یکشنبه 09 بهمن 1390 - 11:58

حفظ اطلاعات کاربران در اینترنت

با گسترش ارتباطات اينترنتي هر روز بيشتر از گذشته، مصاديق مختلف فناوري اطلاعات در زندگي تك‌تك ما رسوخ مي‌كند.

جام جم آنلاين: با گسترش ارتباطات اينترنتي هر روز بيشتر از گذشته، مصاديق مختلف فناوري اطلاعات در زندگي تك‌تك ما رسوخ مي‌كند.
در كنار مزايايي كه اين فضا در اختيارمان قرار مي‌دهد، همانند اجتماعات ديگر، هميشه خطر برملا شدن اسرار خصوصي شما توسط دزدان مجازي و هكرها وجود دارد.

اين موضوع تنها به كاربران شبكه‌هاي اجتماعي مربوط نمي‌شود، امكان نفوذ هكرها به اطلاعات مراكز پزشكي در زماني كه اين داده‌ها به منظور اجراي پروژه‌هاي تحقيقاتي منتشر مي‌شود هم وجود دارد.

به همين دليل امروزه حفظ حريم خصوصي و محافظت از اطلاعات كاربران، يكي از دغدغه‌هاي اصلي شبكه‌هاي مختلف است كه باعث شده تلاش براي حفظ امنيت كاربران بيش از گذشته مورد توجه قرار گيرد.

بر همين اساس، پژوهشگران دانشكده مهندسي كامپيوتر و فناوري اطلاعات دانشگاه صنعتي اميركبير موفق به ارائه مدلي براي حفظ حريم خصوصي داده‌هاي منتشر شده در شبكه‌هاي اجتماعي شدند.

مهندس احمد سحرخيز، طراح اين مدل و كارشناس ارشد مهندسي فناوري اطلاعات با گرايش امنيت اطلاعات، درباره كاركردهاي اين مدل امنيتي مي‌گويد.

حفظ امنيت اطلاعات كاربران اينترنت و شبكه‌هاي مختلف چقدر مهم است و در اين زمينه شبكه‌هاي اجتماعي مختلف چه راهكارهايي را به اعضاي خود ارائه كرده‌اند؟

امروزه با توجه به رشد اثرگذاري رايانه‌ها و سيستم‌هاي مرتبط با رايانه در زندگي مردم در بيشتر جوامع، برقراري راهكارهاي امنيتي جهت حفظ منافع افراد امري ضروري به شمار مي‌رود. در دنياي مجازي، تراكنش‌هاي مالي توسط هر فرد به طور مجزا مي‌تواند صورت گيرد، ارتباطات مختلفي بين افراد به وجود بيايد و به طور كلي از هر واقعيتي در دنياي مادي، مي‌تواند نمودي در دنياي مجازي وجود داشته باشد. اگر كاربران دنياي مجازي، بخصوص كاربران اينترنت احساس امنيت نكنند، ناچار به ترك استفاده از اين ابزارهاي ارزشمند خواهند شد. بعلاوه هر آسيب پذيري امنيتي مي‌تواند باعث ايجاد رخدادهاي مخربي شود كه آثار آن حتي گريبانگير يك جامعه بزرگ شود.

امروزه شبكه‌هاي اجتماعي، محيطي را براي ايجاد ارتباطات بين افراد فراهم كرده‌اند. اين نوع ارتباطات مي‌تواند در ساده‌ترين حالت، ارتباط دوستانه باشد يا ارتباطات ديگري مانند ارتباطات دانشجويان و استادان، پزشكان، پرستاران و بيماران را شامل شوند.

اينچنين ارتباطات در حالي روز به روز گسترش بيشتري مي‌يابند كه يكي از مهم‌ترين نيازهاي افرادي كه در شبكه‌هاي اجتماعي قرار دارند، حفظ حريم خصوصي آنهاست. اين مساله در دوبعد قابل بررسي است.

