

# SID



سرویس های ویژه



سرویس ترجمه تخصصی



کارگاه های آموزشی



بلاگ مرکز اطلاعات علمی



عضویت در خبرنامه



فیلم های آموزشی

## کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی



مباحث پیشرفته یادگیری عمیق؛  
شبکه های توجه گرافی  
(Graph Attention Networks)



کارگاه آنلاین آموزش استفاده از  
وب آو ساینس



کارگاه آنلاین مقاله روزمره انگلیسی



مرکز توسعه فناوری نیرو (مختن)



انجمن کامپیوتر ایران  
Computer Society of Iran

## سامانه حفظ حریم شخصی مبتنی بر تشخیص موقعیت در محیط محاسبات فراگیر

محمد کاظم اکبری

دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی

امیرکبیر

akbarif@aut.ac.ir

حسین نوری خواه

دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی

امیرکبیر

nourikhah@aut.ac.ir

### ۲- حریم شخصی

در قانون اساسی کشور جمهوری اسلامی ایران آمده است:

اصل ۲۵: بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هر گونه تجسس ممنوع است مگر به حکم قانون.

این اصل قانون اساسی، بخشی از قوانینی است که در کشور حریم شخصی را برای مردم تضمین کرده است.

با گسترش ابزارهای مختلف جمع‌آوری، ارسال و پردازش اطلاعات، باید راه‌هایی برای تضمین این حریم ایجاد شود؛ چرا که بدون در نظر گرفتن این راهکارها، سامانه‌های رایانه‌ای بر طبق معمول حجم عظیمی از داده‌های شخصی را ذخیره کرده و امکان دسترسی نامحدود به لحاظ زمانی و مکانی و نیز امکان تحلیل و استنتاج از آن‌ها را فراهم می‌آورد.

یکی از بهترین تحقیقات موجود در زمینهٔ حفظ حریم شخصی در محیط محاسبات فراگیر، [۱] است. بخش اول این تحقیقات، به بررسی مسئله حریم شخصی و تعاریف قانونی و نیز معنای آن از دیدگاه کاربران می‌پردازد. در آن، پیشنهاد شده همان‌گونه که در جامعه قوانینی ارائه گشته و امکان رعایت آن برای شهروندان قانون‌مند فراهم می‌گردد، باید روش مشابهی برای حریم شخصی پیاده شود، چرا که یک سامانهٔ رایانه‌ای صرف بدون تکیه بر قوانین ناظر بر آن، مفید واقع نخواهد شد. مجری این قوانین، با بررسی وضعیت رعایت قواعد مورد توافق حریم شخصی در یک سامانه، مؤسسه یا فرد خاطی را مورد مجازات قرار خواهد داد. البته باید توجه داشت که این سیستم به جای تسهیل استفاده کاربران و دادن حس امنیت به آن‌ها، صرفاً به وسیله‌ای برای طرح دعاوی قانونی بدل نگردد [۲].

### ۳- حریم شخصی در محیط محاسبات فراگیر

حریم شخصی به عنوان یک مسئلهٔ اساسی در کاربردهای محاسبات فراگیر مطرح است. مدل‌های بسیاری برای مقابله با این مخاطرات ایجاد شده‌اند. در یک طرح موفق، باید از خواست و آن‌چه برای کاربران

چکیده: محاسبات فراگیر به عنوان یکی از شاخه‌های رو به گسترش محاسبات رایانه‌ای به سرعت در حال تبدیل شدن به پارادایم اصلی رایانه‌ها در قرن جدید می‌باشد. در این میان، حیطه شخصی به عنوان عاملی اساسی در گسترش و موفق شدن این چارچوب جدید، شناخته شده است. این مقاله یک مدل جدید برای حفظ حیطه شخصی ارائه می‌دهد که کنترل جمع‌آوری اطلاعات از کاربر با برآورده ساختن ترجیحات او، مدیریت آن‌ها و در نهایت مدیریت چگونگی استفاده از این داده‌ها را ممکن می‌سازد.

### واژه‌های کلیدی: محاسبات فراگیر، حیطه شخصی، تشخیص

موقعیت داخلی

#### ۱- مقدمه

محیط محاسبات فراگیر یک نگرش جدید و آیندهٔ استفاده از رایانه است و قصد دارد که رایانه‌ها و محیط‌های محاسباتی را در زندگی روزمرهٔ انسان‌ها جای دهد و آن‌ها را به صورت یک جزء نامریی و همیشه در دسترس در بیاورد.

