



دانشگاه پیام نور  
دانشکده فنی و مهندسی

پایان نامه

برای دریافت درجه کارشناسی ارشد  
رشته مهندسی کامپیوتر - گرایش نرم افزار  
گروه فناوری اطلاعات و ارتباطات

## ارائه یک چارچوب ارزیابی امنیت برای مدیریت و نظارت بر معماری سرویس گرا

حمیدرضا سلطانی

استاد راهنما:

دکتر سید مهران شرفی

استاد مشاور:

دکتر سید علی رضوی ابراهیمی

اسفند ۱۳۹۰



دانشگاه پیام نور  
دانشکده فنی و مهندسی  
دانشگاه پیام نور مرکز تهران

پایان نامه

برای دریافت درجه کارشناسی ارشد  
رشته مهندسی کامپیوتر - گرایش نرم افزار  
گروه فناوری اطلاعات و ارتباطات

## **ارائه یک چارچوب ارزیابی امنیت برای مدیریت و نظارت بر معماری سرویس گرا**

**حمیدرضا سلطانی**

استاد راهنما:

**دکتر سید مهرا ن شرفی**

استاد مشاور:

**دکتر سید علی رضوی ابراهیمی**

اسفند ۱۳۹۰



## تقدیم به

همسر مهربانم که همواره پشتیبان من در این راه بود

و تقدیم به امیدهای زندگیم؛ نگین و متین که با لطافت

کودکانشان روشنی بخش زندگیمان هستند

و تقدیم به پدر و مادر بزرگوارم که با همتی بلند و راسخ حامی و

مشوقی برای ادامه تمصیلات من بوده اند

## **تشکر و قدردانی:**

**از زحمات و راهنمایی های استاد گرامی  
جناب آقای دکتر مهران شرفی که در طول مدت انجام پایان نامه  
صبورانه و با دقت راهنمای بنده بوده اند صمیمانه تشکر دارم**

**از جناب آقای دکتر علی رضوی ابراهیمی بخاطر عنایت و  
رهنمودهای ارزشمندشان کمال تشکر را دارم.**

## چکیده

امروزه سازمانها برای همکاری و یکپارچگی سیستم های خود و بمنظور بقاء و موفقیت در محیط کسب و کار پویا از اصول معماری سرویس گرا بهره می برند که میزان این گرایش با توجه به ویژگیهای قابل توجه معماری سرویس گرا از جمله اتصال سست، تعامل پذیری و استفاده مجدد در حال افزایش است. اما همین ویژگیها در معماری سرویس گرا چالش ها و مشکلاتی را پیش روی این سیستم ها و فناوریها قرار داده است که از جمله آن می توان به جنبه امنیت اشاره نمود. بنابراین بررسی راهکارها و مدل های امنیتی موجود در زمینه معماری سرویس گرا و ارائه یک چارچوب امنیتی بهبودیافته با رویکرد ارزیابی امنیت ضروری بنظر می رسد. علی رغم تلاشهایی که برای ارائه الگوها و مدل های امنیتی جامع برای SOA شده است، در حال حاضر هنوز فقدان یک ساختار امنیتی جامع برای چارچوب های مختلف سیستم های وسیع SOA که البته ویژگی سادگی فهم معنایی آن را دارا باشد وجود دارد. لذا هدف اصلی این تحقیق برای آدرس دهی این نیازها، ارائه یک چارچوب بهبودیافته برای تضمین امنیت SOA و در نتیجه بهبود تحلیل و نظارت بر آن می باشد. چارچوب ارائه شده از تکنیک های مهندسی معکوس ترکیب شده با پایگاه دانش امنیت بهره می برد که با تقویت پایگاه دانش با استفاده از تجربیات امنیتی بدست آمده و نیز بهره مندی از معیارهای اندازه گیری و اصول وزندهی فرآورده های امنیتی، باعث تقویت قدرت تحلیل و ارزیابی امنیت می شود.

