چکیده :

با ظهور معماری سرویس گرا، چشم انداز سرمایه گذاری نرم افزار از تعاملات انحصاری،مولفه های بسته به یک ارتباطات باز و استاندارد فردی ،مولفه های خود توصیف به نام سرویس انتقال یافت. برای استفاده بهینه از سازمان مورد نظر و صرفه جویی در هزینه و زمان روش مناسب معماری سرویس‌گرا قابل پیاده سازی می باشد. با این هدایت از به هم ریختگی و بار ترافیک کار کاسته و در نقطه مقابل به سرعت انتقال اطلاعات سیستم مورد نظر افزوده شده است. این معماری یک قالب معماری نرم افزار است که در پی تقسیم اطلاعات سیستم به مجموعه‌ای از مولفه‌های مستقل به هم پیوسته است،به دلیل خاصیت ذاتی اتصال ضعیف معماری سرویس گرا ، امکان اعمال تغییرات در زمان اجرای فرآیند ، از طرف افراد غیر مجاز در سیستم وجود دارد. از اینرو امنیت در این سبک پیاده سازی از جایگاه بسیار مهمی برخوردار است. در این پژوهش به تحقیق در رابطه با وب سرویس پرداخته شده و اجزاء آن مورد بررسی قرار داده شده است. رویکرد پیشنهادی روی لایه پیام بیان شده است. این رویکرد پس از بررسی پروتکل soap با استفاده از پنهان نگاری به بیان راه حلی پرداخته است که باعث افزایش امنیت شده است .رویکردارائه شده در سطح کتابخانه پروتکل soap پیاده سازی شده است. قابلیت اطمینان در رویکردی پیشنهادی با قابلیت اطمینان دو الگوریتم RSA وDES مقایسه شده نتایج بدست آمده ،نتیجه بدست آمده باعث افزایش قابلیت اطمینان شده است.

کلمات کلیدی : معماری سرویس گرا، وب سرویس، امنیت، لایه پیام، قابلیت اطمینان .

۱- مقدمه

به منظور توسعه سیستمهای کاربردی سازمانی تجرید اجزاء معماری می بایست به اندازه سطح تجرید دامنه کاری سازمان ارتقاء یافته باشد . رویکردهای سنتی شیءگرا و مبتنی بر مولفه برای ساخت چنین سیستم هایی ناکافی بوده ومنجربه ایجادرویکرد نوین مبتنی‌بر سرویس که ازسطح تجرید بالاتری برخوردار می باشد ، شده است . معماری مبتنی بر سرویس به عنوان یکی از سبکهای معماری پیشرو در راه حلهای سازمانی نیز مطرح است . این سبک معماری به جنبه‌های توسعه سیستم ، نظیر تحلیل و طراحی‌راه حل‌مرتبط است .

وب سرویسها به عنوان یکی از بارزترین نمودهای معماری سرویس گرا در عصر حاضر، از این قاعده مستثنی نبوده به طوریکه بایستی ضمن بهره گیری از مزایای بی شمار آن در عصر حاضر در راستای یکپارچه سازی تعاملات بنگاهها از طریق وب به مسائل و اصول امنیتی آن نیز توجه کافی شود.

هدف اصلی‌این‌گزارش شناخت مفهوم وب سرویس و بررسی پروتکل soap جهت افزایش امنیت آن می باشد. وندی و همکارانش در مقاله " طراحی و پیاده سازی مبتنی بر SOA پل های مانیتورینگ سیستم لایه داده ها "یک نوع معماری بر پایه سیستم نظارت را تجزیه و تحلیل کرده و سپس به ارائه و پیاده سازی سیستم بر پایه لایه داده در چارچوب تکنولوژی وب سرویس برای حل مسائل سیستم های ناهمگن پرداخته است [۱] . پوپسکو وهمکارانش در مقاله " انطباق طبقه–محور از برنامه‌های کاربردی چند لایه "با استفاده از الگو یک روش پویا و قابل انعطاف منطبق بر برنامه های کاربردی چند لایه ارائه داده است [۲] . در این مقاله سرویس ، به عنوان روشی جهت دسترسی به یک توانایی با محدودیتها و سیاستهای مشخص، معرفی شده است. معماری سرویس گرا اطلاعات را به

