



دانشگاه اصفهان

دانشکده فنی و مهندسی

گروه مهندسی کامپیوتر

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

ارائه یک مدل‌سازی برای توسعه کاربردهای بی‌نشانی

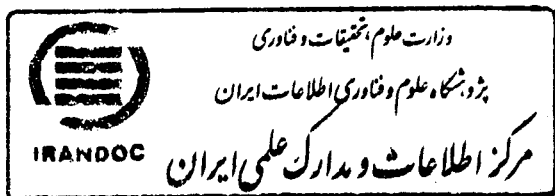
استاد راهنما:

دکتر بهروز ترک‌لادانی

پژوهشگر:

مرضیه ایسپره

مهر ماه ۱۳۸۸

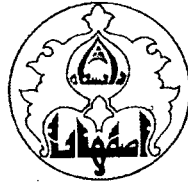


۱۵۹۵۴۳

۱۳۹۰/۳/۲۲

کلیه حقوق مادی مترتب بر نتایج مطالعات، ابتکارات
و نوآوری های ناشی از تحقیق موضوع این پایان نامه
متعلق به دانشگاه اصفهان است.

شيوه نگارش پايان نامه
رعايت شده است
تخصیلات تکمیلی دانشگاه اصفهان



دانشگاه اصفهان

دانشکده فنی و مهندسی

گروه مهندسی کامپیوتر

پایان نامه ی کارشناسی ارشد رشته ی مهندسی کامپیوتر گرایش 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
خصوصاً 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. غالباً 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 متدولوژی برای طراحی و توسعه کاربردهای بی نشانی ارائه نموده ایم.

این متدولوژی 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 متدولوژی، 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 متدولوژی ارائه نموده ایم. در نهایت نیز این متدولوژی ارزیابی شده است.

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

فهرست مطالب

صفحه	عنوان
فصل اول: کلیات	
۱-۱	مقدمه..... ۱
۲-۱	مسائل مطرح در زمینه بی نشانی و انگیزه این تحقیق..... ۲
۳-۱	مروری بر ساختار پایان نامه..... ۵
فصل دوم: بی نشانی	
۱-۲	مقدمه..... ۶
۲-۲	پروتکل های تامین بی نشانی..... ۸
۱-۲-۲	پروتکل Mix-Net..... ۸
۲-۲-۲	پروتکل مسیریابی پیازی..... ۱۱
۳-۲-۲	پروتکل Crowd..... ۱۳
۴-۲-۲	پروتکل تامین بی نشانی عامل های متحرک..... ۱۵
۳-۲	کاربردهای بی نشانی..... ۱۶
۱-۳-۲	پست الکترونیک..... ۱۷
۲-۳-۲	پرداخت الکترونیک..... ۱۷
۳-۳-۲	صندوق الکترونیک..... ۱۸
۴-۳-۲	انتخابات الکترونیک..... ۱۹
۵-۳-۲	پویش وب..... ۱۹
۴-۲	متدلوژی های توسعه کاربردهای بی نشانی..... ۲۰
۱-۴-۲	کارهای موجود در زمینه متدلوژی های توسعه کاربردهای بی نشانی..... ۲۱
۲-۴-۲	کارهای موجود در زمینه تحلیل نیازهای بی نشانی..... ۲۵
۳-۴-۲	کارهای مشابه در زمینه تبیین و توصیف نیازهای بی نشانی..... ۲۹

۳۰	۴-۴-۲ کارهای مشابه در زمینه پیاده سازی کاربردهای بی نشانی
۳۳	۵-۲ جمع بندی

فصل سوم: مدل توصیف بی نشانی (AnonymityModel)