**واژه های کلیدی:** ارزیابی امنیت، معماری سرویس گرا، چارچوب ارزیابی امنیت، پایگاه دانش امنیت، تحلیل امنیت، مدیریت و نظارت امنیت

## فهرست مطالب

صفحه	عنوان
۱	فصل ۱ مقدمه
۲	۱-۱. مقدمه
۳	۲-۱. تعریف مسئله و سؤالات اصلی تحقیق
۴	۳-۱. سابقه و ضرورت انجام تحقیق
۵	۴-۱. اهداف تحقیق
۶	۵-۱. فرضیه ها
۶	۶-۱. روش انجام تحقیق
۷	۷-۱. ساختار کلی پایان نامه
۸	فصل ۲ اصول معماری سرویس گرا
۹	۱-۲. مقدمه
۱۰	۲-۲. روش سرویس گرایی برای طراحی فرایند کسب و کار
۱۳	۳-۲. عناصر معماری سرویس گرا
۱۳	۱-۳-۲. سرویس
۱۶	۲-۳-۲. مصرف کننده
۱۷	۳-۳-۲. ثبت سرویس
۱۷	۴-۳-۲. تأمین کننده سرویس
۱۷	۵-۳-۲. معماری سرویس گرای اولیه
۱۸	۴-۲. پیاده سازی فنی معماری سرویس گرا
۱۹	۱-۴-۲. زبان توصیف سرویس های وب
۲۰	۲-۴-۲. پروتکل دسترسی آسان به اشیاء
۲۰	۳-۴-۲. توصیف، کشف و یکپارچه سازی فراگیر
۲۱	۵-۲. شیء گرایی
	۶-۲. خصوصیات پشتیبانی شده با معماری سرویس گرا (یکپارچگی معماری سرویس گرا)
۲۱	۱-۶-۲. ضرورت چابکی و اتصال سست
۲۴	۲-۶-۲. لزوم قابلیت دید یا قابلیت کشف

۲۴	..... لزوم سازگاری ۳-۶-۲
۲۴	..... لزوم قابلیت استفاده مجدد ۴-۶-۲
۲۵	..... اصول طراحی معماری سرویس گرا ۷-۲
۲۵	..... قرارداد سرویس ۱-۷-۲
۲۶	..... سرویس های اتصال سست ۲-۷-۲
۲۷	..... انتزاع سرویس ۳-۷-۲
۲۸	..... قابلیت استفاده مجدد سرویس ۴-۷-۲
۲۹	..... خودمختاری سرویس ۵-۷-۲
۳۰	..... بی حالتی سرویس ۶-۷-۲
۳۰	..... قابلیت کشف سرویس ۷-۷-۲
۳۱	..... ترکیب سرویس ۸-۷-۲
۳۲	..... فصل ۳ امنیت در معماری سرویس گرا
۳۳	..... ۱-۳ مقدمه
۳۴	..... ۲-۳ رده بندی امنیت معماری سرویس گرا
۳۷	..... ۱-۲-۳ معیارهای امنیت
۳۷	..... ۲-۲-۳ راه حل های امنیت
۳۸	..... ۳-۲-۳ تهدیدهای امنیتی
۳۸	..... ۴-۲-۳ دارایی های امنیت
۳۹	..... ۵-۲-۳ صفات امنیت
۴۰	..... ۳-۳ استانداردهای امنیتی معماری سرویس گرا
۴۱	..... ۴-۳ راهکارهای رمزنگاری
۴۲	..... ۵-۳ چالش های امنیت معماری سرویس گرا
۴۴	..... ۶-۳ ارزیابی امنیت اطلاعات معماری سرویس گرا
۴۶	..... ۱-۶-۳ استاندارد ISO/IEC 27002:2005
۴۶	..... ۲-۶-۳ چارچوب های نظارت معماری سرویس گرا
۴۹	..... ۷-۳ مؤلفه های امنیت اطلاعات
۴۹	..... ۱-۷-۳ نظارت امنیت اطلاعات SOA
۵۰	..... ۲-۷-۳ مدیریت امنیت اطلاعات SOA
۵۳	..... ۳-۷-۳ مدل امنیت اطلاعات SOA
۵۷	..... ۴-۷-۳ چارچوب سیاست امنیت اطلاعات



