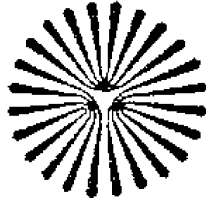


ای نام تو بهترین سرآغاز



دانشگاه پیام نور

دانشکده فنی و مهندسی

گروه علمی مهندسی فناوری اطلاعات و ارتباطات

پایان نامه کارشناسی ارشد

در رشته مهندسی کامپیوتر - گرایش نرم افزار

عنوان

ارائه روشی جدید برای مدل سازی صفت کیفی امنیت در معماری نرم افزار

نگارش

علی مقدوری

استاد راهنما

دکتر رضا رافع

استاد مشاور

دکتر احمد فراهی

زمستان ۱۳۸۸

تصویب نامه

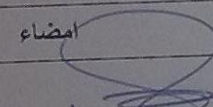
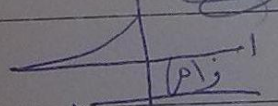
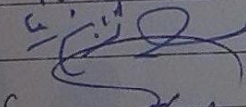

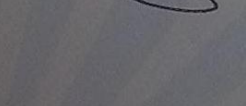
پایان نامه کارشناسی ارشد رشته رشته مهندسی کامپیوتر نرم افزار "تحت عنوان:

"ارائه روشی جدید برای مدل سازی صفت کیفی امنیت در معماری نرم افزار"

تاریخ دفاع: ۸۹/۶/۱۷ ساعت: ۳۰:۱۳-۱۲

نمره: ۱۵ - درجه ارزشیابی:

هیات داوران:

داوران	نام و نام خانوادگی	مرتبیه علمی	امضاء
استاد راهنما	دکتر رضا رافع	استاد	
استاد مشاور	دکتر احمد فراهی	استاد	
استاد داور داخلی	دکتر آرش قربان نیا		
استاد داور خارجی	دکتر اسلام ناظمی		
نماینده گروه	دکتر رضا عسکری مقدم		

چکیده

هدف اصلی مهندسی نرم افزار، تولید سیستم با کیفیت است. یکی از مهمترین مراحل که کیفیت یا صفات کیفی در آن مورد توجه قرار می گیرد مرحله تولید معماری نرم افزار سیستم می باشد. در این مرحله، نیازهای کیفی و تاکتیک های برآورده کننده آنها مدل شده و مورد ارزیابی قرار می گیرند. هدف این پایان نامه ارائه رویکردی جدید برای حل مسئله مدلسازی صفات کیفی در معماری نرم افزار بخصوص صفت کیفی امنیت در معماری نرم افزار می باشد برای ارائه این رویکرد بر پایه چارچوب ISLab مراحل ایجاد یک روش مدلسازی جدید برای مدل نمودن مدیریت اعتماد در سطح معماری نرم افزار نشان داده خواهد شد. مدیریت اعتماد، یکی از تاکتیک های دستیابی به امنیت بوده و با مدلسازی آن امکان ارزیابی میزان دستیابی به امنیت در معماری نرم افزار فراهم می گردد. مهمترین خروجی پژوهش انجام شده، یک پروفایل گسترش یافته بر پایه UML به نام T-UML می باشد که توانایی مدلسازی مدیریت اعتماد در سطح معماری نرم افزار را دارد. همچنین مدل های ایجاد شده توسط T-UML، مدل هایی با قابلیت ارزیابی می باشند.

واژه های کلیدی: مدلسازی صفات کیفی، مدیریت اعتماد، کنترل دسترسی، معماری نرم افزار، UML.

فهرست مطالب

گفتار اول: معرفی موضوع (تعریف صورت مسئله)

۱	۱-۱ مقدمه
۴	۲-۱ طرح مسئله (تعریف مسئله و بیان سوال‌های اصلی تحقیق)
۴	۳-۱ اهداف تحقیق
۵	۴-۱ محدوده تحقیق
۶	۵-۱ سابقه و ضرورت انجام تحقیق
۷	۶-۱ جنبه جدید بودن و نوآوری طرح
۷	۷-۱ روش انجام تحقیق
۷	۱-۷-۱ روش و ابزار گردآوری اطلاعات
۸	۲-۷-۱ جامعه آماری و نمونه
۸	۳-۷-۱ روش تجزیه و تحلیل اطلاعات
۸	۸-۱ کاربردهای تحقیق
۹	۹-۱ ساختار پایان نامه
۱۰	۱۰-۱ زمان‌بندی مراحل انجام تحقیق

