بسم الله الرحمن الرحيم

**دانشگاه صنعتی اصفهان**
دانشکده برق و کامپیوتر

# حفظ حریم خصوصی در شبکه‌های اجتماعی

رساله دکترای مهندسی کامپیوتر

**فاطمه راجی**

استادان راهنما
**دکتر محمد داورپناه جزی**
**دکتر علی میری**

**۱۳۹۲**

**دانشگاه صنعتی اصفهان**
دانشکده برق و کامپیوتر

رساله دکترای رشته‌ی مهندسی کامپیوتر خانم فاطمه راجی

تحت عنوان

# حفظ حریم خصوصی در شبکه‌های اجتماعی

در تاریخ ۱۳۹۲/۱۱/۱۷ توسط کمیته‌ی تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت.

| | |
|---|---|
| ۱- استاد راهنمای رساله | دکتر محمد داورپناه جزی |
| ۲- استاد راهنمای رساله | دکتر علی میری |
| ۳- استاد مشاور رساله | دکتر مسعودرضا هاشمی |
| ۴- استاد داور | دکتر بهروز ترک‌لادانی |
| ۵- استاد داور | دکتر محمد حسین منشئی |
| ۶- استاد داور | دکتر محمد دخیل‌علیان |
| سرپرست تحصیلات تکمیلی دانشکده | دکتر سید محمدعلی خسروی‌فرد |

خداوند بزرگ را بسیار شاکرم که به من نعمت زندگی کردن عطا نمود و لطف خود را شامل حال من کرد تا بتوانم در مسیر علم و دانش گام بردارم.
بر خود لازم می‌دانم که از راهنمائی و تشویقهای آقای دکتر علی میری در کلیه مراحل انجام این پژوهش قدردانی نمایم. از آقایان دکتر محمد داورپناه-جزی و دکتر مسعودرضا هاشمی که یاریگر من در انجام موفق این رساله بودند، صمیمانه سپاسگزاری می‌کنم. از آقایان دکتر سلیمان‌فلاح، دکتر ترک‌لادانی، دکتر منشئی و دکتر دخیل‌علیان که زحمت داوری این رساله را متقبل شدند تشکر می‌نمایم. از آقایان دکتر خسروی‌فرد و دکتر عمومی نمایندگان تحصیلات تکمیلی دانشکده در جلسه دفاع سپاسگزاری می‌کنم. همچنین از کلیه معمان و اساتید دوران تحصیلم از ابتدا تاکنون تشکر و قدردانی می‌نمایم.
از پدر و مادر و همسرم که همواره پشت و پناهم بوده و بزرگترین نعمت خداوند برایم هستند، از صمیم قلب قدردانی می‌نمایم. از برادرانم سپاسگزاری می‌کنم که در نبود من در ایران، امور اداری تحصیلاتم را پیگیری می‌کردند. در آخر از بزرگترین سرمایه زندگی‌ام، صدرای کوچکم تشکر می‌نمایم.

تقدیم به حضرت دوست که هرچه دارم از اوست،

تقدیم به پدر و مادر عزیزم که دعای خیرشان همواره پشتیبان من است،

تقدیم به همسر مهربانم که همراهی‌اش بهانه‌ای برای ادامه راه من است و

تقدیم به پسر دلبندم که به شوق در آغوش کشیدن بی دغدغه‌اش، به انجام

رساندن این رساله بر من هموار گشت.

