

بررسی امنیت در سیستم‌های اطلاعاتی توسعه یافته با روش معماری سرویس‌گرا (SOA)

محمد رضا تقوا^۱، ماندانا ایزدی^۲

چکیده: مزایا و ویژگی‌های خاص معماری سرویس‌گرا و گسترش به‌کارگیری این معماری، در عمل مباحث امنیتی مرتبط با SOA را که در پاره‌ای از موارد متفاوت از اصول امنیتی سیستم‌های اطلاعاتی سنتی است، به دنبال دارد. هدف از این نوشتار، بررسی ابعاد مختلف امنیتی و ارائه راهکارهایی برای امنیت در سیستم‌های اطلاعاتی با معماری سرویس‌گرا است. امید است که نتایج این پژوهش بتواند به مدیران IT در برقراری یک سیستم اطلاعاتی ایمن و ایمن‌سازی هر چه بهتر معماری سرویس‌گرا یاری رساند. پژوهش حاضر از دید هدف کاربردی و از دیدگاه روش انجام پژوهش، توصیفی شمرده می‌شود. در این مطالعه بعد از استخراج مهم‌ترین شاخص‌ها، از نمونه آماری در این باره پرسش به‌عمل آمد. پس از گردآوری داده‌ها با کمک آزمون تی، به تجزیه و تحلیل آنها پرداخته شد. سپس با کمک تحلیل سلسله‌مراتبی داده‌ها، مهم‌ترین ابعاد امنیتی و زیر ابعاد مربوط به هر یک، به ترتیب اهمیت اولویت‌بندی شدند.

واژه‌های کلیدی: امنیت وب سرویس، سرویس، معماری سرویس‌گرا.

۱. استادیار دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی، تهران، ایران
۲. کارشناس ارشد رشته مدیریت فناوری اطلاعات، دانشگاه علامه طباطبائی، تهران، ایران

تاریخ دریافت مقاله: ۱۳۹۱/۰۸/۲۰

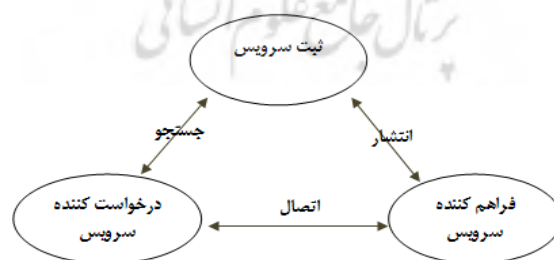
تاریخ پذیرش نهایی مقاله: ۹۲/۰۵/۱۶

نویسنده مسئول مقاله: ماندانا ایزدی

E-mail: m_izadi85@yahoo.com

مقدمه

معماری سرویس‌گرا که امروزه اکثر سازمان‌ها در سراسر جهان آن را پذیرفته‌اند، توانسته است افزون‌بر حل برخی مشکلات، مزایای زیادی را برای سازمان‌ها به همراه داشته باشد؛ اما علاوه بر مزایای بی‌شماری که این معماری به همراه دارد، ویژگی‌های خاص معماری سرویس‌گرا، از جمله باز بودن مرزهای آن، موجب شده تا امنیت این سیستم اطلاعاتی در مقایسه با سایر سیستم‌های اطلاعاتی بیشتر در معرض خطر قرار گیرد. به همین دلیل محافظت از این نوع سیستم‌های اطلاعاتی که یک نوع دارایی سازمان به‌شمار می‌روند، اهمیت بسیاری پیدا می‌کند (ایزدی، ۱۳۸۹). در همین ارتباط، هدف این پژوهش بررسی ابعاد مختلف امنیتی و ارائه راهکارهایی برای برقراری امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا است. معماری سرویس‌گرا دارای ساختار توزیع شده‌ای است و تأکید آن بر تجزیه عملیات کسب‌وکاری پیچیده به اجزایی است که قابل استفاده مجدد باشد و مزایای بیشتری را از استانداردهای فرآیندهای کسب‌وکاری ارائه دهد که این اجزا، همان سرویس‌ها هستند. به گفته‌ای، سرویس‌ها اجزای توزیع شده با رابطه‌ای تعریف شده هستند که پیام‌های XML را پردازش و تبادل می‌کنند. یکپارچگی و تعامل بین سرویس‌ها از طریق فناوری وب سرویس و از طریق استانداردهایی مانند WSDL، SOAP، UDDI انجام می‌شود (Hammar, 2006). مدل پایه SOA از سه جزء اصلی درخواست‌کننده سرویس، فراهم‌کننده سرویس و کشف سرویس تشکیل شده است که ارتباط این سه عامل شامل منتشر کردن، پیدا کردن و متصل شدن به سرویس است. فراهم‌کننده سرویس پیاده‌سازی، از طریق شبکه به ارائه توضیحات آن سرویس برای عامل کشف سرویس می‌پردازد. درخواست‌کننده معمولاً درخواست پیدا کردن سرویس را به عامل کشف سرویس می‌دهد تا از طریق آن به توضیحات ارائه شده سرویس و محل آن دسترسی پیدا کند. سپس با به‌کارگیری این اطلاعات به فراهم‌کننده سرویس، متصل شده و از سرویس ارائه شده استفاده می‌کند (Chodavarapu & Kanneganti, 2007).



نمودار ۱. مدل پایه معماری سرویس‌گرا (Chodavarapu & Kanneganti, 2007)

در واقع این معماری به دلیل ماهیت توزیع‌پذیری، تعامل‌پذیری ذاتی، قابلیت استفاده مجدد، دسترسی باز و ویژگی‌های دیگر، دارای جنبه‌ها و نیازمندی‌های جدید و بیشتری نسبت به روش‌های قبلی است، بنابراین مدل امنیتی SOA باید به گونه‌ای باشد که ضمن حفظ امنیت، موجب شود تا چابکی، انعطاف‌پذیری، استفاده بهتر از سرویس‌ها و امکانات درون‌سازمانی و بین‌سازمانی فراهم شود (Hafner, 2009).

یکی از مسائل دیگری که در امنیت SOA باید مورد توجه قرار گیرد، بازنگه‌داشتن سرویس‌ها و قابلیت تعامل بین آنها است. از آنجا که استفاده از وب سرویس، گسترده‌ترین نگرش پذیرفته‌شده در به‌کارگیری SOA است، به همین دلیل بیشتر جنبه‌های امنیتی در این نوع معماری بر امنیت وب سرویس‌ها متمرکز است (Fareghzadeh, 2009).