گفتار دوم: صفات کیفی در معماری نرم‌افزار

۱۱	۱-۲ مقدمه
۱۱	۲-۲ معماری نرم‌افزار
۱۳	۳-۲ ارتباط معماری نرم‌افزار و صفات کیفی
۱۴	۴-۲ اندازه‌ها، متریک‌ها و شاخص‌ها
۱۵	۵-۲ سناریوهای صفات کیفی
۱۷	۶-۲ دستیابی به صفات کیفی
۱۷	۱-۶-۲ تاکتیکهای معماری
۱۸	۲-۶-۲ الگوهای معماری
۱۸	۳-۶-۲ مدلسازی تاکتیک‌ها و الگوهای معماری
۱۹	۷-۲ فرایند کلی مدلسازی و ارزیابی صفات کیفی در معماری نرم‌افزار

۲۱	۲-۷-۱ امکان‌سنجی صفات کیفی
۲۲	۲-۸ خلاصه گفتار
گفتار سوم: مفاهیم پایه امنیت و کارهای انجام شده	
۲۵	۳-۱ مفاهیم پایه
۲۵	۳-۱-۱ مروری بر امنیت
۲۶	۳-۱-۲ مدل‌های امنیتی
۲۶	۳-۱-۲-۱ مدل‌های کنترل دسترسی
۳۰	۳-۱-۲-۲ مدل مدیریت اعتماد
۳۲	۳-۱-۲-۳ تفاوت مدیریت اعتماد با کنترل دسترسی مبتنی بر نقش
۳۴	۳-۱-۲-۴ مدل جریان اطلاعات
۳۴	۳-۲ جایگاه کار ارائه شده در امنیت
۳۶	۳-۳ کارهای انجام شده
۳۷	۳-۳-۱ مدل فرایند
۳۹	۳-۳-۲ مدل‌سازی کنترل دسترسی در سیستم‌های امن
۴۰	۳-۳-۱-۲ مدل‌سازی کنترل دسترسی با زبان UML
۴۵	۳-۳-۲-۳ مدل‌سازی کنترل دسترسی با زبان‌های غیر UML
۴۶	۳-۴ مقایسه روش‌های ارائه شده
۴۷	۳-۵ خلاصه گفتار
گفتار چهارم: پروفایل T-UML	
۵۱	۴-۱ مقدمه
۵۳	۴-۲ مفاهیم پایه
۵۳	۴-۲-۱ عناصر اصلی مدل‌سازی مدیریت اعتماد در چارچوب RT
۵۶	۴-۲-۲ مدل‌سازی یک سیستم نمونه به وسیله چارچوب RT
۵۶	۴-۲-۳ نقاط ضعف مدل‌سازی سیستم به وسیله چارچوب RT
۵۷	۴-۳ مدل‌سازی مدیریت اعتماد با زبان UML
۵۷	۴-۳-۱ متا مدل UML

۵۸	۲-۳-۴ رویکردهای ممکن برای گسترش UML در مدیریت اعتماد در سطح معماری
۶۲	۳-۳-۴ مکانیزمهای گسترش زبان UML از طریق محدود کردن آن
۶۳	۱-۳-۳-۴ محدود کردن عناصر مدلسازی در سطح متامدل به کمک OCL
۶۴	۴-۴ پروفایل T-UML برای مدلسازی مدیریت اعتماد در سطح معماری نرم افزار
۶۵	۱-۴-۴ مدلسازی موجودیتها
۶۵	۲-۴-۴ مدلسازی نقش
۶۷	۳-۴-۴ مدلسازی رابطه اعطا کردن نقش به نقش (وکالت)
۶۷	۴-۴-۴ مدلسازی رابطه "داشتن صفت"
۶۸	۵-۴-۴ مدلسازی رابطه "مالکیت یک نقش"
۶۹	۶-۴-۴ مدلسازی رابطه "عضویت"
۷۰	۷-۴-۴ مدلسازی واسطها
۷۱	۸-۴-۴ رابطه "دسترسی به یک واسط"
۷۲	۹-۴-۴ خلاصه گسترشهای ارائه شده
۷۴	۵-۴ ارزیابی مدل‌های ایجاد شده
۷۶	۶-۴ الگوهای معماری برای مدلسازی مدیریت اعتماد در سطح معماری نرم افزار
۷۶	۱-۶-۴ الگوی معماری برای نمایش عضویت یک جزء در یک نقش
۷۶	۲-۶-۴ الگوی معماری برای نمایش اعطا کردن یک نقش به نقش دیگر
۷۷	۳-۶-۴ الگوی نقش‌های سلسله مراتبی
۷۸	۴-۶-۴ الگوی معماری اعطا کردن چند گانه
۷۹	۷-۴ ارائه یک مثال برای مدلسازی به کمک T-UML

