فصلنامه علمی-ترویجی پدافند غیرعامل

سال چهارم، شماره ۲، تابستان ۱۳۹۲، (پیاپی ۱۴): صص ۶۵-۷۷

نقش سیستم‌های تشخیص نفوذ در امنیت سرویس‌های وب

صادق بجانی[۱]، محمدرضا حسنی آهنگر[۲]، مصطفی اخضمی[۳]

تاریخ دریافت: ۹۲/۰۴/۱۸
تاریخ پذیرش: ۹۲/۰۵/۲۲

چکیده

سرویس‌های وب در توسعه معماری سرویس‌گرا و معماری‌های توزیع‌شده نقش مهمی برعهده دارند. سرویس‌های وب با فراهم کردن امکان استفاده مجدد از کدهای نرم‌افزاری و در نتیجه، کاستن هزینه‌های برنامه‌نویسی و ارتباطی، همچنین به‌دلیل استفاده از اینترنت به‌عنوان بستر انتقال داده و استقلال از سکوهای سخت‌افزاری و نرم‌افزاری، در سال‌های اخیر بسیار مورد توجه قرار گرفته‌اند. امّا از سوی دیگر، سرویس‌های وب با چالش‌های امنیتی خاصی مواجه هستند. این موضوع زمانی اهمّیت بیشتری می‌یابد که سازمان‌ها، متکی بر ارائه سرویس در قالب سرویس‌های وب باشند. در این‌صورت با ضعف سیستم‌های امنیتی رایج در حفاظت از سرویس‌های وب، این سازمان‌ها در برابر انواع تهدیدات شناخته‌شده و ناشناخته که سرویس‌های وب را تهدید می‌کنند، بی‌دفاع هستند. امروزه سیستم‌های تشخیص نفوذ برای تکمیل سطوح دفاعی سامانه‌های نرم‌افزاری سازمان‌ها در فضای سایبر کاملاً شناخته‌شده هستند. تحقیق در خصوص روش‌ها و معماری‌های تشخیص نفوذ در سرویس‌های وب جهت تقویت مسائل مربوط به پدافند غیرعامل در سازمان‌هایی که از سرویس‌های وب استفاده می‌کنند، مهم‌ترین هدف این مقاله به‌شمار می‌آید. در این خصوص، مقایسه بین معماری‌های تشخیص نفوذ، برای رسیدن به یک ادراک سطح بالا از روش تشخیص نفوذ در سرویس‌های وب، به ارتقاء سیستم‌های تشخیص نفوذ رایج برای فعالیت در سطح سرویس وب یا ایجاد سیستم‌های تشخیص نفوذ خاص این سرویس‌ها در کنار سایر ابزارهای امنیتی کمک زیادی خواهد کرد.

کلیدواژه‌ها: سیستم تشخیص نفوذ، وب‌سرویس، تشخیص نفوذ مبتنی بر امضاء، تشخیص نفوذ مبتنی بر ناهنجاری، پدافند غیرعامل

۱- مربی و عضو هیئت علمی گروه مهندسی کامپیوتر دانشگاه جامع امام حسین(ع) sbejani@ihu.ac.ir
۱- استادیار و عضو هیئت علمی گروه مهندسی کامپیوتر دانشگاه جامع امام حسین(ع) mrhassani@iust.ac.ir
۲- دانشجوی کارشناسی ارشد کامپیوتر دانشگاه جامع امام حسین(ع) mostafa_akhzami@yahoo.com - نویسنده مسئول

۱- مقدمه

در سال‌های اخیر، فناوری‌ها و استانداردهای جدیدی برای توسعه نرم‌افزار ارائه شده است. وب‌سرویس، یک مدل برای سرویس‌های توزیع‌شده است که از قابلیت دسترسی ساده و واسط‌های تعریف‌شده استفاده می‌کند. وب‌سرویس، نرم‌افزاری است که دسترسی به اطلاعات و سیستم‌های پردازش اطلاعات را به‌صورت توزیع‌شده فراهم می‌کند. سرویس‌های وب برپایه SOAP[1]، WSDL[2]، XML[3] و UDDI[4] استوارند. پروتکل SOAP وظیفه انتقال اطلاعات مبتنی بر XML را برعهده دارد. WSDL زبان توصیف سرویس وب، و UDDI محل ذخیره و دسترسی عمومی مشخصات وب‌سرویس است[۱].