مجموعه ای از مولفه های مستقل به هم پیوسته تقسیم می نماید. . این مولفه ها می توانند از روشهای متفاوتی مانند یک برنامه کاربردی، کشف شوند . معماری سرویس گرابه عنوان یکی از اصول پایه است که وب سرویسها به عنوان یکی از نمادهای معماری سرویس گرا همیشه به آن وابسته بوده است. امنیت انتقال پیام در مسیر ارتباطی سرور و کلاینت همواره یکی از مسائل مورد بحث وب سرویسها بوده است.از اینروررویکرد پیشنهادی پس از بررسی امنیت سطح پیام با ارائه رویکردی نوین در سطح پروتکل SOAP قابلیت اطمینان سیستم را بهبود بخشیده است .در این مقاله اصول ارتباط و ترتیب ارجاء ماژولهای مورد استفاده پرداخته شده است.سپس نتایج بدست آمده بررسی و ارائه خواهند شد.

۲- سرویس

عملی که به وسیله یک سرویس دهنده انجام می شود و از نظرسرویس گیرنده ارزشمندمی باشد یا به عبارتی، سرویس ، رفتار قرادادی تعریف شده ایست که هر قطعه ای می تواند آنرا جهت استفاده سایر قطعات در سیستم تهیه و پیاده سازی نماید. سرویس ها مکانیزمی را برای یکپارچگی برنامه ها فراهم می کنند.

۳- سرویس های وب[۱]

سرویس های وب را باید نوعی فناوری برای تحقق ویژگی استقلال از سکو در معماری سرویس گرا دانست . یک سرویس وب، نوعی سیستم نرم افزاری است که جهت تعامل ماشین با ماشین در سطح شبکه طراحی شده استو دارای یک تعریف قابل پردازش توسط ماشین با نام $WSDL$[۲] است .

وب سرویس در سطح وب از طریق اینترنت قابل دسترس است و به هیچ سیستم عامل خاصی وابسته نیست .تمام اطلاعات مورد نیاز در فایل XML قرار دارند .که توسط مصرف کننده سرویس برای پردازش ارسال می شوند .پیاده سازی وب سرویس با کلاسهای جاوا و ایجاد یک شیئ سرویس (که در اسناد xml توصیف می شوند) انجام می گیرد [۳] .

٤- استانداردهای پایه در وب سرویسها

بطور کلی پنج استاندارد کلی برای وب سرویسها تعریف شده است که دو مورد آنها به عنوان استانداردهای عمومی از قبل وجود داشته اند این دو مورد عبارتند از [۴] :

---

[۱] Web service

[۲] Web service definition language

- XML به عنوان فرمت کلی برای توصیف مدلها، انواع فرمتها و انواع داده ها بکار می رود .در واقع استانداردهای وب سرویسها بر اساس XML Name Space و XSD ،XML ۱.۰ بنا نهاده شده است.
- HTTPهمچنین HTTPS پروتکلهایی که اینترنت از آن استفاده میکند. HTTP یکی از پروتکلها، برای ارسال پیغامهادر اینترنت می باشد.ای پروتکل برای ارسال پیغامهای وب سرویسهااز طریق شبکه اینترنت استفاده می شود.

سه استاندارد اصلی دیگر بصورت ویژه برای وب سرویسها بکار برده می شود.

- WSDL به عنوان معرف رابط سرویس است .در واقعWSDL دو جنبه متفاوت از سرویس را نشان میدهد .یکی از آنها مشخصات که شامل نام و دیگر پارامترها است و دیگری نحوه اتصال شامل پروتکلها و محل قرار گیری سرویس است.
- SOAP استانداردی که پروتکل وب سرویس را تعریف میکند .همانطور که ذکر گردید HTTP ، پروتکلی است که توسط اینترنت بکار گرفته می شود، SOAP دارای فرمت ویژه ای برای تبادل اطلاعات وب سرویسها از طریق این پروتکل است.
- UDDIاستانداردی در راستای مدیریت، ثبت و یافتن وب سرویسها است.