گفتار پنجم: مطالعه موردی

۸۳	۱-۵ مقدمه
۸۳	۲-۵ تعریف مسئله
۸۳	۳-۵ حل مسئله
۸۴	۱-۳-۵ نیازمندی‌های مسئله
۸۵	۲-۳-۵ سناریو صفت کیفی
۸۶	۳-۳-۵ معماری کلی سیستم

- ۸۹ ۴-۵ مدل‌سازی سیستم از دیدگاه مدیریت اعتماد
- ۸۹ ۱-۴-۵ سناریو یک، دسترسی رایگان دانشجویان و اساتید دانشکده
- ۹۰ ۲-۴-۵ سناریو دو، امکان خریداری مقالات توسط دانشجویان دانشکده‌های
دیگر

گفتار ششم: ارزیابی معماری

- ۹۴ ۱-۶ مقدمه
- ۲-۶ روش‌های ارزیابی مبتنی بر سناریو
- ۹۵ ۱-۲-۶ روش تحلیل معماری نرم افزار (SAAM)
- ۹۶ ۲-۲-۶ روش تحلیل معماری با دید تعادلی (ATAM)
- ۹۸ ۳-۲-۶ روش تحلیل هزینه و سود (CBAM)
- ۱۰۲ ۳-۶ آنالیز و طراحی سیستم
- ۱۰۲ ۱-۳-۶ به دست آوردن سناریوهای کیفی سیستم
- ۱۰۲ ۲-۳-۶ سناریو صفت کیفی
- ۱۰۳ ۳-۳-۶ به دست آوردن معماری سیستم
- ۱۰۵ ۴-۶ بررسی امکان ارزیابی معماری ایجاد شده به روش CBAM
- ۱۰۸ ۵-۶ نتیجه‌گیری بررسی قابلیت ارزیابی مدل‌های معماری ایجاد شده

گفتار هفتم: نتیجه‌گیری و کارهای آینده

- ۱۰۱ ۱-۷ نوآوری‌ها و دستاوردهای پروژه
- ۱۰۱ ۱-۱-۷ ارائه پروفایل T-UML
- ۱۰۱ ۲-۱-۷ استفاده از چارچوب ISLab در حوزه معماری نرم‌افزار
- ۱۰۱ ۳-۱-۷ ارزیابی کارهای قبلی در زمینه مدل‌سازی کنترل دسترسی و اعتماد
- ۱۰۲ ۴-۱-۷ ارزیابی پروفایل توسعه یافته
- ۲-۷ پیشنهاد برای ادامه کار
- ۱۰۲ ۱-۲-۷ توسعه پروفایل T-UML
- ۱۰۳ ۲-۲-۷ استفاده و استانداردسازی چارچوب ISLab در حوزه‌های مختلف
- ۱۰۳ ۳-۲-۷ انجام پژوهش در زمینه مهندسی نرم‌افزار سیستم‌های امن

۱۱۴	پیوستار ۱- فهرست منابع
۱۱۹	پیوستار ۲- معرفی ISLab
۱۳۴	پیوستار ۳- واژه‌نامه فارسی به انگلیسی
۱۳۹	پیوستار ۴- واژه‌نامه انگلیسی به فارسی