سرویس‌های وب با توجه به تعاریف مبتنی بر استاندارد آن، امروزه جایگاه خاصی در ارتباطات توزیع‌شده یافته‌اند. موضوع امنیت سرویس‌های وب، مسئله‌ای است که پس از ظهور چنین فناوری، اهمیت بسیاری یافت. استانداردها و تدابیر امنیتی مختلفی در خصوص توسعه، نصب و راه‌اندازی یک سرویس وب وجود دارد. تنوع و پیچیدگی این قبیل استانداردها و رعایت کلیه موازین آن و حفظ سازگاری آن‌ها با یکدیگر، یک موضوع چالش برانگیز در استفاده از آن‌ها است. از یک طرف، ماهیت عمومی بودن سرویس‌های وب، آن‌ها را در برابر انواع حملات شناخته‌شده و ناشناخته قرار می‌دهد و از طرف دیگر، ابزارهای امنیتی رایج، قابلیت شناسایی و سد کردن حملاتی که از این سرویس‌ها سوءاستفاده می‌کنند را ندارند. با درک این کاستی‌ها، ابزارهایی مثل دیوار آتش سرویس‌های وب، به‌مرور زمان پا به عرصه وجود گذاشتند. امّا برای تکمیل سدهای دفاعی، جای خالی سیستم‌های تشخیص نفوذ با قابلیت درک محتوی پیام‌های سرویس‌های وب، کاملاً مشهود است.

در این شرایط، ضرورت وجود سیستم‌های تشخیص نفوذ، که توانایی کشف حمله‌ها را داشته باشند، احساس می‌شود. از نظر روش‌های تحلیل می‌توان رویکردهای موجود در سیستم‌های تشخیص نفوذ را به دو دسته اصلی: ۱) تشخیص سوءاستفاده و ۲) تشخیص ناهنجاری تقسیم کرد. در دسته اول، شناخت از طریق الگوهای ازقبل‌تعریف‌شده حاصل می‌شود. امّا دسته دوم سعی در تشخیص ناهنجاری‌ها و هرگونه حمله جدید را دارد. نفوذگرها هر روز روش‌های جدیدی برای اختلال در سرویس‌های وب کشف می‌کنند. بنابراین برای داشتن یک محیط امن باید سرویس‌های وب با روش‌های مناسبی خود را در برابر حمله‌های جدید و ناشناخته نیز امن سازند.

۱-۱- بیان مسئله

معماری سرویس‌گرا رهیافتی برای ساخت سیستم‌های توزیع‌شده است که کارکردهای نرم‌افزاری را در قالب سرویس ارائه می‌کند. این رهیافت برای یکپارچه‌سازی فناوری‌ها در محیطی که انواع مختلفی از سکوهای نرم‌افزاری و سخت‌افزاری وجود دارند، مناسب است. همچنین سرویس‌ها، هم توسط دیگر نرم‌افزارها قابل فراخوانی هستند و هم برای ساخت سرویس‌های جدید مورد استفاده قرار می‌گیرند. سرویس‌های وب به یک فناوری بنیادی برای یکپارچه کردن کاربردها و ردوبدل کردن داده‌ها در معماری سرویس‌گرا تبدیل شده‌اند. اگرچه استفاده از وب‌سرویس‌ها، کاهش هزینه نگهداری و امکان استفاده مجدد در تولید سیستم‌های توزیع‌شده‌ی تحت وب را به‌دنبال دارد، امّا قرار گرفتن در محیط‌های بازی مانند اینترنت، محدودیت‌ها و ناپایداری‌هایی را در استفاده از این سرویس‌ها ایجاد می‌کند.

