حریم خصوصی و امنیت اطلاعات در شبکه های اجتماعی

جاسم خدابخشی هفشجانی[۱]، سودابه خدابخشی[۲]، طیبه نایبی[۳]

[۱] دانشجوی کارشناسی ارشد ، گروه کامپیوتر ، دانشگاه آزاد اسلامی واحد نجف آباد
Jasem_kh@sco.iaun.ac.ir

[۲] دانشجوی کارشناسی ارشد ، گروه کامپیوتر ، دانشگاه آزاد اسلامی واحد نجف آباد
soudabeh_k@yahoo.com

[۳] دانشجوی کارشناسی ارشد ، گروه کامپیوتر ، دانشگاه آزاد اسلامی واحد نجف آباد
tnayebi@gmail.com

چکیده

شبکه های اجتماعی آنلاین به بخش مهمی از فعالیت های آنلاین در وب تبدیل شده اند و جزء یکی از رسانه های پر نفوذ هستند.شبکه های اجتماعی آنلاین با فاصله فیزیکی نامحدود به کاربران وب، ابزارهای جالب جدیدی برای برقراری ارتباط، تعامل و معاشرت ارائه می دهند. در حالی که این شبکه ها به اشتراک گذاری داده ها را به صورت مکرر ایجاد می کنند و ارتباطات بین کاربران را فورا ممکن می سازند ، مسائل مورد بحث بسیاری مربوط به حریم خصوصی وجود دارد که آشکار می شود.یکی از این مسائل این است که چگونه از حمله به حریم خصوصی جلوگیری کنیم هنگامی که اطلاعات شخصی بسیار زیادی در دسترس باشد.در این مقاله ما به مسائل مربوط به حریم خصوصی افراد در شبکه های اجتماعی می پردازیم که با توسل به تجزیه و تحلیل شبکه های اجتماعی و روش های لینک کاوی این کار را انجام میدهیم. همچنین به توصیف بازنمودهای مشترک اساسی شبکه های اجتماعی می پردازیم،پس از آن، نشان می دهیم که چگونه حمله به حریم خصوصی می تواند در تجزیه و تحلیل شبکه های اجتماعی و تکنیک لینک کاوی برای فاش کردن اطلاعات حساس کاربر تاثیر بگذارد.

کلمات کلیدی

شبکه های اجتماعی آنلاین،حریم خصوصی ، لینک کاوی ، گراف و تهدیدات حریم خصوصی

۱- مقدمه

در چند سال گذشته، شبکه های اجتماعی آنلاین با تجربه، رشد نمایی در تعدادی از کاربران خود داشته و در مقدار عظیمی از اطلاعات دسترس پذیر بوده است. بسیاری از شبکه های اجتماعی آنلاین مانند Facebook ،LinkedIn ،Google+ و Twitter به کاربران وب ابزارهای جالب جدید برای برقراری ارتباط و اشتراک گذاری اطلاعات ارائه می دهند. با گسترش شبکه های اجتماعی آنلاین، به اشتراک گذاری اطلاعات در این شبکه ها به اهمیت روز افزون آنها تبدیل شده است. بدیهی است که شبکه های اجتماعی آنلاین راه مبتکرانه برای جمع آوری داده ها از طریق معاشرت و ارتباط با کاربران پیدا کرده اند. جای تعجب نیست، هنگامی که کاربران اجتماعی در ارتباط و تعامل هستند،و تمایل به فاش کردن اطلاعات شخصی خود بصورت آزادانه را دارند. برای کنترل دسترسی به این اطلاعات شخصی و برای به اجرا درآوردن حفاظت از آن، شبکه های اجتماعی آنلاین از تعدادی مکانیسم های کنترل ساخته شده استفاده کردند و آن را ترویج می کنند [۱] . با این حال، کاربران شبکه های اجتماعی اغلب موفق نیستند که به طور کامل از پروفایل هایشان محافظت کنند و داده های شخصی از اشکال نامطلوب دسترسی به آن شده است. شبکه های آنلاین اجتماعی ممکن است از طراحی درگیری مسائل رنج می برند مانند امنیت و حریم خصوصی در مقابل قابلیت ها و جامعه پذیری و ممکن است عمدا یا به طور تصادفی اطلاعات کاربران را برای اشخاص غیر مجاز و یا اشخاص ثالث فاش کنند[۲] .در ادامه ما در مورد حریم خصوصی در شبکه های اجتماعی که یکی از جذاب ترین چالش های شبکه های اجتماعی است بحث می کنیم. ما همچنین بر اهمیت داده های شبکه

های اجتماعی تمرکز می کنیم و توضیح می دهیم که چگونه تجزیه و تحلیل شبکه و روش های داده کاوی ،در فهم رفتار کاربران و شبکه ها مفید است و یک منبع می تواند به خطر حفظ حریم خصوصی تبدیل شود.

