

شناسایی و بررسی رابطه عوامل و ابعاد تأثیرگذار بر امنیت نظام‌های اطلاعاتی گسترش یافته با روش معماری خدمت‌گرا

ماندانا ایزدی^۱ | محمدرضا تقوا^۲

۱. [پدیدآور رابط] کارشناسی ارشد مدیریت فناوری اطلاعات؛ دانشگاه علامه طباطبایی
m_izadi85@yahoo.com

۲. دکتری مدیریت توسعه سیستم‌ها؛ استادیار؛ گروه مدیریت؛ دانشگاه علامه طباطبایی
taghva@yahoo.com

مقاله پژوهشی

دریافت: ۱۳۹۳/۰۱/۱۷

پذیرش: ۱۳۹۳/۰۴/۱۰

دوره ۳۰ شماره ۱

صص. ۲۸۵-۳۰۵

چکیده: هدف این

مزایای خاص معماری خدمت‌گرا موجب گسترش روزافزون این نوع معماری در سراسر جهان گردیده است. اما بعضی از ویژگی‌های خاص این نوع معماری موجب گردیده که امنیت این نوع نظام اطلاعاتی نسبت به سایر نظام‌های اطلاعاتی در معرض مخاطره بیشتر قرار گیرد. هدف این مقاله، شناسایی و بررسی رابطه عوامل و ابعاد تأثیرگذار بر امنیت نظام‌های اطلاعاتی است که با روش معماری خدمت‌گرا توسعه یافته‌اند. در این پژوهش ابتدا از روش تحلیل عاملی به منظور شناختن متغیرهای مکنون و آشکار استفاده گردید. سپس، مدل معادلات ساختاریافته با استفاده از نرم‌افزار Amos به دست آمد و در نهایت، مقدار تأثیرگذاری هر یک از ابعاد امنیتی بر امنیت کل معماری خدمت‌گرا با استفاده از مدل معادلات ساختاریافته مشخص گردید. نتایج تحقیق نشان می‌دهد که امنیت در سطح شبکه و خدمات وب و امنیت در سطح پیام بر روی امنیت معماری خدمت‌گرا تأثیر معناداری دارد و خروجی نرم‌افزار نشان‌دهنده مناسب بودن مدل ساختار برآزش یافته است.

کلیدواژه‌ها: نظام‌های اطلاعاتی؛ معماری خدمت‌گرا؛ خدمات وب

فصلنامه علمی پژوهشی
پژوهش‌نامه پردازش و مدیریت اطلاعات

پژوهشنامه پردازش و مدیریت اطلاعات

فصلنامه علمی پژوهشی

شاپا (چاپی) ۸۲۲۳-۲۲۵۱

شاپا (الکترونیکی) ۸۲۳۱-۲۲۵۱

نمایه در LISA، ISC و Scopus

http://jipm.irandoc.ac.ir

پژوهشگاه علوم و فناوری اطلاعات ایران

۱. مقدمه

واقعیت موجود در دنیای امروز این است که سازمان‌ها باید به شکلی سریع نسبت به تغییرات تجاری واکنش نشان دهند و از سرمایه‌های موجود در برنامه‌های کاربردی و زیربنایی به‌منظور تمرکز بر روی نیازمندی‌های تجاری جدیدتر استفاده نمایند. معماری خدمت‌گرا را که از سال ۱۹۹۹ توسط سه شرکت، آی‌بی‌ام^۱، مایکروسافت^۲ و سان^۳ بر اساس خدمات وب معرفی گردید، می‌توان رویکردی جدید در دنیای نظام‌های اطلاعاتی و نرم‌افزار دانست که با رفع محدودیت‌ها و نواقص معماری پیشین توانسته است، به‌عنوان بهترین گزینه در این زمینه محسوب شود. این معماری را می‌توان چارچوبی وسیع و استاندارد دانست که خدمات در آن ساخته شده، استقرار می‌یابند، و مدیریت می‌شوند و هدفش افزایش چابکی زیرساخت‌های فناوری اطلاعات در جهت واکنش سریع نسبت به تغییرات در نیازهای کسب‌وکار است (فقیه ۱۳۸۷). معماری خدمت‌گرا مبتنی بر الگوی تعاملی خاصی است که شامل سه عامل فراهم‌کننده خدمت، در خواست‌کننده خدمت، و کشف خدمت است. فراهم‌کننده خدمت از طریق شبکه به ارائه توضیحات آن خدمت برای عامل کشف خدمت می‌پردازد. درخواست‌کننده معمولاً درخواست پیدا کردن خدمت را به عامل کشف خدمت می‌دهد تا از طریق آن به توضیحات ارائه‌شده خدمت و محل آن دسترسی پیدا کند. سپس، با به‌کارگیری این اطلاعات به فراهم‌کننده خدمت متصل شده و از خدمت ارائه‌شده استفاده می‌کند (Chodavarapu & Kanneganti 2007). معماری خدمت‌گرا بر پایه ساخت نظام‌های توزیع شده است. منظور از نظام توزیع شده، مجموعه‌ای از خدمات‌های مستقل است که از دیدگاه کاربران همچون یک نظام منسجم عمل می‌کند. یکی از مهم‌ترین اهداف نظام توزیع شده این است که کاربران به‌راحتی به منابع راه دور دسترسی داشته باشند و آنها را به روش کنترل شده و مؤثر به اشتراک بگذارند. در معماری خدمت‌گرا صحبت از یکپارچگی و استقلال نسبتاً زیاد خدمات‌ها و قابلیت تعامل بین خدمات‌های درون سازمانی و برون سازمانی است. منظور از استقلال زیاد یا اتصالات سست خدمات‌ها، قابلیت تعامل بین خدمات‌ها به‌صورت مستقل از کدنویسی و