۵- امنیت در وب سرویسها

مقوله امنیت اطلاعات یکی از حیاتی ترین اجزای چرخه رو به رشد فناوری اطلاعات است. بنگاهها با ورود به دنیای اطلاعات از یک طرف از امکانات و تسهیلات این شاهراه اطلاعاتی بهره مند شده و از طرف دیگر خودرا در معرض تهاجمات ناخواسته از طرف خرابکاران اینترنتی قرار میدهند. آنچه در این میان باید در نظر داشت، بهره گیری از امکانات اطلاعاتی موجود با توجه به اصول و استانداردهای امنیتی پیشنهادی از طرف ارگانها وموسسات ذیصلاح است. در این میان وب سرویسها نیز به عنوان یکی از بارزترین نمودهای معماری سرویس گرا در عصر حاضر ، از این قاعده مستثنی نبوده، بطوریکه میبایست ضمن بهره گیری از مزایای بی شمار آن درعصر حاضر در راستای یکپارچه سازی تعاملات بنگاهها از طریق وب به مسائل و اصول امنیتی آن نیز توجه کافی شود. در ادامه به بررسی استانداردهای امنیتی دروب سرویسها پرداخته خواهد شد [۵]:

٦- امنیت در پیغام رسانی

- وب سرویسها برای تعاملات خود از شاهراه اینترنت بهره میگیرند و ازSOAP و پروتکلهای انتقال در اینترنت مانندHTTP،اغلب برای ایجاد ارتباط استفاده میکنند. نظر به اینکه پروتکلSOAP از ابتدا با اصول امنیتی طراحی نشده

است لذا مستعد حملات مختلف از طرف خرابکاران اینترنتی می باشد. بنابراین برای پوشش ضعفهای امنیتی راهکارهای مختلفی ارائه شده است که از مهمترین آنها میتوان به موارد زیر اشاره کرد.

- HTTP از طریق SSL/TLS[۳] : با توجه به اینکه پیامهای SOAP از طریق پروتکل HTTP منتقل می شوند ، بنابراین بکارگیری پروتکل SSL/TLS برای امن سازی ارتباطات انتها به انتها میتواند یکی از راهکارهای امنیتی تلقی گردد.

- XML Encryption و XML Signature :دو استاندارد فوق الذکر توسط کنسسرسیوم جهانی وب (W۳C) برای امضا و رمز نگاری فایلهای XML ارائه شده است. نظر به اینکه تمام پیامهای SOAP به فرمت XML نوشته میشود، لذا توسعه دهندگان وب سرویسها با بهره گیری از استانداردهای فوق می توانند عملیات امضای دیجیتال یا رمز نگاری پیامهای SOAPرا انجام دهند .

- WS-Security :این استاندارد نیز در راستای ارائه مکانیزمهایی برای ایجاد امنیت لازم در پیامهایSOAP از طریق . XML Signatureو XML Encryption تعریف شده است.

یک پیغام SOAP از سه بخش مهم تشکیل شده است: پوشش[۴] ، سرآیند[۵] ، بدنه [۶]. قسمت پوشش برای بسته‌بندی کردن کل پیغام به کار می‌رود. این بخش محتوای پیغام را توصیف و گیرنده آن را مشخص می‌کند. بخش بعدی پیغام‌های SOAP ، سرآیند آن است که یک بخش اختیاری می‌باشد و مطالبی مانند امنیت و مسیریابی را توضیح می‌دهد. بدنه پیغام SOAP بخشی است که داده های مورد نظر در آن جای می‌گیرند. داده ها بر مبنای XML هستند و از یک مدل خاص که الگوها[۷] آن را توضیح می‌دهند تبعیت می‌کنند. این الگوها به گیرنده کمک می‌کنند تا متن را به درستی تفسیر کند. پیغام‌های SOAP توسط سرورهای SOAP گرفته و تفسیر می‌شود تا در نتیجه آن، وب سرویس‌ها فعال شوند و کار خود را انجام دهند[۶] .