۶۱	۸-۳. فناوریهای تحلیل امنیت
۶۱	۳-۸-۱. روش های تحلیل استاتیک
۶۲	۳-۸-۲. روش های تحلیل پویا
۶۲	۳-۸-۳. ابزار SAVE
۶۴	۳-۸-۴. ابزار SCA
۶۵	فصل ۴ معرفی چارچوب پیشنهادی
۶۶	۴-۱. مقدمه
۷۰	۴-۲. مرحله استخراج
۷۱	۴-۳. پایگاه دانش
۷۲	۴-۳-۱. اهداف امنیتی
۷۳	۴-۳-۲. شاخص ها
۷۴	۴-۳-۳. برچسب های امنیتی
۷۴	۴-۳-۴. فرآورده های امنیتی
۷۶	۴-۴. مرحله شناسایی
۷۸	۴-۵. مرحله تحلیل
۷۹	فصل ۵ تحلیل و ارزیابی چارچوب
۸۰	۵-۱. مقدمه
۸۱	۵-۲. مدل وزن دهی قواعد برچسب امنیتی
۸۷	۵-۲-۱. معیارهای وزندهی فرآورده های امنیتی
۸۸	۵-۳. معیار شدت
۹۰	۵-۴. معیار اعتبار
۹۳	فصل ۶ نتیجه گیری و پیشنهادها
۹۴	۶-۱. نتیجه گیری تحقیق
۹۵	۶-۲. نوآوری تحقیق
۹۵	۶-۳. پیشنهادها و کار آینده
۹۷	<b>مراجع</b>
۱۰۱	<b>واژه نامه</b>

## فهرست اشکال

صفحه	عنوان
۱	فصل ۱ مقدمه
۸	فصل ۲ اصول معماری سرویس گرا
۱۰	شکل ۲-۱. الگوها و دیدگاه های تاثیرگذار در ظهور سرویس گرایی (ارل، ۲۰۰۵).....
۱۱	شکل ۲-۲. اتصال مستقیم سرویس ها (بیوکر و همکاران، ۲۰۰۷).....
۱۲	شکل ۲-۳. اتصال از طریق بکارگیری زیرساخت سرویس گرا (بیوکر و همکاران، ۲۰۰۷).....
۱۳	شکل ۲-۴. معماری سرویس گرا نیازمند انتزاع امنیت است (بیوکر و همکاران، ۲۰۰۷).....
۱۴	شکل ۲-۵. سرویس (سرویسن، ۲۰۰۵).....
۱۴	شکل ۲-۶. مفهوم سرویس در روابط انسانی (ارل، ۲۰۰۵).....
	شکل ۲-۷. انجام فعالیت تجاری تحویل توسط سه شخص مختلف در نقش سرویس های مجزا
۱۶	(ارل، ۲۰۰۵).....
۱۸	شکل ۲-۸. روابط عناصر تشکیل دهنده معماری سرویس گرا (ارل، ۲۰۰۵).....
۱۹	شکل ۲-۹. پیاده سازی فنی معماری سرویس گرا (ارل، ۲۰۰۵) و (لیگل، ۲۰۰۷).....
۲۰	شکل ۲-۱۰. نمای ساده از یک پیام SOAP (اندری و همکاران، ۲۰۰۴).....
۲۸	شکل ۲-۱۱. چارچوب معماری لایه ای معماری سرویس گرا (IBM، ۲۰۰۸).....
۳۲	فصل ۳ امنیت در معماری سرویس گرا
۳۵	شکل ۳-۱. CIA و امنیت SOA (تینیس، ۲۰۰۹).....
۳۷	شکل ۳-۲. رده بندی امنیت اطلاعات در معماری سرویس گرا (ساولا و همکاران، ۲۰۰۷).....
۴۵	شکل ۳-۳. محیط های IT سنتی و SOA (IBM، ۲۰۰۸).....
	شکل ۳-۴. ناکارآمدی TLS/SSL و دیدگاه های سنتی قابلیت اعتماد داده ها در SOA (کنگانتی،
۵۶	(۲۰۰۸).....
۵۹	شکل ۳-۵. چرخه حیات سرویس گرایی از یک چشم انداز امنیتی (IBM، ۲۰۰۷).....

۶۵	فصل ۴ معرفی چارچوب پیشنهادی
۶۹	شکل ۴-۱. چارچوب پیشنهادی ارزیابی امنیت معماری سرویس گرا .....
۷۶	شکل ۴-۲. مثال- درخت برچسب ساده .....
۷۹	فصل ۵ تحلیل و ارزیابی چارچوب
۸۲	شکل ۵-۱. مثال رستوران
۸۳	شکل ۵-۲. مثال- برچسب امنیتی سرویس حالتمدار .....
۸۴	شکل ۵-۳. مثال برچسب امنیتی در سرویس بدون حالت .....
۸۵	شکل ۵-۴. مثال رستوران در حالت برچسب زده شده .....
۸۶	شکل ۵-۵. منتخب پایگاه دانش برای هدف امنیتی قابلیت اعتماد (جانگ، ۲۰۱۱) .....
۹۰	شکل ۵-۶. مثال محاسبه معیار شدت و اعتبار .....
۹۳	فصل ۶ نتیجه گیری و پیشنهادها