1. IBM
2. Microsoft
3. SUN

مکان خدمات است، به گونه‌ای که خدمات‌ها در زمان اجرا می‌توانند تغییر مکان داده، روال‌های داخلی خود را تغییر دهند، یا حتی از یک فناوری جدیدتر استفاده کنند؛ بدون آنکه تأثیری منفی بر خدمت‌گیرندگان گذاشته شود. معماری خدمت‌گرا با طبیعت اتصال آزادانه خود به سازمان‌ها امکان بهره‌گیری از خدمات جدید یا ارتقاء خدمات موجود را فراهم می‌آورد و امکانی را برای قابل استفاده نمودن خدمات‌ها در کانال‌های متفاوت فراهم می‌سازد که می‌تواند علاوه بر مزایای رقابتی، همچون چابکی و انعطاف‌پذیری که به‌وجود می‌آورد، تهدیدها و چالش‌هایی را نیز برای این نظام اطلاعاتی فراهم نماید. این ویژگی‌های خاص معماری خدمت‌گرا موجب گردیده که این نظام اطلاعاتی نسبت به سایر نظام‌های اطلاعاتی در معرض خطر بیشتر قرار گیرد و از آنجا که هر نظام اطلاعاتی به‌عنوان دارایی مهم اکثر سازمان‌ها محسوب می‌شود، به مخاطره‌افتادن امنیت نظام اطلاعاتی، سازمان‌ها را با مشکلات بسیاری همچون دسترسی به اطلاعات محرمانه، سوءاستفاده مالی، تخریب اطلاعات، از کار انداختن سرور و ... مواجه خواهد نمود. از طرفی، ویژگی خاص این معماری موجب گردیده که بررسی و مطالعه امنیت در این نوع معماری نیز به‌طور خاص و مختص به همین معماری انجام گیرد. این امر، ضرورت و لزوم مطالعه امنیت در معماری خدمت‌گرا و شناسایی و ارتباط عوامل تأثیرگذار بر آن را آشکار می‌سازد. مزایای رقابتی معماری خدمت‌گرا سبب رشد روزافزون این معماری، به‌ویژه در دو دهه اخیر در سراسر جهان شده است. اما ویژگی خاص معماری خدمت‌گرا، از جمله خاصیت توزیع‌شدگی و بازبودن مرزهای آن، موجب شده که امنیت این معماری با چالش‌هایی، همچون نبودن مفهوم پیوستگی، احراز هویت برای خدمات بیرونی، امنیت بین مرزها، امنیت برنامه‌های کاربردی و ... که از ترکیب چندین خدمت تشکیل شده‌اند، همراه باشد. گرچه هر ساله تعداد مقاله‌هایی که به جنبه خاصی از امنیت معماری خدمت‌گرا می‌پردازند، در حال افزایش است، اما به نظر می‌رسد، به دلیل نوبودن این نوع معماری و عدم شناخت بسیاری از خبرگان حوزه نظام‌های اطلاعاتی و شبکه و چالش‌های موجود در زمینه امنیت معماری خدمت‌گرا، تاکنون مطالعات چندانی به‌ویژه با رویکرد کلی و مدیریتی در این زمینه انجام نشود. هدف این پژوهش شناسایی و بررسی رابطه عوامل و ابعاد تأثیرگذار بر امنیت نظام‌های اطلاعاتی است که با روش معماری خدمت‌گرا توسعه یافته‌اند تا به تصمیم‌گیری بهتر مدیران و مجریانی کمک کند که مسئول برقراری

امنیت در نظام‌های اطلاعاتی با معماری خدمت‌گرا هستند.

در این تحقیق، به منظور بررسی و استخراج عوامل تأثیرگذار بر امنیت معماری خدمت‌گرا، نخست، ادبیات پژوهش مربوطه مورد مطالعه قرار گرفت و پس از مصاحبه با خبرگان و استخراج شاخص‌های نهایی، به تهیه پرسشنامه، جمع‌آوری و تجزیه و تحلیل داده‌ها با کمک تکنیک تحلیل عاملی پرداخته شد و در نهایت با کمک نرم‌افزار Amos مدل نهایی استخراج گردید. این تحقیق شامل ۲ سؤال اصلی و ۷ فرضیه به شرح زیر است:
سؤال‌های اصلی تحقیق:

- ◇ عوامل تأثیرگذار بر امنیت نظام اطلاعاتی توسعه‌یافته با روش معماری خدمت‌گرا کدامند؟
- ◇ شدت و جهت تأثیرگذاری این عوامل بر امنیت نظام اطلاعاتی توسعه‌یافته با روش معماری خدمت‌گرا چگونه است؟
فرضیه‌های تحقیق به شرح زیر است:
- ◇ فرضیه ۱: بین امنیت در سطح طراحی و پیاده‌سازی معماری و امنیت در نظام‌های اطلاعاتی توسعه‌یافته با روش معماری خدمت‌گرا تأثیر معناداری وجود دارد.
- ◇ فرضیه ۲: بین امنیت در سطح شبکه و خدمات وب و امنیت در نظام‌های اطلاعاتی توسعه‌یافته با روش معماری خدمت‌گرا تأثیر معناداری وجود دارد.
- ◇ فرضیه ۳: بین امنیت در سطح پیام و امنیت در نظام‌های اطلاعاتی توسعه‌یافته با روش معماری خدمت‌گرا تأثیر معناداری وجود دارد.
- ◇ فرضیه ۴: امنیت در قسمت مدیریت، بر روی امنیت در نظام‌های اطلاعاتی توسعه‌یافته با روش معماری خدمت‌گرا تأثیر معناداری دارد.
- ◇ فرضیه ۵: بین امنیت در سطح منابع فیزیکی و محیط و امنیت در نظام‌های اطلاعاتی توسعه‌یافته با روش معماری خدمت‌گرا تأثیر معناداری وجود دارد.
- ◇ فرضیه ۶: بین امنیت در سطح منابع انسانی و امنیت در نظام‌های اطلاعاتی توسعه‌یافته با روش معماری خدمت‌گرا تأثیر معناداری وجود دارد.
- ◇ فرضیه ۷: بین امنیت در سطح برنامه‌های کاربردی و امنیت در نظام‌های اطلاعاتی توسعه‌یافته با روش معماری خدمت‌گرا تأثیر معناداری وجود دارد.

۲. ادبیات پژوهش

معماری خدمت‌گرا به دلیل مزایای بی‌شمار خود، امروزه از سوی اکثر سازمان‌ها در سراسر جهان پذیرفته شده است. ویژگی خاص معماری خدمت‌گرا موجب شده است که امنیت این معماری نسبت به سایر نظام‌های اطلاعاتی در معرض خطر بیشتر قرار گیرد. در حال حاضر، یکی از مشکلات بزرگ در گسترش این معماری، چالش‌های امنیتی موجود در آن است. از مهم‌ترین چالش‌های امنیتی معماری خدمت‌گرا می‌توان به توسعه معماری خدمت‌گرا، پذیرش ملزومات سخت‌افزاری و نرم‌افزاری، نبودن مفهوم پیوستگی، اداره کردن امنیت بین مرزها، و اداره کردن امنیت در کاربردهایی که از چندین خدمت ترکیب شده است، اشاره نمود (Gossele & Mackey 2006).

بنابراین، به منظور برقراری امنیت در نظام‌های اطلاعاتی با روش معماری خدمت‌گرا لازم است که ابتدا به بررسی عوامل تأثیرگذار بر امنیت معماری خدمت‌گرا پرداخته شود.

امنیت در سطح طراحی و معماری

یکی از موارد مهم و تأثیرگذار بر امنیت معماری خدمت‌گرا نحوه طراحی و معماری این نظام اطلاعاتی است. هافنر و بریو استفاده از گذرگاه خدمت سازمانی و امنیت به‌عنوان یک خدمت را به‌منزله دو عامل اصلی برای ایجاد امنیت در طراحی ساختار معماری خدمت‌گرا معرفی نموده‌اند (Hafner & Berue 2009).