مهم‌ترین جنبه‌های امنیتی که باید در معماری سرویس‌گرا به آن توجه شود، شامل: در نظر گرفتن یک سیاست امنیتی جامع، در نظر گرفتن امنیت به‌منزله یک سرویس و مورد توجه قرار دادن عواملی همچون احراز هویت، کنترل دسترسی، تمامیت و محرمانگی پیام، امنیت سطح پیام، امنیت در سطح نقل و انتقال، در دسترس بودن یک سرویس یا یک درخواست، ممیزی به‌معنای بررسی و حسابرسی داده‌ها، فرآیندها، تراکنش‌های انجام شده در سیستم‌های اطلاعاتی، مدیریت کردن امنیت، مدیریت کردن سیاست، مدیریت سیاست امنیتی، نظارت و مدیریت ریسک و عوامل دیگری چون امنیت منابع انسانی، امنیت محیط و امنیت منابع فیزیکی و مانند آن می‌شود (Siming & Babar, 2010; Xiaoming, 2006). در این پژوهش، برای بررسی و استخراج ابعاد مختلف امنیتی و ارائه راهکارهایی برای امنیت این نوع معماری، نخست ادبیات پژوهش مربوط به آن مورد مطالعه قرار گرفت و پس از مصاحبه با خبرگان و استخراج شاخص‌های نهایی، به تهیه پرسش‌نامه، جمع‌آوری و تجزیه و تحلیل داده‌ها پرداخته شد و نتیجه نهایی ارائه شد.

بیان مسئله

مزایای رقابتی معماری سرویس‌گرا سبب رشد روزافزون این معماری، به‌ویژه در دو دهه اخیر در سراسر جهان شده است؛ اما ویژگی خاص معماری سرویس‌گرا، از جمله خاصیت توزیع‌شدگی و باز بودن مرزهای آن موجب شده تا امنیت این معماری با چالش‌هایی همچون نبودن مفهوم پیوستگی، احراز هویت برای سرویس‌های بیرونی، امنیت بین مرزها، امنیت برنامه‌های کاربردی که از ترکیب چندین سرویس تشکیل شده‌اند و ... همراه باشد. گرچه هر ساله تعداد مقاله‌هایی که به جنبه خاصی از امنیت معماری سرویس‌گرا می‌پردازند، در حال افزایش است؛ اما به نظر می‌رسد به دلیل نو پا بودن این نوع معماری و عدم شناخت بسیاری از خبرگان حوزه سیستم‌های

اطلاعاتی و شبکه و چالش‌های موجود در زمینه امنیت معماری سرویس‌گرا، هنوز کتاب‌ها و مقاله‌های چندانی در این زمینه تألیف نشده است. هدف این پژوهش کمک به تصمیم‌گیری بهتر مدیران و مجریانی است که مسئول برقراری امنیت در سیستم‌های اطلاعاتی با معماری سرویس‌گرا هستند. این پژوهش در قالب هفت فرضیه اصلی و سی‌وسه فرضیه فرعی است که فرضیه‌های اصلی به شرح زیر هستند:

فرضیه ۱: امنیت در قسمت طراحی و پیاده‌سازی معماری، می‌تواند به‌منزله یکی از شاخص‌های مؤثر در برقراری امنیت سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا شمرده شود.

فرضیه ۲: امنیت شبکه و وب سرویس، می‌تواند به‌منزله یکی از شاخص‌های مؤثر در برقراری امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا شمرده شود.

فرضیه ۳: امنیت داده، می‌تواند به‌منزله یکی از شاخص‌های مؤثر در برقراری امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا شمرده شود.

فرضیه ۴: امنیت در قسمت مدیریت، می‌تواند به‌منزله یکی از شاخص‌های مؤثر در برقراری امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا شمرده شود.

فرضیه ۵: امنیت در قسمت منابع فیزیکی و محیط، می‌تواند به‌منزله یکی از شاخص‌های مؤثر در برقراری امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا شمرده شود.

فرضیه ۶: امنیت در قسمت منابع انسانی، می‌تواند به‌منزله یکی از شاخص‌های مؤثر در برقراری امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا شمرده شود.

فرضیه ۷: امنیت در قسمت برنامه‌های کاربردی، می‌تواند به‌منزله یکی از شاخص‌های مؤثر در برقراری امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا شمرده شود.

ادبیات نظری پژوهش

معماری سرویس‌گرا، روشی برای ساخت سیستم‌های توزیع شده‌ای است که در آنها عملکرد سیستم، به‌صورت سرویس در اختیار کاربران یا سایر سرویس‌ها قرار می‌گیرد. این نوع معماری به‌دلیل مزایای بی‌شمار خود، امروزه از سوی اکثر سازمان‌ها در سراسر جهان پذیرفته شده است. ویژگی خاص معماری سرویس‌گرا، از جمله باز بودن مرزهای آن، موجب شده است تا امنیت این معماری نسبت به سایر سیستم‌های اطلاعاتی بیشتر در معرض خطر قرار گیرد. در حال حاضر یکی از مشکلات بزرگ در گسترش این معماری، چالش‌های امنیتی موجود در آن است. از دسته مهم‌ترین جنبه‌های امنیتی معماری سرویس‌گرا مواردی است که در زیر اشاره شده است:

سیاست امنیتی: یک سیاست امنیتی، اهداف، محدوده امنیت اطلاعات مطلوب، اهمیت امنیت به‌منزله یک عامل مهم برای توسعه سازمان، پشتیبانی به‌منظور معرفی سیستم‌های امنیتی، اصول اولیه به‌کارگیری امنیت اطلاعات، مسئولیت که مرتبط هستند به معرفی این سیستم‌ها، اسناد و آیین‌نامه‌هایی برای کارمندان در رابطه با سیستم‌های امنیتی را تعریف می‌کند (Ashley, Buecker, 2007).

امنیت به‌منزله یک سرویس: به‌طور کلی در مدل امنیت به‌منزله یک سرویس، منطق امنیت به‌صورت بخشی از یک کاربرد یا بخشی از منطق یک سرویس نیست، بلکه به‌صورت مجزا و متمرکز در یک سرویس امنیتی پیاده‌سازی می‌شود. تمامی تبادلات به‌صورت داده، پیام، درخواست و... نخست تحت کنترل و نظارت این سرویس قرار می‌گیرد (دارا، ۱۳۸۸).

احراز هویت: احراز هویت در شبکه‌های رایانه‌ای، بدین معناست که یک سرویس‌دهنده بتواند تشخیص دهد فرد یا سرویسی که تقاضایی را روی آن سیستم دارد، مجاز است یا نه؟ (دارا، ۱۳۸۸).

کنترل دست‌یابی: کنترل دست‌یابی را می‌توان جلوگیری از استفاده غیرمجاز از منابع دانست. بدین معنا که چه کسی می‌تواند به منبع دسترسی داشته باشد، دست‌یابی تحت چه شرایطی می‌تواند انجام گیرد و کسانی که به منابع دست‌یابی دارند، چه کارهایی می‌توانند انجام دهند (دارا، ۱۳۸۸).