۲- شبکه های اجتماعی

۲-۱- یک شبکه اجتماعی چیست ؟

یک شبکه اجتماعی، یک ساختار اجتماعی است که از گره‌هایی (که عموما فردی یا سازمانی هستند) تشکیل شده است که توسط یک یا چند نوع خاص از وابستگی به هم متصل‌اند. به بیان دیگر، یک شبکه اجتماعی سایت یا مجموعه سایتی است که به کاربرانی که دوست دارند علاقه‌مندی‌ها ، افکار، فعالیتهای خودشان را با دیگر به اشتراک بگذارند و دیگران هم با آنان به اشتراک بگذارند. شبکه ها به مدل بسیاری از سیستم های پرکاربرد استفاده شده اند مانند وب جهانی ، شبکه های کامپیوتری ، شبکه های بیوشیمیایی ، شبکه های پخش و شبکه های اجتماعی. هر یک از این شبکه ها یک ساختار است که شامل مجموعه ای از بازیگران به نمایندگی از آنها است. به عنوان مثال، صفحات وب بر روی شبکه جهانی وب یا افراد در یک شبکه اجتماعی، با هم توسط روابط متصل، به نمایندگی از پیوندهای بین صفحات وب و یا دوستی بین افراد ارتباط دارند. علاوه بر این خواص ساختاری (بازیگران و روابط)، شامل تعدادی از مفاهیم اساسی مانند روابط، زوج، زیرگروهها، و گروه هایی که شبکه ها مشخص اند هستند.

۲-۲- شبکه های اجتماعی آنلاین

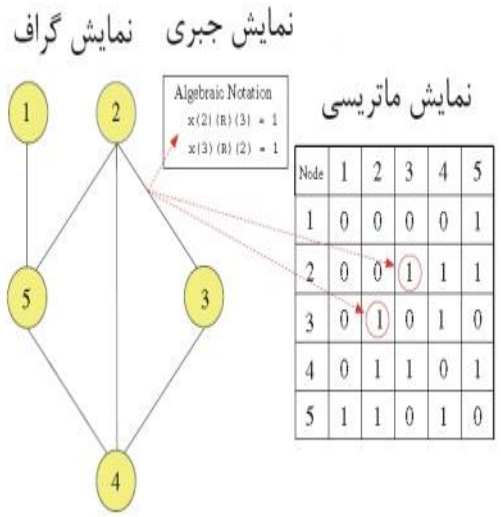
مهمترین هدف شبکه‌های اجتماعی گسترش ارتباطات میان فردی است. شبکه‌های اجتماعی آنلاین، عموما سرویس های مبتنی بر وب هستند. سرویس آنلاین، پلتفرم یا سایتی محسوب می شوند که مردم در آنها می توانند، نظرات، علاقه مندی ها و در یک کلام محتوا ایجاد و با دوستان و سایرین به اشتراک بگذارند. شبکه‌های اجتماعی آنلاین ، به‌خصوص آن‌هایی که کاربردهای معمولی و غیرتجاری دارند، مکان‌هایی در دنیای مجازی هستند که مردم خود را به‌طور خلاصه معرفی می‌کنند و امکان برقراری ارتباط بین خود و همفکرانشان را در زمینه‌های مختلف مورد علاقه فراهم می‌کنند.

۲-۳- چگونه یک شبکه اجتماعی را نشان دهیم ؟

پیدا کردن نماینده ای مناسب که می تواند تسهیل کارآمد و دقیق تفسیر داده های شبکه را نشان دهد، یک گام مهم در مطالعات شبکه های اجتماعی است. فقط گراف ها به عنوان مجموعه ای از گره های به هم پیوسته هستند ،شبکه های اجتماعی بر پایه و اساس بازیگران متصل از طریق روابط ساخته شده است. استفاده از گراف یک ابزار قدرتمند بصری و وسیله رسمی برای نشان دادن شبکه های اجتماعی بکار برده شده است.

۲-۳-۱- چرا گراف ها ؟

نمادهای بسیاری برای نشان دادن شبکه های اجتماعی وجود دارد: نمادهای جبری، ماتریس، و گراف. شبکه های اجتماعی روابط ارزشی و ویژگی های مربوط به کاربر را نگه می دارند که نمادهای جبری نمی توانند آنها را اداره کنند. ماتریس ها عمدتا برای شبکه های کوچک کارآمد می باشد. در نتیجه، با توجه به اندازه بزرگ شبکه های اجتماعی، ماتریس ها مناسب ترین راه برای نشان دادن این شبکه ها نیستند. برای نشان دادن یک شبکه اجتماعی با استفاده از ماتریس، یک ماتریس دو طرفه، که sociomatrix نامیده می شود، می تواند مورد استفاده قرار گیرد. sociomatrix شامل سطر و ستون است که دلالت بر بازیگران اجتماعی دارد، و شماره و یا نمادها در سلولی که دلالت بر روابط موجود هستند.در شکل ۱ نمایش شبکه اجتماعی را به هر سه روش نشان داده ایم.



