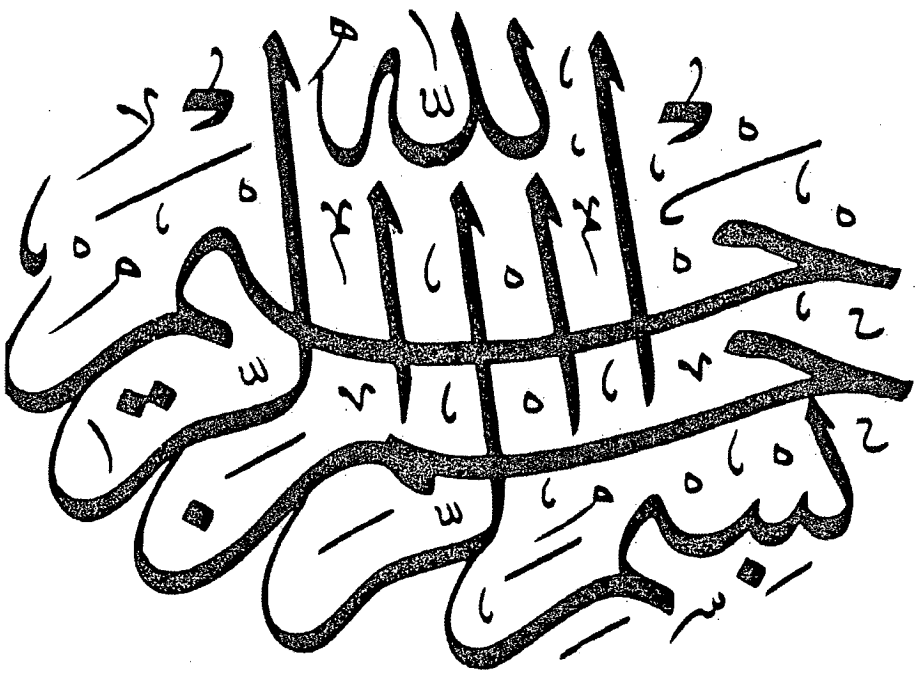

دانشگاه اصفهان

دانشکده فنی و مهندسی

گروه مهندسی کامپیوتر

پایان نامه ی کارشناسی ارشد رشته ی مهندسی کامپیوتر گرایش نرم افزار

ارائه یک متدلوژی برای توسعه کاربردهای بی نشانی

استاد راهنما:

دکتر بهروز ترک لادانی

پژوهشگر:

مرضیه ایسپره

مهر ماه ۱۳۸۸

دانشگاه اصفهان

دانشکده فنی و مهندسی

گروه مهندسی کامپیوتر

پایان نامه ی کارشناسی ارشد رشته ی مهندسی کامپیوترگرایش نرم افزار

خانم مرضیه اسپیره تحت عنوان

ارائه یک متدلوژی برای توسعه کاربردهای بی نشانی

در تاریخ ۸۸/۷/۲۸ توسط هیأت داوران زیر بررسی و با درجه عالی به تصویب نهایی رسید.

۱- استاد راهنمای پایان نامه دکتر بهروز ترک لادانی با مرتبه ی علمی استادیار امضا

۲- استاد داور داخل گروه دکتر ناصر نعمت بخش با مرتبه ی علمی استادیار امضا

۳- استاد داور خارج از گروه دکتر مهدی برنجکوب با مرتبه ی علمی استادیار امضا

امضای مدیر گروه

با سپاس فراوان از

آنان که در راه کسب علم و معرفت برای من آنچه در توان داشتند انجام دادند خصوصا جناب آقای دکتر ترک لادانی که بدون یاری ایشان تحقق این پایان نامه امکان پذیر نبود.

تقدیم به

پدر و مادر عزیزم که هر آنچه دارم از برکت وجود ایشان است

و

همسر مهربانم که همواره مشوق راه دانشم بوده اند

چکیده: کاربردهای بسیاری وجود دارند که نیازمند تامین بی نشانی هستند. به همین علت تاکنون روش ها و پروتکل های مختلفی برای تامین این نیازهای بی نشانی ارائه شده اند. اما نیازهای بی نشانی در کاربردهای مختلف متفاوت است و هر یک ویژگی های خاص خود را دارا هستند. بنابراین طراحی و ارائه روش های تامین بی نشانی کار ساده ای نیست. غالبا این روش ها به صورت ابتکاری طراحی شده اند و طراحان روش های متفاوتی را برای رسیدن به نتیجه طی نموده اند. در واقع تاکنون کار صریح و روشنی برای توصیف و تحلیل واضح نیازهای بی نشانی و پیاده سازی آنها به صورت ساختار یافته و قاعده مند وجود ندارد. ما در این پایان نامه یک متدلوژی برای طراحی و توسعه کاربردهای بی نشانی ارائه نموده ایم.