تمامیت و محرمانگی پیام: تمامیت پیام، تضمین می‌کند پیام یا داده‌های دریافتی، به‌طور دقیق همان چیزی است که از جانب نهاد مجاز ارسال شده است و فاقد هرگونه تغییر، درج، حذف یا تکرار است.

محرمانگی را می‌توان به‌معنای حفاظت اطلاعات از افشاگری غیر مجاز دانست. به‌گفته‌ای اطلاعات فقط باید برای افراد مجاز در دسترس باشد که معمولاً در دو سطح پیام و نقل و انتقالات به‌کار برده می‌شود (دارا، ۱۳۸۸).

در دسترس بودن: در دسترس بودن یک سرویس یا درخواست، نشان‌دهنده این است که آن سرویس قادر است پاسخ به یک سرویس را به‌موقع فراهم کند و اطمینان می‌دهد که سرویس‌ها، زمانی که درخواست در بسیاری از محیط‌های SOA کلیدی است، در دسترس هستند (دارا، ۱۳۸۸).

امنیت در سطح پیام: برای امنیت در سطح پیام، می‌توان از مسیریابی پیام‌ها استفاده کرد؛ یعنی پیام‌ها به‌سمت نقاط انتهایی معتبری که مد نظر است، هدایت می‌شوند. برای مثال، پیام

در صورتی به سمت سرویس A هدایت می‌شود که درخواست‌کننده، ویژگی‌های X و Y را داشته باشد. یک دیدگاه دیگر اینست که بخش‌های مختلف یک پیام، می‌توانند به‌طور مجزا محافظت شوند تا در مسیر پیام، تنها توسط بخش‌هایی که مورد نظر است، قابل استفاده باشد (دارا، ۱۳۸۸).

امنیت در سطح نقل و انتقالات: برای امنیت در سطح نقل و انتقالات از SSL/TLS برای مخفی کردن شبکه‌های ارتباطی از اده مشتریان سرویس استفمی‌شود. کاربردها به کمک SSL/TLS کانال‌های ایمنی را برای تبادل داده‌ها برقرار می‌کنند (دارا، ۱۳۸۸).

ممیزی: ممیزی به معنای بررسی و حسابرسی داده‌ها، فرآیندها، تراکنش‌های انجام شده در سیستم‌های اطلاعاتی است که به منظور برآورده شدن ملزومات امنیتی انجام می‌گیرد (Ashley & Buecker, 2007).

مدیریت امنیت: مدیریت امنیت، مدیریت تمامی مراحل و راهکارهای امنیتی از ایجاد و تأمین امنیت، محافظت و نگهداری، کنترل و بازرسی امنیت و... را شامل می‌شود (دارا، ۱۳۸۸).

مدیریت سیاست: اهدافی که به‌وسیله کسب‌وکار ایجاد شده و به حرکت درآمده‌اند، اکنون باید به‌وسیله زیرساخت‌ها اجرا شوند. مدیریت سیاست یک چارچوبی را برای اجرا کردن سیاست فراهم می‌کند (Ashley & Buecker, 2007).

مدیریت سیاست امنیتی: مدیریت سیاست‌های امنیتی با معرفی سیاست‌های کسب‌وکاری و با معرفی سیاست‌های خاص سرویس، مانند امنیت، شاخص‌های عملکرد، سیاست‌های مطمئن و... آغاز می‌شود. این سیاست‌ها به‌وسیله زیرساخت‌ها برای امنیت دسترسی به اطلاعات، فراهم کردن دسترسی، نگهداری، توانایی ممیزی و مانند آنها اداره می‌شود (Ashley & Buecker, 2007).

ادبیات تجربی پژوهش

در زمینه امنیت اطلاعات در معماری سرویس‌گرا، پژوهش‌های متعددی انجام شده است، از آن دسته می‌توان به دسترسی چارچوب کنترل امنیت هوشمند و معماری سرویس‌گرا (Yamany & Miriam, 2010)، مشکلات سرویس‌دهی وب در طراحی معماری سرویس‌گرا (Yue & Tao, 2012)، معماری سرویس‌گرا برای امنیت سیستم شبکه همراه (Rosado & Eduardo, 2011)، امنیت و کاربرد آن در برنامه‌های معماری سرویس‌گرا (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 هیچکدام با یک دید کلی و یک رویکرد سیستمی به بررسی این موضوع نپرداخته‌اند.

الیمنی و همکاران (۲۰۱۰) در پژوهشی با عنوان «دسترسی چارچوب کنترل امنیت هوشمند و معماری سرویس‌گرا»، بیان کردند یکی از مشکلات بزرگ گسترش معماری سیستم‌گرا چالش‌های امنیتی موجود در آن است؛ چراکه مسئولیت امنیت SOA به هر دو گروه ارائه‌دهندگان و مصرف‌کنندگان، وابسته است. آنان معتقدند در سال‌های اخیر، تلاش‌های زیادی برای رفع این نواقص انجام شده است که از آن دسته، دسترسی به استانداردهای امنیتی شبکه وب که شامل WS-Security و WS-Policy، بوده است. در این پژوهش یک چارچوب هوشمند امنیتی پیشنهاد شده است که شامل دو عامل مهم در زمینه دستیابی به امنیت است: ۱. احراز هویت و امنیت خدمات (NSS) و ۲. سرویس 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 سیستم خودکار را فراهم می‌کند (Yamany & Miriam, 2010).

یو و تائو (۲۰۱۲) در پژوهشی با عنوان «مشکلات سرویس‌دهی وب در طراحی معماری سرویس‌گرا» بیان کرده‌اند که با توسعه جهانی استفاده از فناوری SOA، مسائل امنیتی خدمات تارنما (وب‌سایت) که بر اساس پلت‌فرم ناهمگون شکل گرفته‌اند، به‌طور فزاینده‌ای برجسته و مهم خواهد شد. در این پژوهش دو راهکار امنیتی برای خدمات سرویس‌دهی ارائه شده است (Yue & Tao, 2012).

روسادو و همکاران (۲۰۱۱) در مطالعه‌ای با موضوع معماری سرویس‌گرا برای امنیت سیستم شبکه همراه بیان کردند که امنیت در سیستم‌های شبکه همراه، بسیار ضروری است؛ در حالی که تأمین امنیت این سیستم‌ها به‌دلیل کمبود منابع در این دستگاه‌ها، سخت و پیچیده است. در این پژوهش برای حفظ امنیت این سیستم‌ها، از مدلی بر اساس طراحی معماری سرویس‌گرا 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).