۷- رویکرد پیشنهادی

---

[۳] secure sockets layer/ Transport Layer Security

[۴] Envelope

[۵] Header

[۶] Body

[۷] Schemas

امنیت پیام لایه انتقال : در لایه انتقال، امنیت سطح پیام در بالای امنیت لایه انتقال پیام برپایه end-to-end قرار گرفته است . امنیت لایه انتقال به وسیله تعاملات برنامه کاربردی وب سرویس شناخته شده این تعاملات تحت عنوان SSL/TSL تضمین شده است. SSL وابسته به تکنولوژی گواهینامه X.۵۰۹و سیستم های کلیدعمومی برای کار باقسمت دیگربرای حفاظت در سطح یکپارچگی و محرمانگی اطلاعات انتقال یافته است . ممکن است در طول مسیرانتقال داده ها به دلیل عدم امضاء دستکاری شوند.به دلیل راه نقطه به نقطه انتقال پیام باعث میشود که مسیر پیام به اندازه کافی انعطاف پذیر نباشد .

۸- پروتکل Soap conf[۸]

روش امنیتی لایه پیام با تکیه بر سرویس گرایی در وب سرویس، امنیت باید در لایه پیام اعمال شود. دو روش امنیتی که برای وب سرویس موجود می باشد تگ امنیتی لایه پیام ، که حامل پیام SOAP است و از طرف دیگر مولفه دستی بسته بندی شده امنیت در پیام SOAP است که در این پژوهش ، فرآیند امنیتی سطح پیام ، در پیام SOAP پیاده سازی سازی شده است .

تگ بدنه پیام SOAP، حاوی پیام مورد تقاضا از طرف سرور یا کلاینت می باشد .این پیام که در متنXML قرار دارد در حین ارسال قابل بازیابی می باشد .پروتکل ارائه شده برای جلوگیری از دستکاری پیام در طول مسیر انتقال ، قبل از ارسال در سطح کتابخانه، این پروتکل امضا خواهد شد بعد از دریافت پیام ابتدا پیام مربوطه شناسایی و سپس رمز گشایی می شود .ایده مورد بررسی در این پژوهش به تمرکز بر روی طول پیام پرداخته است. بدین صورت که قبل از ارسال پیام تقاضا کننده سرویس از طرف کتابخانه SOAP ، پیام ،طول پیام شمرده خواهد شد و به سرویس دهنده ارسال خواهد شد. بعد از دریافت آن به وسیله ارائه دهنده پیام، طول دریافتی پیام باید با طول پیام ، بعد از رمز گشایی چک شود اگر نتیجه بدست آمده برابر با نتیجه ارسال شده باشد ، پیام رمز گشایی شده به سطح بالاتر کتابخانه ، ارسال خواهد شد ، در غیر این صورت به فرستنده پاسخی مبنی بر نادرست بودن پیام دریافت شده ارسال خواهد شد . شکل ۵-۲ چارچوب امنیتی وب سرویس افزوده شده با ماژول LenMess Module وپروتکل SOAP CONF[۹] را نشان می دهد.

شکل ۵-۲ : چارچوب امنیتی وب سرویس افزوده شده با ماژولLenMessage

---

[۸] SOAP CONFIDENCE

[۹] Soap

قبل از ارسال پیام های soap در این الگوریتم نیاز است، اطلاعات soapfurther یک گره را کشف شوند .این اطلاعات در قسمت سر[۱۰] هر گره قرار دارند.پس از آن قسمت سر امضاء دیجیتال خواهد شد و در یک عکس پنهان خواهد گشت. هر ماژول Exsoapfur گره میانی مسیر انتقال پیام است.که عمدتا مسئول افزودن اطلاعات soapfurther و فرآیند امضا است .عکس مربوطه در مسیر مشخص برای استفاده ارائه دهنده سرویس قرار داده میشود.پس از دریافت آن توسط سرور ٔپیام ذخیره شده در عکس استخراج شده و در گره مربوطه ذخیره میگردد.گره حاصل شامل متن رمز شده است .در مرحله نهایی پیام مربوطه از گره بدست آمده حاصل میشود.