عاملی اساسی در این میان، «حفظ حریم خصوصی کاربر» است که بدون آن محاسبات فراگیر تحقق نمی‌یابد. ارائهٔ راهکاری برای تعامل مناسب با کاربر از طریق تعریف و رعایت سیاست‌هایی برای کار با اطلاعات جمع‌آوری شده از کاربر، بحث اصلی این مقاله است.

این راهکار با استفاده از یک سامانهٔ تشخیص موقعیت در داخل ساختمان ایجاد می‌شود که بر مبنای سنجش شدت سیگنال شبکه بی‌سیم کار می‌کند. حفظ حیطه شخصی نیز با استفاده از پروتکل‌های مرتبط P3P و APPEL توسط سیستم انجام می‌گیرد.

روش مقایسه و شبیه‌سازی به این صورت است که یک سیستم نرم‌افزاری مشابه سیستم واقعی پیاده‌سازی شده و دو حالت استفاده از اعلان کننده سیاست شخصی و نیز مدل جدید ارائه شده، از لحاظ زمان یافتن سرویس برای کاربران مورد مقایسه قرار می‌گیرد.

فناوری مهم است، آگاه بود. این کار کمی دشوار است، چرا که تحقیقات کمی مورد کاربران بالقوه محاسبات فراگیر وجود دارد که طراحان بتوانند از آن استفاده کنند.

چیزی که طراحی را پیچیده تر می کند، این حقیقت است که محاسبات جامع معمولاً تعبیه شده یا ناپیدا هستند و این برای کاربران تشخیص حضور دستگاهها و جمع آوری اطلاعات را دشوارتر می کند. از آنجایی که کاربران درک محدودی از فناوری دارند، مشکلات بسیاری در زمینه حریم شخصی، طراحی و مسائل ایمنی به وجود می آید. [۳]

#### ۴- تشخیص موقعیت

سامانه پیشنهادی از یک روش تشخیص موقعیت داخل ساختمان استفاده می کند. بنابراین برخی از این سامانهها بررسی شده اند:

#### ۱-۴ موقعیت یابی درون ساختمان

این سامانه، علاوه بر این نیاز به یک سیستم موقعیت یابی درون ساختمان دارد. روش های متفاوتی برای تخمین موقعیت کاربر و نیز تشخیص اتاقی که کاربر در آن قرار دارد، ارائه شده است که چند مورد از آنها به شرح زیر هستند:

1. PlaceLab: تشخیص از طریق سنجش شدت سیگنال (بلوتوث، شبکه بی سیم، شبکه تلفن همراه): یک سامانه معروف در این زمینه، PlaceLab [۶] است که در مؤسسه تحقیقاتی شرکت اینتل ایجاد شده است. در این سامانه شدت سیگنال قبلاً ثبت شده و بعد با مقایسه با مقدار اصلی، موقعیت کاربر را تخمین می زند. با استفاده از شبکه تلفن همراه دقت حداکثر تا حدود ۱۰۰ متر، و با استفاده از شبکه بی سیم، نزدیک ۱۳ متر خواهد بود [۴].
2. RADAR: تشخیص از طریق ترکیب شدت سیگنال چند منبع: یک سامانه معروف که با استفاده از این روش ایجاد شده است، RADAR [۸] است که توسط مؤسسه تحقیقاتی شرکت مایکروسافت ایجاد شده است. این سامانه دقتی نزدیک به ۱.۵ متر را تأمین می کند که دقت مناسبی به شمار می رود.
3. Nibble: این روش بر اساس یک مدل احتمالاتی مبتنی بر شبکه بی زین ایجاد شده و قادر است در صورت وجود دو نقطه دسترسی متفاوت شبکه بی سیم، با دقت بیش از ۹۷٪ تخمین بزند که کاربر در چه اتاقی از ساختمان قرار دارد.
4. BAT: این سیستم مبتنی بر نصب تعدادی فرستنده در محیط و سپس استفاده از یک سیستم پردازش سیگنال برای بررسی تغییرات و محاسبه موقعیت مکانی است. دقت این سیستم در حد ۳ سانتیمتر است. [۵]

در [۷] با استفاده از نرم افزار PlaceLab، یک سامانه امنیتی برای کنترل مکانی لپ تاپ های یک مؤسسه ارائه شده است. این مقاله پس از

بررسی سامانه Locus، ترجیح می دهد که به استفاده از PlaceLab که کد آن در اختیار است اکتفا کرده و از آن بهره ببرد.

این سامانه متشکل از یک سرویس دهنده و تعدادی سرویس گیرنده است که بر روی لپ تاپها نصب شده و با بررسی شدت سیگنال و مقایسه آن با شدت سیگنالی که قبلاً اندازه گیری شده، موقعیت لپ تاپ را تخمین زده و بر روی سرور به روزرسانی می نماید.