۳۵	۱-۳ مقدمه
۳۶	۲-۳ نشانی و انواع آن
۳۹	۳-۳ مدل توصیف بی نشانی
۳۹	۱-۳-۳ ساختار بی نشانی
۴۱	۲-۲-۳ ماهیت بی نشانی
۴۳	۳-۲-۳ ضابطه بی نشانی
۴۴	۴-۲-۳ جمع بندی مدل
۴۵	۴-۳ بررسی موردی
۴۵	۱-۴-۳ پروتکل Mix-Net
۴۶	۲-۴-۳ روش مسیریابی پیازی
۴۸	۳-۴-۳ پروتکل تامین بی نشانی عامل های متحرک
۴۹	۴-۴-۳ سرویس پست الکترونیک
۵۰	۵-۴-۳ سرویس پرداخت الکترونیک
۵۱	۵-۳ جمع بندی

فصل چهارم: بسطی از UML برای کاربردهای بی نشانی (AnonymityUML)

۵۲	۱-۴ مقدمه
۵۳	۲-۴ UML و روش های بسط آن
۵۵	۳-۴ AnonymityUML

۶۰	۴-۴ بررسی موردی
۶۰	۱-۴-۴ سیستم پرداخت الکترونیک
۶۴	۲-۴-۴ پروتکل تامین بی نشانی عامل های متحرک
۶۷	۵-۴ جمع بندی

فصل پنجم: واسط بی نشانی (AnonymityAPI)

۶۹	۱-۵ مقدمه
۷۰	۲-۵ معماری سیستم های تامین کننده بی نشانی
۷۲	۳-۵ تکنیک های پایه تامین بی نشانی
۷۳	۱-۳-۵ تکنیک های پایه تامین بی نشانی در لایه ارتباطات
۷۶	۲-۳-۵ تکنیک های پایه تامین بی نشانی در لایه کاربرد
۷۸	۳-۳-۵ تکنیک های پایه تامین بی نشانی مشترک در دو لایه
۸۰	۴-۳-۵ تجزیه و تحلیل چند پروتکل بی نشانی
۸۲	۴-۵ AnonymityAPI
۸۴	۱-۴-۵ معماری AnonymityAPI
۸۵	۲-۴-۵ کلاس Send
۸۷	۳-۴-۵ کلاس Receive
۸۹	۴-۴-۵ کلاس EncryptMessage
۹۱	۵-۴-۵ کلاس CompressMessage
۹۳	۶-۴-۵ کلاس PadMessage
۹۴	۷-۴-۵ کلاس FilterMessage
۹۵	۹-۴-۵ کلاس CacheMessage
۹۷	۱۰-۴-۵ کلاس DelayMessage
۹۷	۵-۵ پیاده سازی موردی
۱۰۰	۶-۵ جمع بندی

فصل ششم: جمع بندی و راهکارهای آینده

۱-۶	مقدمه.....	۱۰۱
۲-۶	مروری بر نتایج حاصل.....	۱۰۲
۳-۶	ارزیابی متدلوژی.....	۱۰۳
۴-۶	راهکارهای آینده.....	۱۰۴

پیوست ها

۱۰۵	پیوست ۱: کد AnonymityAPI.....	
۱۱۷	پیوست ۲: یک پیاده سازی ساده از برخی کلاس های AnonymityAPI.....	
۱۲۰	پیوست ۳: پیاده سازی الگوریتم Mix Net با استفاده از AnonymityAPI.....	
۱۲۳	منابع و مآخذ.....	

فهرست شکلها

صفحه	عنوان
	فصل دوم: بی نشانی
۸.....	شکل ۱-۲: روش Mix-Net.....
۱۲.....	شکل ۲-۲: پیاز ایجاد شده در فرستنده.....
۱۵.....	شکل ۳-۲: روش Crowd.....
۱۶.....	شکل ۴-۲: پروتکل تامین بی نشانی عامل های متحرک.....
۲۰.....	شکل ۵-۲: گراف اتصال برای سیستم دانشجویی مجازی.....
۲۱.....	شکل ۶-۲: گراف Petri Net برای سیستم دانشجویی مجازی.....
۲۲.....	شکل ۷-۲: اسکیمای EKD.....
۲۳.....	شکل ۸-۲: مدل مفهومی PriS.....
۲۴.....	شکل ۹-۲: مدل هدف سیستم انتخابات الکترونیک.....