يكي حفظ حريم خصوصي آنها در لحظه‌اي كه در شبكه‌هاي اجتماعي مشغول فعاليت هستند و ديگري زماني كه داده‌هاي آنها از سوي مراكز سرويس‌دهنده به منظور اجراي پروژه‌هاي تحقيقاتي منتشر مي‌شود.

بعد دوم، موضوعي است كه از حدود سال 2007 مورد توجه دانشمندان قرار گرفته است. تاكنون در اين زمينه، حملاتي عليه حريم خصوصي داده‌هاي منتشر شده شبكه‌هاي اجتماعي شناسايي شده‌اند و براي هر كدام از آنها مدل‌هايي با داشتن نواقصي ارائه شده است البته تعداد اين حملات و مدل‌ها بسيار محدود است و اين نشان مي‌دهد چنين مبحثي در دنياي علم، جاي تفكر و انديشه دارد.

مدلي كه شما براي حفظ حريم خصوصي داده‌هاي منتشر شده در شبكه‌هاي اجتماعي در مقابل برخي از اين حملات ارائه كرده‌ايد، دقيقا چيست؟

در مدلي كه ارائه كرده‌ايم، حملات همسايگي را مورد توجه قرار داده‌ايم. با استفاده از اين مدل، مي‌توان داده‌هاي هر نوع شبكه اجتماعي را منتشر كرد و از حفظ حريم خصوصي افراد در برابر حملات همسايگي از هر مرتبه‌اي اطمينان حاصل كرد.

اين نوع حمله براي نخستين بار در سال 2008 مطرح شد و تاكنون هيچ مدل جامعي كه براي تمام شبكه‌هاي اجتماعي از هر نوعي و بخصوص در برابر حملات همسايگي از هر مرتبه‌اي كاربرد داشته باشد، ارائه نشده بود.

لطفا درباره حملات همسايگي توضيح دهيد. در اين خصوص چه مطالعاتي صورت گرفته است؟

به طور كلي، حملات همسايگي، نوعي ازحملات با دانش قبلي هستند. در اين نوع حمله، فرد مهاجم با اطلاعاتي كه از ارتباطات همسايگي فرد قرباني در شبكه اجتماعي دارد، مي‌تواند وي را در شبكه اجتماعي منتشر شده شناسايي كند و به اين وسيله خواهد توانست حريم خصوصي فرد قرباني و افراد زياد ديگري را به واسطه آن نقض كند.

به اين ترتيب، حملات همسايگي مرتبه اول مورد مطالعه قرار گرفت سپس روند پژوهش به سمت حملات همسايگي از هر مرتبه‌اي همگرا شد. متاسفانه مدل خاصي در اين زمينه ارائه نشده بود كه اين موضوع نيز بر سختي كار مي‌افزود.

حملات با دانش قبلي يعني چه؟

اين موضوع به بعد دوم حفظ حريم خصوصي برمي‌گردد؛ زماني كه داده‌هاي انبوهي براي تحليل و داده كاوي منتشر مي‌شوند، مستقل از تحليل‌ها و نتايج ارزشمند، ممكن است حريم خصوصي اطلاعات افرادي كه در داده‌هاي انبوه حضور داشته‌اند، نقض شود. اين مساله با راهكارهاي ساده مانند حذف هويت‌هاي منحصر به فرد قابل حل نيست. چراكه ممكن است فرد مهاجم براي دستيابي به اطلاعات شخصي افراد در اين داده‌ها، با استفاده از اطلاعات و دانش قبلي خود بتواند حريم خصوصي يك يا تعدادي از افراد را نقض كند. اين در حالي است كه داده‌هاي انبوه مي‌تواند داده‌هاي شبكه‌هاي اجتماعي باشد كه ساختارهاي بسيار پيچيده و اطلاعات خصوصي زيادي را از افراد در بردارند.