گذرگاه خدمت سازمانی یک بستر نرم‌افزاری جامع است که از استانداردهای وب استفاده می‌کند تا مجموعه متنوعی از ساختارهای ارتباطی را روی چندین پروتکل انتقالی پشتیبانی کند. به عبارتی، این گذرگاه وظیفه یکسان‌سازی و مدیریت جریان اطلاعات ما بین نرم‌افزارهای سازمانی را بر عهده خواهد گرفت. مهم‌ترین وظیفه آن پشتیبانی و تبدیل پروتکل‌های مختلف به یکدیگر و تبدیل خدمات وب مورد نظر به یک استاندارد قابل فهم است. آنها معتقدند که در مدل امنیت به‌عنوان یک خدمت، منطق امنیت به‌صورت بخشی از یک برنامه کاربردی و یا بخشی از منطق یک خدمت نیست، بلکه به‌صورت مجزا و متمرکز به شکل یک خدمت‌دهنده امنیتی پیاده‌سازی می‌گردد. تمامی تبدلات به‌صورت داده، پیام، درخواست و ... ابتدا تحت کنترل و نظارت این خدمت‌دهنده امنیتی قرار می‌گیرد. یک خدمت‌دهنده امنیتی اعمال مرتبط با کنترل دسترسی مانند احراز هویت،

اختیارسنجی، رمزگذاری و رمزگشایی پیام‌ها، تشخیص امضاها، الکترونیکی، ثبت پیام‌ها و ... را انجام می‌دهد. بنابراین، در این روش دیگر نیازی به فراخوانی مستقیم خدمت نیست. این خدمت‌دهنده خود به‌طور ضمنی وارد عمل می‌شود و تمامی تبادلات داده، پیام، تراکنش و ... تحت کنترل این خدمت‌دهنده قرار می‌گیرد (دارا ۱۳۸۸).

امنیت شبکه

منظور از امنیت شبکه برقراری امنیت و جلوگیری از هر گونه آسیب و تهدید در ساختار و تمامی منابع اصلی شبکه است. منابع شبکه شامل سوئیچ‌ها، روترها، فایروال‌ها، اطلاعات عملیات شبکه، مانند جداول مسیریابی و پیکربندی و منابع اطلاعاتی متصل به شبکه مانند پایگاه داده و سرورهای اطلاعاتی و ... می‌باشد.

محققان بسیاری همچون منزل امنیت شبکه و وب را یک عامل اصلی در امنیت معماری خدمت‌گرا دانسته‌اند (Menzel 2007)؛ چرا که استفاده از خدمات وب، گسترده‌ترین نگرش پذیرفته شده در به کارگیری معماری خدمت‌گراست. به همین دلیل بیشتر جنبه‌های امنیتی در این نوع معماری بر امنیت خدمات وب متمرکز است. WSDL, SOAP, UDDI, XML اجزای اصلی تکنولوژی وب هستند که برای پیاده‌سازی خدمات وب به کار می‌روند. بنابراین، توجه به جنبه‌های امنیتی این پروتکل‌ها در امنیت خدمات وب اهمیت بسیاری دارد (Fareghzadeh 2009).

از عوامل مؤثر بر امنیت شبکه و وب، مجزاسازی فضای آدرس، فیلتر کردن پورت‌ها، کنترل ترافیک، محکم کردن پایه‌های امنیتی و ... را می‌توان نام برد.

امنیت در سطح پیام

اماراو و پرساد امنیت در سطح پیام را به‌عنوان یک عنصر مهم در ایجاد امنیت در ساختارهای توزیع شده مبتنی بر خدمت برشمرده‌اند (Ramarao & persad 2008). از دیدگاه اماراو و پرساد برای امنیت در سطح پیام و یا همان بسته اطلاعاتی می‌توان از مسیریابی پیام‌ها استفاده کرد؛ یعنی پیام‌ها به سمت نقاط انتهایی معتبری که مد نظر است، هدایت می‌شوند. برای مثال، پیام در صورتی به سمت خدمت A هدایت می‌شود که درخواست کننده، ویژگی‌های X و Y را داشته باشد. یک دیدگاه دیگر این است که

بخش‌های مختلف یک پیام می‌توانند به‌طور مجزا محافظت شوند تا در مسیر پیام، تنها توسط بخش‌هایی که مورد نظر است، قابل استفاده باشند. از عوامل مؤثر بر امنیت پیام می‌توان به محرمانگی پیام، جامعیت، دسترس‌پذیری، احراز هویت، تعیین سطح اختیار، و امنیت در سطح نقل و انتقالات اشاره کرد (دارا ۱۳۸۸).

مدیریت امنیت

هافنر و بریو در تحقیقات خود به این نتیجه رسیده‌اند که یکی دیگر از عواملی که در امنیت معماری خدمت‌گرا باید مورد توجه قرار گیرد، مدیریت است (Hafner & Berue 2009). آنها معتقدند که مدیریت شامل سه فاکتور مدیریت امنیت، مدیریت سیاست، و مدیریت سیاست امنیتی است. مدیریت امنیت، مدیریت تمامی مراحل و راهکارهای امنیتی از ایجاد و تأمین امنیت، محافظت و نگهداری، کنترل و بازرسی امنیت و ... را شامل می‌شود.

مدیریت سیاست، اهدافی است که به وسیله کسب و کار ایجاد شده و به حرکت درآمده‌اند، اکنون باید به وسیله زیرساخت‌ها اجرا شوند. مدیریت سیاست، چارچوبی را برای اجرا کردن سیاست فراهم می‌کند.

مدیریت سیاست‌های امنیتی با معرفی سیاست‌های کسب و کاری و با معرفی سیاست‌های خاص آن خدمت‌مانند امنیت، شاخص‌های عملکرد، سیاست‌های مطمئن و ... آغاز می‌شود. این سیاست‌ها به وسیله زیرساخت‌ها برای امنیت دسترسی به اطلاعات، فراهم کردن دسترسی، نگهداری، توانایی ممیزی و مانند آنها اداره می‌شود (Casola 2007).

امنیت برنامه‌های کاربردی

منظور از امنیت در سطح برنامه‌های کاربردی استفاده از سخت‌افزار، نرم‌افزار، و روش‌هایی است که به منظور حفاظت از این برنامه‌ها در مقابل تهدیدهای بیرونی به کار برده می‌شود. سیمینگ بر این عقیده است که برنامه‌های کاربردی نیز از جمله عواملی است که توجه‌نکردن به آن، امنیت این نوع نظام اطلاعاتی را به مخاطره می‌اندازد (Siming 2010). آنها بر این باورند که میزان امنیت در برنامه‌های کاربردی تا حد زیادی به قابلیت دسترسی آن برنامه کاربردی در سطح شبکه بستگی دارد. هر چه قابلیت دسترسی آن برنامه

کاربردی در سطح شبکه بیشتر باشد، در مقابل گستره متنوعی از تهدیدها، آسیب پذیرتر می شود. امنیت در این گونه برنامه‌ها احتمال دسترسی، دزدی، اصلاح و یا حذف کردن داده‌های حساس توسط کدهای مخرب را به حداقل می‌رساند (Siming & Babar 2010).