فصل سوم: مدل توصیف بی نشانی (AnonymityModel)

۳۵.....	شکل ۱-۳: انواع مختلف نشانی موجودیت.....
۳۶.....	شکل ۲-۳: انواع مختلف نشانی پیام.....
۳۷.....	شکل ۳-۳: ساختار کلی سرویس ارائه بی نشانی در ارتباطات.....

فصل چهارم: بسطی از UML برای کاربردهای بی نشانی (AnonymityUML)

۵۰.....	شکل ۱-۴: بسطی از UML برای دامنه GIS و نحوه استفاده از آن.....
۵۶.....	شکل ۲-۴: UsecaseView بی نشانی خریدار از دید فروشنده.....
۵۶.....	شکل ۳-۴: UsecaseView بی نشانی خریدار از دید بانک.....
۵۷.....	شکل ۴-۴: UsecaseView بی نشانی خریدار از دید ناظر محلی/اسراسری.....
۵۸.....	شکل ۵-۴: دیاگرام Deployment سیستم خرید الکترونیک.....

شکل ۴-۶: UsecaseView بی نشانی مالک عامل از دید میزبان آن	۵۹
شکل ۴-۷: UsecaseView بی نشانی عامل از دید میزبان آن	۵۹
شکل ۴-۸: دیاگرام Deployment پروتکل عامل های متحرک	۶۰

فصل پنجم: واسط بی نشانی (AnonymityAPI)

شکل ۵-۱: معماری یک میان افزار بی نشان کننده	۶۴
شکل ۵-۲: فلوچارت پروتکل Crowd	۷۲
شکل ۵-۳: فلوچارت پروتکل Mix Net	۷۳
شکل ۵-۴: فلوچارت پروتکل عامل های متحرک	۷۴
شکل ۵-۵: خروجی حاصل از اجرای برنامه Sender	۸۸
شکل ۵-۶: خروجی حاصل از اجرای برنامه Mix	۸۸

فهرست جدولها

صفحه	عنوان
فصل دوم: بی نشانی	
۲۵.....	جدول ۱-۲: انواع بی نشانی براساس سه ویژگی ارتباط.....
۲۸.....	جدول ۲-۲: برخی از Stereotype های UMLSec.....
فصل سوم: مدل توصیف بی نشانی (AnonymityModel)	
۳۸.....	جدول ۱-۳: انواع بی نشانی موجودیت.....
۳۹.....	جدول ۲-۳: انواع بی نشانی پیام.....
فصل چهارم: بسطی از UML برای کاربردهای بی نشانی (AnonymityUML)	
۵۲.....	جدول ۱-۴: AnonymityUML Stereotypes.....
۵۳.....	جدول ۲-۴: AnonymityUML Tagged values.....
فصل پنجم: واسط بی نشانی (AnonymityAPI)	
۷۶.....	جدول ۱-۵: ویژگی های کلاس Send.....
۷۶.....	جدول ۲-۵: متدهای کلاس Send.....
۷۷.....	جدول ۳-۵: کلاس درونی کلاس Send.....
۷۸.....	جدول ۴-۵: ویژگی های کلاس Receive.....
۷۸.....	جدول ۵-۵: متدهای کلاس Receive.....
۷۹.....	جدول ۶-۵: ویژگی های کلاس EncryptMessage.....
۸۰.....	جدول ۷-۵: متدهای کلاس EncryptMessage.....
۸۱.....	جدول ۸-۵: متدهای کلاس CompressMessage.....