آيا مدل شما در شبكه‌هاي اجتماعي همچون فيس‌بوك، توييتر، گوگل پلاس و... كاربرد دارد يا منظور از شبكه‌هاي اجتماعي، چيز ديگري است؟

سحرخيز: حفظ حريم خصوصي، موضوع تازه‌اي است و هنوز حملات زيادي در اين حوزه ناشناخته مانده‌اند، به همين دليل شبكه‌هاي اجتماعي تاكنون تنها از مدل‌هاي محدودي براي حفظ حريم خصوصي كاربران خود استفاده مي‌كرده‌اند
اين مدل مي‌تواند روي هر شبكه اجتماعي اعمال شود. براي توضيح بيشتر، لازم است بگويم شبكه‌هاي اجتماعي مي‌توانند بين موجوديت‌هايشان، يك يا چند نوع ارتباط در نظر بگيرند. به عنوان مثال در يك شبكه اجتماعي ارتباطات همكاري، دوستي، تحقيقاتي و از اين قبيل بين افراد مختلف وجود داشته باشد. همچنين برخي ارتباطات ممكن است محرمانه يا حساس باشند يا اين‌كه اطلاعات محرمانه‌اي را در بر داشته باشند. ويژگي منحصر به فرد اين مدل، پوشش دادن تمام شبكه‌هاي اجتماعي از هر نوع است، بخصوص اين كه ارتباطات و اطلاعات حساس و محرمانه را هم مورد توجه قرار مي‌دهد.

مگر خود اين شبكه‌ها براي حفظ امنيت كاربرانشان، سيستم‌ها و ابزارهاي لازم را به كار نمي‌برند؟

با توجه به اين‌كه بحث حفظ حريم خصوصي طبق آنچه گفته شد، موضوع تازه‌اي است و هنوز حملات زيادي در اين حوزه ناشناخته مانده‌اند، به همين دليل اين شبكه‌ها تاكنون تنها از مدل‌هاي موجود براي حفظ حريم خصوصي كاربران خود استفاده مي‌كرده‌اند.

به عنوان مثال، تاكنون هر سازماني كه داده‌هاي شبكه‌هاي اجتماعي خود را به منظور مطالعات و تحقيقات منتشر مي‌كرده است، به حملات همسايگي از هر مرتبه‌اي، نمي‌توانسته توجه كند، زيرا مدلي براي مقابله با اين حملات، تاقبل از اين مدل وجود نداشته است. بخصوص زماني اين مساله بيشتر ملموس بوده است كه شبكه‌هاي اجتماعي چند رابطه‌اي به عنوان داده‌هاي منتشر شده انتخاب مي‌شدند.

براي فهم بيشتر آنچه در اين پروژه انجام شده است، به زبان ساده مراحل طراحي اين مدل را توضيح دهيد؟

در اين مدل، هويت‌هاي منحصر به فرد افراد كه تاثير ويژه‌اي بر نتايج داده‌كاوي و تحليل‌هاي آماري روي داده‌هاي انبوه ندارند، حذف مي‌شود. اين مدل در چهار گام كلي اجرا مي‌شود، ابتدا شناسايي و استخراج همسايگي‌هاي دو فرد مورد بررسي قرار مي‌گيرد. سپس در گام دوم، معيارهايي براي هزينه‌هاي ناشي (مراحل كاري) از هرگونه تغيير در داده‌ها ارائه و محاسبه مي‌شود. در اين بخش، به

پارامترهاي مهمي اشاره شده است. بخصوص كه هزينه مربوط به ارتباطات مازاد براساس نوع ارتباط افزوده شده با استفاده از پارامتري در اختيار صاحبان داده‌ها قرار مي‌گيرد تا بتوان به حداكثر بازدهي در خروجي مدل دست يابيم. در گام سوم به بي‌نام‌سازي همسايگي‌هاي دو فرد پرداخته مي‌شود و در گام نهايي، با توجه به سه گام اول همسايگي‌هاي افراد شناسايي شده و با استفاده از بي‌نام‌سازي دو فرد و هزينه بي‌نام سازي، به تغيير در داده‌هاي اوليه مي‌پردازيم: به گونه‌اي كه كمترين هزينه تغييرات را در نهايت داشته باشيم. به اين شيوه با حداقل هزينه، داده‌هاي يك شبكه اجتماعي را مي‌توان منتشر كرد و از حفظ شدن حريم خصوصي افراد در مقابل حملات همسايگي اطمينان حاصل كرد.