Node	1	2	3	4	5
1	0	0	0	0	1
2	0	0	1	1	1
3	0	1	0	1	0
4	0	1	1	0	1
5	1	1	0	1	0

شکل (۱) : نمایش شبکه های اجتماعی

بنابراین، بازنمایی مبتنی بر گراف به مراتب رایج ترین شکل برای مدل سازی شبکه های اجتماعی است [۳]. نمایش گرافیکی شبکه های اجتماعی باعث تسهیل درک، برچسب زدن و مدل سازی خواص بسیاری از این شبکه ها است. از این رو، گراف ها می توانند خواص مختلف داده های اجتماعی و ویژگی های خودشان را نشان دهند. جزئیات بیشتر در مورد مزایا و معایب هر یک از مدل ها در جدول زیر ارائه شده است.

جدول (۱) : نوع نمایش شبکه های اجتماعی(مزایا و معایب)

نوع نمایش	مزایای استفاده	معایب
نمادهای جبری	مفید برای شبکه های چند رابطه ای که به کمک آنها می توان براحتی ترکیبی از روابط را نشان داد.	نمی تواند روابط با ارزش و ویژگی های مربوط به کاربر را تحمل کند.
ماتریس ها	کارآمد برای شبکه های کوچک آسان برای نشان دادن روابط بین مجموعه ای از عامل ها (یک ماتریس برای هر رابطه) مسئولیت رسیدگی به شبکه های اجتماعی بزرگ	بهترین انتخاب برای شبکه های اجتماعی بزرگ نیست. برای استفاده دشوار است هنگامی که داده های شبکه شامل اطلاعات در صفات باشند. تکنیک های تجسم

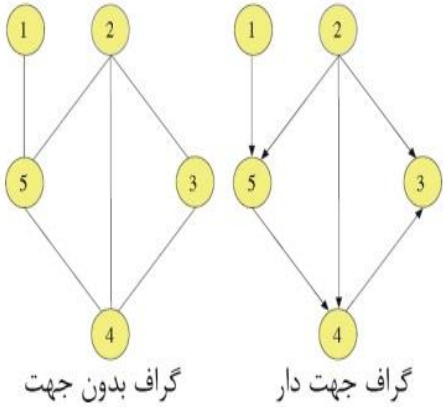
مقیاس پذیر مورد نیاز است.		
گراف های علامت دار و با ارزش دارند که مورد استفاده قرار می گیرد برای نشان دادن روابط با ارزش	واژگان غنی که به راحتی شبکه های اجتماعی را مدل می کند، فراهم می کند. (برچسب، ارزش ها، وزن، و غیره) عملیات ریاضی را فراهم می کند که که می تواند برای تعیین کمیت خواص ساختاری و اثبات قضایای مبتنی بر گراف استفاده شود	گراف ها

۲-۳-۲- نمایش گراف

گراف ها معمولا برای نمایش شبکه ها در زمینه های مختلف از قبیل زیست شناسی، جامعه شناسی و علوم کامپیوتر مورد استفاده قرار می گیرند [۴]. گرافها از گره ها برای نشان دادن بازیگران تشکیل شده اند ، و لبه ها برای نشان دادن روابط. شرایط گره ها و اشیاء معمولا به معنی بازیگران استفاده می شود. به همین ترتیب، لبه ها نیز ممکن است پیوند ها یا روابط نامیده شود. گره ها با لبه های متعدد برای نشان دادن جفت روابط از بازیگران مربوط با بیش از یک رابطه استفاده می شود. بیشتر به طور رسمی، یک گراف(G = (V, E ،شامل مجموعه ای از گره ها V، و مجموعه ای از لبه ها ، E است. تعداد عناصری که در V و E هستند، به ترتیب اشاره به n = | | V | | تعداد گره ها و m = | | E | | تعداد لبه ها دارد. برای نشان دادن اشکال مختلف از داده ها و برای مدل خواص ساختاری از شبکه های اجتماعی،گراف ها می توانند لبه داشته باشند و گره ها برچسب دار یا بدون برچسب باشند ، وزن دار یا بدون وزن باشند و که در ادامه توضیح می دهیم.