استانداردها و توصیه‌نامه‌های نسبتاً زیادی توسط سازمان‌ها و اشخاص درگیر در توسعه سرویس‌های وب برای تأمین امنیت آن‌ها، تدوین و منتشر شده است. در این راستا، می‌توان واسط‌هایی ایجاد کرد و بخش‌هایی از امنیت سرویس‌های وب را به آن‌ها سپرد. دیوار آتش سرویس وب، قابلیت دفاع از سرویس‌های وب در برابر تهدیدات و مخاطرات استفاده از این سرویس‌ها را برعهده دارد. امّا این مجموعه به تنهایی تضمینی برای اطمینان از امنیت در سطح سرویس‌های وب ایجاد نمی‌کند. امروزه سیستم‌های تشخیص نفوذ برای تکمیل سطوح دفاعی سازمان‌ها در فضای سایبر کاملاً شناخته‌شده هستند. بنابراین، سیستم تشخیص نفوذ در کنار دیوار آتش وب‌سرویس، به‌عنوان مکانیزمی برای حفظ بقای وب‌سرویس‌ها در مقابل حملات عمدی و خطاهای غیرعمدی، از اهمیت زیادی برخوردار است.

۱-۲- ضرورت و اهمیت تحقیق

پیچیدگی و دشواری به‌کارگیری کلیه استانداردها و توصیه‌نامه‌های امنیتی موجود در توسعه سرویس‌های وب از یک سو، و وجود کاستی در زمینه ابزارهای امنیتی خاص سرویس‌های وب از سوی دیگر، ضرورت و اهمیت ابزارهای امنیتی در سطح سرویس‌های وب را نشان می‌دهد. این موضوع، زمانی اهمیت بیشتری می‌یابد که سازمان‌ها، متکی بر ارائه سرویس در قالب سرویس‌های وب باشند. در این‌صورت با ضعف سیستم‌های امنیتی رایج در حفاظت از سرویس‌های وب، این سازمان‌ها کاملاً در برابر انواع تهدیدات شناخته‌شده و ناشناخته که سرویس‌های وب را تهدید می‌کنند، بی‌دفاع هستند. بنابراین با توجه به تعریف پدافند غیرعامل که عبارت است از مجموعه اقداماتی که باید انجام شود تا در صورت بروز جنگ، خسارات احتمالی به حداقل میزان خود برسد، باید راهکارهای مناسبی جهت تشخیص نفوذ در سرویس‌های وب در نظر گرفته شود.

۱-۳- اهداف تحقیق

تحقیق در خصوص روش‌های تشخیص نفوذ در سرویس‌های وب،

1- Simple Object Access Protocol
2- Web Services Description Language
3- eXtensible Markup Language
4- Universal Description, Discovery and Integration

مقایسه چند نمونه از معماری‌های سیستم تشخیص نفوذ مربوط به وب‌سرویس‌ها، و ارائه راهکاری مناسب برای تشخیص نفوذ در سرویس‌های وب، مهم‌ترین هدف این پژوهش به‌شمار می‌آید. در این خصوص، مقایسه این معماری‌ها و بررسی نقاط قوت و ضعف آن‌ها، برای رسیدن به یک ادراک سطح بالا از روش تشخیص نفوذ در سرویس‌های وب کمک زیادی خواهد کرد.

۱-۴- سؤالات تحقیق

- مزایا و معایب انواع روش‌های تشخیص نفوذ چیست؟
- انواع روش‌های تشخیص نفوذ در وب‌سرویس‌ها کدامند؟
- سازوکارهای سیستم تشخیص نفوذ در وب‌سرویس‌ها چیست و معایب و مزایای آن‌ها کدام است؟

۱-۵- روش تحقیق و ابزار جمع‌آوری

از آن‌جایی که این تحقیق اقدام به بررسی و مقایسه روش‌های تشخیص نفوذ می‌نماید، «علمی» است و چون نتایج آن به‌صورت کاربردی قابل استفاده در سیستم تشخیص نفوذ وب‌سرویس‌ها است، از نوع کاربردی است، در نتیجه، این تحقیق، از نوع علمی- کاربردی است.

روش جمع‌آوری اطلاعات نیز از منابع کتابخانه‌ای و اینترنتی و اسناد و مدارک تخصصی موجود در این زمینه صورت گرفته است.

۱-۶- روش تجزیه‌وتحلیل

روش تجزیه‌وتحلیل مورد استفاده در این تحقیق، به‌صورت روش مقایسه‌ای است که سه نمونه از سیستم‌های تشخیص نفوذ وب‌سرویس‌ها را بررسی و مورد مقایسه قرار داده است.