امنیت منابع فیزیکی

از دیدگاه ویلی و وینگ در صد بزرگی از ریسک‌های نظام‌های اطلاعاتی نتیجه دسترسی غیرمجاز به حوزه نظام‌های اطلاعاتی، صدمات فیزیکی به منابع نظام‌های اطلاعاتی، سرقت دارایی و ... هستند (Weilye & Wing 2005). در صورتی که میزان کافی از حفاظت برای سنجش فیزیکی و امنیت محیطی به کار برده شود، می‌توان از بسیاری از این تهدیدها جلوگیری کرد. در امنیت منابع فیزیکی می‌توان به امنیت تجهیزات و کنترل‌های عمومی اشاره کرد. منظور از امنیت تجهیزات، حفاظت و نگهداری مطمئن سطح امنیتی نظام‌های اطلاعاتی است و کنترل‌های عمومی، کنترل‌های فراگیری هستند که بر زیرساخت فناوری اطلاعات سازمان حاکمیت دارند و بر همه بخش‌های کاربردی اعمال می‌شوند. این کنترل‌ها شامل کنترل بر فرایند پیاده‌سازی نظام، کنترل‌های نرم‌افزاری، کنترل‌های سخت‌افزاری فیزیکی، کنترل‌های عملیات رایانه‌ای، کنترل‌های امنیت داده‌ها، مقررات اجرایی، استانداردها و رویه‌ها می‌شود (Weilye & wing 2005).

امنیت منابع انسانی

امنیت منابع انسانی به معنای ایجاد و برقراری امنیت در کار نیروی انسانی است که مرتباً در حال کار با نظام‌های اطلاعاتی هستند و به منظور جلوگیری از هر گونه صدمه و آسیب به مجموعه نظام اطلاعاتی مطرح است. محققان بسیاری از جمله کندولین امنیت منابع انسانی و پرسنل را یکی از عوامل تأثیرگذار بر امنیت معماری خدمت‌گرا دانسته و آن را از مهم‌ترین عناصر تأثیرگذار بر شمرده است. وی به آموزش، تحصیل و آگاهی از جمله شاخص‌های امنیت منابع انسانی اشاره نموده است (Candolin 2007).

۱-۲. پیشینه تجربی

در زمینه امنیت اطلاعات در معماری خدمت‌گرا پژوهش‌های متعددی انجام شده است. از آن دسته می‌توان به دسترسی چارچوب کنترل امنیت هوشمند و معماری

خدمت‌گرا (Yamany & Miriam 2010)، مشکلات خدمت‌دهی وب در طراحی معماری خدمت‌گرا (Yue & Tao 2012)، معماری خدمت‌گرا برای امنیت نظام شبکه همراه (Rosado & Eduardo 2011)، و امنیت و کاربرد آن در برنامه‌های معماری خدمت‌گرا (Hangjung & Nazareth 2010) اشاره کرد؛ اما اکثر این مطالعات با یک رویکرد فنی و هر کدام تنها به یک جنبه خاص امنیت این معماری پرداخته‌اند و کمابیش هیچ کدام با یک دید کلی و یک رویکرد مدیریتی به بررسی این موضوع نپرداخته‌اند.

◇ الیمنی و همکاران در پژوهشی با عنوان «دسترسی چارچوب کنترل امنیت هوشمند و معماری خدمت‌گرا» بیان کردند که یکی از مشکلات بزرگ گسترش معماری خدمت‌گرا چالش‌های امنیتی موجود در آن است؛ چرا که مسئولیت امنیت معماری خدمت‌گرا به هر دو گروه ارائه‌دهندگان و مصرف‌کنندگان وابسته است (Yamany & Miriam 2010). آنان معتقدند که در سال‌های اخیر، تلاش‌های زیادی برای رفع این نواقص انجام شده و از آن دسته، دسترسی به استانداردهای امنیتی شبکه وب است که شامل WS-Security و WS-Policy می‌باشد. در این پژوهش یک چارچوب هوشمند امنیتی پیشنهاد شده که شامل دو عنصر مهم در زمینه دستیابی به امنیت است: ۱. احراز هویت و امنیت خدمات (NSS) و ۲. خدمات مختار (AS). در این پژوهش از سه نوع مختلف داده‌کاوی استفاده شده است: ۱. قوانین انجمن که به پیش‌بینی حمله‌ها کمک می‌کند؛ ۲. مکعب پردازش تحلیلی برخط برای مجوز استفاده و ۳. الگوریتم کاوش استخراجی که دسترسی به کنترل نمایندگی حقوق و نظام خودکار را فراهم می‌کند (Yamany & Miriam 2010).

یو و تائو در پژوهشی با عنوان «مشکلات خدمت‌دهی وب در طراحی معماری خدمت‌گرا» بیان کرده‌اند که با توسعه جهانی استفاده از فناوری معماری خدمت‌گرا، مسائل امنیتی خدمات تارنما (وبسایت) که بر اساس سطوح ناهمگون شکل گرفته‌اند، به‌طور فزاینده‌ای برجسته و مهم خواهد شد. در این پژوهش دو راهکار امنیتی برای خدمات مربوط به خدمت‌دهی ارائه شده است (Yue & Tao 2012).

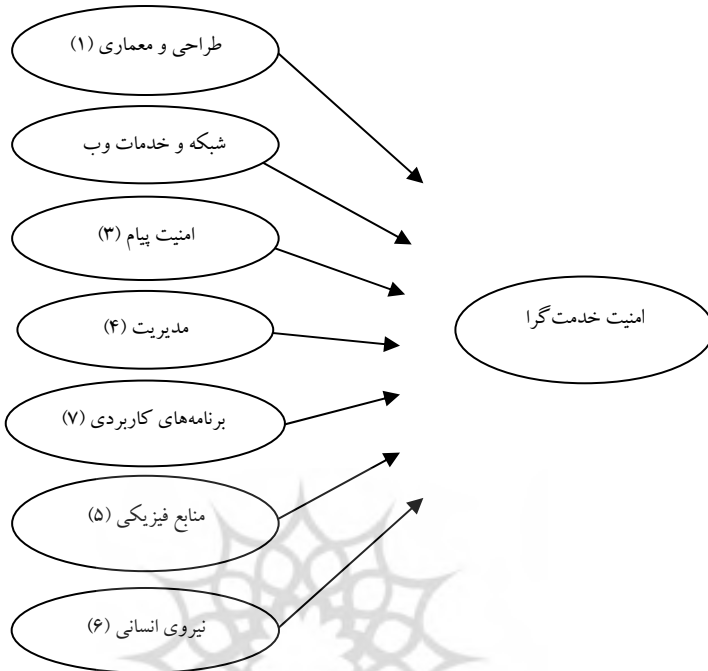
◇ روسادو و همکاران در مطالعه‌ای با موضوع معماری خدمت‌گرا برای امنیت شبکه همراه بیان کردند که امنیت در نظام‌های شبکه همراه بسیار ضروری است؛ در حالی که تأمین امنیت این نظام‌ها به دلیل کمبود منابع در این دستگاه‌ها سخت و پیچیده است. در

این پژوهش برای حفظ امنیت این نظام‌ها، از مدلی بر اساس طراحی معماری خدمت‌گرا استفاده شده است. این مدل تا اندازه‌ای محدودیت‌های دسترسی به امنیت شبکه‌های تلفن همراه را برآورده می‌کند؛ اما نتایج پژوهش نشان می‌دهد که این مدل به‌طور کامل راهگشا نبوده است (Rosado & Eduardo 2011).