بعد از پیاده سازی الگوریتم مربوطه ، یک کلاس حمله کننده به وسیله PHP برای آزمایش حمله به پیام SOAP شبیه سازی شده است.در جدول۸-۱ ، شش مفهوم زمان مورد استفاده برای رمزنگاری و تاثیر امنیت الگوریتم ارائه شده بر آن بیان شده است :

CCT(common message coding time),MCT(Important message coding time),UCT(Ultra-important message coding time),CDT(common message decoding time),MDT(Important message decoding time),UDT(Ultra-important message decoding time).

سه مفهوم اول زمان، برای اندازه گیری زمان رمزکردن پیام در الگوریتم مورد استفاده قرار میگیرد.درحالیکه دیگر زمانها برای اندازه گیری زمان رمزگشایی الگوریتم امنیتی استفاده شده اند.همزمان آزمایشهای یکسانی باالگوریتم های قدیمی رمزنگاری مانند DES,RSA انجام شده است . نتایج حاصله در جدول ۸-۱ به نمایش درآمده است :

جسدول ۸-۱ :ارزش زمانی اندازه گیری الگوریتم

[۱۰] Head

همانطور که از جدول ۸-۱ پیداست زمان اجرای بدست آمده روش پیشنهادی در برخی زمانها نسبت به DES, RSA کاهش یافته است.

۹- قابلیت اطمینان

قابلیت اطمینان یکی از نکات کلیدی در هر پروژه نرم افزاری می باشد. امروزه ارزیابی قابلیت اطمینان دارای اهمیت روز افزونی هم در تولیدات انبوه نرم افزارو هم در سیستم های دارای حساسیت بالا می باشد.

یکی از این سیستم ها ، سیستم نرم افزار انتقال وب سرویس می باشد که تحت وضعیت حمله و دستبرد داده هادر مسیر انتقال داده ها و فایل های ایکس ام ال قرار می گیرد.از این رو قابلیت اطمینان در طراحی این سیستم ها از اهمیت بالایی برخوردار می باشد. جهت حفظ عملکرد صحیح و کارایی سرویس های وب در طول انتقال، روش های ارزیابی قابلیت اطمینان و نگهداشت پذیری باید در تمام فازهای انتقال بین ارائه کننده سرویس و دریافت کننده سرویس به انجام برسند. بنا به تعریف، قابلیت اطمینان عبارتست از احتمال اینکه محصول بتواند کارایی مورد نظر را تحت شرایط معین و در مدت زمان مشخص حفظ نماید. بنابراین مقدار قابلیت اطمینان عددی مابین ۰ و ۱ می باشد که حالت مربوط به عدد ۱ بیانگر حالت ایده آل است و در آن هرگز عمکرد صحیح محصول مختل نمی شود. روش های ریاضیاتی مبتنی بر روش های آماری شناخته شده بهترین ابزار را جهت مدل کردن مفاهیم قابلیت اطمینان و همچنین انجام برنامه های پیچیده قابلیت اطمینان فراهم می نمایند. قابلیت اطمینان به عنوان یک پارامتر طراحی، قابل مصالحه با سایر پارامترها نظیر هزینه، توان، عملکرد و غیره بوده و از این رو برای سیستم های مختلف باید روش های متفاوتی با توجه به کارایی شان پیاده سازی گردد.
همان طور که در قبل ذکر شد، قابلیت اطمینان به صورت احتمال اینکه عملکرد صحیح یک محصول در طول یک زمان مشخص و تحت شرایط معین دچار شکست نشود تعریف می گردد.

کودر و ریچاردسون دو فرمول را برای محاسبه هماهنگی درونی آزمون ها ارائه نموده اند. فرمول اول برآوردی از میانگین ضرایب قابلیت اعتماد برای تمام طرق ممکن تنصیف (دو نیمه کردن) را به دست می آورد. ضریب قابلیت اطمینان برابر است با[۷]:

در این رابطه ، n تعداد زمان ها بب است که در آن مساله مورد آزمایش قرار گرفته است ، p احتمال اینکه وب سرویس در مسیر تعیین شده دچار تغییر نشود ، q احتمال اینکه وب سرویس در زمان تعیین شده دچار تغییر شود و s^2 واریانس زمان های کل می باشد.