## فهرست جداول

---

۱	فصل ۱ مقدمه
۸	فصل ۲ اصول معماری سرویس گرا
۳۲	فصل ۳ امنیت در معماری سرویس گرا
۴۰	جدول ۳-۱. استانداردهای امنیتی رایج در معماری سرویس گرا
۴۷	جدول ۳-۲. کنترل های امنیت اطلاعات SOA (چتی، ۲۰۱۰)
۶۰	جدول ۳-۳. چالش های امنیت اطلاعات معماری سرویس گرا (چتی، ۲۰۱۰)
۶۵	فصل ۴ معرفی چارچوب پیشنهادی
۷۹	فصل ۵ تحلیل و ارزیابی چارچوب
۹۳	فصل ۶ نتیجه گیری و پیشنهادها

## فهرست علائم اختصاری

---

ACL	Access Control List	لیست کنترل دسترسی
BI	Business Intelligence	کسب و کار هوشمند
BPM	Business Process Management	مدیریت فرایندهای کسب
CIA	Confidentiality, Integrity and Availability	قابلیت اعتماد، یکپارچگی و دسترسی پذیری
EAI	Enterprise Application Integration	یکپارچه سازی برنامه کاربردی سازمان
EMF	Eclipse Modeling Framework	چارچوب مدلسازی اکلیپس
ERP	Enterprise Resource planning	برنامه ریزی منابع سازمانی
ESB	Enterprise Service Bus	گذرگاه سرویس سازمانی
J2EE	Java 2 Enterprise Edition	نسخه دوم سازمانی جاوا
JDT	Java Development Tools	ابزارهای توسعه جاوا
LDAP	Lightweight Directory Access Protocol	پروتکل دسترسی به فهرست سبک وزن
RBAC	Role-Based Access Control	کنترل دسترسی نقش-محور
SAML	Security Assertion Markup Language	زبان نشانه گذاری تأیید امنیت
SAVE	Software Architecture Visualization and Evaluation	ارزیابی و مجازی سازی معماری نرم افزار
SCA	Service Component Architecture	معماری مؤلفه سرویس
SOA	Service Oriented Architecture	معماری سرویس گرا
SOAP	Simple Object Access Protocol	پروتکل دسترسی آسان به اشیاء

SSL	Secure Socket Layer	لایه سوکت امن
TLS	Transform Layer Security	امنیت سطح انتقال
UDDI	Universal Description Discovery and Integration	توصیف، کشف و یکپارچه سازی فراگیر
WSDL	Web services description language	زبان توصیف سرویس ها وب
XML	Extensible Markup Language	زبان نشانه گذاری توسعه یافته

# فصل ۱

## مقدمه

## ۱-۱. مقدمه

معماری سرویس‌گرا<sup>۱</sup> یک چارچوب وسیع و استاندارد برای ساخت سیستم‌های توزیع شده ناهمگن است که کارکردهای نرم افزاری را در قالب سرویس ارائه می‌کند و تضمین‌کننده توسعه و یکپارچگی سیستم‌هاست و هدفش افزایش چابکی<sup>۲</sup> فناوری اطلاعات در جهت واکنش سریع به تغییرات در نیازهای کسب و کار است. این سرویس‌ها هم توسط دیگر نرم افزارها قابل فراخوانی هستند و هم برای ساخت سرویس‌های جدید مورد استفاده قرار می‌گیرند.

تکامل و رشد معماری سرویس‌گرا در واقع بیانگر نوعی تبدیل و تحول در کسب و کار و فناوری است. فرصت‌های بوجود آمده از معماری سرویس‌گرا امکان ظهور و پیدایش بالقوه سازمان‌هایی را فراهم می‌سازد که تمام قابلیت‌هایشان به کمک سرویس‌ها و بعضاً بصورت خودکار پیاده سازی شده‌اند. در این سازمان‌ها فرایندها از مرزهای آن‌ها فراتر رفته و بین فراهم‌کنندگان مواد اولیه، مشتریان و کلیه شرکا ارتباط برقرار می‌کنند تا زنجیره‌های ارزش سازمان‌ها کاراتر از گذشته شکل گیرند.