◇ هنگ‌جنگ و همکاران در سال ۲۰۱۰ در پژوهشی با عنوان «امنیت و برنامه‌های کاربردی در معماری خدمت‌گرا؛ موضوعات تجارتي»، معتقدند با پیشرفت کاربرد محاسبات و طراحی معماری خدمت‌گرا و گسترش استفاده از این خدمات، از برنامه‌های کاربردی زیادی با توسعه مؤلفه‌های نرم‌افزاری و شبکه‌های استاندارد استفاده خواهد شد. این برنامه‌ها به لحاظ هزینه و پتانسیل تولید نسبی بالاتر، به وسیله طراحی معماری خدمت‌گرا تعدیل خواهند شد و تنها مشکل موجود، تأمین امنیت کاربری این برنامه‌ها و شبکه‌هاست. در این پژوهش از یک الگوریتم ژنتیک برای یافتن مجموعه‌ای بهینه از خدماتی که از پروسه‌های تجاری این خدمات پشتیبانی کند، استفاده شده است. آنها معتقدند که کاربرد این روش در آینده گسترده‌تر خواهد شد (Hangjung & Nazareth 2010).

۲-۲. مدل مفهومی تحقیق

به‌منظور استخراج مدل امنیت بر نظام‌های اطلاعاتی با روش معماری خدمت‌گرا، ابتدا ادبیات مربوط به آن، مورد مطالعه قرار گرفت و سپس، مدل پیشنهادی ارائه گردید. مدل مفهومی این تحقیق دارای متغیرهای امنیت در سطح شبکه و خدمات وب، مدیریت، معماری، امنیت در سطح پیام و یا بسته اطلاعاتی، منابع فیزیکی، نیروی انسانی، برنامه‌های کاربردی است که در این مدل به‌عنوان متغیر مستقل و امنیت در معماری خدمت‌گرا به‌عنوان متغیر وابسته فرض شده است. فرضیات تحقیق که بر مبنای مدل تدوین شده، در قالب ۷ فرضیه اصلی به بررسی عوامل مؤثر بر امنیت معماری خدمت‌گرا و یا به‌عبارتی، متغیرهای مکنون تأثیرگذار بر امنیت معماری خدمت‌گرا می‌پردازد.



نمودار ۱. مدل مفهومی پژوهش

۳. روش‌شناسی پژوهش

این تحقیق یک تحقیق کاربردی و از لحاظ روش انجام تحقیق، توصیفی محسوب می‌شود. جامعه آماری در نظر گرفته شده در این تحقیق، شامل تمامی خبرگانی می‌شود که در سطح شهر تهران در زمینه امنیت نظام‌های اطلاعاتی که بر پایه معماری خدمت‌گرا پایه‌ریزی شده، مشغول فعالیت بوده‌اند. از آنجا که تعداد این افراد بسیار محدود و پراکنده می‌باشد، برای گسترش جامعه آماری و به دلیل آشنایی و در دسترس بودن، شهر اصفهان را نیز به جامعه آماری خود افزودیم و به افرادی که در زمینه امنیت نظام‌های اطلاعاتی و امنیت شبکه و خدمات وب فعالیت داشته و دانش کافی در مورد معماری خدمت‌گرا را نیز دارا بودند، اکتفا کردیم. جامعه هدف ما (خبرگان) را مدیران فناوری اطلاعات، مدیران امنیت شبکه و اطلاعات، کارشناسان امنیت نرم‌افزار و شبکه، کارشناسان نظام مدیریت امنیت اطلاعات که دارای دانشی در مورد معماری خدمت‌گرا بوده و بیش از ۳ سال سابقه

فعالیت داشتند، تشکیل می‌دهند. از آنجا که تعداد افراد فعال در زمینه معماری خدمت‌گرا و یا دارای دانش کافی در این زمینه همچنان محدود و پراکنده می‌باشند، نمونه‌گیری به صورت هدفمند و در دسترس انجام شد. ابزار گردآوری اطلاعات، پرسشنامه بوده است و از بین ۲۴۰ پرسشنامه توزیع شده، ۲۲۵ پرسشنامه دریافت گردید. پرسشنامه مورد استفاده، یک پرسشنامه محقق ساخته است که از مطالعه ادبیات تحقیق و مصاحبه با چند تن از خبرگان این حوزه حاصل گردیده است. روایی تحقیق از طریق مطالعه مبانی نظری و با استفاده از نظرات استادان و متخصصان در این زمینه حاصل شد. همچنین، از طریق مدل‌یابی معادلات ساختاری و تحلیل عاملی، روایی پرسشنامه نیز مورد تحلیل و تأیید قرار گرفت. پایایی ابزار تحقیق با استفاده از نرم‌افزار Spss از طریق آزمون ضریب آلفای کرونباخ محاسبه شد که مقدار آن برابر با ۰/۷۹ به دست آمد. سپس، برای سازگاری درونی در مدل ساختاری برای هر یک از ابعاد امنیتی نیز به طور مجزا آلفای کرونباخ محاسبه شد. برای تجزیه و تحلیل داده‌ها از تحلیل عاملی و مدل معادلات ساختاری با کمک نرم‌افزار Amos استفاده شد. شاخص‌های سنجش امنیت معماری خدمت‌گرا و هر یک از ابعاد امنیتی آن به طور خلاصه، در جدول شماره ۱ گردآوری شده است.

جدول ۱. شاخص‌های سنجش امنیت معماری خدمت‌گرا و هر یک از ابعاد امنیتی

عامل	آیتم	آلفای کرونباخ
امنیت معماری خدمت‌گرا	میزان دفعات خرابی نظام (Heather & Hondo 2005)	۰/۷۲۶
	درصد احتمال وقوع آسیب‌ها (Heather & Hondo 2005)	
	کنترل دسترسی به سایر خدمات (Heather & Hondo 2005)	
	میزان انطباق با الزامات قانونی (Heather & Hondo 2005)	
	امکان جداسازی داده‌های حساس (Heather & Hondo 2005)	
	میزان بازیافت اطلاعات (Heather & Hondo 2005)	

عامل	آیتم	آنفای کروناخ
امنیت شبکه و خدمات وب	مجزا سازی فضای آدرس (Buecker et.al 2007) فیلتر کردن پورت‌ها (Buecker et.al 2007) کنترل ترافیک (Buecker et.al 2007) محکم کردن پایه‌های امنیتی (Buecker et.al 2007)	۰/۷۸۳
امنیت در سطح مدیریت	مدیریت ریسک (دارا ۱۳۸۸) مدیریت سیاست امنیتی (دارا ۱۳۸۸) مدیریت سیاست (دارا ۱۳۸۸)	۰/۵۱۱
امنیت در سطح معماری	امنیت به‌عنوان یک خدمت (Heather & Hondo 2005) پروکسی و ESB (Heather & Hondo 2005)	۰/۷۰۹
امنیت در سطح پیام	محرمانگی (Jonnaganti 2009) جامعیت (Jonnaganti 2009) دسترس پذیری (Jonnaganti 2009) احراز هویت (Jonnaganti 2009) تعیین سطح اختیار (Jonnaganti 2009) نقل و انتقال (Jonnaganti 2009)	۰/۷۳۲
امنیت در سطح منابع فیزیکی	تجهیزات (Buecker et.al 2007) کنترل‌های عمومی (Buecker et. al, 2007)	۰/۴۳۱
امنیت در سطح نیروی انسانی	تحصیل (Jonnaganti 2009) آموزش (Jonnaganti 2009) آگاهی (Jonnaganti 2009)	۰/۷۰۱