زو و همکاران در سال ۲۰۱۰ در پژوهشی با عنوان «امنیت و کاربرد در برنامه‌های معماری سرویس‌گرا؛ موضوعات تجارتي»، معتقدند با پیشرفت کاربرد محاسبات و طراحی معماری سرویس‌گرا 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، به‌وسیله طراحی معماری سرویس‌گرا تعدیل خواهند شد و تنها مشکل موجود، تأمین امنیت کاربری این برنامه‌ها و شبکه‌ها است. 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).

روش پژوهش

این پژوهش از دید هدف کاربردی و از نظر روش‌شناسی، توصیفی شمرده می‌شود. این پژوهش در چارچوب هفت فرضیه اصلی و سی‌وسه فرضیه فرعی، به بررسی ابعاد مختلف امنیتی و زیرابعاد مربوط به آنها پرداخته است. بُعد امنیتی اول (امنیت در پیاده‌سازی و طراحی معماری سرویس)، بُعد امنیتی دوم (امنیت سطح شبکه و وب)، بُعد امنیتی سوم (امنیت در سطح داده)، بُعد امنیتی چهارم (امنیت در بخش مدیریت سیستم اطلاعاتی)، بُعد امنیتی پنجم (امنیت در بخش منابع فیزیکی و محیط)، بُعد امنیتی ششم (امنیت منابع انسانی)، بُعد امنیتی هفتم (امنیت برنامه‌های کاربردی) است. هر یک از این ابعاد امنیتی نیز خود دارای زیر ابعادی هستند.

جدول ۱. نتایج پایایی هر یک از ابعاد امنیتی

محاسبه آلفای کرونباخ برای هر بُعد امنیتی	تعداد سؤال‌های مربوط به هر فرضیه	فرضیه‌ها
۰/۷۱۲	۲	فرضیه ۱- بُعد امنیتی اول (امنیت در پیاده سازی و طراحی معماری سرویس‌گرا) (Heather, 2005)
۰/۷۳۲	۷	فرضیه ۲- بُعد امنیتی دوم (امنیت سطح شبکه و وب) (Ashley & Buecker, 2007)
۰/۷۶۶	۸	فرضیه ۳- بُعد امنیتی سوم (امنیت داده) (Jonnaganti, 2009)
۰/۸۱۲	۳	فرضیه ۴- بُعد امنیتی چهارم (امنیت در قسمت مدیریت) (دارا، ۱۳۸۸)
۰/۸۲۱	۲	فرضیه ۵- بُعد امنیتی پنجم (امنیت منابع فیزیکی) (Ashley & Buecker, 2007)
۰/۸۱۲	۳	فرضیه ۶- بُعد امنیتی ششم (امنیت منابع انسانی) (Jonnaganti, 2009)
۰/۷۴۲	۸	فرضیه ۷- بُعد امنیتی هفتم (امنیت منابع کاربردی) (Ashley & Buecker, 2007)

روش محاسبه جامعه آماری و نمونه‌گیری

جامعه آماری در نظر گرفته شده در این پژوهش، شامل تمامی خبرگانی می‌شود که در سطح شهر تهران در زمینه امنیت سیستم‌های اطلاعاتی که بر پایه معماری سرویس‌گرا پایه‌ریزی شده، مشغول فعالیت بوده یا دست‌کم سه سال سابقه کار در زمینه امنیت سیستم‌های اطلاعاتی و امنیت شبکه را داشته و از دانش کافی در مورد معماری سرویس‌گرا برخوردار باشند. از آنجا که تعداد افرادی که در این زمینه مشغول فعالیت هستند، بسیار محدود و پراکنده است و اندازه دقیق جامعه آماری در دسترس نبود، بر اساس بررسی انجام گرفته و شناسایی خبرگان و کارشناسان این حوزه، نمونه‌گیری به صورت قضاوتی انجام گرفت و از حدود ۴۷ پرسش‌نامه توزیع شده، ۴۰ پرسش‌نامه دریافت شد که مشخصات پاسخ‌دهندگان در جدول شماره ۱ آورده شده است.

جدول ۲. مشخصات خبرگان

ردیف	سمت	نوع تخصص	تعداد	تحصیلات	تجربه
۱	مدیر فناوری اطلاعات	امنیت اطلاعات و شبکه، فناوری اطلاعات	۳	کارشناس و کارشناس ارشد (سخت‌افزار، نرم‌افزار، مهندسی فناوری اطلاعات)	۳ سال به بالا
۲	مدیر امنیت شبکه و اطلاعات	امنیت اطلاعات و شبکه، فناوری اطلاعات	۱۲	کارشناس و کارشناس ارشد (سخت‌افزار، نرم‌افزار، مهندسی فناوری اطلاعات)	۳ سال به بالا
۳	کارشناس ارشد امنیت شبکه	امنیت اطلاعات و شبکه، فناوری اطلاعات	۴	کارشناس و کارشناس ارشد (سخت‌افزار، نرم‌افزار، مهندسی فناوری اطلاعات)	۳ سال به بالا
۴	کارشناس سیستم مدیریت امنیت اطلاعات	امنیت اطلاعات و شبکه، فناوری اطلاعات	۶	کارشناس و کارشناس ارشد (سخت‌افزار، نرم‌افزار، مهندسی فناوری اطلاعات)	۳ سال به بالا
۵	کارشناس امنیت شبکه و نرم‌افزار	امنیت اطلاعات و شبکه، فناوری اطلاعات	۱۴	کارشناس و کارشناس ارشد (سخت‌افزار، نرم‌افزار، مهندسی فناوری اطلاعات)	۳ سال به بالا
۶	کارشناس ارتباطات شبکه	امنیت اطلاعات و شبکه، فناوری اطلاعات	۱	کارشناس و کارشناس ارشد (سخت‌افزار، نرم‌افزار، مهندسی فناوری اطلاعات)	۳ سال به بالا

ابزار و روش گردآوری داده‌ها

روش گردآوری اطلاعات نیز با استفاده از دو شیوه کتابخانه‌ای و استفاده از پرسش‌نامه انجام گرفته است. روایی پژوهش از طریق مطالعه مبانی نظری و با استفاده از نظر استادان و متخصصان در این زمینه لحاظ شد و پایایی ابزار پژوهش از طریق آزمون ضریب آلفای کرونباخ محاسبه شد که مقدار آن برابر با ۰/۹۳۵ به دست آمد. برای پاسخ‌دهی به سؤال‌های پژوهش و تحلیل داده‌ها از روش‌های آماری استفاده شد. با توجه به اینکه جامعه پژوهش حاضر نرمال و تعداد نمونه آن بیش از ۳۰ نفر بود، داده‌های جمع‌آوری شده از طریق پرسش‌نامه به صورت استنباطی و با استفاده از آزمون تی - استیودنت مورد تجزیه و تحلیل قرار گرفت. با توجه به اینکه