فرمول دوم: برای استفاده از فرمول ذیل باید شرایط برگزاری آزمون های زمانی برای وب سرویس ها یکسان باشد[۷] :

رابطه ۹-۲ :

انحراف معیار عددی است که مشخص میکند تا چه فاصله ای از مقدار متوسط داده ها، هنوز واریانس وجود دارد. برای بدست آوردن انحراف معیار در این پروژه ریشه دوم واریانس حساب شده است[۷].

رابطه ۹-۳ :

R۱ میانگین زمان درخواست از ابتدای برنامه یعنی ارسال درخواست تازمانیکه پاسخ سرور به برنامه کلاینت برگشت داده شده و اجرای آن تمام شود ، می باشد. R۲ میانگین زمان ارسال درخواست به سرور توسط کلاینت می باشد .R۳ میانگین زمان ارسال پاسخ از سرور به کلاینت می باشد.R۴ میانگین زمان محاسبه صحت اطلاعات پاسخ سرور، توسط کلاینت از طرف سرور می باشد .

میانگین داده های مورد بررسی پس از ۱۰۰۰ بار تکرار درخواست کلاینت و ارسال پاسخ سرور ارائه گردیده است .

نتایج حاصل از محاسبات زمان های R۴،R۳،R۲،R۱ در جدول ذیل به نمایش گذاشته شده است .

جدول ۹-۱ :ارزش محاسبات زمان ارسال و پاسخ درخواست .

قابلیت اطمینان مورد بررسی در جدول زیر به نمایش گذاشته شده است .قابلیت اطمینان بدست آمده برای زمانهای درخواست ،زمان ارسال اطلاعات،زمان پاسخ ،زمان صحت اطلاعات ، مورد بررسی قرار گرفته است.

جدول ۹-۲:ارزش محاسبه ضریب اطمینان .

نمودارهای بدست آمده از دو رویکرد مورد بررسی ورویکرد پیشنهادی در ذیل بیان شده است .در این نمودارها قابلیت اطمینان حاصل زمانهای R۴،R۳،R۲،R۱ به صورت مجزا در نمورهای متفاوت رسم و مقایسه شده است .

نمودار۹-۱ قابلیت اطمینان r۴

نمودار۹-۲ قابلیت اطمینانR۳

نمودار۹-۳ قابلیت اطمینانR۲

همانگونه که نمودار ۹-۳ نشان می دهد قابلیت اطمینان در زمان پاسخ سرور در رویکرد پیشنهادی نسبت به دو روش DES،RSA افزایش یافته است .

نمودار ۹-۴ قابلیت اطمینان R۱

۱۰- نتیجه

در این گزارش به تحقیق در رابطه با معماری سرویس گرا ، مفهوم سرویس و پروتکل های مورد استفاده در برنامه های تحت معماری سرویس گرا پرداخته شده است .الگوریتم جدیدی مبتنی بر پروتکل SOAP با استفاده از استگانوگرافی ارائه شده است.

در این الگوریتم سعی بر شناسایی روش امنیتی با استفاده از پنهان نم.دن پیام در تصویرجهت ارسال به درخواست گیرنده و تایید پیام از طرف دریافت کننده پیام شده است .این تایید واطمینان در مورد پیام هایی کاربرد دارد که طول و محتوای آنها در مسیر از طرف یک مهاجم تغییر کند . قابلیت شناسایی پیام از طریق این روش از کاربر غیر مجاز گرفته می شود.الگوریتم ارائه شده درجهت افزایش امنیت لایه پیام ارائه شده است. الگوریتم مورد نظر را با روشهای RSAو DESمقایسه شده است ، نتایج ونمودارهای بدست آمده باعث افزایش قابلیت امنیت در الگوریتم ذکر شده نسبت به روشهای دیگر رمز نگاری شده است.

منابع :