۲-۳-۳- گراف های جهت دار و بدون جهت

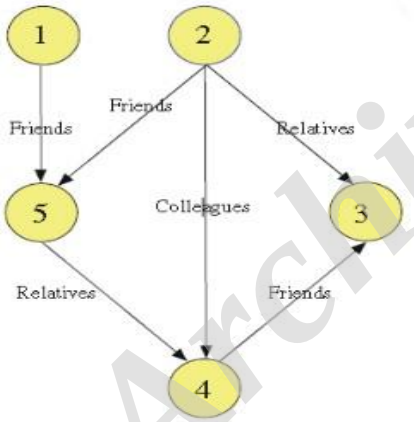
در گراف بدون جهت ، ترتیب رئوس متصل به لبه مهم نیست. ما به هر لینک توسط یک زوج به گره i و j مانند E(I,j) و یا eij، مراجعه می کنیم i و j پایان گره ها از لینک هستند. گرافی جهت دار است که توسط مجموعه ای از گره ها و مجموعه ای از لبه های جهت دار تعریف شده باشد. ترتیب دو گره مهم است: eij نشان دهنده لینک از i به j ، و و eij ≠ EJi . جهت لینک ها را گرافیکی نشان می دهند و لبه های جهت دار توسط فلش به تصویر کشیده است . بسته به نوع ماهیت ارتباط (نامتقارن و یا متقارن)، نمودار شبکه اجتماعی را می توان بدون جهت و یا جهت دار نشان داد . در واقع، شبکه های اجتماعی را می توان به عنوان گراف های بدون جهت مدل کرد هنگامی که روابط بین بازیگران متقابل هستند . (به عنوان مثال، روابط متقارن در فیس بوک جایی که eij یا eji هر دو معنی یک لینک دوستی بین کاربرi و کاربرJ). شبکه های اجتماعی نیز می تواند به عنوان گراف جهت دار مدل سازی کرد هنگامی که روابط دو طرفه نیستند. در شکل ۲ به ترتیب، یک نماینده از گراف بدون جهت و گراف جهت دار که هر دو با N = 5 (تعداد گره) و M = 6 (تعداد یال) هستند را نشان می دهیم.



شکل (۲) : گراف های جهت دار و بدون جهت

۲-۳-٤- گراف های برچسب دار و بدون برچسب

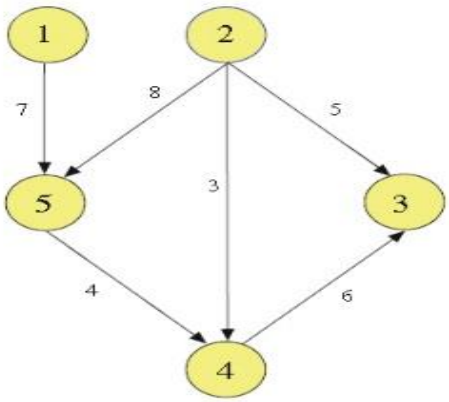
برچسب ها مهم هستند زیرا آنها می توانند به نوع روابط بین شناسایی بازیگران شبکه های اجتماعی باشند. هنگامی که گراف ها برچسب گذاری می شوند ، این بدان معنی است که یک برچسب استفاده می شود برای نشان دادن نوع لینک که ارتباط بین گره های متصل به برچسب مشخص می شود. شکل ۳ یک گراف برچسب دار که در آن نوع ارتباط بین بازیگران مرتبط نشان داده شده است را نشان می دهد. در شبکه های اجتماعی، ارتباط را می توان برای سازماندهی اطلاعات تماس بر اساس نوع ارتباط آنها استفاده کرد.



شکل (۳) : گراف برچسب دار

۲-۳-۵- گراف های وزن دار و بدون وزن

وزن نشان دهنده قدرت روابط بین بازیگران شبکه های اجتماعی است. هنگامی که گراف ها وزن دار هستند ، این بدان معنی است که لبه های آنها با اختصاص وزن عددی W است ، که می تواند نشانه های مختلف از قبیل ظرفیت لینک ارائه ، قدرت لینک ، سطح تعامل یا شباهت بین گره های متصل (به عنوان مثال،تعداد پیام هایی که بازیگران رد و بدل کرده اند و تعداد دوستان مشترک) را نشان دهد. شکل ۴ یک گراف وزن دار (در مقیاس ۰ تا ۱۰) را نشان می دهد که در آن مقادیر عددی به لینک اختصاص داده و سطحی از تعامل بین بازیگران شبکه اجتماعی را نشان می دهد.



شکل (٤) : گراف وزن دار

۳- داده های شبکه های اجتماعی

شبکه های اجتماعی به پلت فرم مهمی برای اتصال کاربران، به اشتراک گذاری اطلاعات و منبع ارزشمندی از داده های شبکه اجتماعی تبدیل شده اند. بنابراین، در دسترس بودن چنین داده هایی نشان دهنده فرصتی برای برای مطالعه مردم و تجزیه و تحلیل این شبکه ها است. با این حال، منابع مختلف داده ها در شبکه های اجتماعی نه تنها به عنوان درک مجموعه ای از ارزش ها و مخازن دانش است، بلکه در دسترس بودن آنها تبدیل به شکلی از تهدید می شود و به وسیله آنها می توان توسط مهاجمان به افشای اطلاعات مختلف حساس پرداخت.

۳-۱- داده ها چگونه جمع آوری شده اند؟

به طور سنتی، بسیاری از داده های شبکه های اجتماعی از طریق پرسشنامه به منظور مطالعه شبکه ها جمع آوری می شوند. این مطالعات می تواند بصورت مصاحبه چهره به چهره ،نظرسنجی تلفنی و یا پرسشنامه مبتنی بر کامپیوتر انجام شود.این روش های مرسوم، دارای محدودیت های بسیاری از نظر مقیاس پذیری، ذهنیت، تناقض و غیره می باشد.امروزه استفاده از روش استخراج داده های الکترونیکی در جمع آوری داده های شبکه های مرتبط سودمند بوده است، و موفقیت خود را به گسترش حوزه های مختلف نشان داده است[۵]. بسیاری از سیستم های شبکه های اجتماعی توسعه یافته برای جمع آوری داده ها و و تجزیه و تحلیل ساخته شده اند. در حال حاضر، شبکه های اجتماعی به کاربران برای تبادل انواع اطلاعات از جمله پیام ها، عکس ها و مطالب را اجازه می دهد.