فهرست اشکال

۳	شکل ۱-۱ تعداد آسیب‌پذیری‌های گزارش شده بر حسب سال توسط CERT/CC
۳	شکل ۲-۱ تعداد حملات گزارش شده بر حسب سال توسط CERT/CC
۱۶	شکل ۱-۲ بخش‌های تشکیل دهنده سناریو صفت کیفی [1]
۱۷	شکل ۲-۲ نمونه‌ای از تاکتیک‌های معماری امنیت [1]
۲۰	شکل ۳-۲ فرایند کلی مدل‌سازی و ارزیابی صفات کیفی در معماری نرم‌افزار
۲۹	شکل ۱-۳ کنترل دسترسی مبتنی بر نقش (RBAC)
۳۰	شکل ۲-۳ اجزا تشکیل دهنده سیستم RBAC سلسله مراتبی
۳۵	شکل ۳-۳ جایگاه کار ارائه شده در درخت پژوهش امنیت
۳۵	شکل ۴-۳ جایگاه کار انجام شده در درخت پژوهش معماری نرم‌افزار
۳۷	شکل ۵-۳ مهندسی نرم‌افزار سیستم‌های امن به عنوان یک تکنولوژی لایه ای
۵۲	شکل ۱-۴ مراحل طی شده برای ایجاد زبان مدل‌سازی T-UML
۵۸	شکل ۲-۴ معماری چهار لایه UML در مدل‌سازی
۵۹	شکل ۳-۴ متا مدل UML محدود شده برای مدل‌سازی مدیریت اعتماد
۶۰	شکل ۴-۴ گسترش متا مدل UML برای مدل‌سازی مدیریت اعتماد
۶۴	شکل ۵-۴ بخشی از متا مدل UML
۶۵	شکل ۶-۴ گسترش کلاس UML برای مدل‌سازی جزء
۶۵	شکل ۷-۴ گسترش کلاس UML برای مدل‌سازی نقش
۶۷	شکل ۸-۴ گسترش Association در UML برای مدل‌سازی رابطه اعطا کردن
۶۸	شکل ۹-۴ گسترش Association در UML برای مدل‌سازی رابطه داشتن صفت
۶۹	شکل ۱۰-۴ گسترش Association در UML برای مدل‌سازی رابطه مالکیت نقش
۷۰	شکل ۱۱-۴ گسترش Association در UML برای مدل‌سازی رابطه عضویت
۷۱	شکل ۱۲-۴ گسترش واسط در UML برای مدل‌سازی واسط امن
۷۲	شکل ۱۳-۴ گسترش Association در UML برای مدل‌سازی رابطه دسترسی
۷۶	شکل ۱۴-۴ الگوی معماری عضویت در یک نقش
۷۷	شکل ۱۵-۴ الگوی معماری اعطا کردن یک نقش به نقش دیگر (اعتماد)
۷۸	شکل ۱۶-۴ الگوی معماری نقش‌های سلسله مراتبی
۷۹	شکل ۱۷-۴ الگوی معماری اعطا کردن چند گانه

- شکل ۴-۱۸ مدل‌سازی سناریو ارائه کد کاربری و کلمه عبور ۸۰
- شکل ۴-۱۹ مدل‌سازی سناریو ارائه کد کاربری و کلمه عبور و قرار دادن در زیر مجموعه پیام نور ۸۰
- شکل ۴-۲۰ مدل‌سازی سناریو مدیریت اعتماد ۸۱
- شکل ۵-۱ سناریو امنیت برای جلوگیری از دسترسی کاربران غیر عضو کتابخانه ۸۵
- شکل ۵-۲ سناریو امنیت برای جلوگیری از دسترسی فارغ التحصیلان ۸۶
- شکل ۵-۳ سناریو کارایی برای انتقال تغییرات ۸۶
- شکل ۵-۴ سناریو قابلیت استفاده در حذف یا اعطای دسترسی به کلیه اساتید یا دانشجویان ۸۶
- شکل ۵-۵ معماری متمرکز برای سیستم ارائه مقالات ۸۷
- شکل ۵-۶ معماری توزیع شده برای سیستم ارائه مقالات ۸۸
- شکل ۵-۷ مدل‌سازی سناریو دسترسی نامحدود دانشجویان و اساتید به سیستم ارائه مقالات ۹۰
- شکل ۵-۸ مدل‌سازی سناریو خرید مقالات برای اعضای دانشکده‌های دیگر ۹۱

فهرست جداول

۹	جدول ۱-۱ خلاصه مراحل و زمان انجام تحقیق
۲۲	جدول ۱-۲ ماتریس انتخاب موضوع برای انتخاب یکی از صفات کیفی
۳۹	جدول ۱-۳ مقایسه فرایندهای مدلسازی سیستم‌های امن
۴۷	جدول ۲-۳ مقایسه روش‌های مدل سازی کنترل دسترسی و مدیریت اعتماد
۶۱	جدول ۱-۴ مقایسه سه رویکرد مختلف در استفاده از UML برای مدلسازی مدیریت اعتماد
۷۳	جدول ۲-۴ پروفایل گسترش‌های انجام شده (کلیشه‌ها)
۷۳	جدول ۳-۴ پروفایل گسترش‌های انجام شده (برچسب‌ها)
۷۴	جدول ۴-۴ نحوه نگاشت عناصر T-UML به RT
۸۴	جدول ۱-۵ نیازمندی‌های کارکردی مسئله
۸۴	جدول ۲-۵ نیازمندی‌های امنیتی مسئله
۸۵	جدول ۳-۵ نیازمندی‌های کارایی مسئله
۸۵	جدول ۴-۵ نیازمندی‌های قابلیت استفاده

گفتار اول

معرفی موضوع (تعریف صورت مسئله)

۱-۱ مقدمه

در حال حاضر یکی از مهمترین صفات هر سیستم نرم‌افزاری، کیفیت است. با پیشرفتهای انجام شده و گسترش ابزارهای گوناگون برای توسعه نرم‌افزار، توسعه نرم‌افزارهایی که کارکردهای مورد نظر مشتریان را برآورده سازند، به امری آسان و سریع تبدیل شده است. هم‌اکنون تفاوت بین دو نرم‌افزار را توانایی نرم‌افزارها در برآورده ساختن صفات کیفی مورد انتظار تعیین می‌کند.