# فهرست مطالب

**عنوان** **صفحه**

## فهرست اشکال

**عنوان** **صفحه**

# فهرست جداول

**عنوان** **صفحه**

## چکیده

در سالهای اخیر، شبکه‌های اجتماعی آنلاین، رشد قابل توجهی از نظر تعداد کاربران و محبوبیت داشته‌اند. در شبکه‌های اجتماعی، کاربران از طریق اشتراک اطلاعات مختلف با یکدیگر در ارتباط هستند. یکی از مهمترین مشکلات شبکه‌های اجتماعی، فاش‌شدن اطلاعات خصوصی کاربران و در نتیجه نقض حریم خصوصی آنها می‌باشد. بخصوص اینکه فراهم‌کنندگان شبکه‌های اجتماعی، کنترل کاملی بر روی اطلاعات کاربران دارند. زیرا فراهم‌کنندگان، اطلاعات کاربران را بطور دائمی ذخیره کرده و از آنها در جهت مقاصد بازاریابی مورد استفاده قرار می‌دهند. از طرف دیگر تنظیمات حریم خصوصی گنجانده‌شده در این شبکه‌ها کنترل کاملی به کاربران در جهت مدیریت و خصوصی‌سازی دسترسی به اطلاعات اشتراکی‌شان توسط کاربران دیگر نمی‌دهد.

اخیراً کارهائی در جهت ارائه یک شبکه اجتماعی با حفظ حریم خصوصی کاربران انجام شده‌اند. ولی این روشها بطور دقیق نیازمندی حریم خصوصی کاربران در شبکه اجتماعی را مشخص نکرده‌اند. همچنین روشهای قبلی نتوانسته‌اند حریم خصوصی موردنیاز کاربران را فراهم کنند بطوریکه در بیشتر آنها هدف اصلی فقط حذف نقش فراهم‌کننده شبکه اجتماعی است. علاوه براین در این روشها مراحل اجرای عملیات اصلی کاربر در طول جلسه با شبکه اجتماعی به صورت واضح و روشن بیان نشده‌اند. در نهایت اینکه در تمامی این روشها تحلیل حریم خصوصی و تحلیل کارائی عملیات کاربر در شبکه اجتماعی نادیده گرفته شده‌اند.

در این رساله روشهائی در جهت طراحی یک شبکه اجتماعی با حفظ حریم خصوصی کاربران در معماریهای متمرکز، غیرمتمرکز و P2P با استفاده از سیستم رمزنگاری انتشار پیشنهاد داده می‌شوند تا نیازمندی حریم خصوصی کاربران را براساس ویژگیهای معماری مربوطه بطور کامل فراهم کنند. روش پیشنهادی مبتنی بر معماری متمرکز با بکارگیری طرف سوم معتمد و بهره‌گیری از اشتراک تنظیمات حریم خصوصی بین کاربران، بنا نهاده شده است. در روش پیشنهادی مبتنی بر معماری غیرمتمرکز اول، مدیریت کامل اشتراک و دسترسی به داده‌ها به خود کاربران، محول می‌شود. در این روش، کاربران داده‌های خود را به صورت رمزشده بر روی طرف سوم نیمه‌معتمد، ذخیره می‌نمایند. در روش پیشنهادی مبتنی بر معماری غیرمتمرکز دوم بدون فاش‌شدن اطلاعات اشتراکی کاربران، قسمتی از بار محاسباتی بر روی طرف سوم نیمه‌معتمد می‌باشد. همچنین کنترل دسترسی پویا به کمک طرف سوم نیمه‌معتمد فراهم می‌شود. در معماری پیشنهادی مبتنی بر ساختار P2P، علاوه بر فراهم کردن حریم خصوصی، نیازمندی اصلی ساختار P2P یعنی دسترس‌پذیری داده‌های اشتراکی کاربران با ارائه دو الگوریتم ایجاد می‌شود. به صورتیکه کاربران، داده‌های خود را بر روی برخی گره‌های شبکه، کپی می‌کنند تا مخاطبان مجاز داده‌هایشان بتوانند در زمانهای آنلاین بودن در شبکه اجتماعی به آنها دسترسی یابند. استراتژیهای دسترس‌پذیری پیشنهادی به صورت جدید مفهوم دسترس‌پذیری را با حریم خصوصی داده ترکیب می‌کنند.