٤- توسعه و تدابیر در شبکه های اجتماعی

تجزیه و تحلیل شبکه های اجتماعی در حوزه های برنامه های مختلف از جمله به عنوان شبکه های ارتباطی ایمیل ، شبکه یادگیری ، شبکه های تروریستی و شبکه های اجتماعی آنلاین استفاده شده است [۶]. این آثار تلاش برای پاسخ به تعداد انگشت شماری از سوالات است از جمله نحوه متصل شدن یک بازیگر در شبکه چگونه است ؟ با نفوذ ترین بازیگران در شبکه چه کسانی هستند؟یک بازیگر در یک شبکه چگونه مرکزی دارد؟ مرکزیت شامل جهت اهمیت دادن به بازیگران از یک گراف با استفاده از اتصال خود در درون شبکه می باشد. چند معیار مبتنی بر ساختار برای محاسبه مرکزیت یک بازیگر در یک شبکه مانند درجه، نزدیکی، و بین مرکزیت بودن ارائه شده است.

۵- تهدیدات حریم خصوصی

در دسترس بودن داده های شبکه های اجتماعی نگاه های جامعه دانشگاهی ، تبلیغات شخص ثالث و خدمات دولتی به منظور تجزیه و تحلیل داده ها را به خود جلب کرده است. بی نام کردن این شبکه ها قبل از آزاد کردن آنها برای به اجرا درآوردن حفظ حریم خصوصی مهم است. یک مهاجم می تواند به طور بالقوه با اشاره به هدف قرار دادن ساختار شبکه و با استفاده از دانش پس زمینه به هویت واقعی کاربران پی بردد. بی نام کردن اطلاعات شبکه های اجتماعی بسیار چالش برانگیز تر از بی نام کردن داده های رابطه ای است [۷]. همانطور که قبلا گفته شد، شبکه های اجتماعی را می توان به عنوان گراف نشان داد و در نتیجه داده های شبکه های اجتماعی می تواند به صورت پیش پردازش شده باشد و از طریق اقدامات تجزیه و تحلیل شبکه های اجتماعی آنالیز کرد. علاقه زیادی به مطالعه شبکه های بی نام وجود دارد که هنگامی مهاجم اطلاعات پیش زمینه در مورد ساختار شبکه دارد.حملات متعددی در این شبکه ها وجود دارد. در نوع اول این حملات، حملات فعال هستند، که مهاجمان قادر به ایجاد تغییر در شبکه قبل از انتشار آن بودند و به طور بالقوه می تواند با قرار دادن گره ها و لبه ها به شبکه ، زیر گراف بسیار قابل تشخیص ساخت.

حملات منفعل، نوع دیگری از حملات هستند که پس از بی نام کردن شبکه و بدون قرار دادن گره ها و یا لبه جدید منتشر می شوند. به طور خاص، اطلاعات ساختاری ن مربوط بهزدیک ترین درجات از گره ها و همسایگان خود در یک شبکه است.می توان اشاره کرد که درجه یک گره در یک گراف، در میان دیگر ویژگی های ساختاری، می تواند تا حد زیادی باعث تشخیص گره از گره های دیگر بشود. در نتیجه، حملات می تواند تا حد زیادی از ویژگی های ساختاری شبکه که تبدیل به ویژگی های شناسایی می شود، بهره مند شوند. هر شبکه اجتماعی که تمام تلاش خود را در راستای اجرای حفظ حریم خصوصی کاربران دارد باید دقت زیادی در کاهش آسیب پذیری از روابط آن داشته باشد، به وسیله نمایش ندادن تعداد دقیق اتصالات که هر یک از کاربران دارند. به طور خلاصه، تجزیه و تحلیل شبکه های اجتماعی به مجموعه ای از اقدامات که به طور گسترده برای مطالعه ویژگی های شبکه ها و رفتارهای کاربران فراهم می کند استفاده می شود. حملات حریم شخصی کاربران می توانند از مزایای تجزیه و تحلیل شبکه های اجتماعی برای پی بردن به دانش بیشتر درباره کاربران شبکه های اجتماعی با استفاده از اطلاعات ساختاری استفاده کنند. علاوه بر این، گسترش شبکه های اجتماعی آنلاین منجر به ایجاد و تولید مقدار بسیار عظیمی از داده های در دسترس در شبکه ها است. یک ضرورت مهم که شبکه های اجتماعی اجرا میکنند ، حفاظت از حریم خصوصی داده های خود و و کاربران و همچنین ارتباطات بین کاربران است[۸].