۱-۷- ساختار تحقیق

در این مقاله در بخش ۲، ابتدا تعاریف سیستم تشخیص نفوذ مطرح شده و در بخش ۳، طبقه‌بندی سیستم‌های تشخیص نفوذ مورد بررسی قرار گرفته است. در بخش ۴ به بررسی وب‌سرویس‌ها پرداخته شده و در بخش ۵ نیز سه نمونه از معماری‌های سیستم تشخیص نفوذ وب‌سرویس مورد بررسی و مقایسه قرار گرفته است. در بخش ۶، راهکار پیشنهادی برای سیستم‌های تشخیص نفوذ در وب‌سرویس‌ها ارائه شده است. در نهایت، این مقاله با نتیجه‌گیری و ذکر مراجع خاتمه می‌یابد.

۲- تعاریف سیستم تشخیص نفوذ

در این بخش، تعاریفی در مورد نفوذ، سیستم تشخیص نفوذ، انواع سیستم‌های تشخیص نفوذ و روش‌های تشخیص نفوذ ارائه شده است.

۲-۱- نفوذ

نفوذ را می‌توان به‌عنوان اقداماتی که سعی می‌کند جامعیت، محرمانگی و دسترس‌پذیری منابع را به‌خطر اندازد، تعریف نمود[۶].

نفوذ، حاصل یک حمله عمدی و بدخواهانه روی مجموعه‌ای از آسیب‌پذیری‌های سیستم است که در بهترین شرایط، باعث بروز دسترسی‌های غیرمجاز، و در بدترین شرایط باعث ایجاد خرابی یا رفتارهای غیرقابل پیش‌بینی در سیستم می‌شود[۲].

۲-۲- تشخیص نفوذ

تشخیص نفوذ، فرایند نظارت و تجزیه و تحلیل وقایع در یک سیستم کامپیوتری یا شبکه به‌منظور تشخیص فعالیت‌های غیرعادی است[۶].

۲-۳- سیستم تشخیص نفوذ

یک سیستم تشخیص نفوذ، یک دستگاه یا نرم‌افزار کاربردی است که بر شبکه یا فعالیت‌های سیستم برای تشخیص فعالیت‌های مخرب و یا نقض سیاست‌ها نظارت کرده و گزارش‌ها را به مدیریت ارسال می‌کند[۷].

سیستم‌های تشخیص نفوذ، وظیفه شناسایی و تشخیص هرگونه استفاده غیرمجاز به سیستم، سوءاستفاده و یا آسیب‌رسانی توسط کاربران داخلی و خارجی را برعهده دارند. سیستم‌های تشخیص نفوذ به‌صورت سیستم‌های نرم‌افزاری و سخت‌افزاری ایجاد شده و هر کدام مزایا و معایب خاص خود را دارند. سرعت و دقّت، از مزایای سیستم‌های سخت‌افزاری است و عدم شکست امنیتی آن‌ها توسط نفوذگران، قابلیت دیگر این‌گونه سیستم‌ها است. امّا استفاده آسان از نرم‌افزار، قابلیت انطباق‌پذیری در شرایط نرم‌افزاری و تفاوت سیستم عامل‌های مختلف، عمومیت بیشتری را به سیستم‌های نرم‌افزاری می‌دهد و در کل، این‌گونه سیستم‌ها انتخاب مناسب‌تری هستند. سیستم‌های تشخیص نفوذ، برای کمک به مدیران امنیتی سیستم در جهت کشف نفوذ و حمله به‌کار گرفته شده‌اند. هدف یک سیستم، تشخیص نفوذ جلوگیری از حمله نیست؛ بلکه تنها هدف آن، کشف و شناسایی حملات و تشخیص اشکالات امنیتی در سیستم یا شبکه‌های کامپیوتری و اعلام آن به مدیر سیستم است. عموماً سیستم‌های تشخیص نفوذ در کنار دیوارهای آتش و به‌صورت مکمل امنیتی برای آن‌ها مورد استفاده قرار می‌گیرند[۳].

۲-۳-۱- وظایف سیستم‌های تشخیص نفوذ

سیستم‌های تشخیص نفوذ دارای عملکردها و وظایف مختلفی هستند که برخی از آن‌ها عبارت‌اند از:

- نظارت و تجزیه‌وتحلیل کاربران و فعالیت‌های سیستم.
- بررسی تنظیمات سیستم و آسیب‌پذیری‌های آن.
- بررسی جامعیت و درستی سیستم‌های حیاتی و فایل‌های داده.