در تمامی روشهای پیشنهادی، محرمانگی داده‌های اشتراکی کاربران در مقابل فراهم‌کننده شبکه اجتماعی و کاربران غیرمخاطب فراهم می‌شود. علاوه بر این کاربران قادر خواهند بود دوستان خود را تحت رابطه‌های اجتماعی مختلفی که با دوستان دارند، تقسیم‌بندی نمایند. همچنین کاربران می‌توانند اجازه‌های دسترسی متفاوتی برای رابطه‌های تعریف‌شده تعیین کنند. در این راستا کاربران این امکان را دارند که بطور پویا دوستان جدیدی را به این رابطه‌ها اضافه کنند و یا در هر زمان، دوستانی که عضو این رابطه‌ها هستند را از این رابطه‌ها حذف نمایند. کاربران، رابطه‌های خود را به صورتی مدیریت می‌کنند که هیچ‌کس حتی دوستانشان از لیست دوستان یا وجود رابطه‌های اجتماعی کاربران با دوستانشان در فضای شبکه اجتماعی، آگاه نمی‌شوند. علاوه بر این کاربران به صورت انعطاف‌پذیر، داده‌های خود را با هر ترکیبی از دوستان و رابطه‌های تعریف‌شده‌شان به اشتراک می‌گذارند. نتایج بررسی مبسوط روشهای پیشنهادی نشان می‌دهند که نه تنها این روشها توانسته‌اند (بخصوص در رابطه با کارهای گذشته) نیازمندیهای اساسی حریم خصوصی را در شبکه اجتماعی فراهم نمایند، بلکه در شرایط واقعی به صورت کارا عمل می‌نمایند.



**کلمات کلیدی:** شبکه‌های اجتماعی، حریم خصوصی، کنترل دسترسی، رمزنگاری انتشار

# فصل اول
# مقدمه

## ۱-۱ کلیات

واژه شبکه اجتماعی[1] برای اولین بار در سال ۱۹۵٤ با این تعریف مطرح شد که به جمع‌شدن افراد در گروههای مشخص ۱۰۰ تا ۱۵۰ نفری در قالب انجمنها، شبکه اجتماعی گفته می‌شود [۱]. یک شبکه اجتماعی آنلاین (OSN[2]) هم یک شبکه اجتماعی در فضای اینترنت است و به وب‌سایتی گفته می‌شود که مربوط به انجمنهای آنلاین با کاربران اینترنتی است. با توجه به اینکه تمرکز تحقیقات این رساله، شبکه اجتماعی در فضای اینترنت است در ادامه به جای استفاده از واژه شبکه اجتماعی آنلاین از واژه شبکه اجتماعی استفاده می‌شود.

بطور کلی هدف از ایجاد شبکه‌های اجتماعی، شبیه‌سازی تعاملات اجتماعی زندگی افراد است. به همین دلیل در سایتهای شبکه اجتماعی به کاربران اجازه داده می‌شود تا علاقه‌مندیها و فعالیتهای خود را با دیگران به اشتراک بگذارند. هر شبکه اجتماعی منبع بزرگی از اطلاعات شخصی[3] افراد است [۲]. در این شبکه‌ها از کاربران خواسته می‌شود تا پروفایلی از بیوگرافی خود تهیه کنند. به این صورت که اطلاعاتی مانند نام، عکس، تاریخ تولد، اطلاعات تماس با فرد، وضعیت تأهل، دیدگاه سیاسی و مذهبی، علائق، سرگرمی‌ها، سوابق تحصیلی و غیره خود را در شبکه اجتماعی وارد نمایند. هر کاربر در این محیط، مجموعه‌ای از کاربران دیگر که عضو شبکه اجتماعی هستند را به

[1] Social Network
[2] Online Social Network
[3] Personal Information

لیست دوستان خود اضافه می‌کند، فعالیتهای روزمره و حالتهای روحی خود را بیان می‌کند، عکس و فیلم آپلود می‌کند، به دوستانش پیام می‌فرستد، کاربران دیگر با علائق مشابه را جستجوکرده و با آنها ارتباط برقرار می‌کند. بنابراین با استفاده از شبکه‌های اجتماعی، کاربران می‌توانند از امکاناتی که تا پیش از این از طریق سایتهای مختلف دریافت می‌کردند را یکجا با عضویت در یک شبکه اجتماعی در اختیار داشته باشند. به همین دلیل هم کاربران اغلب زمان آنلاین خود در اینترنت را به حضور در شبکه‌های اجتماعی اختصاص می‌دهند.