این سیستم مانند RADAR و PlaceLab نیاز به تنظیم شدن پیش از استفاده دارد و پس از آن می تواند خروج لپ تاپ یا PDA که این نرم افزار بر روی آن نصب شده از یک محدوده مشخص را اعلام نماید. این سیستم به عنوان یک کاربرد ساده از تشخیص موقعیت مکانی داخل ساختمان مطرح شده است.

مقاله [۹] ارائه کننده بهبودهایی است که تولیدکنندگان سیستم RADAR پس از طرح اولیه ارائه کرده اند. این سامانه روش رهگیری ممتد موقعیت کاربر برای جلوگیری از نویزها و خطاهای لحظه ای را پیشنهاد کرده است. با این روش، و با توجه به محدودیت سرعت حرکت کاربر، از نویزها و حرکت های لحظه ای بیش از محدوده ممکن جلوگیری شده و پیش بینی های ناممکن از تخمین موقعیت کاربر کنار گذاشته می شوند.

بدن انسان با درصد آب بالا جاذب مناسبی برای امواج الکترومغناطیس به شمار می رود. بنابراین حضور کاربران در محیط تأثیر قابل توجهی در شدت سیگنال دریافتی دارد و دقت تخمین موقعیت را کاهش می دهد. برای حل این مشکل، پروفایل های مختلفی در زمان های متفاوت ایجاد شده و سامانه RADAR به صورت خودکار پروفایل ها فعال را تغییر می دهد.

مقاله [۱۰] روشی را برای تخمین موقعیت کاربر به کار می برد که نیاز برای برنامه ریزی اولیه و تمرین اولیه را کاهش می دهد. در حقیقت، با تعداد کمی داده های مربوط به شدت سیگنال چند نقطه دسترسی، می توان با دقت مناسبی موقعیت کاربر را تخمین زد.

این سامانه با موقعیت مکانی به صورت یک مکان مشخص سر و کار دارد و آن را با یک اسم (مثلاً نام اتاق) مشخص می کند. کاربران می توانند با حضور در نقاط مختلف، شدت سیگنال نقاط دسترسی مختلف را سنجیده و با مشخص کردن نماد مکانی، آن را به سرور اعلام کنند.

در آزمون های انجام شده، این سامانه توانسته تنها با ۱۰ بار سنجش شدت سیگنال و ارائه آن به سرور توانسته با سنجش مکانی را در اتاق های کوچک یک محیط آزمایشی با دقت بیش از ۹۰ درصد به انجام برساند.

۱. پروتکل P3P: این پروتکل برای بیان سیاست های حیطه شخصی مورد استفاده قرار می گیرد.

۲. پروتکل APPEL: این پروتکل برای بیان ترجیحات حیطة شخصی کاربر مورد استفاده قرار می‌گیرد.

## ۵- مدل ارائه شده

مدل ارائه شده بر اساس مدل قبلی PawS است که در دانشگاه ETH زوریخ ارائه شده است. در سامانه پیشنهادی ما، موضوع حیطة مورد بررسی قرار گرفته و یک روش برای حل موضوع حیطة شخصی ارائه گشته است. در ابتدا یک شرح کلی بر روش مدل خود که در شکل ۱ نمایش داده شده است، ارائه می‌کنیم.

در این سیستم قرار است که کاربر از سرویس‌های موجود در محیط بهره‌مند شود و با توجه به انتخاب خود از آن‌ها استفاده کند. نکته مهم این است که این سرویس‌ها برای انجام کار خود نیاز به اطلاعات زمینه‌ای دارند و برای دستیابی به آن باید از کاربر و محیطی که او با آن تعامل دارد، اطلاعاتی جمع‌آوری نمایند. به طور مثال ممکن است که موقعیت کاربر مورد نیاز باشد، یا نیاز به تصویربرداری از او پیش بیاید.

در این‌جا همان‌طور که در قسمت‌های گذشته توضیح داده شد، بحث حیطة شخصی او به میان می‌آید. یعنی باید روش‌هایی برای محدود کردن اطلاعات جمع‌آوری شده، نظارت بر جمع‌آوری و استفاده از آن‌ها و نیز اطمینان از تطابق این وضعیت با خواست کاربر وجود داشته باشد.