معماری نرم‌افزار یک برنامه یا سیستم کامپیوتری، ساختار یا ساختارهایی از سیستم می‌باشد، که دربرگیرنده اجزاء، صفات قابل مشاهده آن اجزا و ارتباط بین آنها باشد [9]. معماری نرم‌افزار یک سیستم نرم‌افزاری، شامل اولین تصمیمات طراحی سیستم می‌باشد و این تصمیمات زیربنای فعالیت‌های طراحی، پیاده‌سازی، استقرار و نگهداری سیستم است. همچنین معماری نرم‌افزار، یکی از مهمترین عناصر قابل ارزیابی در فرایند توسعه نرم‌افزار می‌باشد [11]. بنابراین برای طراحی سیستمی که نیازهای کیفی مورد نظر را برآورده سازد، تولید معماری نرم‌افزار مهمترین گام در دستیابی به کیفیت در نرم‌افزار و همچنین ارزیابی صفات کیفی است.

برای دستیابی به کیفیت در مدل‌های فرآیند توسعه نرم‌افزار مبتنی بر معماری^۱، معمولاً ابتدا نیازهای کیفی سیستم به طور دقیق و قابل اندازه‌گیری تعیین شده و سپس معماری نرم‌افزار مربوطه طراحی می‌گردد. پس از طراحی معماری، می‌توان به ارزیابی آن پرداخت و تغییرات لازم را در طراحی مورد نظر ایجاد کرد. بنابراین دو مرحله اساسی در مدل‌های فرایند توسعه نرم‌افزار مبتنی بر معماری، مراحل طراحی و ارزیابی معماری نرم‌افزار است. این دو بخش در ارتباط مستقیم با یکدیگر بوده و هریک مکمل دیگری می‌باشد. برای ایجاد امکان ارزیابی صفات کیفی مورد نظر در معماری در مرحله طراحی معماری، باید به ازای هر صفت کیفی، یک مدل از معماری نرم‌افزار ایجاد شود. این مدل‌ها نحوه دستیابی به صفت کیفی را نشان داده و با ارزیابی آنها می‌توان مشخص نمود به چه میزان صفت کیفی مورد نظر برآورده شده است. برای طراحی معماری نرم‌افزار، نیاز به تاکتیک معماری^۲ و الگوهای معماری^۳ است. برای برآورده ساختن صفات کیفی در معماری نرم‌افزار، می‌توان

¹ - Architecture Centric

² - Architectural Tactics

³ - Architectural Patterns

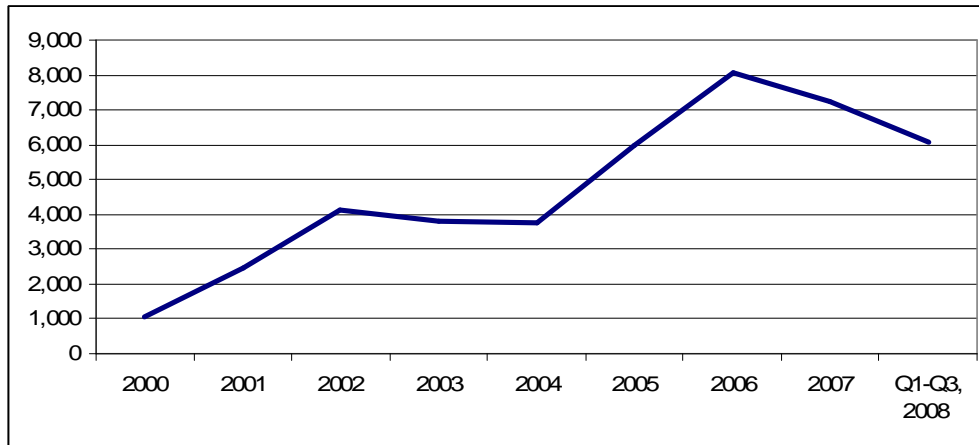
تعدادی تاکتیک معماری معرفی کرد. این تاکتیک‌ها روش‌هایی در راستای برآورده کردن صفات کیفی مذکور هستند. به عنوان مثال، صفت کیفی امنیت دارای تعدادی تاکتیک معماری بوده که صفت کیفی امنیت را در سطح معماری نرم‌افزار برآورده می‌کنند. به عنوان نمونه‌هایی از این تاکتیک‌ها می‌توان به تشخیص هویت کاربران، محدود کردن دسترسی کاربران، تشخیص نفوذ، کنترل دسترسی، مدیریت اعتماد و... اشاره کرد که فهرست کامل این تاکتیک‌ها در ادامه ارائه می‌شود. بنابراین منظور از مدلسازی صفات کیفی در این پایان نامه، ایجاد مدلی از معماری بوده که بیانگر یک صفت کیفی باشد و نحوه دستیابی به صفت کیفی توسط یک تاکتیک مشخص در آن ارائه شده باشد. همچنین مدل ایجاد شده باید قابل ارزیابی باشد. برای دستیابی به هدف مذکور، در این پایان نامه صفت کیفی امنیت انتخاب شده و روشی جدید برای مدلسازی مدیریت اعتماد که یکی از تاکتیک‌های دستیابی به امنیت می‌باشد، ارائه شده است. اصلی‌ترین علت انتخاب امنیت به عنوان صفت کیفی نمونه در این پایان نامه، افزایش روز افزون نیاز به امنیت در سیستم‌های کامپیوتری بوده است.

