ای نام تو بهترین سرآغاز

دانشگاه پیام نور

دانشکده فنی و مهندسی

گروه علمی مهندسی فناوری اطلاعات و ارتباطات

پایان‌نامه کارشناسی ارشد

در رشته مهندسی کامپیوتر - گرایش نرم‌افزار

عنوان

# ارائه روشی جدید برای مدل‌سازی صفت کیفی امنیت در معماری نرم‌افزار

نگارش

علی مقدوری

استاد راهنما

دکتر رضا رافع

استاد مشاور

دکتر احمد فراهی

زمستان ۱۳۸۸

شماره: .....
تاریخ: .....
پیوست: .....

جمهوری اسلامی ایران
وزارت علوم تحقیقات و فناوری

مجتمع فنی و مهندسی

دانشگاه پیام نور
دانشگاه پیام نور استان تهران

# تصویب نامه

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

## "ارائه روشی جدید برای مدل سازی صفت کیفی امنیت درمعماری نرم افزار"

تاریخ دفاع : ۸۹/۶/۷ ساعت: ۱۲-۱۳:۳۰

نمره: ۱۸/ — درجه ارزشیابی:

### هیات داوران:

| داوران | نام و نام خانوادگی | مرتبه علمی | امضاء |
|---|---|---|---|
| استاد راهنما | دکتررضا رافع | استادیار | |
| استادمشاور | دکتراحمدفراهی | استادیار | |
| استادداوردا خلی | دکترآرش قربان نیا | | |
| استادداورخارجی | دکتراسلام ناظمی | | |
| نماینده گروه | دکتر رضا عسکری مقدم | | |

تهران،خیابان استاد نجات الهی،تقاطع خیابان سپند کوچه هشتم، پلاک ۱۱
تلفن: ۸۸۹۰۴۱۲۷
دورنگار: ۸۸۹۰۳۳۱۰
www.fani.tpnu.ac.ir

## چکیده

هدف اصلی مهندسی نرم‌افزار، تولید سیستم با کیفیت است. یکی از مهمترین مراحلی که کیفیت یا صفات کیفی در آن مورد توجه قرار می‌گیرد مرحله تولید معماری نرم‌افزار سیستم می‌باشد. در این مرحله، نیازهای کیفی و تاکتیک‌های برآورده کننده آنها مدل شده و مورد ارزیابی قرار می‌گیرند. هدف این پایان‌نامه ارائه رویکردی جدید برای حل مسئله مدلسازی صفات کیفی در معماری نرم‌افزار بخصوص صفت کیفی امنیت در معماری نرم‌افزار می‌باشد برای ارائه این رویکرد بر پایه چارچوب ISLab مراحل ایجاد یک روش مدلسازی جدید برای مدل نمودن مدیریت اعتماد در سطح معماری نرم‌افزار نشان داده خواهد شد. مدیریت اعتماد، یکی از تاکتیکهای دستیابی به امنیت بوده و با مدلسازی آن امکان ارزیابی میزان دستیابی به امنیت در معماری نرم‌افزار فراهم می‌گردد. مهمترین خروجی پژوهش انجام شده، یک پروفایل گسترش یافته بر پایه UML به نام T-UML می‌باشد که توانایی مدلسازی مدیریت اعتماد در سطح معماری نرم‌افزار را دارد. همچنین مدل‌های ایجاد شده توسط T-UML، مدل‌هایی با قابلیت ارزیابی می‌باشند.



واژه‌های کلیدی: مدلسازی صفات کیفی، مدیریت اعتماد، کنترل دسترسی، معماری نرم‌افزار، UML.

# فهرست مطالب

**گفتار ششم: ارزیابی معماری**



**گفتار هفتم: نتیجه‌گیری و کارهای آینده**

## فهرست اشکال

# فهرست جداول

# 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، پیاده سازی، استقرار و نگهداری سیستم است. همچنین معماری نرم‌افزار، یکی ازمهمترین عناصر قابل ارزیابی در فرایند توسعه نرم‌افزار می‌باشد[11]. بنابراین برای طراحی سیستمی‌که 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[1]، معمولا 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[2] و الگوهای معماری[3] است. برای برآورده ساختن صفات کیفی در معماری نرم‌افزار، می‌توان