سرویس‌های وب<sup>۳</sup> را باید نوعی فناوری برای تحقق ویژگی استقلال از سکو و ابزاری برای پیاده سازی معماری سرویس‌گرا دانست. یک سرویس وب بهترین راه حل برای پیاده سازی معماری سرویس‌گرا است (الوآسی<sup>۴</sup>، ۲۰۰۸).

---

<sup>1</sup> Service Oriented Architecture (SOA)

<sup>2</sup> agility

<sup>3</sup> web services

<sup>4</sup> Oluwaseyi



## ۲-۱. تعریف مسئله و سؤالات اصلی تحقیق

نیازمندی‌های حیاتی امنیت برای محفوظ نگه‌داشتن یک سیستم اطلاعاتی عبارتند از قابلیت اعتماد، یکپارچگی و دسترس پذیری (CIA)<sup>۱</sup>. اما درمورد SOA نیازمندیهای اضافی دیگری چون اعتبارسنجی<sup>۲</sup>، تعیین اختیارات<sup>۳</sup>، حسابرسی<sup>۴</sup> و رد انکار<sup>۵</sup> داریم. در چارچوب ارائه شده در این تحقیق از ترکیب تکنیک‌های مختلفی برای ارزیابی امنیت یک سیستم معماری سرویس‌گرا استفاده شده است، که از آن جمله می‌توان به تحلیل استاتیک و تکنیک‌های مهندسی معکوس جهت جمع‌آوری اطلاعات مرتبط با امنیت گردآوری دانش مربوط به نیازمندیهای امنیتی سیستم در یک پایگاه دانش اشاره نمود. کارهای بسیاری در زمینه تحلیل استاتیک نرم افزار انجام شده است، مانند (هاورمایر<sup>۶</sup>، ۲۰۰۴) و (لیوشیتز<sup>۷</sup>، ۲۰۰۵، ۲۰۰۶). برای ارزیابی امنیت یک سیستم نرم افزاری در (جانگ<sup>۸</sup>، ۲۰۱۱) از روش تحلیل استاتیک استفاده شده که جهت تقویت آن از یک مدل پایگاه دانش بهره گرفته شده است. ارزیابی امنیت یک صفت کیفی مشخص در یک سطح معماری هنوز در ابتدای راه است. روش‌های پشتیبانی شده با ابزار کمی وجود دارند که امنیت را در سطوح بالاتر تجرید نسبت به کد منبع<sup>۹</sup> توسعه دهند. در (سهر و برگر<sup>۱۰</sup>، ۲۰۱۰) یک روش معماری مرکزی برای تحلیل امنیت استاتیک معرفی شده است که از یک ابزار مهندسی معکوس جهت استخراج اطلاعات ساختاری از کد منبع استفاده شده است.

<sup>1</sup> Confidentiality, Integrity and Availability

<sup>2</sup> authentication

<sup>3</sup> authorization

<sup>4</sup> accountability

<sup>5</sup> non-repudiation

<sup>6</sup> Hovemeyer

<sup>7</sup> Livshits

<sup>8</sup> Jung

<sup>9</sup> source code

<sup>10</sup> Sohr, B. Berger

سؤال‌های اصلی مطرح شده عبارتند از:

- آیا قدرت تحلیل و ارزیابی امنیت در چارچوب ارائه شده تقویت شده است؟
- چارچوب پیشنهادی چگونه و تا چه اندازه امنیت را در سطح معماری سرویس‌گرا تأمین می‌کند؟
- آیا برای غیر متخصصان یا کاربران کم تجربه در زمینه امنیت، قابل فهم و ساده است؟
- آیا ابزار ارزیابی چارچوب پیشنهادی مستقل از زبان برنامه نویسی و فناوری است؟

### ۳-۱. سابقه و ضرورت انجام تحقیق

امروزه سازمانها برای همکاری و یکپارچگی سیستم‌های خود و بمنظور بقاء و موفقیت در محیط کسب و کار پویا از اصول معماری سرویس‌گرا بهره می‌برند که میزان این گرایش با توجه به ویژگی‌های قابل توجه معماری سرویس‌گرا از جمله اتصال سست<sup>۱</sup>، تعامل پذیری<sup>۲</sup> و استفاده مجدد<sup>۳</sup> در حال افزایش است. اما همین ویژگیها در معماری سرویس‌گرا چالش‌ها و مشکلاتی را پیش روی این سیستم‌ها و فناوری‌ها قرار داده است که از جمله آن می‌توان به جنبه/امنیت اشاره نمود. بنابراین بررسی راهکارها و مدل‌های امنیتی موجود در زمینه معماری سرویس‌گرا و ارائه یک چارچوب امنیتی بهبودیافته با رویکرد ارزیابی امنیت ضروری بنظر می‌رسد. متأسفانه آزمایش کیفیت جنبه امنیت سیستم‌های نرم افزاری امر ساده‌ای نمی‌باشد. تاکنون تلاشهایی برای ارائه الگوها و مدل‌های امنیتی جامع برای SOA شده است و مقالات، پایان نامه‌ها و چندین کتاب توسط محققان و مؤلفان در این باره عرضه شده است. با این حال در حال حاضر