۴. یافته‌های پژوهش

پیش از انجام تحلیل‌های آماری لازم برای آزمون فرضیات پژوهش و به‌منظور بررسی روایی متغیرها و عوامل مورد سنجش و در صورت لزوم حذف برخی گویه‌های کاهنده این روایی از آماره اندازه‌گیری کفایت نمونه‌گیری کایسر-مایر-اولکین (KMO) و آزمون کرویت بارتلست استفاده نمودیم. در این پژوهش برای ۳۹ متغیر شناخته‌شده، ۱۱ گویه‌ای که مقادیر اشتراک استخراجی کمتر از ۰/۰۵ داشتند، حذف گردید و سپس مقدار آماره اندازه‌گیری KMO و آزمون کرویت بارتلست محاسبه گردید که با انجام محاسبه‌های لازم مقدار آماره KMO برابر با ۰/۷۸۱ و سطح معنی‌داری آزمون بارتلست برابر با ۰/۰۰۰ به‌دست آمد. از آنجا که مقدار شاخص کفایت نمونه‌ای بیشتر از ۰/۵ است، می‌توان نتیجه گرفت که کوواریانس موجود بین آیتم‌های طرح‌شده برای سنجش سازه‌های اصلی تحقیق به اندازه کافی برای استخراج حداقل یک عامل کافی است. از طرف دیگر، سطح معنی‌داری کوچک‌تر از ۰/۰۵ برای آزمون بارتلست نیز حاکی از تفاوت معنادار ماتریس همبستگی مشاهده‌شده با ماتریس همبستگی صفر است. به این معنا که ضرایب همبستگی بین آیتم‌ها با صفر تفاوت معنادار داشته و می‌توان انجام تحلیل عاملی را در بین آیتم‌های پرسشنامه تحقیق دارای توجیه آماری دانست. با توجه به زیربنای نظری موجود برای آیتم‌های پرسشنامه، در این تحقیق از تحلیل عاملی تأییدی بهره گرفته شده است. بعد از انجام این آزمون، به سراغ تحلیل عاملی تأییدی و آزمون‌های برازش مدل می‌رویم. نتایج این تجزیه و تحلیل به همراه مدل تحلیل عاملی تأییدی برای امنیت در نظام‌های اطلاعاتی توسعه‌یافته با روش معماری خدمت‌گرا در جدول شماره ۲ خلاصه گردیده است.

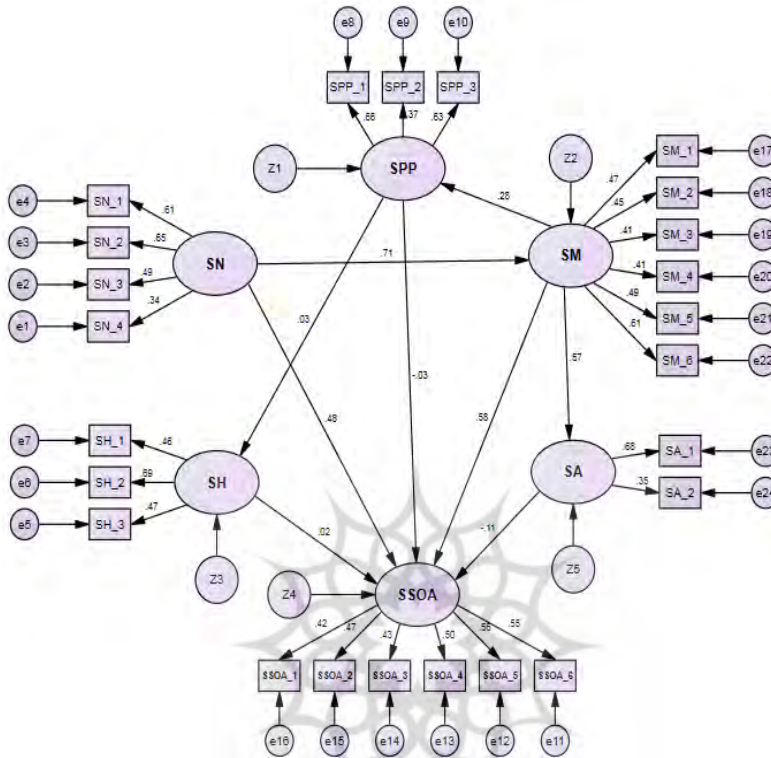
پرتال جامع علوم انسانی

جدول ۲. خلاصه نتایج تحلیل عاملی تأییدی

آیتم	بار عاملی	عامل	آیتم	بار عاملی	عامل
SOA1	۰/۴۲۲	امنیت معماری	SM1	۰/۴۷۰	امنیت پیام
SOA2	۰/۴۷۴	خدمت‌گرا	SM2	۰/۴۵۴	
SOA3	۰/۴۲۶		SM3	۰/۴۰۶	
SOA4	۰/۵۰۳		SM4	۰/۴۰۸	
SOA5	۰/۵۶۱		SM5	۰/۴۹۴	
SOA6	۰/۵۵۵		SM6	۰/۶۱	
SH1	۰/۴۶۰	منابع انسانی	SPP1	۰/۶۶۱	برنامه‌های
SH2	۰/۶۸۶		SPP2	۰/۳۶۷	کاربردی
SH3	۰/۴۷۱		SPP3	۰/۶۳۴	
SN1	۰/۶۱۱	شبکه و	SA1	۰/۶۸۱	طراحی و
SN2	۰/۶۵۳	خدمات وب	SA2	۰/۳۴۹	پیاده سازی
SN3	۰/۴۹۲				
SN4	۰/۳۳۷				

بر گرفته از نتایج پژوهش

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی



نمودار ۲. مدل تحلیل عاملی تأییدی برای امنیت معماری خدمت‌گرا

نتایج محاسبات مربوط به شاخص‌های برازش مدل در جدول شماره ۳ خلاصه گردیده است.

جدول ۳. شاخص‌های برازش مدل

CMIN/DF	CFI	PNFI	AGFI	PCFI	RMSEA
۱/۴۴۲	۰/۸۹۱	۰/۵۶۰	۰/۸۶۲	۰/۷۴۷	۰/۰۴۴

برگرفته از نتایج پژوهش

شاخص‌های برازش مدل نشان می‌دهند که داده‌های تجربی تحقیق، مدل نظری تدوین شده را مورد تأیید و حمایت قرار می‌دهند. به عبارت دیگر، برازش داده به مدل برقرار است. کای اسکور نسبی یا کای اسکور هنجار شده $CMIN/DF=1/442$ است که در بازه مطلوب ۱ تا ۵ می‌باشد. مقدار $RMSEA=0/044$ است که از مقدار قابل قبول $0/08$ کوچک‌تر، مقدار PNFI و PCFI هر دو بالای $0/5$ و AGFI بالای $0/85$ است. شاخص CFI $=0/891$ است که همه مقادیر مطلوبی می‌باشند. بنابراین، مدل اندازه‌گیری با توجه به شاخص‌های برازش کلی قابل قبول است.