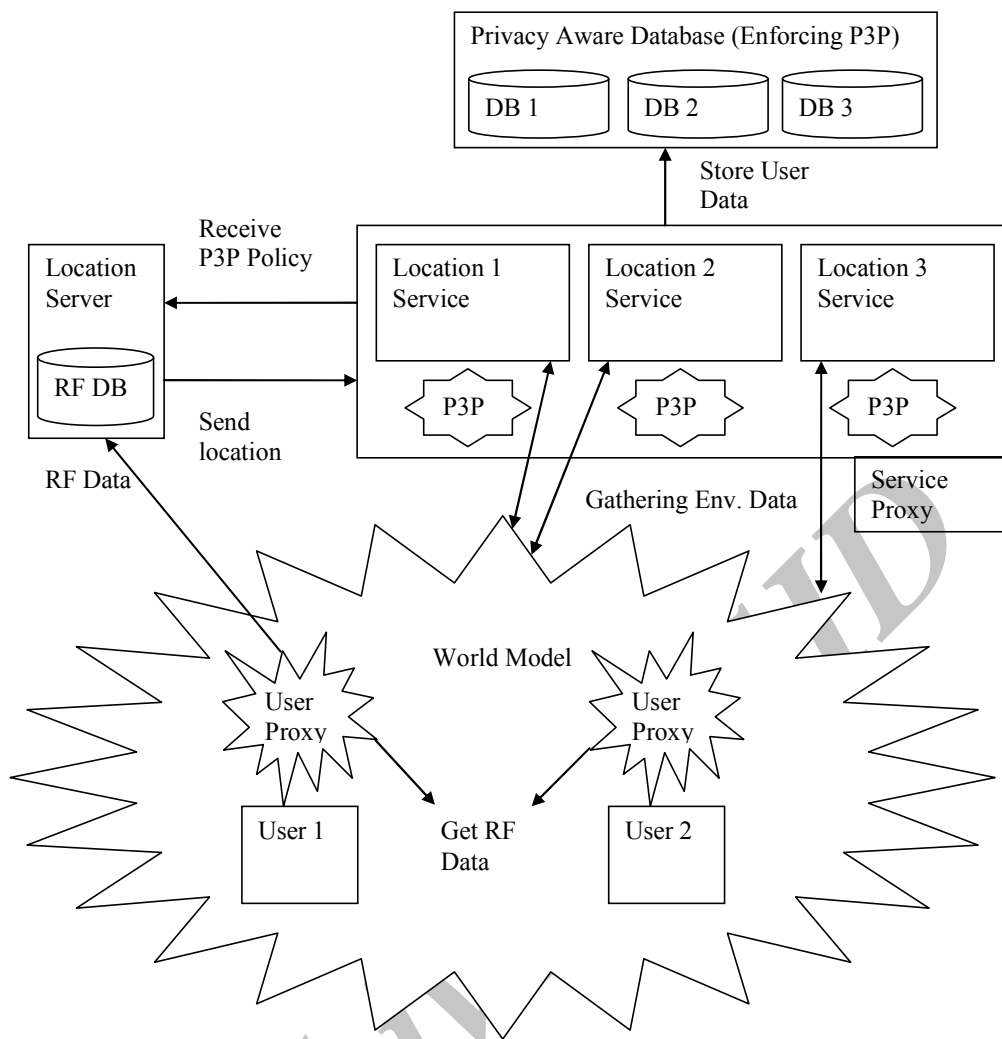
مدل پیشنهادی و سیستم پیاده‌کننده آن، روشی برای برقراری این خواسته‌ها ارائه می‌دهند. بدین صورت که هر کاربری باید برای خود یک مشخص‌کننده ترجیحات حیطة شخصی داشته باشد که باید در قالب پروتکل APPEL بیان شود.

وقتی که کاربر وارد محیط می‌شود، کار یافتن سرویس‌ها و عرضه به او به صورت خودکار توسط سیستم انجام می‌شود، اما او باید از میان سرویس‌های عرضه شده، سرویس مورد نظر خود را انتخاب نماید.

همه سرویس‌ها باید سیاست حیطة شخصی خود را در قالب قابل استفاده برای رایانه و با استفاده از پروتکل P3P تعریف نموده باشند و آن را در آدرس مشخص شده در این استاندارد قرار دهند. قابل ذکر است که استاندارد P3P برای وب پیشنهاد شده و برای محیط محاسبات فراگیر، به آن بخش‌های اضافی الحاق شده است تا قادر به پوشش دادن بحث موقعیت مکانی، صوت، تصویر و ... باشد.

سامانه پیشنهادی سیاست حیطة شخصی سیاست حیطة شخصی سرویس انتخاب شده را در قالب P3P دریافت کرده و با استفاده از الگوریتم‌های مشخص شده، کار تطابق آن را با ترجیحات حیطة شخصی کاربر انجام می‌دهد. در صورتی که این تطابق انجام گرفت، کاربر اجازه استفاده از این خدمات را یافته و آن سرویس دهنده موردنظر شروع به جمع‌آوری اطلاعات می‌نماید و کار خواسته شده را برای کاربر انجام می‌دهد.