اين مدل در چه بخش‌ها و سازمان‌هايي مي‌تواند كاربرد داشته باشد؟

امروزه بسياري از سازمان‌ها در سراسر دنيا، مانند بيمارستان‌ها در برخي كشورها، موظف به انتشار داده‌هاي خود هستند. تحليل و داده‌كاوي داده‌هاي انبوه مي‌تواند نتايج ارزشمند و مهمي را در اختيار قرار دهد. گاهي اين نتايج مي‌تواند كاهش چشمگير هزينه‌هاي هنگفت در يك سازمان يا حتي براي يك دولت و گاهي حتي شناسايي زودهنگام شيوع يك بيماري كشنده را در پي داشته باشد. با اين تفاسير، هر سازماني كه براي توسعه و پيشرفت به تحليل و داده‌كاوي داده‌هاي انبوه احتياج داشته باشد، يا سازماني باشد كه اطلاعات مفيدي از افراد را در اختيار داشته باشد كه منبع داده‌اي مناسبي براي ساير سازمان‌ها به شمار بيايد، مي‌تواند از اين مدل براي حفظ حريم خصوصي افراد در مقابل حملات همسايگي، قبل از اين‌كه داده‌ها را منتشر كند، استفاده كند.

ضريب امنيت اين مدل چقدر است و نسبت به موارد مشابه چه ويژگي‌هايي دارد؟

اين مدل با ويژگي‌هايي كه دارد، اولين بار است كه در دنيا ارائه شده است. تا قبل از اين، مدلي براي حملات همسايگي ارائه شده بود كه تنها حملات همسايگي مرتبه اول را پوشش مي‌داد. همچنين فقط براي شبكه‌هاي اجتماعي كه تنها از يك نوع رابطه تشكيل شده، قابل استفاده است. علاوه بر اينها، در آن مدل ـ كه از سوي دانشمندان دانشگاه Simon Fraser كانادا ارائه شده است ـ ارتباطات و اطلاعات حساس هم مورد توجه قرار نگرفته‌اند.

براي طراحي اين مدل، چه موضوعاتي را مد نظر قرار داده‌ايد؟

ارتباطات چندگانه در شبكه‌هاي اجتماعي يكي از مهم‌ترين ويژگي‌هايي بوده كه جامعيت مدل ارائه شده را رقم زده است. همچنين در اين مدل، تمام حملات همسايگي تحت پوشش قرار گرفته‌اند. اين نيز ويژگي مهم ديگر اين مدل است. در اين مدل، پارامترهاي متعددي در اختيار صاحبان داده‌ها قرار مي‌گيرد تا كيفيت داده‌هاي خروجي نيز حداكثر شود.

در نهايت با اجراي اين مدل، يك كاربر چقدر مي‌تواند از حضور امن در يك شبكه مطمئن باشد؟

اين موضوع اطميناني است كه مركز سرويس‌دهنده يك شبكه اجتماعي بايد به كاربران خود بدهد. در اين حالت، كاربران شبكه‌هاي اجتماعي مطمئن خواهند بود كه حريم خصوصي آنها در داده‌هاي منتشر شده در برابر برخي حملات با دانش قبلي، حفظ خواهد شد. در حال حاضر، كاربران در بيشتر شبكه‌هاي اجتماعي، مساله حريم خصوصي مربوط به انتشار داده‌ها توسط مراكز سرويس‌دهنده را بناچار ناديده مي‌گيرند و اين به دليل نبود ساز و كار مناسب براي اين منظور است.

بهاره صفوي - گروه دانش