جدول ۴. نتایج تحلیل رگرسیون برای آزمون فرضیه‌ها

سطح معناداری P	نسبت بحرانی خطای C.R.	معیار S.E.	برآورد		امنیت معماری
			غیر استاندارد	استاندارد	
0/017	2/396	0/300	0/720	0/484	امنیت معماری خدمات گرا
0/802	0/250	0/079	0/020	0/021	امنیت معماری خدمات گرا
0/018	2/360	0/329	0/777	0/584	امنیت معماری خدمات گرا
0/466	-0/729	0/101	-0/074	-0/114	امنیت معماری خدمات گرا
0/760	-0/305	0/067	-0/020	-0/028	امنیت معماری خدمات گرا

برگرفته از نتایج پژوهش

از آنجا که برای رد فرضیه‌های صفر در سطح اطمینان ۹۵ درصد، مقدار آماره آزمون (نسبت بحرانی یا CR) باید بیشتر از $1/96+$ و یا کمتر از $1/96-$ باشد، و مقدار P-value باید برابر یا کمتر از $0/05$ گردد، بنابراین، با توجه به نتایج جدول ۴ تنها فرضیه دوم و سوم، یعنی امنیت در سطح شبکه و خدمات وب و امنیت در سطح پیام و یا همان بسته

اطلاعاتی تنها فرضیه‌هایی هستند که قابل تأیید می‌باشند. از طرفی نتایج این جدول نشان می‌دهد که این دو شاخص تأثیر مثبتی بر امنیت معماری خدمات‌گرا دارند. بنابراین، فرضیه‌های ۲ و ۳ تأیید می‌شوند.

۵. نتیجه‌گیری و پیشنهادها

معماری خدمات‌گرا یک نوع معماری نظام‌های اطلاعاتی است که دارای مزایا و ویژگی‌های خاصی نسبت به سایر نظام‌های اطلاعاتی سنتی است. این ویژگی‌ها موجب گردیده مباحث امنیتی مرتبط با معماری خدمات‌گرا نیز نسبت به نظام‌های اطلاعاتی سنتی متفاوت باشد. تفاوت اکثر پژوهش‌هایی که در زمینه امنیت معماری خدمات‌گرا صورت گرفته با این پژوهش در آن است که اکثر این پژوهش‌ها با رویکرد فنی و مهندسی بوده و بیشتر به بررسی امنیت در معماری نرم‌افزار با روش معماری خدمات‌گرا پرداخته‌اند. اما در این پژوهش، هدف ما بررسی امنیت در یک نظام اطلاعاتی است که با این روش معماری توسعه پیدا کرده و به جای یک دید فنی و مهندسی سعی شده با یک دید مدیریتی به بررسی عوامل و ابعاد تأثیرگذار بر امنیت در این نوع نظام اطلاعاتی پرداخته شود. بنابراین، هدف این پژوهش شناسایی و بررسی رابطه عوامل تأثیرگذار بر امنیت نظام‌های اطلاعاتی است که با روش معماری خدمات‌گرا توسعه یافته‌اند که در قالب یک مدل مفهومی با روش مدل‌سازی معادلات ساختاریافته ارائه می‌شود. در این پژوهش، پس از مشخص نمودن شاخص‌های اصلی از طریق مراجعه به خبرگان و منابع کتابخانه‌ای، به ارائه مدل پرداخته شد و بر اساس آن ۷ شاخص معرفی شد که ۲ تای آنها به دلیل پایین بودن آلفای کروناخ از محاسبات حذف گردید و ۵ مورد بررسی شد. نتایج تحقیق نشان می‌دهد که از بین ۷ عامل شناسایی شده که در امنیت معماری خدمات‌گرا تأثیرگذار هستند، تنها ۲ عامل امنیت شبکه و خدمات وب و امنیت در سطح پیام و یا همان بسته اطلاعاتی به عنوان عوامل تأیید شده که در امنیت معماری خدمات‌گرا تأثیرگذار هستند، شناسایی شده‌اند. بنابراین، تئوری منزل و همچنین تئوری راماراو و پرساد، مبنی بر اینکه شبکه و خدمات وب و ایجاد امنیت در سطح پیام در برقراری معماری خدمات‌گرا تأثیرگذار هستند، تأیید می‌شوند. بنا بر نتایج تحقیق، فرضیه‌های ۲ و ۳ قابل تأیید هستند و دو عامل امنیت شبکه و خدمات وب با شدت تأثیر ۴۵٪ و همچنین امنیت در سطح پیام و یا همان

بسته اطلاعاتی با شدت تأثیر ۵۵٪ به‌عنوان دو عامل اصلی که در امنیت معماری خدمت‌گرا تأثیر مثبت و معناداری دارند، شناخته شده‌اند. به‌عبارتی، با بالابردن امنیت در سطح این دو عامل اصلی می‌توان تا حد زیادی به افزایش امنیت در سطح این نظام اطلاعاتی که مبتنی بر معماری خدمت‌گرا است، کمک نمود. بدین ترتیب، سؤال‌های تحقیق یعنی عوامل اصلی مؤثر در امنیت معماری خدمت‌گرا و همچنین شدت و جهت آنها نیز پاسخ داده می‌شود. در بُعد امنیت پیام، شش عامل محرمانگی، جامعیت، دسترس‌پذیری، احراز هویت، کنترل دسترسی و نقل و انتقالات به‌عنوان عوامل تأثیرگذار شناسایی شده‌اند. با کمک محرمانگی می‌توان از استراق سمع شدن پیام‌ها و رهگیری آنها جلوگیری نمود. جامعیت پیام تضمین می‌کند که پیام‌ها و یا بسته‌های دریافتی دقیقاً همان چیزی است که توسط نهاد مجاز ارسال شده و فاقد هر گونه تغییر، درج، حذف و یا تکرار است و با کمک احراز هویت می‌توان تشخیص داد که تقاضای فرد بر روی آن سیستم مجاز است یا نه؟

به‌منظور جلوگیری از استفاده غیرمجاز از منابع، بدین معنی که چه کسی می‌تواند به منبع دسترسی داشته باشد، دستیابی تحت چه شرایطی می‌تواند صورت گیرد و کسانی که به منابع دسترسی دارند چه کارهایی می‌توانند انجام دهند، می‌توان از کنترل دستیابی استفاده نمود. برای ایمن کردن داده‌ها باید کانال‌های ایمنی را برای تبادل داده‌ها فراهم کرده و بتوان تمامی داده‌های موجود در کانال را کدگذاری نمود. رعایت اصول امنیتی در تک‌تک این عوامل موجب برقراری امنیت در سطح پیام می‌گردد که این عامل نیز خود با ضریب تأثیر ۵۵٪ باعث افزایش امنیت در معماری خدمت‌گرا می‌شود.