پس از جمع‌آوری اطلاعات، بخش نگهداری داده‌ها مورد بحث قرار می‌گیرد. پایگاه داده‌هایی که اطلاعات جمع‌آوری شده را نگاه می‌دارد، باید یک پایگاه داده‌های آگاه از حیطة شخصی باشد. بدین معنی که مشابه قابلیت‌های اعتبارسنجی و اجازه دسترسی معمول در پایگاه داده‌ها، باید قابلیت استفاده از شرط‌های تعریف شده در سیاست حیطة شخصی سرویس دهنده وجود داشته باشد. تنها کاربران خاصی باید اجازه استفاده از بخش مشخصی از داده‌های فرد را داشته باشند و این افراد در سیاست حیطة شخصی تعریف شده‌اند. همچنین تمام دسترسی به داده‌ها ثبت می‌شود تا در مسائل و مشکلات حقوقی احتمالی مورد استفاده قرار گیرند.



شکل ۱- سامانه پیشنهادی برای حفظ حریم شخصی

لازم به ذکر است که با توجه به این که در این حال تنها دسترسی به اتاق مورد نظر کفایت می‌کند و لازم به دقت بالاتر از یک مکان (اتاق و ...) نیست، اطمینان مناسبی برای کاربر تأمین می‌گردد. سامانه RedPin که به این روش عمل می‌کند، توانسته است با تعداد سنجش اولیه بسیار کم، به دقت بیش از ۹۰-۹۵ درصد در تشخیص اتاقی که کاربر در آن قرار دارد، برسد.

پس از تشخیص موقعیت، آن را برای پروکسی سرویس‌دهنده‌ها (که معمولاً در یک ساختمان یکتا فرد است) می‌فرستیم تا سرویس‌های موجود و نیز سیاست حیطه شخصی آن‌ها دریافت گردند.

مرحله بعدی انتخاب سرویس مناسب از میان سرویس‌های موجود است. پس از این مرحله، سیاست حیطه شخصی آن باید با ترجیحات کاربر تطبیق داده شود و در صورت تطابق، کاربر قادر به استفاده از سرویس خواهد بود و سرویس‌دهنده نیز شروع به جمع‌آوری اطلاعات محیطی کاربر خواهد کرد. در صورت عدم تطابق نیز پیام مناسب به کاربر داده می‌شود.

## ۱-۵ نوآوری سیستم پیشنهادی

بخش اصلی نوآوری سیستم ما، استفاده از یک سامانه موقعیت مکانی است. در سامانه Paws، با استفاده از یک Privacy Beacon سیاست حیطه شخصی یک سرویس دهنده اعلام می‌شود. البته برای سرعت بیشتر، آدرس آن اعلام می‌گشت و دریافت، مذاکره و بقیه کارها بر روی یک پروکسی مناسب بر روی اینترنت به انجام می‌رسید.

در این سیستم برای یافتن سرویس‌های فعلی و نیز سیاست حیطه شخصی آن‌ها از یک سامانه تشخیص موقعیت داخل ساختمان استفاده می‌شود. در این روش، دستگاه همراه هر کاربر که پروکسی شخصی او به شمار می‌رود، با استفاده از رابط بی‌سیم شدت سیگنال به نویز را برای نقاط دسترسی موجود سنجیده و آن را برای سرویس دهنده موقعیت مکانی ارسال می‌نماید. سرویس دهنده موقعیت مکانی نیز با بررسی در پایگاه داده‌های شدت سیگنال و استفاده از یک الگوریتم مناسب، شباهت میان این سنجش را با سنجش‌های قبلی بررسی کرده و نزدیک‌ترین موقعیت ممکن را تشخیص می‌دهد.

## ۶- بهبودهای سیستم جدید

این مدل بهبودهایی را نسبت به مدل ذکر شده ارائه می‌کند که بخشی از آن به شرح زیر است:

۱. حذف بخش اعلان‌کننده سیاست‌های سرویس‌دهنده‌ها و ادغام آن در سرویس دهنده خدمات مرتبط با مکان
۲. استفاده از سخت‌افزارهای عام برای پیاده‌سازی سیستم
۳. بهبود زمان پاسخ سیستم

## ۶-۱ بخش‌های مختلف در مدل

بخش‌های مختلف موجود در این مدل به شرح زیر هستند:

### ۶-۲ خدمات مرتبط با مکان

همان‌طور که توضیح داده شد، خدمات مختلفی در هر اتاق موجود است که کاربر می‌تواند از میان آن‌ها خدمت مورد نظر خود را انتخاب نماید. برای ارائه این خدمات ابتدا باید داده‌ها از مدل محیط استخراج گردند. برای این کار باید درخواستی به آن ارسال شده و پاسخ گرفته شود.