در کنار بسیاری از صفات مثبت و تاثیرات سیستم‌های کامپیوتری در دنیای امروز، وابستگی به این سیستم‌ها، اثرات منفی نیز به همراه دارد. یکی از اثرات منفی، اشکالات روزافزون امنیتی در سیستم‌های کامپیوتری و افزایش حملات علیه این گونه سیستم‌ها می‌باشد. موسسه CERT/CC^۱ سالانه گزارش‌هایی مبنی بر تعداد آسیب‌پذیری‌های^۲ موجود در سیستم‌های کامپیوتری^۳ ارائه می‌دهد. بر اساس گزارش ارائه شده توسط این موسسه [10] در سال ۲۰۰۸ بیش از ۶۰۰۰ آسیب‌پذیری سیستم‌های کامپیوتری توسط منابع معتبر گزارش شده است و این مقدار اگر چه نسبت به دو سال قبل سیر نزولی داشته اما بسیار قابل توجه می‌باشد. (شکل ۱-۱)

¹ Computer Emergency Response Team Coordination Center

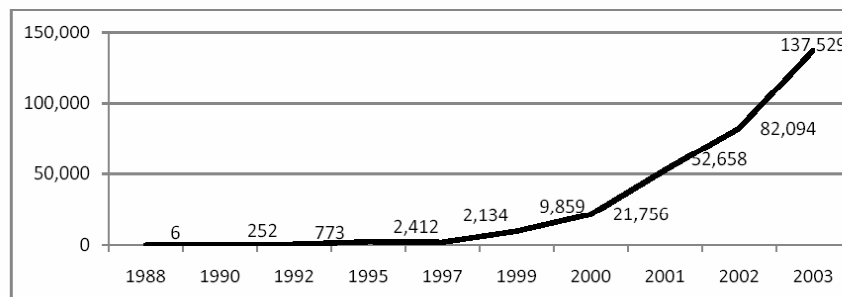
² Vulnerability

^۳- آسیب‌پذیری‌ها اشکالات امنیتی هستند که به صورت رسمی و در مجامع عمومی گزارش داده می‌شوند.



شکل ۱-۱ تعداد آسیب پذیری‌های گزارش شده برحسب سال توسط cert/cc

همچنین CERT/CC تعداد ۱۴۰۰۰۰ حمله امنیتی را در سال ۲۰۰۳ گزارش نموده است. با توجه به افزایش روز افزون کاربران، تعداد این حملات سال به سال و به شدت رو به افزایش می‌باشد، به طوری که این موسسه از سال ۲۰۰۴ به بعد ارائه آمار در زمینه حملات امنیتی را متوقف نمود (شکل ۱-۲). باید توجه داشت که تعداد حملات از تعداد آسیب پذیری‌ها بیشتر می‌باشد، زیرا می‌توان از ناحیه آسیب پذیر، به دفعات متوالی حمله به سیستم‌های کامپیوتری انجام داد.