در پرسش‌نامه از مقیاس لیکرت پنج‌گزینه‌ای استفاده شده است و میانگین این مقیاس ۳ محاسبه شد، بنابراین میانگین جامعه مورد نظر در تحلیل‌ها نیز رقم ۳ در نظر گرفته شده است و آزمون‌های فرض آماری نیز به صورت رابطه شماره ۱ و ۲ در نظر گرفته شده است که ادعای ما در فرض H_1 قرار می‌گیرد

$$H_0: \mu \leq 3 \quad \text{رابطه (۱)}$$

$$H_1: \mu \geq 3 \quad \text{رابطه (۲)}$$

سپس برای وزن‌دهی و اولویت‌بندی کردن مهم‌ترین شاخص‌ها و زیر شاخص‌های مربوط به آنها، با استفاده از روش‌های تصمیم‌گیری چند متغیره برای اولویت‌بندی کردن بر اساس اهمیت و وزن‌دهی به هر یک از شاخص‌ها استفاده شده است.

یافته‌های پژوهش

نتایج و یافته‌های حاصل از تجزیه و تحلیل فرضیه‌ها با کمک آزمون t در سطح $\alpha = 0.05$ به شرح زیر است:

جدول ۳. نتایج تجزیه و تحلیل داده‌های مربوط به ابعاد امنیتی و زیرشاخص‌های آنها

نتیجه‌گیری	مقدار آماره آزمون تی.	شاخص‌های اصلی
رد فرض صفر	۶/۴۸۹	فرضیه ۱
رد فرض صفر	۱۲/۹۳۰	فرضیه ۲
رد فرض صفر	۱۴/۴۱۶	فرضیه ۳
رد فرض صفر	۱۲/۳۲۴	فرضیه ۴
نتیجه‌گیری	مقدار آماره آزمون تی.	زیرشاخص‌های امنیت داده
رد فرض صفر	۱۸/۰۲۸	محرمانگی (Jonnaganti, 2009)
رد فرض صفر	۷/۷۰۶	جامعیت (Jonnaganti, 2009)
رد فرض صفر	۸/۴۷۳	دسترس پذیری (Jonnaganti, 2009)
رد فرض صفر	۶/۶۸۴	احراز هویت (Jonnaganti, 2009)
نتیجه‌گیری	مقدار آماره آزمون تی.	شاخص‌های اصلی
رد فرض صفر	۷/۸۲۹	فرضیه ۵
رد فرض صفر	۱۲/۷۴۵	فرضیه ۶
رد فرض صفر	۱۴/۴۹۳	فرضیه ۷
نتیجه‌گیری	مقدار آماره آزمون تی.	زیرشاخص‌های معماری
رد فرض صفر	۶/۴۰۷	امنیت به‌منزله یک سرویس (Heather, 2005)
رد فرض صفر	۵/۴۵۴	ESB & gateway (Heather, 2005)

ادامه جدول ۳. نتایج تجزیه و تحلیل داده‌های مربوط به ابعاد امنیتی و زیرشاخص‌های آنها

نتیجه‌گیری	مقدار آماره آزمون تی.	زیرشاخص‌های بخش مدیریت
رد فرض صفر	۱۷/۷۱۶	مدیریت سیاست امنیتی (دارا، ۱۳۸۸)
رد فرض صفر	۱۹/۰۷۱	مدیریت ریسک (دارا، ۱۳۸۸)
رد فرض صفر	۱۷/۷۱۶	مدیریت سیاست (دارا، ۱۳۸۸)
نتیجه‌گیری	مقدار آماره آزمون تی.	زیرشاخص‌های امنیت داده
رد فرض صفر	۴/۵۵۵	تعیین سطح دسترسی (Heather, 2005)
رد فرض صفر	۸/۵۴۰	تشخیص و شناسایی (Heather, 2005)
رد فرض صفر	۱۰/۹۸۱	امنیت نقل و انتقال (Heather, 2005)
رد فرض صفر	۱۲/۴۹۰	سیاست امنیتی (Heather, 2005)
نتیجه‌گیری	مقدار آماره آزمون تی.	زیرشاخص‌های منابع فیزیکی
رد فرض صفر	۹/۹۵۱	تجهیزات (Ashley & Buecker, 2007)
رد فرض صفر	۵/۵۳۰	بازبینی‌های عمومی (Ashley & Buecker, 2007)
نتیجه‌گیری	مقدار آماره آزمون تی.	زیرشاخص‌های منابع انسانی
رد فرض صفر	۱۷/۷۱۶	تحصیل (Jonnaganti, 2009)
رد فرض صفر	۵/۷۳۰	آموزش (Jonnaganti, 2009)
رد فرض صفر	۱۷/۷۱۶	آگاهی (Jonnaganti, 2009)
نتیجه‌گیری	مقدار آماره آزمون تی.	زیرشاخص‌های برنامه‌های کاربردی
رد فرض صفر	۱۹/۰۷۱	محرمانگی (Jonnaganti, 2009)
رد فرض صفر	۵/۴۱۴	جامعیت (Jonnaganti, 2009)
رد فرض صفر	۹/۸۰۲	دسترس پذیری (Jonnaganti, 2009)
رد فرض صفر	۱۰/۳۵۶	احراز هویت (Jonnaganti, 2009)
رد فرض صفر	۲/۹۳۳	تشخیص و شناسایی (Jonnaganti, 2009)
رد فرض صفر	۹/۰۶۷	ممیزی و نظارت (Jonnaganti, 2009)
رد فرض صفر	۱۷/۷۱۶	سیاست امنیتی (Jonnaganti, 2009)
رد فرض صفر	۸/۲۰۴	تعیین سطح اختیار (Jonnaganti, 2009)
نتیجه‌گیری	مقدار آماره آزمون تی.	زیرشاخص‌های شبکه
رد فرض صفر	۲/۹۳۳	ایزولاسیون (Ashley & Buecker, 2007)
رد فرض صفر	۸/۴۷۳	کنترل ترافیک (Ashley & Buecker, 2007)
رد فرض صفر	۱۰/۳۵۶	امنیت IP (Ashley & Buecker, 2007)
رد فرض صفر	۵/۴۵۴	محکم کردن پایه‌های امنیتی اجزا (Jonnaganti, 2009)
تأیید فرض صفر	۰/۶۴۹	مدیریت رویدادها (Ashley & Buecker, 2007)
رد فرض صفر	۱۰/۸۹۱	حفاظت در مقابل حمله‌ها (Jonnaganti, 2009)
رد فرض صفر	۱۰/۳۵۶	کشف و جلوگیری از تجاوز (Jonnaganti, 2009)
رد فرض صفر	۵/۸۴۹	امنیت نقل و انتقال (Jonnaganti, 2009)