### ۶-۳ پایگاه داده‌های آگاه از حیطه شخصی

داده‌ها باید در پایگاه داده ذخیره شوند. اما به دلیل عدم دسترسی به یک پایگاه داده آگاه از حیطه شخصی، در حال حاضر این بخش مد نظر قرار نگرفته است. پیاده‌سازی [۱] از یک پایگاه داده‌های آگاه از حیطه شخصی مبتنی بر سامانه مدیریت پایگاه داده‌های اراکل، شامل بیش از ۹۰ هزار خط کد جاواست که نشان‌دهنده حجم زیاد کد لازم برای چنین پیاده‌سازی است.

برای هر یک از خدمات، یک سیاست حریم شخصی با قالب P3P تعریف می‌شود. امکان افزودن ویژگی‌های خاص محیط محاسبات فراگیر در این قالب نیز وجود دارد.

### ۶-۴ خدمات موقعیت مکانی

خدمات موقعیت مکانی قرار است که موقعیت کاربر را به او اعلام کند. بنابراین در ابتدا یک پایگاه داده‌های قدرت سیگنال و نقاط مرتبط آن تشکیل می‌شود. راه دیگر آن است که یک تابع مناسب برای ارائه شدت سیگنال داشته باشیم.

سپس یک شدت مجموعه شدت سیگنال از پروکسی کاربر دریافت شده و توسط یک الگوریتم مناسب، نقطه مورد نظر تشخیص داده شود.

### ۶-۵ پروکسی خدمات

این پروکسی وظیفه ارائه سیاست حیطه شخصی خدمات را بر عهده دارد. برای انجام کار، ابتدا باید موقعیت کاربر توسط خدمات موقعیت مکانی به پروکسی خدمات ارسال شود و سپس پروتکل حریم شخصی با قالب P3P برای خدمات مرتبط دریافت گردد. البته به جای خود

پروتکل، می‌توان یکی از پروتکل‌های موجود را انتخاب کرد. تعداد مشخصی پروتکل تعریف شده و شماره آن اعلام می‌گردد.

پس از این، این سیاست حریم شخصی برای پروکسی کاربر ارسال می‌گردد تا عمل تطبیق با ترجیحات او انجام گیرد.

## ۶-۶ مدل محیط

مدل محیط برای شبیه‌سازی به کار برده می‌شود و اگر بخواهیم سامانه پیشنهادی پیاده‌سازی واقعی شود، باید خدمات قابلیت جمع‌آوری اطلاعات مناسب را داشته باشند. این مدل، قادر است که کارهای زیر را به انجام برساند:

۱. مدل‌سازی حرکت یک کاربر در محیط: کاربران مختلف که به صورت تصادفی وارد ساختمان می‌شوند، به صورت تصادفی بر اساس یکی از چند مدل حرکت موجود، در سیستم حرکت می‌کنند و از اتاقی وارد اتاق دیگر می‌شوند و در نهایت از یکی از درها خارج می‌گردند.

۲. مدل‌سازی و پیدا کردن شدت سیگنال چند نقطه دسترسی در محیط: برای شبیه‌سازی شدت سیگنال در محیط، تابعی تعریف شده است که بر اساس فاصله از نقاط دسترسی و وضعیت اتاق شدت سیگنالی را به آن نقطه نسبت می‌دهد. راه دیگر استفاده از داده‌های ثبت شده از یک سیستم واقعی می‌باشد.

۳. ارسال اطلاعات محیطی یک نقطه بنا به درخواست: خدمات تعریف شده باید بر اساس داده‌های جمع‌آوری شده به کاربر ارائه شوند، بنابراین باید مدل محیطی قادر به ارائه داده‌هایی در مورد کاربر باشد.

بخشی از این مدل محیطی، متکی به شبیه‌ساز ارائه شده در [۱۱] می‌باشد.