نخستین شبکه اجتماعی با نام SixDegrees[۱] در سال ۱۹۹۷ راه‌اندازی شد. پس از آن به مرور شبکه‌های اجتماعی فراوانی با کاربردهای مختلفی مانند سرگرمی، تجارت و غیره بوجود آمدند. به عنوان مثال، LinkedIn[۲] یک شبکه اجتماعی با هدف اتصال شرکتهای تجاری است تا کاربران، سابقه تحصیلی و شغلی خود را با دیگران به اشتراک بگذارند. علاوه بر این، برخی از شبکه‌های اجتماعی به کاربران اجازه می‌دهند تا فقط نوع خاصی از داده‌ها را به اشتراک بگذارند. به عنوان مثال، Flickr[۳] یک شبکه اجتماعی برای اشتراک عکس بین کاربران است و یا YouTube[٤] یک شبکه اجتماعی برای اشتراک آهنگ و ویدئو می‌باشد. البته شبکه‌های اجتماعی همه منظوره مانند Facebook[٥]، Myspace[٦] و Google+[۷] هم ایجاد شده‌اند و از پرطرفدارترین نوع شبکه‌های اجتماعی به حساب می‌آیند. این شبکه‌ها با داشتن میلیونها کاربر همچنان در حال رشد و توسعه هستند.

در حال حاضر چندین میلیارد کاربر شبکه اجتماعی وجود دارد [۳] و به نظر می‌رسد به تدریج، دنیای اینترنت بوسیله این سایتها تسخیر شود. این توجه بالای کاربران به شبکه‌های اجتماعی باعث شده که شرکتهای مختلف در اندیشه ایجاد، خرید و یا بازاریابی در شبکه‌های اجتماعی باشند. به عنوان مثال، شبکه Facebook در جدیدترین ارزش‌گذاری بیش از ۱۰٦ میلیارد دلار تخمین زده شده است [٤].

در ایران هم در چند سال اخیر، شبکه‌های اجتماعی بخصوص با رواج شبکه اجتماعی Orkut[۸] در میان کاربران، بطور گسترده مورد استفاده قرار گرفته است. شبکه اجتماعی Orkut در مدت کوتاهی بین کاربران ایرانی آنقدر سریع رشد کرد تاجائیکه ایران، سومین کشور حاضر در محیط این شبکه شد. به دلیل اهمیت این مبحث جدید و مهم دنیای اطلاعاتی، از سال ۱۳۸۸ تاکنون نشستهای رسمی متعددی با موضوع شبکه‌های اجتماعی به میزبانی مرکز مطالعات

[1] http://www.sixdegrees.com
[2] http://www.linkedin.com
[3] http://www.flickr.com
[4] http://www.youtube.com
[5] http://www.facebook.com
[6] http://www.myspace.com
[7] https://plus.google.com/
[8] http://www.orkut.com

استراتژیک ایران برگزار گردیده تا صاحبنظران حوزه‌های علوم ارتباطات، علوم اجتماعی و علوم سیاسی به ارائه دیدگاههایشان بپردازند [۵].

### ۲-۱ نقض حریم خصوصی در شبکه‌های اجتماعی

امکانات بسیار زیاد شبکه‌های اجتماعی در جهت اشتراک اطلاعات مختلف در محیط شبکه اجتماعی باعث بروز مشکلات حریم خصوصی[1] کاربران شده است. به این مفهوم که کاربران شبکه اجتماعی، کنترل کاملی بر روی انتشار اطلاعات اشتراکی‌شان در فضای شبکه اجتماعی ندارند. اگرچه ممکن است افرادی که به حفظ حریم خصوصی خود بسیار حساس هستند، در ابتدا سعی نمایند از عضویت در شبکه‌های اجتماعی صرفنظر کنند ولی در عمل هنگامیکه بیشتر دوستانشان در این محیطها با یکدیگر در تعامل هستند، آنها نیز ترغیب می‌شوند تا به سراغ این شبکه‌ها آمده و آرام آرام، اطلاعات شخصی خود را فاش نمایند. همچنین به علت عدم آگاهی بیشتر کاربران در انتشار اطلاعاتشان، مشکلات حریم خصوصی مختلفی ایجاد می‌شود.