جدول ۴. نتایج تجزیه و تحلیل راهکارهای امنیتی

نتیجه گیری	مقدار آماره آزمون تی.	راهکارهای امنیت شبکه
رد فرض صفر	۹/۸۷۴	استفاده از فایروال
رد فرض صفر	۸/۸۶۸	ارزیابی آسیب‌ها
رد فرض صفر	۱۳/۸۰	سیاست‌های امنیتی
رد فرض صفر	۸/۸۶۸	پروکسی
نتیجه گیری	مقدار آماره آزمون تی.	راهکارهای امنیت پیام
رد فرض صفر	۸/۸۴۷	WS-security
رد فرض صفر	۱۰/۲۳۲	مسیریابی پیام‌ها
رد فرض صفر	۱۱/۷۷۷	حفاظت از بخش‌های مختلف پیام
نتیجه گیری	مقدار آماره آزمون تی.	راهکارهای امنیت منابع انسانی
رد فرض صفر	۷/۳۴۱	تحصیل
رد فرض صفر	۵/۲۷۹	آموزش
رد فرض صفر	۲۰/۱۵۶	آگاهی
نتیجه گیری	مقدار آماره آزمون تی.	راهکارهای سیاست‌های امنیتی
رد فرض صفر	۱۷/۸۳	WS-security policy
رد فرض صفر	۵/۱۱۱	استفاده از تجرید یا انتزاع در طراحی سیاست‌ها
نتیجه گیری	مقدار آماره آزمون تی.	راهکارهای سطح دسترسی
رد فرض صفر	۹/۰۹۸	دسته‌بندی کاربرد، دیتابیس
رد فرض صفر	۳/۳۲۳	تکنیر سرویس‌ها
نتیجه گیری	مقدار آماره آزمون تی.	راهکارهای احراز هویت
رد فرض صفر	۷/۰۵۴	استفاده از شناسه کاربری
رد فرض صفر	۷/۲۷۴	رمزنگاری با کلید عمومی و خصوصی
رد فرض صفر	۴/۵۲۶	سرویس‌دهنده راهنما
رد فرض صفر	۱۴/۸۶۴	توکن‌های امنیتی
نتیجه گیری	مقدار آماره آزمون تی.	راهکارهای نقل و انتقال
رد فرض صفر	۶/۸۲۹	Ws-reliable messaging
رد فرض صفر	۶/۵۲۵	S-HTTP , SSL/TLS

برای تعیین میزان اهمیت و تأثیری که هریک از این ابعاد و زیر ابعاد مربوط به آنها در برقراری امنیت در سیستم‌های اطلاعاتی سرویس‌گرا دارند، از نظر خبرگان مقایسات زوجی انجام گرفت و با کمک نرم‌افزار expert choice اوزان مربوط به هریک محاسبه شد. سپس با کمک تحلیل سلسله‌مراتبی داده‌ها، هر یک از ابعاد و زیر ابعاد مربوط به آن، بر اساس اهمیت به‌ترتیب زیر اولویت‌بندی شدند.

جدول ۵. اولویت‌بندی ابعاد امنیتی و زیر ابعاد مرتبط با آنها با کمک روش AHP

ردیف	۱	۲	۳	۴	۵	۶	۷
معیارهای اصلی SOA	امنیت داده	امنیت شبکه و وب	امنیت در مدیریت	منابع فیزیکی	امنیت در منابع انسانی	امنیت معماری	برنامه‌های کاربردی
وزن نهایی	۰.۳۲۰	۰.۱۲۰	۰.۱۶۶	۰.۱۶۸	۰.۰۵۸	۰.۲۲۷	۰.۰۹۷
اولویت	۱	۵	۳	۶	۷	۸	۳
زیر شاخص‌های امنیت شبکه و وب	ابزار/لاسنون	کنترل ترافیک بین شبکه	محکم کردن پادهای امنیتی اجزا	امنیت IP	کنشف و جلوگیری از تجاوز	حفاظت در مقابل حمله‌ها	امنیت نقل و انتقال
وزن نهایی	۰.۳۶۶	۰.۲۰۴	۰.۲۹۷	۰.۱۹۳	۰.۱۱۱	۰.۱۰۷	۰.۱۳۳
اولویت	۲	۳	۱	۴	۶	۷	۵
زیر شاخص‌های امنیت داده	محرمانگی	جامعیت	پروسی هویت	سلاج دسترسی	تشخیص و شناسایی	امنیت انتقال	سیاست امنیتی
وزن نهایی	۰.۳۲۲	۰.۱۷۳	۰.۱۶۸	۰.۰۷۴	۰.۱۷۳	۰.۰۵۴	۰.۰۸۱
اولویت	۱	۲	۷	۵	۶	۸	۳
امنیت برنامه‌های کاربردی	محرمانگی	جامعیت	پروسی هویت	سلاج دسترسی	تشخیص و شناسایی	سیاست امنیتی	معماری و نظارت
وزن نهایی	۰.۳۰۱	۰.۱۴۵	۰.۱۳۲	۰.۰۹	۰.۱۶۸	۰.۰۷۵	۰.۰۳
اولویت	۱	۳	۴	۵	۷	۶	۸
مديریت در سطح مدیریت	امنیت در سطح مدیریت	مديریت میاست	مديریت ریسک	مديریت امنیت	مديریت میاست امنیتی	مديریت میاست امنیتی	مديریت میاست امنیتی
وزن نهایی	۰.۵۳۳	۰.۵۳۳	۰.۵۳۳	۰.۵۳۳	۰.۵۳۳	۰.۵۳۳	۰.۵۳۳
اولویت	۱	۱	۲	۲	۲	۲	۳
امنیت منابع فیزیکی	امنیت منابع فیزیکی	تجهیزات	کنترل عمومی	کنترل عمومی	کنترل عمومی	کنترل عمومی	کنترل عمومی
وزن نهایی	۰.۸۳۳	۰.۸۳۳	۰.۸۳۳	۰.۸۳۳	۰.۸۳۳	۰.۸۳۳	۰.۸۳۳
وزن نهایی	۱	۱	۱	۱	۱	۱	۱
زیر شاخص‌های معماری	زیر شاخص‌های معماری	FSB	FSB	FSB	FSB	FSB	FSB
وزن نهایی	۰.۱۳۹	۰.۱۳۹	۰.۱۳۹	۰.۱۳۹	۰.۱۳۹	۰.۱۳۹	۰.۱۳۹
اولویت	۲	۲	۲	۲	۲	۲	۲

همان‌طور که مشاهده می‌شود، در سطح ابعاد امنیتی، بیشترین اوزان به امنیت سطح داده و امنیت در طراحی معماری و کمترین اوزان به امنیت منابع انسانی اختصاص یافته است. بنابراین می‌توان نتیجه گرفت که امنیت سطح داده، بالاترین اهمیت و بیشترین تأثیر را در برقراری امنیت SOA دارد. در سطح زیر ابعاد مربوط به امنیت شبکه و وب، محکم کردن پایه‌های امنیتی اجزا، مجزا کردن فضای آدرس از فرآیندهای دیگر بیشترین میزان تأثیر را در برقراری امنیت شبکه داشته‌اند و کنترل ترافیک بین شبکه، امنیت IP، امنیت نقل و انتقال، کشف و جلوگیری از تجاوز و حفاظت در مقابل حمله‌ها، به ترتیب در اولویت‌های بعدی قرار دارند.