## ۶-۷ پروکسی کاربر

وظایف آن به شرح زیر است:

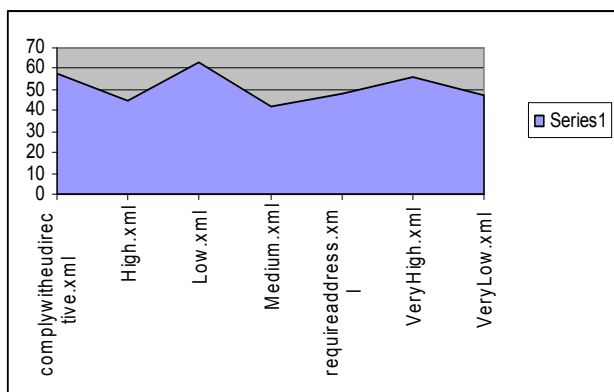
- درخواست اطلاعات شدت سیگنال از مدل محیط
- ارسال اطلاعات شدت سیگنال به سرویس دهنده موقعیت مکانی
- دریافت سیاست حریم شخصی کاربر
- انجام تطابق این سیاست با خواسته‌های کاربر که در قالب APPEL بیان شده‌اند.
- آگاه کردن کاربر از نتیجه تطابق

## ۷- شبیه‌سازی

### ۷-۱ تشخیص موقعیت

برای محیط شبیه‌سازی، یک سامانه تشخیص موقعیت ایجاد شده که می‌تواند با استفاده از شدت سیگنال، موقعیت کاربر را تخمین بزند.

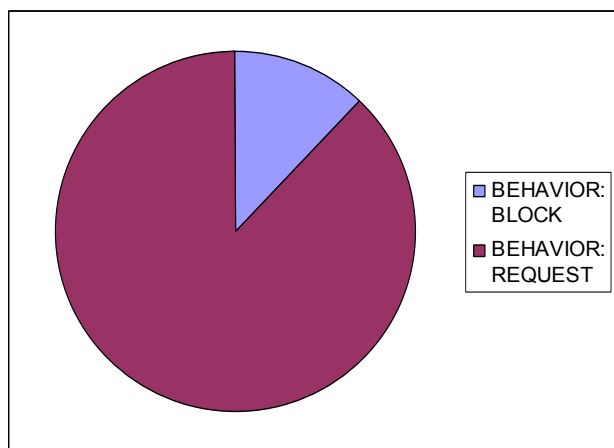
## ۹- درصد موفقیت



شکل ۲- نمودار ترجیحات انتخاب شده

BEHAVIOR: BLOCK 44

BEHAVIOR: REQUEST 315



شکل ۳- درصد موفقیت

خروجی نمونه به صورت زیر می باشد:

POLICY: Policies/EUpolicy.xml

RULESET: rulesets/VeryLow.xml

BEHAVIOR: REQUEST

REQUIRES USER'S CONSENT: no

MEANING: none of the prohibited characteristics have been found in this policy

این بدان معنی است که بدون نیاز به دریافت پاسخ از کاربر، این سرویس قابل ارائه می باشد.

## ۱-۹ بهبود زمانی

اجزای مورد استفاده در یافتن سرویس در دو حالتی که از اعلان کننده سرویس استفاده می شود و مدل طراحی شده، به جز زمان ارتباط با اعلان کننده سرویس، یکسان است. این زمان ارتباط با اعلان کننده، معمولاً بیشتر از ۵ ثانیه است که معمولاً زمان جستجو برای یافتن سرویس دهنده روی این مقدار تنظیم می شود.

در حقیقت، مشابه آن چه در برنامه واقعی تشخیص موقعیت نوشته شده، بر اساس پایگاه داده های سیگنال انجام گرفته است.

## ۲-۷ حیطه شخصی

برای پیاده کردن سیاست حیطه شخصی، باید تطابق میان سیاست های حیطه شخصی تعریف شده و ترجیحات کاربران ایجاد شود.

در برنامه نوشته شده از محیط JRC P3P Policy Workbench استفاده شده که مجموعه نرم افزاری برای کار با سیاست های حیطه شخصی P3P و ترجیحات کاربران در قالب APPEL می باشد.

این محیط که با استفاده از زبان جاوا نوشته شده است، قابلیت ایجاد، ویرایش و نیز تطابق سیاست ها و ترجیحات کاربران را دارد.

در محیط شبیه سازی برای هر کدام از کاربران، یکی از ترجیحات به صورت تصادفی انتخاب شده و کار تطابق با مکانی که تشخیص داده شده کاربر در آنجا قرار دارد، انجام می گیرد.

## ۳-۷ مدل محیط

مدل محیط به گونه ای است که کاربران به صورت تصادفی به این محیط وارد می شوند و اطلاعات مربوط به آن ها نگهداری شده و به سرویس های تأیید شده ارائه می گردد.

## ۸- نتایج شبیه سازی

### ۱-۸ تعداد افراد

شبیه سازی انجام شده به مدت ۱۵ دقیقه انجام شد و در این مدت تعداد ۳۵۹ نفر وارد با فاصله های تصادفی وارد ساختمان شده و از سرویس های مختلف استفاده کردند.