کاربران در هنگام ثبت‌نام در شبکه اجتماعی بایستی اطلاعات شخصی خود را بطور صحیح و درست وارد کنند. حال آنکه تمامی اطلاعات پروفایل کاربران و داده‌هایی که آنها در شبکه اجتماعی با دوستان خود به اشتراک می‌گذارند، تحت کنترل کامل فراهم‌کننده شبکه اجتماعی[2] است. زیرا اطلاعات منتشرشده کاربران بر روی سرورهای شبکه اجتماعی، بطور دائمی ذخیره می‌شود. بنابراین فراهم‌کننده شبکه اجتماعی به اطلاعات اشتراکی کاربران به صورت نامحدود، دسترسی دارد [٦] .

به این نکته توجه شود که کاربران در هنگام ثبت‌نام در شبکه اجتماعی با قبول توافق‌نامه[3] بین خود و فراهم‌کننده، بطور ضمنی به فراهم‌کننده شبکه اجتماعی این اجازه را می‌دهند تا اطلاعات آنها را ذخیره، نمایش و استفاده کند. به عبارت دیگر طبق این توافق‌نامه، حق مالکیت[4] داده‌های کاربران به فراهم‌کننده شبکه اجتماعی، سپرده می‌شود تا بتواند تمامی حقوق لازم برای استفاده و توزیع داده‌های کاربران جهت انجام مقاصد مختلف را بدست آورد [۷-۱۲].

در این شرایط، حریم خصوصی کاربران توسط فراهم‌کننده شبکه اجتماعی به راحتی نقض می‌شود. به عنوان مثال فراهم‌کننده‌ها، اطلاعات شخصی کاربران را جهت مقاصد بازاریابی[5] در اختیار شرکتهای تجاری قرار می‌دهند. اگرچه فراهم‌کنندگان شبکه‌های اجتماعی ادعا می‌کنند که اطلاعات ارائه شده به این شرکتها به صورتی است که

[1] Privacy
[2] Social Network Provider
[3] Terms of Service
[4] Ownership
[5] Marketing

کاربران، قابل شناسائی نیستند ولی متاسفانه بدلیل وجود الگوریتمهای شناسائی دوباره[1]، تضمین چنین ادعائی مشکل می‌باشد [١٤-١٥]. همچنین بطور معمول جهت رسیدگی به پرونده‌های مربوط به نقض حریم خصوصی کاربران، فراهم‌کننده شبکه اجتماعی، اطلاعات شخصی افراد را به دادگاه درخواست کننده، ارائه می‌دهد [١٦,١٤]. از طرف دیگر طبق این توافق‌نامه، اگر کاربران، داده‌ای را از صفحه خود در شبکه اجتماعی پاک کنند و یا حساب کاربری خود را حذف و یا غیرفعال نمایند، اطلاعاتشان همچنان بر روی سرورهای پشتیبان شبکه باقی می‌ماند [٧-١٢].

بسیاری از کاربران بدون خواندن و آگاهی از موارد توافق‌نامه بین خود و فراهم‌کننده به راحتی آنرا قبول می‌کنند. البته کاربران درصورتیکه بخواهند از سرویسهای شبکه اجتماعی استفاده کنند، چاره‌ای جز قبول موارد توافق‌نامه هم ندارند. طبق تحقیقی که در مورد Facebook انجام شده است، ١٤٪ کاربران هیچگونه اطلاعی از توافق‌نامه و موارد مطرح‌شده در آن ندارند، ٤٨٪ کاربران هرگز آنرا نخوانده‌اند، ٢١٪ هم فقط قسمتی از آنرا خوانده‌اند و فقط ٥٪ کاربران دغدغه حفظ حریم خصوصی خود را داشته و قبل از پذیرفتن توافق‌نامه آنرا کاملا" مطالعه کرده‌اند [١٧].