٦- لینک کاوی : وظایف و تهدیدات

با توجه به محبوبیت شبکه جهانی وب، افزایش قدرت محاسباتی و عملکرد، و ظرفیت بالاتر برای جمع آوری و تجزیه و تحلیل داده ها، در مقیاس بزرگ مطالعات شبکه های اجتماعی در حال شکوفایی هستند. مطالعات لینک کاوی با هدف کشف اطلاعات با ارزش و ذاتی از پایگاه داده های بزرگ مربوط به حفظ حریم خصوصی بسیار کارآمد می باشد[۹]. در حالی که اقدامات مرکزیت به طور گسترده ای در تجزیه و تحلیل شبکه های اجتماعی استفاده می شود ، تکنیک های لینک کاوی بر پیشرفتهای اخیر در داده کاوی تکیه می کند و تاکید بر پیوند بین بازیگران شبکه اجتماعی قرار می دهد [۱۰]. در ادامه، ما وظایف مربوط به لینک کاوی را قبل از توصیف تهدیدات حریم خصوصی مربوط به هر وظیفه توصیف می کنیم.

٦-١- توسعه و وظایف

با توجه به ارتباط بین بازیگران شبکه اجتماعی،تکنیک های مختلف داده کاوی در ظهور یک منطقه جدید عادی به نام لینک کاوی کمک می کنند که لینک ها هستند که نشان دهنده الگوهای غنی مرکزی در استخراج دانش پنهان از داده های در دسترس هستند. تجزیه و تحلیل لینک، یادگیری رابطه ای، وب کاوی و گراف کاوی به طور گسترده در میان تکنیک های مورد استفاده در لینک کاوی هستند. با ساخت مدل های ارزیابی ، لینک کاوی می تواند به عنوان داده کاوی کاربردی در شبکه های اجتماعی مورد استفاده قرار گیرد که در آن ها نقش کلیدی ایفا می کنند. نه تنها لینک های شبکه را می توان برای کشف بازیگران برجسته در یک شبکه مورد استفاده قرار داد بلکه به فاش کردن اطلاعات کشف شده مربوط به هویت، کلاس ها و روابط بین بازیگران کمک می کند[۱۱] . در زیر، ما جزئیات تمام وظایفی که بر عهده لینک کاوی است را توضیح می دهیم.

٦-١-١- رویکردهای مربوط به گره

الف) رتبه بندی گره مبتنی بر لینک: هدف از رتبه بندی گره مبتنی بر لینک اولویت بندی بر اساس اهمیت اندازه گیری گره مربوطه می باشد.در لینک کاوی، اندازه گیری مرکزیت (به عنوان مثال، درجه، نزدیکی، و مابین) برای رتبه بندی گره ها به وسیله استخراج ساختار شبکه مورد استفاده قرار می گیرد[۱۲].

ب) رده بندی گره مبتنی بر لینک: رده بندی گره مبتنی بر لینک وظیفه رده بندی گره ها از یک شبکه به یک مجموعه متناهی دسته را را دارد . این نوع از رتبه بندی نه تنها بر صفات گره بلکه بر روی لینک خود بر دیگر گره ها و با ویژگی های این گره در ارتباط است.

ج) خوشه بندی گره مبتنی بر لینک: خوشه بندی گره، گروه اکتشاف نیز نامیده می شود ، هدف آن این است که برای شناسایی گره مشابه و گروه آنها با هم بدون پیش بینی خوشه این کار انجام شود. هردو گره، عضو یک خوشه مشابه، بیشتر شبیه به یکدیگر هستند تا گره دیگر در یک خوشه دیگر.

٦-١-٢- رویکردهای مربوط به لینک

الف) ارزیابی لینک : ارزیابی لینک و یا ارزیابی وجود لینک،وظیفه استنتاج وجود لینک بین دو گره ، بر اساس خواص گره ها است.

ب) ارزیابی نوع لینک : بر خلاف پیش بینی لینک، که در آن هدف پیش بینی وجود ارتباط بین دو گره در یک زمان خاص است، هدف ارزیابی نوع لینک شناسایی نوع لینک های موجود است به عنوان مثال، نوع ارتباط بین دو بازیگر.

٦-١-٣- رویکردهای مربوط به گراف

الف) اکتشاف زیرگراف ها : اکتشاف زیر گراف یکی از وظایف لینک کاوی است که زیرگراف های مشابه در جفت هایی از گرافها را کشف می کند. هدف آن پیدا کردن مجموعه ای از گراف که در میان گرافهای اصولی مشابه هستند.

ب) رده بندی گراف : هدف رده بندی گراف طبقه بندی کل گراف با توجه به رده خاص می باشد. طبقه بندی مستقل هر گره در یک گراف بزرگ کار خسته کننده ای است، گاهی اوقات غیر عملی است، و ممکن است اطلاعات مفید در دسترس از گره های دیگر چشم پوشی شود. نسبتا بیشتر تلاش می شود هر گره در گراف برچسب گذاری و طبقه بندی دسته جمعی شود.