۸۱.....	جدول ۵-۹: متدهای کلاس CompressMessage
۸۲.....	جدول ۵-۱۰: ویژگی های کلاس PadMessage
۸۳.....	جدول ۵-۱۱: متدهای کلاس PadMessage
۸۴.....	جدول ۵-۱۲: متدهای کلاس FilterMessage
۸۴.....	جدول ۵-۱۳: متدهای کلاس ImpersonateMessage
۸۵.....	جدول ۵-۱۴: ویژگی های کلاس CacheMessage
۸۵.....	جدول ۵-۱۵: متدهای کلاس CacheMessage
۸۶.....	جدول ۵-۱۶: کلاس درونی کلاس CacheMessage
۸۶.....	جدول ۵-۱۷: ویژگی های کلاس DelayMessage
۸۶.....	جدول ۵-۱۸: متدهای کلاس DelayMessage

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. سیستم‌های تجارت الکترونیک و دیگر سیستم‌های مبتنی بر وب برای بقاء و ادامه حیات خود نیازمند تامین ویژگی‌های امنیتی هستند تا کاربران آنها با اطمینان خاطر بیشتری به انجام امور خود از طریق این سیستم‌ها پردازند. اگرچه با استفاده از تکنیک‌های رمزنگاری محتوای پیام‌های مبادله شده بین موجودیت‌های مختلف یک سیستم محفوظ می‌ماند اما اطلاعات ارتباطی دیگر همچون طول پیام‌ها، زمان‌های ارتباط، حجم ارتباطات، طرف‌های درگیر در ارتباط و ... قابل مشاهده و دست‌یابی است [۱]. این نوع مشاهدات اطلاعات زیادی در مورد کاربران سیستم‌ها، علایق و الگوهای رفتاری آن‌ها و نحوه ارتباط آنها با یکدیگر در اختیار می‌گذارد که گاهی همین موارد نیز تعیین‌کننده 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 می‌توان اطلاعات آغاز‌کننده ارتباط را از دید پاسخ دهنده آن پنهان نمود.

۲-۱ مسائل مطرح در زمینه بی‌نشانی و انگیزه این تحقیق

امروزه روش‌های ایجاد بی‌نشانی به ویژه با هدف حفظ حریم خصوصی موجودیت‌ها در کاربردهایی نظیر تجارت الکترونیک^۱، انتخابات الکترونیک^۲ و ... مورد توجه قرار گرفته است. همان‌گونه که گفته شد محتوای پیامها با استفاده از روش‌های 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 می‌مانند. گاهی تنها با مشاهده الگوی ارتباطی افراد می‌توان 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 می‌شود. با بی‌نشانی نمودن ارتباطات و داده‌ها می‌توان از افشاء این قبیل اطلاعات جلوگیری نمود. بنابراین بی‌نشانی به عنوان شاخه‌ای از امنیت اطلاعات به شمار می‌رود [۲].

کاربردهای زیادی وجود دارند که به بی‌نشانی نیاز دارند. هر کاربرد براساس نیاز خود، ویژگی‌های بی‌نشانی خاص خود را نیازمند است. یک سیستم پرداخت الکترونیک^۳ را در نظر بگیرید که در آن کاربران می‌توانند در لیست کالاهای مختلف جستجو و کالاهای مورد نظر خود را انتخاب و در نهایت خرید کنند. اغلب خریداران تمایل به افشاء هویت و ویژگی‌های 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 می‌تواند 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 بی‌نشانی خریداران در این سیستم باید به نحو کنترل شده‌ای اعمال شود تا صحت معاملات از بین نرود. بدین معنا که در یک سیستم پرداخت الکترونیک، بی‌نشانی باید به نحوی باشد که در صورت بروز تخلف، بتوان بی‌نشانی آن عمل منفی قانون را حذف نموده و انجام دهنده آن عمل را شناسایی نمود. در واقع توانایی اینکه بتوان دقیقاً 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^۱ 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^۲ 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 چرا که 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^۳ زیر هستند [۴]:

- فاز تحلیل نیازها

1 Online
2 Heuristic
3 Design Cycle

در این فاز نیازهای کارفرمایان^۱ جمع آوری و تحلیل می شود. طراحان نرم افزار با کاربران سیستم مصاحباتی انجام خواهند داد تا نیازها را دریافت نموده و مستند سازی^۲ 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 بر گیرد. 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 متدولوژی 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 نیازهای بی نشانی و محل اعمال آنها در سیستم (که باید در پیاده سازی در نظر گرفته شوند)، به طراحی 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^۳ 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.

۳-۱ 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 می بریم.