متاسفانه مشکل به همین جا ختم نمی‌شود، زیرا بسیاری از اطلاعات اشتراکی کاربران به غیر از فراهم‌کننده شبکه اجتماعی در اختیار طیف بزرگی از کاربران قرار داده می‌شود. عدم فراهم‌سازی امکانات مناسب برای کاربران در جهت تعریف مخاطبان مجاز[2] داده‌های اشتراکی‌شان باعث بوجودآمدن مشکلات حریم خصوصی برای کاربران در شبکه‌های اجتماعی می‌شود. زیرا کاربران قادر نخواهد بود کنترل کاملی بر جریان انتشار اطلاعات اشتراکی خود در این شبکه‌ها داشته باشند. اگرچه به تازگی، شبکه‌های اجتماعی سعی کرده‌اند که به کاربران امکان تنظیم حریم خصوصی خود را بدهند ولی تنظیمات حریم خصوصی تعبیه شده جهت مقابله با مشکلات حریم خصوصی کاربران در شبکه‌های اجتماعی، کافی نیست [١٨]. همچنین تنظیمات پیش‌فرض حریم خصوصی کاربران در این شبکه‌ها قوی نمی‌باشد. در تنظیمات پیش‌فرض حریم خصوصی شبکه اجتماعی، کاربران غیرمجاز به اطلاعات زیادی دسترسی دارند [١٩]. حال آنکه کاربران از این مسئله آگاه نمی‌باشند و یا علیرغم آگاهی از وجود چنین مشکلاتی برای استفاده از سرویسهای رایگان شبکه‌های اجتماعی ناچار به اشتراک اطلاعات شخصی خود در محیط شبکه اجتماعی می‌شوند. در این حالت، بسیاری از اطلاعات کاربران به صورت ناخواسته در اختیار دیگران قرار داده می‌شود.

براساس تحقیقی که بر روی کاربران دانشگاه کارنگی‌ملون آمریکا انجام شده است، ٪٩٠٨ کاربران در پروفایل خود در Facebook عکس خود را آپلود کرده، ٪٨٧.٨ آنها تاریخ تولد، ٪٣٩.٩ آنها هم مکان و موقعیت فعلی خود را مشخص کرده‌اند [١٨]. این درحالی است که با توسعه ابزارهای جستجو و بازیابی اطلاعات، جمع‌آوری اطلاعات

[1] De-Anonymization Algorithms
[2] Authorized Audiences

پروفایل کاربران توسط افراد بدخواه[1] و یا کنجکاو بسیار آسان می‌باشد. به عنوان مثال بر طبق گزارش اخیر شرکت مایکروسافت، ۷۵٪ از استخدام‌کنندگان شرکتها از سایتهای شبکه‌های اجتماعی استفاده می‌کنند تا در مورد کاندیدهای شغلهای موجود در شرکتهای خود، اطلاعات بدست آورند [۲۰].

با توجه به آنکه شبکه اجتماعی با هدف شبیه‌سازی تعاملات اجتماعی کاربران در محیط اینترنت ایجاد شده است، بایستی این امکان را داشته باشد تا کاربران، داده‌های خود را براساس رابطه‌های اجتماعی متفاوت با دوستانشان به اشتراک بگذارند. زیرا رابطه اجتماعی که بین کاربر و هر دوستش وجود دارد متفاوت است. به عنوان مثال، دوستان کاربر در شبکه اجتماعی ممکن است همکلاسی، دوست صمیمی، عضوی از خانواده و یا حتی در حد آشنائی بسیار مختصر با او باشند. بنابراین فقط وجود رابطه دوستی بین کاربران در شبکه اجتماعی برای تنظیم اطلاعات اشتراکی کاربران، کافی نمی‌باشد.

علاوه بر این کاربران ممکن است با یک دوست، رابطه‌های اجتماعی متفاوتی داشته باشند. به عنوان مثال، اگر صدرا و علی تحت عنوان دو دوست در شبکه اجتماعی عضویت داشته باشند، علی می‌تواند هم همکلاسی صدرا و هم دوست صمیمی او باشد. همچنین کاربران ممکن است رابطه اجتماعی مشابهی با دوستان مختلفی داشته باشند. به عنوان مثال، علی و رضا که هر دو از همکلاسی‌های صدرا هستند ممکن است در لیست دوستان صدرا باشند. البته توجه شود که کاربران معمولاً مایل نیستند که دیگران از ماهیت رابطه‌های اجتماعی‌شان آگاه شوند. به عنوان مثال، اگر صدرا دوستش علی را در رابطه‌ای با نام "دوست صمیمی" قرار بدهد، صدرا تمایل ندارد نه تنها علی بلکه دوستان دیگرش مانند رضا بدانند که چه کسانی دوست صمیمی صدرا هستند.