ج) مدل های تولیدی مبتنی بر گراف : مدل تولیدی برای گراف ها سعی می کند به درک ویژگی های شبکه برسیم. با توجه به ورودی شبکه،مدل های مولد می تواند یک شبکه جدید شبیه به ورودی تولید کند. آنهامی توانند با شباهت ساختار و توزیع داده ها به درستی مدل آنها استفاده کند.

٦-٢- تهدیدات حریم شخصی

نگرانی های کاربران در مورد حفظ حریم خصوصی از اطلاعات شخصی خود اخیر در نوع لینک کاوی قرار گرفته است.ما در ادامه وظیفه هر لینک کاوی که می تواند توسط مهاجمان و یا کاربران مخرب مورد سوء استفاده قرار گیرد را توصیف می کنیم.

٦-٢-١- تهدیدات گره های مرتبط

کاربران شبکه های اجتماعی انتظارات قوی از حریم خصوصی دارند. ردیابی تعامل کاربران و بازسازی جزئیات از رفتارهای خود را معمولا مورد توجه قرار نمی دهند . با این حال، رتبه بندی گره مبتنی بر لینک را می توان برای اندازه گیری تاثیر و اهمیت از کاربران شبکه های اجتماعی مورد استفاده قرار داد. بهره برداری از ساختار شبکه امکان پی بردن به روابط معنی دار و تعیین کمیت تعاملات بین کاربران شبکه های اجتماعی است. شناسایی کاربران با نفوذ، که قادر به تحریک کاربران دیگر میباشد، از اهمیت قابل توجهی در بسیاری از حالات دارد[۱۳]. با افزایش تعداد کاربران شبکه های اجتماعی، رتبه بندی گره مبتنی بر لینک در بسیاری از مناطق مانند بازاریابی، انتشار اطلاعات کاربردی و وظایف جمع آوری اطلاعات دولتی به کار برده می شود. پیامدهای حفظ حریم خصوصی از طبقه بندی گره مبتنی بر لینک و گره مبتنی بر لینک خوشه می تواند اطلاعات حساسی مانند عضویت به یک گروه خاص و یا یک حزب سیاسی باشد. طبقه بندی گره و خوشه گره به طور عمده در زمینه امنیت کامپیوتر استفاده شده است. آنها فراتر از یک مورد ساده از شبکه اجتماعی و تبلیغات هدفمند گسترش یافته اند برای رسیدن به کاربردهای حساس مانند شبکه های تروریستی. علاوه بر مشخصات معمول صفات، این فعالیت ها و تعاملات کاربران در طول زمان در میان مهم ترین

منابع اطلاعات هستند. این فعالیت ها و تعاملات آنلاین در صورتهای مختلفی از قبیل برقراری ارتباط ،پیام های مبادله و انتشار عکس آمده است[۱۴]. تکنیک های خوشه بندی گره های مبتنی بر لینک یک منبع بالقوه از تهدیدات حریم خصوصی است.آنها توسط کاربران گروهی که فعالیت مشابه دارند مورد استفاده قرار می گیرد.

٦-۲-۲- تهدید لینک های مرتبط

پیش بینی لینک می تواند نگرانی های حریم خصوصی را افزایش دهد زمانی که لینک پیش بینی شده بین کاربرانی که می خواهند رابطه خود را به صورت خصوصی حفظ کنند.در بسیاری از موارد، لینک می تواند به صورت اطلاعات حساس برای نگهداری داده های حفاظت شده مطرح شود. حملات ناشی ازپیش بینی نوع لینک ها می تواند نوع حساسی از وجود آشکار رابطه دو کاربر در حریم خصوصی باشد که بایستی حفظ شود. بر خلاف پیش بینی لینک، پیش بینی نوع لینک در حفظ خصوصی مربوط به نوع رابطه بین دو کاربر است. این نوع حمله به عنوان لینک شناخته شده است. این حمله زمانی اتفاق می افتد که یک مهاجم قادر به شناسایی هویت فرد در رابطه بین دو کاربر می شود[۱۵]. لینک می تواند دقت و صحت اطلاعات طبقه بندی شده را هنگام تلاش مهاجم به شناسایی اطلاعات مربوط به منافع شخصی، مکان فیزیکی و وابستگی های سیاسی را شناسایی کند.به عنوان مثال، لینک های دوستی مهم تر از لینک های حرفه ای برای پی بردن به منافع شخصی هستند.به عنوان مثال، وابستگی های سیاسی و باورهای دینی، به خصوص اگرتعداد قابل توجهی از دوستان به طور علنی در پروفایل خود چنین طلاعات حساس شخصی خود را به نمایش گذاشته باشند.