<sup>1</sup> loosely coupling

<sup>2</sup> interoperability

<sup>3</sup> reusability

هنوز فقدان یک شیوه جامع که یک توسعه و پیشرفت قاعده مند در ساختار امنیت SOA را ارائه دهد و البته ویژگی‌های ساده‌گی فهم معنایی آن را دارا باشد وجود دارد. اگرچه استانداردهای فنی نظیر امنیت وب سرویس (فرناندز<sup>۱</sup> و همکاران، ۲۰۰۶) موجود است، سیستم‌های SOA هنوز در برابر بسیاری از انواع تهدیدهای اساسی آسیب پذیرند.

لذا هدف اصلی این تحقیق برای آدرس‌دهی این نیازها، ارائه یک چارچوب بهبودیافته برای تضمین امنیت SOA و در نتیجه بهبود نظارت بر آن می‌باشد.

## ۴-۱. اهداف تحقیق

کلیه سازمان‌ها و سیستم‌های فناوری اطلاعات در سراسر دنیا در حال حرکت سریع به سمت معماری سرویس‌گرا هستند. بدیهی است که جوانب امنیت در SOA از مهمترین اهداف مدیران سازمان‌ها جهت مدیریت و نظارت هرچه بهتر سیستم‌ها خواهد بود. هدف اصلی این تحقیق ارائه یک چارچوب امنیتی بهبودیافته برای مدیریت و نظارت بر معماری سرویس‌گرا می‌باشد. با توجه به اهمیت موضوع اهداف جانبی زیادی می‌توان برای این تحقیق برشمرد. از آن جمله می‌توان به موارد زیر اشاره نمود:

- ارائه چارچوبی یکپارچه برای ارزیابی امنیت سیستم‌های سرویس‌گرا که مستقل از فناوری و زبان برنامه نویسی خاصی باشد.
- استفاده از یک مدل پایگاه دانش<sup>۲</sup> در طول مدت فرایند تحلیل و ارزیابی امنیت، جهت بروزرسانی و غنی‌سازی دانش امنیت، با هدف سازگاری با نیازمندیهای امنیتی جدید سیستم و قابلیت توسعه برای پرداختن به مسائل ارزیابی جدید در آینده.

<sup>1</sup> Fernandez

<sup>2</sup> Knowledge Base

## ۵-۱. فرضیه‌ها

- در چارچوب پیشنهادی از تکنیک‌های مهندسی معکوس ترکیب شده با پایگاه دانش جهت تقویت ارزیابی امنیت استفاده شده است.
  - تقویت پایگاه دانش با استفاده از تجربیات امنیتی بدست آمده باعث تقویت قدرت تحلیل و ارزیابی امنیت می‌شود.
  - قابلیت و کیفیت چارچوب پیشنهادی بستگی دارد به کیفیت قواعد برچسب<sup>۱</sup> امنیتی و کامل بودن اطلاعات فراهم شده در پایگاه دانش.
- فرضیه‌های فرعی:
- برای تحقق فرضیات اصلی، نیازمند داشتن دانش کافی درمورد ابزارها، استانداردها و فناوریهای مرتبط با موضوع هستیم.

## ۶-۱. روش انجام تحقیق

- معماری سرویس‌گرا، امنیت و کاربرد امنیت در معماری سرویس‌گرا کم و بیش درک شده‌اند. جهت ارزیابی موضوع، تحقیق باید تکنیک‌های مرتبط مجزا را درجهت یک راه حلی که امنیت را در SOA مهیا می‌کند ترکیب نماید.
- نوع روش تحقیق مطالعه کتابخانه‌ای (منابع تحقیقاتی معتبر و استانداردهای جهانی) در جهت تحقق اهداف ذیل می‌باشد:
- شناخت و درک اصول معماری سرویس‌گرا (با مروری بر ادبیات موضوع).

---

<sup>1</sup> tag