همچنین بایستی به این نکته توجه شود که رابطه‌های اجتماعی کاربران در طول زمان تغییر می‌کند. به عنوان مثال، رضا که تا چند ماه پیش همکلاسی صدرا بود، ممکن است در آینده دوست صمیمی او بشود. علاوه بر اینکه کاربران همواره در حال گسترش دایره آشنائی خود با دیگران هستند. بنابراین بطور مرتب، دوستان جدیدی را به لیست دوستان و رابطه‌های اجتماعی تعریف‌شده خود اضافه می‌کنند. درنهایت با توجه به ماهیت پیچیده رابطه‌های اجتماعی، بسیار اتفاق می‌افتد که کاربران، خواهان به اشتراک‌گذاری داده‌های خود برای رابطه‌های اجتماعی پیچیده‌تری باشند که از ترکیب رابطه‌های اجتماعی‌شان بدست می‌آید. به عنوان مثال صدرا ممکن است بخواهد عکس خود را با آن دسته از دوستان صمیمی که همکلاسی‌اش هم هستند به اشتراک بگذارد. یا متنی را در شبکه به اشتراک بگذارد که

[1] Malicious

برای تمامی همکلاسی‌هایش به جز علی قابل دسترس باشد. در این حالت، کاربران بایستی بتوانند اجازه‌های دسترسی پیچیده[1] و البته متفاوتی بر روی داده‌های اشتراکی خود تعریف کنند.

### ۱-۳ انگیزه

با توجه به همه‌گیرشدن شبکه‌های اجتماعی و اهمیت حفظ حریم خصوصی کاربران، برقراری امکاناتی در جهت حفظ حریم خصوصی کاربران بایستی در هنگام طراحی شبکه اجتماعی[2] درنظر گرفته شود [۲۱]. در سالهای اخیر روشهائی برای طراحی یک شبکه اجتماعی با حفظ حریم خصوصی ارائه شده است. ولی این روشها نتوانسته‌اند حریم خصوصی کاملی برای کاربران شبکه اجتماعی فراهم نمایند. در این روشها که مبتنی بر معماریهای مختلف شبکه ارائه شده‌اند معمولاً هدف اصلی حذف نقش فراهم‌کننده شبکه اجتماعی است. علاوه بر اینکه در این روشها تعریف واضح و کاملی از حریم خصوصی کاربران و چگونگی اجرای عملیات مختلف در شبکه اجتماعی نشده است.

در صورتیکه همانطور که در قسمت ۱-۲ اشاره شد، داده‌های کاربران بایستی هم در مقابل فراهم‌کننده شبکه اجتماعی و هم کاربران غیرمجاز، محرمانه بماند. به عبارت دیگر داده‌های کاربران می‌بایست در مقابل هر مولفه‌ای که در خارج از حوزه مخاطب موردنظر کاربران است به صورت محرمانه حفظ شود. همچنین لازم است که شبکه اجتماعی امکان تعریف رابطه‌های اجتماعی را به کاربران بدهد و البته ماهیت این رابطه‌ها نیز بایستی در مقابل همه کاربران شبکه اجتماعی به صورت محرمانه باشد.

