|  |
| --- |
| **روندهای آتی امنیت در رایانش ابری: یک مطالعه گسترده** |
|  |

نتیجه گیری و کارهای آتی: متدهای مختلفی در آینده برای گمنام کردن داده ها در ابر از سال 2015 تا 2017 بررسی خواهد شد. انتشار میکروداده ها از قبیل داده های سرشماری یا بیماران برای تحقیقات گسترده و دیگر اهداف، حوزه مهمی است که توسط آژانس های دولتی و دیگر تشکلات اجتماعی روی آن تمرکز شده است. روش های سنتی که در مقالات آورده شده اند، روش حذف فیلدهای تشخیصی یکتا مانند شماره امنیت اجتماعی از میکروداده را پیشنهاد می کنند که هنوز افشای اطلاعات حساس می شود، الگوریتم بهینه سازی گمنامسازی K از نوع NP سخت است. به این ترتیب موجب چالش های محاسباتی زیادی می شود. گمنامسازی K با مسئله حمله یکنواختی و حمله زمینه دانش مواجه است. مفهوم تنوع که در مستندات گذشته پیشنهاد شده است ، برای بررسی این موضوع و نیز بررسی محدودیت هاست چرا که در جلوگیری از حملات افشای نسبت ها (حمله چولگی و حمله تشابه)، بدست آوردن آن سخت است و ممکن است حفاظت کافی از حریم شخصی را در برابر صفات حساس در کلاس مربوطه و با تکنیک های خاص محدودیت گذاری مانند نمونه گیری گردکردن سرکوب سلول و مبادله داده نتواند بدست آورد. ارزیابی تکنیک های بینام سازی داده و تکنیک های جلوگیری از افشا داده با جزییات بحث شده اند. کاربرد تکنیک های بینام سازی داده برای طیف های خاصی از داده ها مانند داده های طراحی ، بیان شده است. این خلاصه ، جهت های تحقیقاتی خاصی را در حوزه بی نام سازی پایگاه داده پیشنهاد می کند.

<https://fardapaper.ir/future-cloud-computing-extensive>