در بُعد امنیت شبکه و وب نیز چهار عامل مجزاسازی فضای آدرس، فیلتر کردن پورت‌ها، کنترل ترافیک و محکم کردن پایه‌های امنیتی، شناسایی گردیدند. مجزاسازی فضاهای آدرس کمک می‌کند که بتوان از تداخل فرایندها با فضای آدرس فرایندهای دیگر جلوگیری نمود. در واقع یک نظام اجرایی، هم از فضای آدرس فرایندهایش محافظت می‌کند و هم محیط‌های مجازی را از بین محیط‌های نظام‌های اجرایی متفاوت مجزا می‌سازد. بازبودن پورت‌ها راه‌های نفوذ بر انواع کدهای مخرب را بیشتر می‌کند که با فیلتر کردن پورت‌های غیرضروری می‌توان راه‌حل‌های نفوذ هکرها و ورود کدهای مخرب را بست. عامل دیگری که در امنیت شبکه و وب شناسایی گردید، کنترل کردن ترافیک شبکه است. کنترل ترافیک شبکه موجب می‌گردد که جریان ترافیک شبکه یا دسترسی به

نظام‌های اجرایی را نظارت و کشف ترافیک غیرمعمول و رفتار آنها در شبکه را شناسایی نمود. همچنین، با جداسازی ترافیک می‌توان بعضی از پروتکل‌ها را در مقابل حملات خاص پروتکل‌های سطح بالا محافظت کرد؛ مانند جداسازی SOAP و انواع XML که با کمک بعضی فایروال‌ها انجام می‌شود. به‌علاوه با محکم کردن پایه‌های امنیتی اجزا مانند به‌کارگیری روش‌هایی مثل استفاده از شناسه کاربردی و پسورد در هنگام ورود، نصب فایروال، نصب انواع آنتی‌ویروس‌ها و ... می‌توان از بروز برخی صدمات به ساختار شبکه جلوگیری نمود. رعایت اصول امنیتی در این چهار عامل شناسایی شده، موجب برقراری امنیت در سطح شبکه و وب می‌گردد که خود این عامل نیز با ضریب تأثیر ۴۵٪ باعث افزایش امنیت در معماری خدمت‌گرا می‌شود. از آنجا که ارتباط آنها با امنیت معماری خدمت‌گرا، مثبت و معنادار می‌باشد، افزایش امنیت در این دو شاخص منجر به بالا رفتن امنیت در معماری خدمت‌گرا می‌گردد. در ارزیابی نیکویی برآزش مدل نیز از معیارهای PNFI, AGFI, CMIN/DF, CFI, PCFI, RMSEA استفاده گردید. نتایج تحقیق نشان می‌دهد که مدل تحلیل مسیر، مدل بسیار مناسبی است. لذا با توجه به نتایج پژوهش، پیشنهاد ما به مدیران فناوری اطلاعات این است که با توجه به ویژگی‌های خاص این نوع معماری، برای حفظ و برقراری هر چه بیشتر این نوع نظام اطلاعاتی، دو بُعد ویژه امنیت شبکه و خدمات وب و امنیت در سطح پیام را در اولویت کاری خویش قرار داده و علاوه بر استفاده از روش‌هایی که موجب افزایش امنیت در عوامل ارائه شده می‌گردد، نسبت به استفاده از تکنیک‌هایی که موجب بالابردن امنیت در استانداردهای وب همچون WSDL, UDDI, SOAP و همچنین تکنیک‌هایی همچون استفاده از استاندارد WS-Security و محافظت از بخش‌های مختلف پیام که باعث بالابردن امنیت در سطح پیام می‌گردد، توجه کافی صورت گیرد.

۶. فهرست منابع

- دارا، عمار. ۱۳۸۸. معماری سرویس‌گرا با بررسی دیدگاه‌های امنیتی آن. سمینار کارشناسی ارشد. دانشگاه آزاد اسلامی واحد علوم و تحقیقات، تهران.
- فقیه، مهدی. ۱۳۸۷. بررسی مدل‌های بلوغ معماری سرویس‌گرا. سمینار کارشناسی ارشد. دانشگاه شهیدبهشتی، تهران.

Buecker, A., P. Ashley, M. Borrett, & Lu. Ming. 2007. *Understanding SOA Security Design and*

- Implementation. International Technical Support Organization. Brussels: IBM Redbook Publication.*
- Candolin, C. 2007. *A Security Framework for Service Oriented Architectures*. Proceeding of the 5th Military Communications Conference. 15-17 October, Florida.
- Casola, V. 2007. *A Policy-Based Evaluation framework for Quality and Security in Service Oriented Architectures*. 6th IEEE International Conference Web Services. 3-5 May, Leipzig, Germany.
- Chodavarapu, P. & R. Kanneganti. 2007. *SOA Security*. 8th International Conference Web Services. 10-12 December, Grenoble, France.
- Fareghzadeh, N. 2009. Web Service Security Method To SOA Development. *World Academy of Science Engineering and Technology* 49 (5): 36-48.
- Gossele, J & R. Mackey. 2006. Service oriented architecture: security challenges experts system. *Expert system journal* 21 (2): 48-59.
- Hangjung, Z. & D. Nazareth. 2010. Security and Performance in Service-oriented Application: Trading off Competing Objectives. *Decision Support System* 50 (8): 336-346.
- Heather, H. & M. Hondo. 2005. Security Patterns within a Service-Oriented Architecture. *International Journal of Information Security* 7 (3): 23-34.
- Jonnaganti, V. 2009. An integrated Security Model for the Management of SOA. Master Thesis Work in Software Engineering and Management, university of Gothenburg, Sweden.
- Rosado, D & F. Eduardo. 2011. Security Services Architecture for Secure Mobile Grid Systems. *Journal of Systems Architecture: the EUROMICRO Journal* 57 (5): 240-258.
- Siming, K. & M. A. Babar. 2010. Modeling Security for Service Oriented Applications. Proceeding of The 8th European Conference on Software Architecture 13-15 may, Nottingham.
- Weilye, K. & J. Wing. 2005. Game Strategies in Network Security. *International Journal of Information Security* 4 (2): 17-28.
- Yamany, H. & C. Miriam. 2010. Intelligent Security and Access Control Framework for Secure-Oriented architecture. *Information and Software Technology* 25 (2): 220-236.
- Yue, C. & X. Tao. 2012. Web Services Security Problem Insecure-oriented Architecture. International Conference on Applied Physics and Industrial Engineering 15-18 Jan. Washington.

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

Identification and study of the relationship between factors and dimensions affecting the security of developed information systems using service-oriented architecture

Mohammad Reza taghva¹ | Mandana Izadi²

1. Assistant Professor; Allameh Tabatabaee University; Tehran, Iran taghva@yahoo.com
2. MSc in information technology management, university of Allameh Tabatabaee, Tehran, Iran m_izadi85@yahoo.com

Iranian Journal of
**Information
Processing &
Management**

Iranian Research Institute
for Science and Technology

ISSN 2251-8223

eISSN 2251-8231

Indexed in SCOPUS, ISC & LISA

Vol.30 | No.1 | pp: 285-305

Autumn 2014

Abstract: Certain advantages of service-oriented architecture have led to the spread of this type of architecture around the world. However, some special features of this type of architecture have led to more compromise between the security in the information system and other information systems. The purpose of this paper is to identify and examine the impact of factors and dimensions of the information security system that has developed by using service-oriented architecture. In this study, the exploratory and confirmatory factor analysis have been used to identify overt and covert variables. Then, a structured equation model and AMOS software have been used. Finally, the effect of each security dimension of security service-oriented architecture was specified by using the structural equation model. The results indicate that network-level security, web services and message-level security have a significant positive impact on service-oriented architecture. The software output is indicative of the fact that the structured model is fit.

Keywords: Information Systems; Web Service Security; Service Oriented Architecture