از طرف دیگر کاربران بایستی مشخص کنند چه کسی[3] قادر به دیدن کدام اطلاع اشتراکی آنها است. به عبارت دیگر مطلوب آن است که کاربران، کنترل دسترسی بر روی اطلاعات اشتراکی‌شان داشته باشند. با درنظر گرفتن جنبه‌های اجتماعی، حقوقی، اخلاقی و امنیتی در شبکه اجتماعی، کنترل دسترسی موردنیاز کاربر شبکه اجتماعی بایستی بصورتی باشد که به محض ایجاد رابطه دوستی، کاربر بتواند دوست جدیدش را در رابطه‌های اجتماعی مختلف طبقه‌بندی کند. رابطه‌های تعریف‌شده کاربر هم بایستی این قابلیت را داشته باشند که بیش از یک دوست را بتوان به آنها نگاشت کرد یا یک دوست را در رابطه‌های مختلفی قرار داد. علاوه بر اینکه کاربر بتواند با ترکیب رابطه‌های تعریف‌شده‌اش با یکدیگر رابطه‌های جدیدی تعریف نماید. همچنین این رابطه‌ها قابلیت تغییر در طول زمان را داشته باشند. به عبارت دیگر کاربر بتواند دوستی را به رابطه‌های قبلی تعریف‌شده‌اش اضافه، حذف و یا بطور کامل از

[1] Complex Access Permissions
[2] Privacy-by-Design
[3] Who

سیستمش ملغی کند. در نهایت کاربر به عنوان مالک داده[1] و تنها تصمیم‌گیرنده در تعیین مخاطبان داده‌هایش بتواند اجازه‌های دسترسی[2] بر روی هر نوع داده اشتراکی یا بخشی[3] از آن را براساس شناسه دوست یا رابطه اجتماعی تعریف شده با دوستان تعریف نماید.

به همین دلیل در این رساله روشهائی جهت طراحی یک شبکه اجتماعی با حفظ کامل حریم خصوصی کاربران در معماریهای متمرکز[4]، غیرمتمرکز[5] و P2P[6] با استفاده از سیستم رمزنگاری انتشار[7] پیشنهاد داده شده‌اند. در این روشها کاربران قادرند ارتباطات اجتماعی مختلفی در شبکه اجتماعی داشته باشند بطوریکه حریم خصوصی‌شان بطور کامل، حفظ شود. تحلیل مبسوط روشهای پیشنهادی، نشان دهنده کاربردی‌بودن آنها در شرایط واقعی و همچنین بهبود قابل توجه روشهای پیشنهادی نسبت به روشهای قبلی در این زمینه می‌باشد.

### ۱-۴ مروری بر ساختار رساله

پس از ارائه مقدمه در فصل جاری، در فصل دوم ابتدا با توجه به مشکلاتی که در شبکه‌های اجتماعی پرطرفدار فعلی وجود دارد، نیازمندیهای حریم خصوصی کاربران در شبکه اجتماعی به تفصیل بیان و دسته‌بندی می‌شوند. سپس تکنیکهای موجود جهت برآورده‌کردن نیازمندیهای حریم خصوصی کاربران در شبکه اجتماعی، مورد بررسی قرار می‌گیرد. پس از آن، روشهای ارائه‌شده فعلی برای طراحی شبکه اجتماعی با حفظ حریم خصوصی کاربران در سه نوع معماری متمرکز، غیرمتمرکز و P2P توضیح داده می‌شوند. در نهایت این روشها براساس نیازمندیهای حریم خصوصی کاربران در شبکه اجتماعی با یکدیگر مقایسه می‌شوند.

در فصل سوم، یک روش مبتنی بر معماری متمرکز برای شبکه اجتماعی پیشنهاد داده می‌شود. در این روش با استفاده از طرف سوم[8] و بهره‌گیری از تنظیمات حریم خصوصی مشابه بین کاربران، کنترل اطلاعات اشتراکی کاربران به آنها داده می‌شود.

در فصل چهارم، دو روش مبتنی بر معماری غیرمتمرکز پیشنهاد داده می‌شود. در روش پیشنهادی غیرمتمرکز اول بدون استفاده از طرف سوم، حریم خصوصی کاربران تامین می‌شود. در پیشنهادی غیرمتمرکز دوم از یک طرف سوم،

---

[1] Data Owner
[2] Access Permissions
[3] Item
[4] Centralized Architecture
[5] Decentralized Architecture
[6] Peer-to-Peer Architecture
[7] Broadcast Encryption
[8] Third Party