیر خالی حداقل k است. l-diversity مستلزم آن است که تعداد مقادیر متمایز ویژگی حساس در یک بلوک q غیر خالی حداقل l باشد. t-closeness مستلزم آن است که توزیع مقادیر حساس در یک بلوک q غیر خالی با توجه به تابع فاصله بین توزیع ها، نزدیک به توزیع در مجموعه داده کلی باشد.

۱۳) در دیتاست ما داده متن توضیح فیلم یا نام و رمز، عکس فیلم‌ها، تاریخ خرید یا امتیاز دهی و آدرس IP وجود دارد. همانطور که گفتیم، امنیت متن‌های مربوط به نام، نام کاربری و رمز عبور افراد و تاریخ ها و آدرس IP ها مهم است. پس برای این موارد از روشهای security-oriented یا امنیت محور استفاده می‌کنیم. برای مواردی مانند عکس‌ها می‌توان از شاخه دیگر یعنی دیتا محور استفاده کرد. در این موارد می‌خواهیم عکس‌های مختلف را در یک اندازه ثابت داشته باشیم و تا حدی از حجم داده بکاهیم.

۱۴) در رمزنگاری، توابع هش رمزنگاری را می توان به دو دسته اصلی تقسیم کرد. در دسته اول آن دسته از توابعی هستند که طرح های آنها بر اساس مسائل ریاضی است و امنیت آنها از برهان های دقیق ریاضی، نظریه پیچیدگی و formal reduction ناشی می شود. این توابع را Provably Secure Cryptographic Hash Functions می نامند. ساختن اینها بسیار دشوار است و نمونه های کمی معرفی شده است. استفاده عملی آنها محدود است. در

دسته دوم توابعی هستند که بر اساس مسائل ریاضی نیستند، بلکه بر اساس ساختارهای ساخته شده برای این هدف خاص هستند که در آن بیت های پیام برای تولید هش مخلوط می شوند. سپس اعتقاد بر این است که شکستن آنها سخت است، اما هیچ مدرک رسمی ارائه نشده است. تقریباً تمام توابع هش در استفاده گسترده در این دسته قرار دارند. برخی از این توابع قبلاً شکسته شده اند و دیگر مورد استفاده قرار نمی گیرند. هش هایی هستند بر اساس یک مسئله سخت ریاضی یا ساختاری خاصی هستند که خیلی سخت یا اطلا نمی‌توان آنها را شکست. شکستن هش یعنی اینکه از روی خروجی تابع به داده واقعی برسیم. این روش‌ها برای تولید داده از روی داده اصلی تولید شده اند که داده اصلی را فاش نکنند.

در علوم کامپیوتر، هش حساس به محلی بودن (LSH) یک تکنیک الگوریتمی است که موارد ورودی مشابه را با احتمال زیاد در سطل ها مشابه هش می کند. (تعداد سطل ها بسیار کمتر از جهان آیتم های ورودی ممکن است.) از آنجایی که موارد مشابه در سطل های یکسانی قرار می گیرند، این تکنیک می تواند برای خوشه بندی داده ها و جستجوی نزدیکترین همسایه استفاده شود. تفاوت آن با تکنیک های هش قبلی در این است که برخورد هش به حداکثر می رسد، نه به حداقل می رسد. از طرف دیگر، این تکنیک را می توان راهی برای کاهش ابعاد داده های با ابعاد بالا در نظر گرفت. آیتم های ورودی با ابعاد بالا را می توان به نسخه های کم بعدی کاهش داد و در عین حال فاصله نسبی بین موارد را حفظ کرد. الگوریتم‌های جستجوی تقریبی نزدیک‌ترین همسایه مبتنی بر درهم‌سازی معمولاً از یکی از دو دسته اصلی روش‌های درهم‌سازی استفاده می‌کنند: یا روش‌های مستقل از داده، مانند هش‌سازی حساس به محلی بودن (LSH). یا روش‌های وابسته به داده، مانند هش کردن با رعایت محلی بودن (LPH).

۱۵) تابع پیش پردازش در برابر حملات برخورد در توابع Hash مقاومت ایجاد می کند. در این روش، پیام داده شده (ورودی) قبل از هش شدن، از قبل پردازش می شود. منطق پشت پیش پردازش این است که پیام داده شده قبل از

ارسال به تابع هش تصادفی تر می شود. این امر افزونگی در داده های ورودی را کاهش می دهد و در نتیجه منجر به کاهش احتمال یافتن برخورد می شود. به این روش، پیش پردازش پیام می گویند. برای جلوگیری از برخورد هش، از تابع پیش پردازش پیام برای افزایش تصادفی شدن و کاهش افزونگی یک پیام ورودی استفاده می کنیم. تابع پیش پردازش پیام شامل 4 مرحله از جمله به هم زدن بیت های پیام، استفاده از تابع T فشرده سازی و LFSR است که این مراحل آنتروپی پیام ورودی را در پایان 4 دور افزایش می دهد و خروجی تصادفی تر می شود.

برای جلوگیری از حمله brute force می‌توان از salt استفاده کرد. Salt یک رشته است که قبل از تولید hash ورودی آن را با ورودی کانکت می کنیم. ممکن است salt را مثلا در وسط ورودی قرار دهیم. جایی که ورودی را تقسیم می‌کنیم را فقط خودمان می دانیم.