آنالیز حریم خصوصی در شبکه های اجتماعی آنلاین از منظر تئوری گراف

چکیده : پذیرش بسیار گسترده شبکه های اجتماعی آنلاین (OSNs) پرسش های بسیاری را در مورد کنترل حریم خصوصی و دسترسی افزایش می دهد. صرف نظر از ماهیت خاص محوری یا غیر محوری از OSN، درجه ای از امنیت و حریم خصوصی که محقق می شود ، به شدت وابسته به خواص گراف تئوریک از گراف اجتماعی می باشد که در واقع نماینده روابط دوستی واقعی بین کاربران است . ما در این مقاله، رابطه بین توپولوژی گراف شبکه های اجتماعی و حریم خصوصی قابل تحقق را تجزیه و تحلیل می کنیم . سه معیار در این مقاله رعایت شده است که عبارتند از ، توزیع درجه،ضریب خوشه بندی و زمان اختلاط، که بینش اساسی در مورد درجه حریم خصوصی در OSNها را نشان می دهد . در این مقاله پیشنهاد می کنیم که چگونه از این بینش برای طراحی OSN های آینده با حریم خصوصی مورد پسند ، بهره برداری شود .

I. معرفی

شبکه های اجتماعی آنلاین (OSNs) به مفهوم اشتراک گذاشتن و کشف محتوای تولید شده توسط کاربران اشاره کرده و کاربری آن توسط دوستان در نظر گرفته می شود. پذیرش بسیار گسترده شبکه های اجتماعی آنلاین (OSNs) پرسش های بسیاری را در مورد سیاست های دسترسی و افشاگری گسترش می دهد؛ امروزه اخبار در مورد مسائل حریم خصوصی مانند شرکت های کاریابی[1] ، هکرهایی که از ارائه دهندگان خدمات شبکه اجتماعی (SNS) باج خواهی می کنند[2] ، بیمه هایی که تسهیلات را برای مشتریان خود قطع می کنند[3] در رسانه ها بسیار فراوانند.

متاسفانه، راه حل های حفاظت از حریم خصوصی ارائه شده توسط برنامه های OSN موجود نشان داد که عدم رضایت در این بخش به استحکام آن مربوط نیست . OSNهای غیر محوری (مثال [۱]، [۲]، [۳]) تلاش کردند تا این مشکل را با اجتناب از تصویب هر نهاد دانای مطلق اصلاح کنند . نهادی که می تواند به طور مستقیم داده های کاربران را مدیریت و از آن سوء استفاده کرده و زیرساختی را برای مدیریت داده های کاربر و ذخیره سازی توزیع شده (اغلب در معماری Peer-to-Peer) پیشنهاد دهد. چنین راه حل هایی هنوز هم برخی از نقاط ضعف موجود در حفظ حریم خصوصی را نشان می دهند.

در این مقاله، نشان می دهیم که درجه حفظ حریم خصوصی یک برنامه OSN، محوری یا غیر محوری، به شدت به خواص توپولوژیکی گراف اجتماعی که نشان دهنده دوستی (روابط اعتماد) بین کاربران واقعی OSN