در اولویت‌بندی زیر ابعاد مربوط به امنیت داده، محرمانگی، تمامیت، دسترس‌پذیری بالاترین تأثیر؛ در بخش امنیت برنامه‌های کاربردی، محرمانگی، دسترس‌پذیری؛ در قسمت پیاده‌سازی معماری، پروکسی؛ در برقراری امنیت در سطح مدیریت، مدیریت سیاست؛ در امنیت منابع انسانی، آموزش و در قسمت امنیت منابع فیزیکی، تجهیزات بیشترین تأثیر را در برقراری امنیت معماری سرویس‌گرا دارند.

در یک جمع‌بندی کلی از نتایج حاصل از داده‌های پژوهش، راهکارهای امنیتی SOA را می‌توان به دو دسته کلی تقسیم کرد. این نتایج به‌طور خلاصه در جداول شماره ۶ و ۷ نشان داده شده است.

جدول ۶. راهکارهای امنیتی مشابه با سایر سیستم‌های اطلاعاتی

امنیت در بخش انسانی	تحصیل (Jonnaganti, 2009)
	آموزش (Jonnaganti, 2009)
	آگاهی (Jonnaganti, 2009)
امنیت سیاست‌های امنیتی	استفاده از استاندارد WS-security policy (Ashley & Buecker, 2007)
	استفاده از تجرید یا انتزاع در طراحی سیاست‌ها (Ashley & Buecker, 2007)
امنیت در سطح نقل و انتقال	استفاده از استاندارد WS-addressing (Ashley & Buecker, 2007)
	استفاده از استاندارد WS-reliable messaging (Ashley & Buecker, 2007)
	استفاده از پروتکل S-HTTP, SSL/TLS (Ashley & Buecker, 2007)
امنیت برای احراز هویت	استفاده از شناسه کاربری، کلمه عبور، اثر انگشت (Ashley & Buecker, 2007)
	اصول رمزنگاری با کلید عمومی و خصوصی (Ashley & Buecker, 2007)
	استفاده از سرویس‌دهنده راهنما (Ashley & Buecker, 2007)
	استفاده از توکن‌های امنیتی (Ashley & Buecker, 2007)

ادامه جدول ۶. راهکارهای امنیتی مشابه با سایر سیستم‌های اطلاعاتی

تعیین سطح دسترسی	دسته‌بندی کردن کاربردها، دیتابیس‌ها و روش‌های مشابه (Ashley & Buecker, 2007)
	استفاده از تکثیر سرویس‌ها (Ashley & Buecker, 2007)
جامعیت	استفاده از امضای دیجیتالی (Jonnaganti, 2009)
	استفاده از پروتکل نقل و انتقال SSL/TLS (Ashley & Buecker, 2007)
محرمانگی	استفاده از استاندارد XML encryption (Ashley & Buecker, 2007)
	استفاده از تکنیک‌های رمزگذاری (Jonnaganti, 2009)
	استفاده از پروتکل نقل و انتقال SSL/TLS (Ashley & Buecker, 2007)
امنیت شبکه	امنیت IP (Weily & Wing, 2005)
	فایروال‌های سخت‌افزار (Menzel, 2007)
	ارزیابی آسیب‌ها (اسکن منظم سیستم‌های شبکه و زیرساختار) (Ashley & Buecker, 2007)
	سیاست‌های امنیتی ورود کاربر (Ashley & Buecker, 2007)
	پروکسی (Ashley & Buecker, 2007)
	سیستم‌های کشف وضعیت‌های نامطلوب (ADS) (Ashley & Buecker, 2007)
	سیاست‌های ایزولاسیون شبکه‌ها (Ashley & Buecker, 2007)

جدول ۷. راهکارهای امنیتی مختص SOA

امنیت در بخش طراحی و پیاده سازی	استفاده از پروکسی، برای اداره کردن امنیت HTTP/S و برای مجزا کردن تماس میان فراهم کننده و مشتری سرویس (Menzel, 2007)
	استفاده از گیت وی برای اداره کردن امنیت XML (Menzel, 2007)
	استفاده از گذرگاه سرویس سازمانی برای اجرای کنترل‌های امنیتی (Menzel, 2007)
برقراری امنیت بین مرزهای سازمانی	استفاده از پروکسی برای کنترل کردن امنیت درخواست‌های مبتنی بر پروتکل نقل و انتقال HTTP (Menzel, 2007) استفاده از گیت وی برای بررسی و کنترل درخواست‌های SOAP (Menzel, 2007) مدیریت کردن سیاست‌های معتبر و هویت‌های یکپارچه شده بین مرزهای سازمان (Menzel, 2007)
امنیت سرویس‌های ترکیبی	استفاده از یک سیاست امنیتی مجزا برای سرویس‌های ترکیب شده (Afshar & Kavantzaz, 2006)
	مدیریت کردن سیاست‌های معتبر و هویت‌های یکپارچه شده بین مرزهای سازمان (Afshar & Kavantzaz, 2006)
امنیت در سطح پیام	حفاظت از بخش‌های مختلف پیام، به گونه‌ای که در مسیر پیام تنها بخش‌هایی که مورد نظر است، قابل استفاده باشد (Afshar & Kavantzaz, 2006)
	استفاده از استاندارد WS-security (Menzel, 2007)