شکل ۱-۲ تعداد حملات گزارش شده بر حسب سال توسط CERT/CC

یکی از دلایل افزایش روز افزون مشکلات امنیتی در سیستم‌های کامپیوتری، مکانیزم ساخت نرم‌افزار و محیطی که نرم‌افزار در آن اجرا می‌شود، می‌باشد. امروزه نرم‌افزارها از اجزاء مختلف تولید شده توسط سازندگان گوناگون، ساخته می‌شوند. بنابراین امنیت درونی این اجزاء به تنهایی برای امنیت سیستم نرم‌افزار کافی نیست، بلکه باید ارتباط بین اجزاء و نحوه چینش آنها در کنار

یکدیگر به گونه‌ای باشد که برای امنیت سیستم، مشکلی ایجاد نکند. همچنین نرم‌افزارهای امروزی معمولاً در سیستم‌های مبتنی بر شبکه و توزیع شده استقرار می‌یابند. این گونه سیستم‌ها با اتصال به شبکه اینترنت در دسترس حملات گوناگون از سوی رخنه‌گران در سراسر دنیا قرار خواهند داشت. بنابراین باید مکانیزم‌هایی اتخاذ نمود که سیستم‌های نرم‌افزاری توزیع شده از تهدید افراد ناشناس مصون بمانند. بنابراین امنیت همچون نیازهای کیفی دیگر باید در معماری نرم‌افزار مورد توجه قرار گرفته و مدل شود.

۲-۱ طرح مسئله (تعریف مسئله و بیان سوال‌های اصلی تحقیق)

هدف اصلی مهندسی نرم‌افزار، تولید سیستم با کیفیت است. اولین مرحله‌ای که کیفیت یا ویژگی‌های کیفی در آن مورد توجه قرار می‌گیرند مرحله معماری نرم‌افزار سیستم می‌باشد [1]. در این مرحله نیازهای کیفی و تاکتیک‌های برآورده کننده آنها مدل شده و مورد ارزیابی قرار می‌گیرند [9] در این پایان‌نامه هدف اینست که رویکرد جدیدی برای حل مسئله مدلسازی صفت کیفی امنیت در معماری نرم‌افزار ارائه شود. در این راستا سوالات زیر مطرح است:

آیا مدلسازی به ارزیابی صفات کیفی بخصوص امنیت کمک می‌کند؟

مراحل ایجاد مدلسازی که منجر به ارزیابی بهتر شود کدام است؟

چگونه می‌توان زبانی برای مدلسازی با معیار فوق تعریف کرد؟

چگونه می‌توان از روش تعریف شده در یک محیط عملیاتی استفاده کرد؟

۳-۱ اهداف تحقیق

مطالعات کلاسیک انجام شده درباره امنیت سیستم‌های کامپیوتری بر روی چگونگی اطمینان از محرمانگی، یکپارچگی و در دسترس بودن سیستم‌های کامپیوتری متمرکز است [34]. در این زمینه معمولاً به تولید پروتکل‌های ارتباطی امن رمزنگاری و به کاربرد مکانیزم‌های امنیتی خارجی پس از تولید نرم‌افزار توجه شده است. با وجود مطالعات زیاد انجام شده در امنیت، توجه بسیار کمی به نحوه ساخت و مهندسی امنیت در نرم‌افزار شده است و این امر به گسترش ساخت نرم‌افزار با استفاده از اجزاء گوناگون و نیاز به روش مهندسی در ایجاد ارتباط و قرار دادن اجزاء کنار هم از اهمیت

زیادی برخوردار گشته به گونه‌ای که با وجود حملات اندک بر روی روش‌های رمزنگاری [12] عمده حملات انجام شده بر روی سیستم‌های نرم‌افزاری به علت طراحی ضعیف و غلط بوده است. به همین علت برای جلوگیری از گسترش روز افزون حملات باید علاوه بر تولید سیستم امن از دیدگاه رمزنگاری به جنبه مهندسی نرم افزار آن نیز توجه داشت.

بنابراین امنیت همچون نیازهای کیفی دیگر باید در معماری نرم افزار مورد توجه قرار گیرد. در این پایان‌نامه با استفاده از چارچوب **Islab** [6] که در متن پایان‌نامه جزئیات آن بررسی خواهد شد به مدل‌سازی صفت کیفی امنیت در سطح معماری و سپس به مسئله مدل‌سازی صفت کیفی امنیت و تاکتیک مدیریت اعتماد پرداخته خواهد شد. برای این منظور زبان **UML** برای مدل‌سازی انتخاب شده و به مسائل این زبان در مدل‌سازی امنیت اشاره می‌شود و با ارائه یک پروفایل برای این زبان در واقع زبان مدل‌سازی جدیدی ارائه می‌شود و در پایان مطالعه موردی برای سیستم بانک اطلاعاتی نمونه از دانشگاه پیام نور خواهیم داشت. بطور خلاصه اهداف اصلی تحقیق شامل موارد زیر می‌باشد:

۱- ارائه پروفایلی مبتنی بر **UML** که در واقع گسترشی بر این زبان می‌باشد که با اضافه کردن توانایی مدل‌سازی کنترل دسترسی و مدیریت اعتماد در سطح معماری نرم‌افزار بتوان آنرا برای ارزیابی معماری‌های امن بکار برد.