این متدلوژی شامل سه بخش برای پوشش فازهای تحلیل، طراحی و پیاده سازی در توسعه سیستم های نرم افزاری می باشد. هر فاز در این پایان نامه در یک فصل جداگانه آمده است. با کمک این متدلوژی، علاوه بر تسهیل طراحی و پیاده سازی روش های بی نشانی، تحلیل و ارزیابی روش های بی نشانی موجود نیز روشمند تر انجام خواهد شد. همچنین ما یک میان افزار بی نشانی براساس این متدلوژِی ارائه نموده ایم. در نهایت نیز این متدلوژی ارزیابی شده است.

واژگان کلیدی: بی نشانی، متدلوژی، کاربردهای بی نشانی، میان افزار بی نشانی

فهرست مطالب

عنوان **صفحه**

عنوان صفحه

عنوان صفحه

فصل پنجم: واسط بی نشانی(AnonymityAPI)

عنوان صفحه

فهرست شکلها

عنوان صفحه

عنوان **صفحه**

فصل پنجم: واسط بی نشانی(AnonymityAPI)

فهرست جدولها

عنوان **صفحه**

عنوان صفحه

فصل اول: کلیات

۱-۱ مقدمه

استفاده از شبکه‌های کامپیوتری و خصوصا اینترنت در سال‌های اخیر در زمینه‌های مختلفی چون تجارت الکترونیک افزایش یافته است. سیستم های تجارت الکترونیک و دیگر سیستم های مبتنی بر وب برای بقاء و ادامه حیات خود نیازمند تامین ویژگی های امنیتی هستند تا کاربران آنها با اطمینان خاطر بیشتری به انجام امور خود از طریق این سیستم ها بپردازند. اگرچه با استفاده از تکنیک های رمز نگاری محتوای پیام های مبادله شده بین موجودیت های مختلف یک سیستم محفوظ می ماند اما اطلاعات ارتباطی دیگر همچون طول پیام ها، زمان های ارتباط، حجم ارتباطات، طرف های در گیر در ارتباط و ... قابل مشاهده و دست یابی است[۱]. این نوع مشاهدات اطلاعات زیادی در مورد کاربران سیستم ها، علایق و الگوهای رفتاری آن ها و نحوه ارتباط آنها با یکدیگر در اختیار می گذارد که گاهی همین موارد نیز تعیین کننده محتوای ارتباطات خواهد بود.

جهت حل این مشکلات، روشهای مبتنی بر بی‌نشانی به عنوان ابزاری در جهت حفاظت حریم خصوصی افراد پیشنهاد شدند. با ایجاد بی‌نشانی، ارتباط بین آغازکننده ارتباط و پاسخ دهنده آن از دید ناظرین پنهان می‌ماند. همچنین می توان اطلاعات آغاز کننده ارتباط را از دید پاسخ دهنده آن پنهان نمود.

۱-۲ مسائل مطرح در زمینه بی نشانی و انگیزه این تحقیق

امروزه روش های ایجاد بی نشانی به ویژه با هدف حفظ حریم خصوصی موجودیت ها در کاربردهایی نظیر تجارت الکترونیک[1]، انتخابات الکترونیک[2] و ... مورد توجه قرار گرفته است. همان گونه که گفته شد محتوای پیامها با استفاده از روش های رمزنگاری محافظت می‌شوند ولی مسیر پیام، مبدا و مقصد پیام، مدت و زمان ارسال پیام، حجم پیام ارسالی و اطلاعاتی از این دست روشن و مشخص باقی می مانند. گاهی تنها با مشاهده الگوی ارتباطی افراد می توان به اطلاعات ارزشمندی در مورد آنها دست یافت. دسترسی به این قبیل اطلاعات در مورد اشخاص یا نهادهای درگیر در یک ارتباط معمولاً مورد قبول آنها نیست و به نوعی نقض حریم خصوصی آنها تلقی می شود. با بی نشان نمودن ارتباطات و داده ها می توان از افشاء این قبیل اطلاعات جلوگیری نمود. بنابراین بی نشانی به عنوان شاخه ای از امنیت اطلاعات به شمار می رود[۲].