### ۲-۸ سیاست ها و ترجیحات حیطه شخصی

سیاست های تعریف شده، سه سیاست بودند که با نام های EU-Policy، Policy1.xml و Policy2.xml تعریف شده و به صورت تصادفی اختصاص می یافتند.

۷ حالت مختلف هم برای ترجیحات حیطه شخصی در نظر گرفته شده که به شرح زیر می باشد:

complywithdirective.xml	58
High.xml	45
Low.xml	63
Medium.xml	42
requireaddress.xml	48
VeryHigh.xml	56
VeryLow.xml	47

- [2] Pollach I., "What's Wrong with Online Privacy Policies," *Communications of the ACM*, Vol. 50, No. 9, September 2007.
- [3] Bhaskar P., Ahamed S. I., "Privacy in Pervasive Computing and Open Issues," *The Second International Conference on Availability, Reliability and Security (ARES'07)*, 2007.
- [4] LaMarca A. et al, "Place Lab: Device Positioning Using Radio Beacons in the Wild," *Proceedings of International Conference on Pervasive Computing*, June 2005.
- [5] Harle R., Beresford A., "The Bat System," *Ubiquitous Computing Workshop*, 2002.
- [6] PlaceLab project, available online at <http://placelab.org>
- [7] Bangs A., Haerinck S., "Location Aware Security Application," Bachelor of Science Thesis, Worcester Polytechnic Institute, 2006.
- [8] Bahl P., Padmanabhan V., "RADAR: An In-Building RF-based User Location and Tracking System," *Infocom*, 2000
- [9] Bahl P., Padmanabhan V., "Enhancements to the RADAR User Location and Tracking System," Technical Report MSR-TR-00-12, Microsoft Research, February 2000.
- [10] Bolliger P., "Redpin - Adaptive, Zero-Configuration Indoor Localization through User Collaboration," *Proceedings of the First ACM International Workshop on Mobile Entity Localization and Tracking in GPS-less Environment Computing and Communication Systems*, San Francisco, USA, September 2008.
- [11] Anwari M., "A Context Aware Advertisement Scheduler for Pervasive Computing Environments," Bachelor of Science Thesis, Amirkabir University, Tehran, Iran, 2008.

با حذف این بخش، در هر ارتباط، این مقدار صرفه‌جویی می‌شود و چون در قبال هر پردازش به طور میانگین تنها ۵۰۰ میلی ثانیه صرف خواندن و پردازش سیاست‌ها می‌گردد، به وضوح بهبود زمانی قابل توجهی در زمان یافتن سرویس و بررسی و تطبیق سیاست‌ها خواهیم داشت.

#### ۱۰- نتیجه‌گیری

برای پیاده‌سازی سیستم‌های محاسبات فراگیر، مواردی مانند امنیت و حیطه شخصی نقشی اساسی دارد. در این مقاله، ما یک ساختار جدید برای حفظ حیطه شخصی در محاسبات فراگیر ارائه دادیم که با استفاده از سیاست‌های مشخص شده توسط سرویس‌ها و ترجیحات کاربران، قادر به رعایت قوانین تعریف شده در این سیاست‌ها بود.

در این ساختار، با تکیه بر مدل‌های قبلی مانند Paws یک سامانه جدید طراحی شد که با تغییرات داده شده، به جای استفاده از سامانه اعلان کننده حیطه شخصی، از یک سرویس دهنده متمرکز در هر ساختمان بهره می‌برد و با تکیه بر یک سیستم تشخیص موقعیت داخل ساختمان، قابلیت یافتن سرویس‌ها، و بررسی و مذاکره بر روی سیاست‌های ارائه شده را دارد.

همچنین، با حذف بخش اعلان کننده، به دلیل حذف ارتباطات مادیون قرمز یا بلوتوث، هم صرفه‌جویی قابل توجهی در زمان یافتن سرویس و مذاکره ایجاد گشت، و هم سیستم با سخت افزارهای عام، قابل پیاده‌سازی شد.

#### مراجع

- [1] Langheinrich M., "Personal Privacy in Ubiquitous Computing, Tools and System Support," PHD thesis, Swiss Federal Institute of Technology Zurich, 2005.



# SID



سرویس های  
ویژه



سرویس ترجمه  
تخصصی



کارگاه های  
آموزشی



بلاگ  
مرکز اطلاعات علمی



عضویت در  
خبرنامه



فیلم های  
آموزشی

## کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی



مباحث پیشرفته یادگیری عمیق؛  
شبکه های توجه گرافی  
(Graph Attention Networks)



کارگاه آنلاین آموزش استفاده از  
وب آوساینس



کارگاه آنلاین مقاله روزمره انگلیسی