- شناسایی الگوهای فعالیت منعکس‌کننده حملات شناخته‌شده.
- شناسایی الگوهای فعالیت غیرطبیعی از طریق تجزیه‌وتحلیل آماری.
- مدیریت پیگیری و برجسته‌سازی تخطی کاربران از سیاست‌ها یا فعالیت‌های طبیعی.
- اصلاح خطاهای پیکربندی سیستم.
- نصب و راه‌اندازی تله[1] برای ثبت اطلاعات نفوذگران [۸ و ۹].

۲-۳-۲- ویژگی یک سیستم تشخیص نفوذ مطلوب

ویژگی‌های و الزامات یک سیستم تشخیص نفوذ مطلوب عبارت‌اند از:

- یک سیستم تشخیص نفوذ مطلوب، باید بدون نظارت انسان به‌طور مداوم کار کند.
- سیستم تشخیص نفوذ باید تحمل‌پذیر خطا باشد. به این معنی که باید با وجود خطا، به‌کار خود ادامه دهد و بعد از راه‌اندازی مجدد، پایگاه دانش خود را از دست ندهد.
- در برابر خرابکاری، مقاوم باشد.
- سیستم باید بتواند از خود محافظت کرده و حملات به خود را شناسایی نماید.
- سیستم تشخیص نفوذ باید سربار کمی را بر سیستم تحمیل کند. نمی‌توان سیستم تشخیص نفوذی که سرعت کامپیوتر را کم می‌کند، به آسانی مورد استفاده قرار داد.
- انحراف از رفتار طبیعی سیستم را باید در نظر داشته باشد.
- باید به آسانی، متناسب با مسئله سیستم باشد. هر سیستم دارای یک الگوی استفاده مختلف است و مکانیزم دفاعی باید به‌راحتی با این الگوها سازگار شود.
- باید با تغییر رفتار سیستم در طول زمان، مانند اضافه شدن برنامه‌های جدید به سیستم، خود را تطبیق دهد[۱۰].
- هدف از یک سیستم تشخیص نفوذ، تشخیص حملات است. با این وجود، تشخیص حملات در مراحل اولیه، به‌منظور کاهش تأثیر آن‌ها مهم است.
- سیستم باید قادر باشد تا حملات را با اطمینان تشخیص دهد و عاری از هشدارهای غلط باشد.
- سیستم باید قادر باشد مقدار زیادی از داده‌ها را بدون تاثیر بر عملکرد و حذف آن‌ها، کنترل نماید. یعنی سرعتی که سیستم، الگوهای حسابرسی را ایجاد و پردازش می‌کند، باید بزرگتر یا مساوی سرعت ورود الگوهای حسابرسی جدید باشد.
- سیستمی که بتواند یک هشدار تولیدشده توسط تشخیص نفوذ را به رویداد امنیتی واقعی پیوند دهد، مطلوب است. چنین سیستمی در تحلیل سریع حملات کمک خواهد کرد و نیز ممکن است پاسخ موثری به نفوذ ارائه کند[۱۱].

1- Traps

۲-۳-۳- اجزاء سیستم تشخیص نفوذ

یک سیستم تشخیص نفوذ، به‌طور معمول از اجزاء زیر تشکیل شده است.