کاربردهای زیادی وجود دارند که به بی نشانی نیاز دارند. هر کاربرد براساس نیاز خود، ویژگی های بی نشانی خاص خود را نیازمند است. یک سیستم پرداخت الکترونیک[3] را در نظر بگیرید که در آن کاربران می توانند در لیست کالاهای مختلف جستجو و کالاهای مورد نظر خود را انتخاب و در نهایت خرید کنند. اغلب خریداران تمایل به افشاء هویت و ویژگی های شخصی خود چون علایق و الگوهای رفتاری شان را ندارند. اما حتی با پنهان نمودن شناسه صحیح و واقعی کاربران، دنباله اعمال و سوابق عملکرد کاربر می تواند هویت وی یا علایق و ترجیحات او را آشکار نماید. بنابراین، علاوه بر پنهان نمودن شناسه کاربر، پنهان نمودن ارتباط بین اعمال مختلف او در سیستم خرید نیز مورد نیاز است. اما نکته قابل توجه این است که بی نشانی خریداران در این سیستم باید به نحو کنترل شده ای اعمال شود تا صحت معاملات از بین نرود. بدین معنا که در یک سیستم پرداخت الکترونیک، بی نشانی باید به نحوی باشد که در صورت بروز تخلف، بتوان بی نشانی آن عمل منافی قانون را حذف نموده و انجام دهنده آن عمل را شناسایی نمود. در واقع توانایی اینکه بتوان دقیقا مسئولیت کارها را به افراد یا عناصر خاص در سیستم نسبت داد، این

---

1 Electronic Commerce
2 Electronic Voting
3 Electronic Payment

امکان را فراهم می آورد که با در نظر گرفتن قوانین و سیاست هایی در سیستم، افراد را از انجام اعمال مغایر با منافع کل سیستم منع نمود[۳].

در مقابل، یک سیستم مشاوره پزشکی برخط[1] را در نظر بگیرید که در آن به بیماران مشاوره پزشکی می دهند به نحوی که هویت بیمار پنهان بماند. از آنجا که سوابق پزشکی بیمار در امر مشاوره نقش مهمی دارد، پنهان نمودن سوابق عملکرد بیمار (یا به عبارتی مکاتبات قبلی بیمار با پزشک) صحیح نبوده و در ارائه مشاوره صحیح خلل قابل توجهی ایجاد خواهد نمود. بنابراین بر خلاف سیستم پرداخت الکترونیک که نیازمند پوشش سوابق عملکرد خریداران بود، در این کاربرد پوشش سوابق ارتباطی بیمار صحت مشاوره را از بین خواهد برد.

با وجود چنین تفاوت هایی در نیازهای بی نشانی کاربردهای مختلف، تعاریف و دسته بندی دقیقی از مفاهیم بی نشانی، نیازها و ویژگی های مختلف بی نشانی و روش طراحی آنها ارائه نشده است. البته تاکنون برای تامین نیازهای بی نشانی کاربردهای متفاوت و پروتکل های مختلفی ارائه شده است اما هر کدام از آنها به صورتی ابتکاری[2] و متفاوت ارائه شده و متدلوژی مشخص و معینی برای تشخیص و تبیین و تامین نیازمندی های بی نشانی استفاده نشده است. در حالیکه داشتن یک متدلوژی برای توسعه نرم افزار، خصوصا نرم افزارهای امنیتی، امری ضروری است، چرا که وجود یک متدلوژی در هر زمینه ای و از جمله بی نشانی، توانایی تحلیل و توصیف دقیق نیازهای کاربرد را به طراحان می دهد و بنابراین پیچیدگی تحلیل و طراحی نرم افزار کاهش می یابد. علاوه بر این باعث صرفه جویی در وقت و هزینه خواهد شد چراکه طراحی دقیق منجر به شناسایی و حذف مشکلات سیستم در فاز طراحی و قبل از پیاده سازی کامل سیستم می شود.

در این پایان نامه قصد داریم یک متدلوژی برای توسعه کاربردهای بی نشانی ارائه دهیم که پیچیدگی های موجود در تحلیل و طراحی کاربردها و پروتکل های بی نشانی را کاهش داده و طراحی و پیاده سازی کاربردهای بی نشانی ساده تر و به صورتی سیستماتیک امکانپذیر شود.

متدلوژی های مختلف دارای فازهای مختلفی هستند اما غالب متدلوژی های توسعه نرم افزار دارای چرخه طراحی[3] زیر هستند[۴]:

- فاز تحلیل نیاز ها

---

1 Online
2 Heuristic
3 Design Cycle

در این فاز نیازهای کارفرمایان[1] جمع آوری و تحلیل می شود. طراحان نرم افزار با کاربران سیستم مصاحباتی انجام خواهند داد تا نیاز ها را دریافت نموده و مستند سازی[2] کنند. خروجی این فاز مجموعه مستندی از نیازهای کارفرمایان است.