۲- استفاده از چارچوب **Islab** در فرایند ارائه شیوه مدل‌سازی بخصوص مدل‌سازی تاکتیک‌های امنیتی.

۳- ارائه چارچوبی عملی برای ایجاد روشی جدید برای مدل‌سازی صفت کیفی امنیت در معماری نرم افزار که می‌توان آن را برای سایر صفات نیز بکار برد.

۴- مقایسه روش جدید ارائه شده با چند روش قبلی و مطرح در این خصوص.

۵- ارائه چارچوبی محدود برای ارزیابی زبانهای مدل‌سازی که به کمک آن بتوان نقاط ضعف و قوت هر روش را تعیین نمود.

۱- ۴ محدوده تحقیق

این تحقیق پیرامون موضوعاتی از قبیل تعاریف، مفاهیم، اصول، فازها، ابزارهای مدل‌سازی در سطوح معماری نرم‌افزار بویژه امنیت جهت ارزیابی جنبه‌ها، دیدگاه‌ها، ویژگی‌ها، مزایا، معایب و نقاط ضعف و قوت آنها در حوزه مهندسی نرم‌افزار و مدل‌سازی در حوزه معماری نرم‌افزار بطور موثر انجام گرفته است. در این خصوص از شیوه مطالعه موردی و ارزیابی مبتنی بر صفت که در چارچوب **ISLab** روشی استاندارد به حساب می‌آید استفاده می‌شود و از نظرات متخصصین در

حوزه نرم افزار (اما به شکل غیر رسمی^۱) جهت ارزیابی روش پیشنهادی استفاده شده است. به عبارت دیگر موضوعاتی که در این طرح مورد بررسی قرار می‌گیرد بر اساس اصول مهندسی نرم افزار و اصول و مفاهیم معماری نرم افزار نشأت گرفته و بر پایه آن ایجاد شده است.

۱-۵ سابقه و ضرورت انجام تحقیق

امروزه انواع مختلفی از مدل‌های امنیتی در حوزه امنیت مطرح می‌باشند. سه مدل مطرح از مدل‌های امنیتی عبارتند از مدل کنترل دسترسی، مدل مدیریت اعتماد و مدل جریان اطلاعات. سه نوع اصلی در مدل‌های کنترل دسترسی، مدل‌های DAC^۲ و MAC^۳ و RBAC^۴ می‌باشند [63]. مدل RBAC نسبت به سایر مدلها مدلی جدیدتر محسوب می‌شود که امروزه استفاده از آن در کاربردهای تجاری رو به افزایش است. مدل RBAC توانایی نگاشت ساختار سازمانی طبیعی یک سازمان در مسئله کنترل دسترسی را دارد. در این مدل دو مشکل اصلی روش‌های کلاسیک کنترل دسترسی حل شده است. مدل مدیریت اعتماد، چارچوبی برای توصیف خط‌مشی‌های امنیتی در سیستم‌های توزیع شده، با توانایی توصیف روابط اعتماد بین اجزای سیستم می‌باشد [27]. از سیستم‌های مدیریت اعتماد مطرح می‌توان به Policy Marker [27]، KeyNote [28] و SD3 [29] اشاره کرد. با توجه به تعریف ارائه شده از مدیریت اعتماد، برای توصیف روابط اعتماد، چندین مفهوم مختلف وجود داشته که در ادامه معرفی خواهند شد. هدف این پایان‌نامه ارائه روشی برای مدلسازی صفت کیفی امنیت و به طور خاص مدل مدیریت اعتماد مبتنی بر نقش در سطح معماری می‌باشد. با توجه به اینکه مدل مدیریت اعتماد سیستم باید توانایی مدلسازی خط‌مشی‌های امنیتی سازمان را نیز داشته باشد راه حل ارائه شد باید دارای توانایی مدلسازی کنترل دسترسی باشد و با توجه به اینکه مدل مدیریت اعتماد انتخاب شده، مدل مدیریت اعتماد مبتنی بر نقش است، روش جدید، مدل کنترل دسترسی مبتنی بر نقش را نیز پوشش خواهد داد.

^۱ - در این پایان‌نامه برای اثبات موضوع ارائه شده، تاکید بر مطالعه موردی است و نقطه نظرات متخصصین بطور غیررسمی دریافت شده و مورد استناد قرار گرفته زیرا نتوانستیم زمان زیادی از آنها برای مطالعه و پاسخ به سوالات و پر کردن پرسشنامه بگیریم.

^۲ Discretionary Access Control

^۳ Mandatory Access Control

^۴ Role Based Access Control