---

[1] - Architecture Centric

[2] - Architectural Tactics

[3] - Architectural Patterns

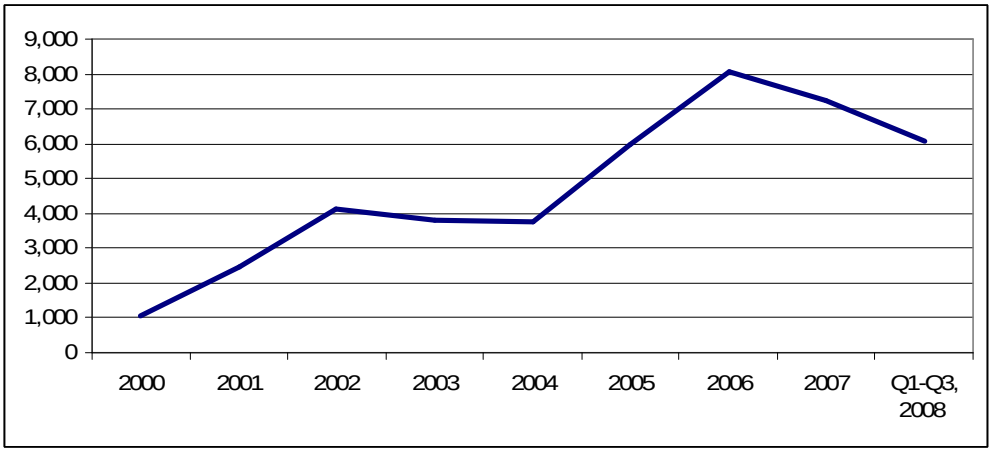
تعدادی تاکتیک معماری معرفی کرد. این تاکتیک‌ها روش‌هایی در راستای برآورده کردن صفات کیفی مذکور هستند. به عنوان مثال، صفت کیفی امنیت دارای تعدادی تاکتیک معماری بوده که صفت کیفی امنیت را در سطح معماری نرم‌افزار برآورده می‌کنند. به عنوان نمونه‌هایی از این تاکتیک‌ها می‌توان به تشخیص هویت کاربران، محدود کردن 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، اشکلات روزافزون امنیتی در سیستم‌های کامپیوتری و افزایش حملات علیه این گونه سیستم‌ها می‌باشد. موسسه CERT/CC [1] سالانه گزارش‌هایی مبنی بر تعداد آسیب‌پذیری‌های[2] موجود در سیستم‌های کامپیوتری[3] 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

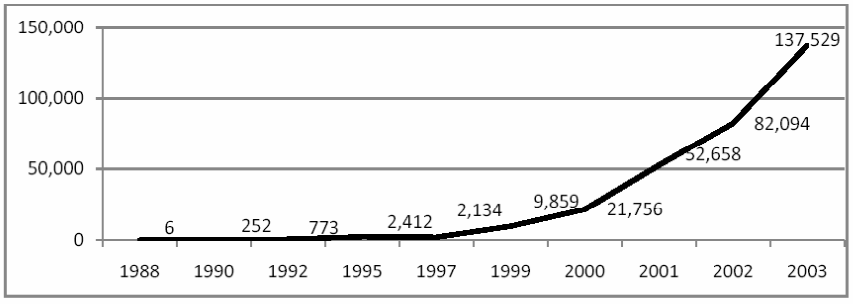
[2] Vulnerability

۳- آسیب پذیری‌ها اشکالات امنیتی هستند که به صورت رسمی‌و در مجامع عمومی‌گزارش داده می‌شوند.




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

همچنین CERT/CC تعداد ۱۴۰۰۰۰حمله امنیتی را در سال ۲۰۰۳ گزارش نموده است. باتوجه 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.

## ۱-۲ 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 می گیرند مرحله معماری نرم افزار سیستم می باشد[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 نرم افزار ارائه شود. در این راستا سوالات زیر مطرح است:

آیا مدلسازی به ارزیابی صفات کیفی بخصوص امنیت کمک می کند؟

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

چگونه می توان زبانی برای مدلسازی با معیار فوق تعریف کرد؟

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

## ۱-۳ 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 معمولا به تولید پروتکل‌های ارتباطی امن رمزنگاری و به کاربردن مکانیزم‌های امنیتی خارجی پس از تولید نرم افزار 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 اجزاءگوناگون 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 انـدک بـر روی روش‌هـای رمزنگـاری [12] عمده حملات انجام شده بر روی سیستم‌های نرم‌افزاری به علت طراحی ضعیف و غلط بـوده اسـت. به همین علت برای جلوگیری از گسترش روز افزون حملات باید عـلاوه بـر تولیـد سیـستم امـن 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 قرارگیرد. در این پایان‌نامه با استفاده از چارچوب Islab [6] که در متن پایان نامه جزئیات آن بررسی خواهد شـد بـه مدلسازی صفت کیفی امنیت در سطح معماری و سپس به مـسئله مدلـسازی صـفت کیفـی امنیـت 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 واقـع زبان مدلسازی جدیدی ارائه می‌شود و در پایان مطالعه موردی برای سیستم بانک اطلاعاتی نمونـه 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 آنـرا بـرای ارزیـابی 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، فازهـا، ابزارهـای مدلـسازی در سطوح معماری نرم‌افزار بویژه امنیت جهت ارزیابی جنبه‌ها، دیدگاه‌ها، ویژگـی‌هـا، مزایـا، معایـب و نقاط ضعف و قوت آنها در حوزه مهندسی نرم‌افزار و مدلسازی در حوزه معمـاری نـرم‌افـزار بطـور موثر انجام گرفته است. در این خصوص از شیوه مطالعه موردی و ارزیابی مبتنـی بـر صـفت کـه در چارچوب ISLab روشی استاندارد به حساب می‌آید استفاده مـی‌شـود و از نظـرات متخصـصین در

حوزه نرم‌افزار(اما به شکل غیر رسمی[1]) جهت ارزیابی روش پیشنهادی استفاده شده است. به عبارت دیگر موضوعاتی که در این طرح مورد بررسی قرار می‌گیرد بر اساس اصـول مهندسـی نـرم‌افـزار و اصول و مفاهیم معماری نرم‌افزار نشات 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[2] وMAC[3] وRBAC[4] 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 خط مشی‌های 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 .

---

[1]- دراین 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.

[2] Discretionary Access Control

[3] Mandatory Access Control

[4] Role Based Access Control