- فاز طراحی مفهومی

هدف از این فاز تولید یک طراحی مفهومی برای کاربرد است به نحوی که از مکانیزم پیاده سازی مستقل باشد. این فاز دو هدف اصلی را در بر می گیرد. اول آنکه طراحی باید همه نیازهای فاز اول را در برگیرد. دوم آنکه یک ساختار صحیحی از سیستم که فهم آن نیز ساده باشد ارائه نماید.

- فاز پیاده سازی

در این فاز مفاهیمی که در فاز قبل به دست آمده است به یک مکانیزم پیاده سازی نگاشت خواهد شد.

در این پایان نامه برای پوشش فاز اول متدلوژی توسعه کاربردهای بی نشانی AnonymityModel ارائه شده است که یک مدل مفهومی توصیف بی نشانی می باشد. این مدل به تعریف دقیق بی نشانی و مفاهیم مرتبط با آن پرداخته و با در نظر گرفتن همه جنبه های بی نشانی، به ارائه یک دسته بندی از انواع سرویس های بی نشانی و ویژگی های آنها پرداخته است. بنابراین این مدل برای تحلیل و توصیف نیازهای بی نشانی طیف وسیعی از کاربردهای بی نشانی می تواند استفاده شود.

در فاز دوم AnonymityUML ارائه شده است، بسطی از UML برای کاربردهای بی نشانی. این بسط منطبق بر AnonymityUML بوده و بنابراین توصیف و تبیین نیازهای بی نشانی که از فاز اول استخراج شده اند بوسیله آن به راحتی صورت می پذیرد. AnonymityUML با تاکید بر قابلیت های بی نشانی، نوع نیاز های بی نشانی و محل اعمال آنها در سیستم (که باید در پیاده سازی در نظر گرفته شوند) ، به طراحان سیستم در طراحی صحیح و ساده تر سیستم یاری می رساند.

در فاز سوم پس از شناخت و استخراج تکنیک های پایه تامین بی نشانی در سیستم ها و نوع سرویس بی نشانی که هر یک تامین می نمایند، به ارائه یک واسط نرم افزاری برای پیاده سازی کاربردها و پروتکل های بی نشانی در لایه ارتباطات با نام AnonymityAPI پرداخته ایم. این واسط به صورت یک بسته[3] جاوایی نوشته شده و همه تکنیک های پایه تامین بی نشانی در لایه ارتباطات را در بر می گیرد. طراحان سیستم های بی نشانی می توانند با

---

1 Stakeholders
2 Document
3 Package

افزودن jar فایل این بسته جاوایی به کاربردهای مختلف و پیاده سازی کلاس های آن بر حسب نیاز خود، تکنیک های پایه مورد نیاز خود را فراخوانی و استفاده نمایند.

۱-۳ مروری بر ساختار پایان نامه

ساختار پایان نامه به این ترتیب است. در فصل دوم ابتدا مفهوم بی نشانی مطرح شده و سپس کارهای انجام شده در زمینه پروتکل های تامین بی نشانی، کاربردهای بی نشانی و متدلوژی های ارائه شده در این زمینه مطرح و بررسی خواهند شد. در فصل سوم AnonymityModel ارائه خواهد شد و براساس آن نیاز های بی نشانی چند پروتکل مهم تامین بی نشانی و چند کاربرد بی نشانی استخراج می شوند. در فصل چهارم AnonymityUML با استفاده از روش های استاندارد بسط UML ارائه می شود. این بسط همه موارد مطرح شده در AnonymityModel را در بر می گیرد. در انتهای این فصل نیز یک کاربرد و یک پروتکل نمونه با استفاده از AnonymityUML توصیف و طراحی خواهد شد.

در فصل پنجم پس از بررسی و استخراج تکنیک های پایه تامین بی نشانی و تعیین نوع سرویس بی نشانی که هر یک تامین می نمایند، AnonymityAPI در قالب یک بسته جاوایی ارائه می شود. در انتهای این فصل نیز یک پروتکل نمونه با استفاده از این واسط پیاده سازی می شود. همچنین نحوه استفاده از تکنیک های پایه در طراحی کاربردهای بی نشانی با استفاده از چند مثال تشریح می شود. در نهایت در فصل ششم پس از بیان نتایج و ارزیابی متدلوژی، با ارائه پیشنهادات بحث را به پایان می‌بریم.