٦-۲-۳- تهدیدات وابستگی گراف

حملات تلاش برای کشف زیرگراف برای به دست آوردن اطلاعات جدید در مورد شبکه ناشناخته با استفاده از زیرگراف ساختاری نمایش داده می شود . زیرگراف به شکلی موثر در ساختارهای مشابه در شبکه های اجتماعی بزرگ مفید هستند که با استفاده از دو نوع اصلی از حملات نمایش داده می شوند : حملات فعال و غیر فعال[۱۶]. در هر دو نوع از حملات، اطلاعات ساختاری استفاده شده برای نشان دادن هویت های واقعی کاربران را مورد هدف قرار می دهد.در نتیجه حملات کشف زیر گراف می تواند برای سازش حریم خصوصی کاربران و بالا بردن هویت خود مخاطبین و مشکلات افشای لینک های اجتماعی مورد استفاده قرار گیرد.

۷- نتیجه

در این تحقیق ما یک دید کلی در مورد حفظ حریم خصوصی در شبکه های اجتماعی معرفی کردیم و معانی مختلف و متمایز، درک ویژگی های شبکه اجتماعی را توضیح دادیم. ما در شبکه اجتماعی اقدامات تجزیه و تحلیل های مختلف و تکنیک های لینک کاوی را بررسی کردیم. از همه چالش های شبکه های اجتماعی، حمایت از حریم خصوصی برای همه کاربران بسیار مهم است. عدم امکان تامین حفاظت مطلوب از حفظ حریم خصوصی ممکن است عواقب نامطلوب در محبوبیت شبکه های اجتماعی و از جمله در میزان اطلاعاتی که کاربران شبکه های اجتماعی در حال حاضر به اشتراک می گذارند ، داشته باشد. بنابراین سایت های شبکه های اجتماعی باید به کاربران خود انواع ابزار های پشتیبانی را ارائه دهند.

مراجع

[1] Liu, Y., Gummadi, K.P., Krishnamurthy, B., Mislove, A.: Analyzing facebook privacy settings: user expectations vs. reality. In: Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference. IMC '11, pp. 61–70. ACM, New York (2011)

[2] Zhang, C., Sun, J., Zhu, X., Fang, Y.: Privacy and security for online social networks: challenges and opportunities. IEEE Netw. 24(4), 13–18 (2010)

[3] Newman, M.: The structure and function of complex networks. SIAM Rev. 45(2), 167–256 (2003)

[4] Fortunato, S.: Community detection in graphs. Phys. Rep. 486(3–5), 75–174 (2010)

[5] Gonzalez-Bailon, S.: Opening the black box of link formation: Social factors underlying the structure of the web. Soc. Network 31(4), 271–280 (2009)

[6] Mislove, A., Marcon, M., Gummadi, K.P., Druschel, P., Bhattacharjee, B.: Measurement and analysis of online social networks. In: Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement. IMC '07, pp. 29–42. ACM, New York (2007)

[7] Zhou, B., Pei, J.: The k-anonymity and l-diversity approaches for privacy preservation in social networks against neighborhood attacks. Knowl. Inform. Syst. 28(1), 47–77 (2011)

[8] Liu, K., Terzi, E.: Towards identity anonymization on graphs. In: Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data. SIGMOD '08, pp. 93–106. ACM, New York (2008)

[9] Zheleva, E., Getoor, L.: Preserving the privacy of sensitive relationships in graph data. In: Bonchi, F., Ferrari, E., Malin, B., Saygin, Y. (eds.) Privacy, Security, and Trust in KDD.Volume 4890 of Lecture Notes in Computer Science, pp. 53–171. Springer, Berlin/Heidelberg (2008)

[10] Getoor, L., Diehl, C.P.: Link mining: a survey. SIGKDD Explor. Newsl. 7(2), 3–12 (2005)

[11] [11]. Wu, X., Kumar, V., Ross, Q., Ghosh, J., Yang, Q.,Motoda, H.,McLachlan, G., Ng, A., Liu, B., Yu, P., Zhou, Z.H., Steinbach, M., Hand, D., Steinberg, D.: Top 10 algorithms in data mining. Knowl. Inform. Syst. 14(1), 1–37 (2008)

[12] Lin, Z., Wang, L., Guo, S.: Recommendations on social network sites: From link mining perspective. In: International Conference on Management and Service Science, 2009. MASS '09, pp. 1–4 (Sept. 2009)

[13] Segal, E.,Wang, H., Koller, D.: Discovering molecular pathways from protein interaction Bioinformatics 19(SUPPL. 1), i264–i272 (2003)

[14] Adali, S., Sisenda, F., Magdon-Ismail, M.: Actions speak as loud as words: predicting relationships from social behavior data. In: Proceedings of the 21st International Conference on World Wide Web. WWW '12, pp. 689–698. ACM, New York (2012)

[15] Zheleva, E., Getoor, L.: Preserving the privacy of sensitive relationships in graph data. In: Bonchi, F., Ferrari, E., Malin, B., Saygin, Y. (eds.) Privacy, Security, and Trust in KDD. Volume 4890 of Lecture Notes in Computer Science, pp. 53–171. Springer, Berlin/Heidelberg (2008)

[16] Hay, M., Miklau, G., Jensen, D., Towsley, D., Li, C.: Resisting structural re-identification in anonymized social networks. VLDB J. 19(6), 797–823 (2010)