نتیجه گیری و پیشنهادها

برای برقراری امنیت در هر سیستم اطلاعاتی، مدیران و دست‌اندرکاران برقراری امنیت، باید ابعاد و جنبه‌های مختلف امنیتی را مورد توجه قرار دهند، به گونه‌ای که در ایجاد یک سیستم اطلاعاتی ایمن به آنها کمک کند. در یک مقایسه کلی، تفاوت نتایج این پژوهش با پژوهش‌های پیشین در این است که با رویکردی متفاوت به مقوله امنیت در سیستم‌های اطلاعاتی با معماری سرویس‌گرا نگریده شده است. این پژوهش برخلاف اکثر پژوهش‌ها، به جای بررسی امنیت از یک جنبه خاص و با یک رویکرد فنی، از دید سیستمی و مدیریتی به بررسی تمامی ابعاد و جنبه‌های امنیتی مورد نیاز یک مدیر IT که برای برقراری امنیت در یک سیستم اطلاعاتی سرویس‌گرا باید مورد توجه قرار دهد با در نظر گرفتن میزان اهمیت و تأثیر هر یک، پرداخته شده است. در این پژوهش هفت بُعد مختلف امنیتی در یک سیستم اطلاعاتی سرویس‌گرا مورد بررسی قرار گرفته است. با توجه به اینکه تمام فرضیه‌های این پژوهش در سطح اطمینان ۹۵ درصد مورد تأیید قرار گرفتند، می‌توان ادعا کرد که برقراری امنیت در سطح مدیریت، امنیت در سطح معماری، امنیت در سطح شبکه و وب سرویس، امنیت در سطح برنامه‌های کاربردی، امنیت در سطح منابع فیزیکی و محیط، امنیت در سطح منابع انسانی و امنیت در سطح داده، می‌توانند به منزله ابعاد (شاخص‌های) اصلی چارچوب امنیتی مورد استفاده قرار گیرند. در ادامه برای بهبود در برقراری امنیت در سیستم‌های اطلاعاتی سرویس‌گرا، راهکارهایی ارائه شده است که این راهکارها را می‌توان به دو دسته کلی تقسیم کرد.

دسته اول راهکارهایی است که مشابه راهکارهای امنیتی در سایر سیستم‌های اطلاعاتی است، مانند استفاده از اصول رمزنگاری در قسمت احراز هویت یا تکثیر سرویس‌ها برای افزایش سطح دسترسی.

دسته دوم راهکارهای امنیتی هستند که بیشتر به معماری سرویس‌گرا اختصاص دارند، مانند استفاده از گذرگاه سرویس‌سازمانی برای اجرای کنترل‌های امنیتی در قسمت طراحی معماری، استفاده از WS-security برای امنیت سطح پیام و مانند آنها. انتظار ما بر این است که این ابعاد امنیتی و راهکارهای ارائه شده، تا اندازه‌ای به تصمیم‌گیری بهتر مدیران و مجریانی مسئول برقراری امنیت در سیستم‌های اطلاعاتی با معماری سرویس‌گرا کمک کند و بتواند امنیت را در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا تا حد زیادی برقرار کند.

با توجه به ویژگی خاص معماری سرویس‌گرا از جمله سیستم‌های توزیع شده، داشتن مرزهای باز و تعامل با سرویس‌های بیرونی، به تمامی مدیرانی که در این حوزه مشغول فعالیت هستند پیشنهاد می‌شود:

۱. در هنگام تدوین سیاست‌های امنیتی، به‌ویژه سیاست‌های امنیتی مربوط به کنترل دسترسی و سیاست‌های مربوط به سرویس‌های ترکیبی که گاهی از ترکیب سرویس‌های بیرونی و درونی تشکیل یافته‌اند، دقت و توجه کافی داشته باشند.
۲. نسبت به استفاده از روش‌هایی که موجب بالا بردن امنیت در استانداردهای وب (همچون WSDL, UDDI, SOAP) می‌شود، توجه کافی داشته باشند. همچنین علاوه بر کنترل دسترسی با استفاده از فهرست راهنما، روش‌های دیگر کنترل دسترسی (مانند مدل کنترل دسترسی مبتنی بر رول) را مد نظر قرار دهند.

منابع

- ایزدی، م. (۱۳۸۹). *امنیت در سیستم‌های اطلاعاتی توسعه یافته با روش معماری سرویس‌گرا*. پایان‌نامه کارشناسی ارشد رشته مدیریت فناوری اطلاعات، دانشکده مدیریت، دانشگاه علامه طباطبایی.
- دارا، ع. (۱۳۸۸). *معماری سرویس‌گرا با بررسی دیدگاه‌های امنیتی آن*، سمینار کارشناسی ارشد. دانشگاه آزاد اسلامی واحد علوم و تحقیقات.
- Afshar, M., Kavantzias, N., Turlapati, R. (2006). Best Practices for Securing Your SOA: A Holistic Approach. *Java Developers Journal*, 8(2):11-23.
- Brose, G. (2003). *Service Web Services with SOAP Security Proxies*. Proceeding of the 13th International Conference, 7-9 September, Dresden, Germany.
- Buecker, A., Ashley, P. & Borrett, M., Readshaw, N. (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 for Quality and Security in Service Oriented Architectures. 6th IEEE International Conference Web Services, 3-5 May, Leipzig, Germany.
- Chodavarapu, P. and Kanneganti, R. (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.

- Hafner, M. (2009). Security Engineering for Service-oriented Architecture. *6th IEEE International Conference Web Services*, 6-8 February, Heidelberg, Germany.
- Hammar, K. (2006). *Towards a Stochastic Model for Integrated Security and Depend Ability Evaluation*. Proceeding of the 9th International Conference on Availability, Reliability and Security, 3-5July, Washington.
- Hangjung, Z., Nazareth, D. (2010). Security and Performance in Service-oriented Application: Trading off Competing Objectives. *Decision support system*, 50(8) 336-346.
- Heather, H., Hondo, M. (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.
- Menzel, M. (2007). SOA Security- secures Cross- Organizational Service Composition. *Stuttgarter Software Technik Forum*, 21(4): 41-53.
- Rosado, D. Eduardo, F. (2011). Security Services Architecture for Secure Mobile Grid Systems. *Journal of Systems Architecture: the EUROMICRO Journal*, 57(5): 240-258.
- Siming, K. & Babar, M. (2010). *Modeling Security for Service Oriented Applications*. Proceeding of The 8th European Conference on Software Architecture, 13-15 May, Nottingham.
- Weilye, K. & Wing, J. (2005). Game Strategies in Network Security. *International Journal of Information Security*, 4(2): 17-28.
- xiaoming, B. (2006). *the Study on Secure Distributed Workflow Architecture Based SOA*. Proceeding of the 4th International Conference on Power System Technology, 8-10july, florida.
- Yamany, H., Miriam, C. (2010). Intelligent Security and Access Control Framework for Secure-Oriented architecture. *Information and Software Technology*, 25 (2): 220-236.
- Yue, H. & Tao, X. (2012). *Web Services Security Problem Insecure-oriented Architecture*. International Conference on Applied Physics and Industrial Engineering, 24(6): 1635-1641.