- **پیش‌پردازش داده**[2]: این مؤلفه، مسئول جمع‌آوری و ارائه اطلاعات حسابرسی (در یک قالب خاص) است، که به‌وسیله مؤلفه بعدی (تحلیل‌گر) جهت ساخت یک تصمیم، استفاده می‌شود. بنابراین، کار این مؤلفه مرتبط با جمع‌آوری داده‌ها از منبع مورد نظر و تبدیل آن به یک قالب است که توسط تحلیل‌گر قابل درک باشد. داده‌های مورد استفاده برای تشخیص نفوذ، از دو مسیر تهیه می‌شوند. یکی استفاده از الگوهای دسترسی کاربر به خصوصیات شبکه (مانند آدرس IP منبع و مقصد و نوع بسته‌ها) و دیگری داده‌های مربوط به برنامه‌ها و رفتار سطح سیستم (مانند دنباله‌ای از فراخوانی‌های سیستمی تولید شده توسط یک فرایند) است. این داده‌ها به عنوان الگوهای حسابرسی مورد ارجاع قرار داده می‌شوند.
- **تحلیل‌گر (آشکارساز نفوذ**[3]): تحلیل‌گر یا آشکارساز نفوذ، مؤلفهٔ اصلی است که الگوهای حسابرسی را جهت تشخیص حملات، تجزیه‌وتحلیل می‌کند. تطبیق الگوهای مختلف، یادگیری ماشین، داده‌کاوی و روش‌های آماری می‌توانند به‌عنوان آشکارسازهای نفوذ استفاده شوند. قابلیت تحلیل‌گر جهت تشخیص حملات، اغلب تعیین‌کننده قدرت سیستم است.
- **موتور پاسخ**[4]: این مؤلفه، مکانیزم واکنش را کنترل می‌کند و زمانی که تحلیل‌گر یک حمله را تشخیص داد، چگونگی پاسخ را تعیین می‌کند. سیستم ممکن است یک هشدار، بدون در نظر گرفتن اقدامی علیه منبع ایجاد کند؛ یا این‌که ممکن است منبع را برای یک دوره زمانی ازپیش‌تعریف‌شده، مسدود نماید. چنین اقدامی بستگی به سیاست‌های امنیتی ازپیش‌تعریف‌شده شبکه دارد[۱۱].
- **رابط کاربر**: رابط کاربر در سیستم تشخیص نفوذ، به کاربر این امکان را می‌دهد تا خروجی سیستم را مشاهده نموده و یا رفتار سیستم را کنترل کند. این مؤلفه در برخی سیستم‌ها معادل با مدیر یا کنسول است[۸].

۳- طبقه‌بندی سیستم‌های تشخیص نفوذ

طبقه‌بندی سیستم‌های تشخیص نفوذ، در شکل (۱) نشان داده شده است. این طبقه‌بندی، خانوادهٔ سیستم‌های تشخیص نفوذ را با توجه به خصوصیات آن‌ها تعریف می‌کند. چهار نوع مختلف از سیستم‌های تشخیص نفوذ، در دسترس هستند. روش‌های تشخیص نفوذ را

2- Data Preprocessor
3- Intrusion Detector
4- Response Engine

می‌توان به دو روش: ۱) روش‌های مبتنی بر امضاء[1] و ۲) روش‌های مبتنی بر ناهنجاری[2] تقسیم‌بندی نمود. یک دسته‌بندی دیگر سیستم‌های تشخیص نفوذ را می‌توان با توجه به منبع داده‌های استفاده‌شده برای تشخیص نفوذ، ایجاد کرد.

این طبقه‌بندی می‌تواند بر اساس اطلاعات دریافتی از یک میزبان واحد (که سیستم تشخیص نفوذ مبتنی بر میزبان[3] نامیده می‌شود) و اطلاعات دریافتی از بخش‌های کاملی از شبکه‌ای که تحت نظارت است (که سیستم تشخیص نفوذ مبتنی بر شبکه[4] نامیده می‌شود)، ایجاد شود. هر سیستم تشخیص نفوذ می‌تواند با توجه به فعالیت خود بر روی برنامه‌های کاربردی مستقل یا برنامه متمرکز که یک سیستم توزیع‌شده را ایجاد می‌کند، طبقه‌بندی شود. سیستم‌های مستقل به‌صورت جداگانه و بدون هیچ عاملی کار می‌کنند. امّا برنامه‌های متمرکز، با عامل‌های خودمختار که قادر به گرفتن تصمیمات انحصاری و اقدامات واکنشی هستند، کار می‌کنند. یک سیستم تشخیص نفوذ به‌عنوان سیستم مبتنی بر رفتار نیز قابل طبقه‌بندی است. رفتار در تشخیص، پاسخ سیستم تشخیص نفوذ بعد از تشخیص حمله را مشخص می‌کند. این رفتار را می‌توان به رفتار فعال یا غیرفعال در پاسخ به حمله تقسیم‌بندی نمود[۱۲].

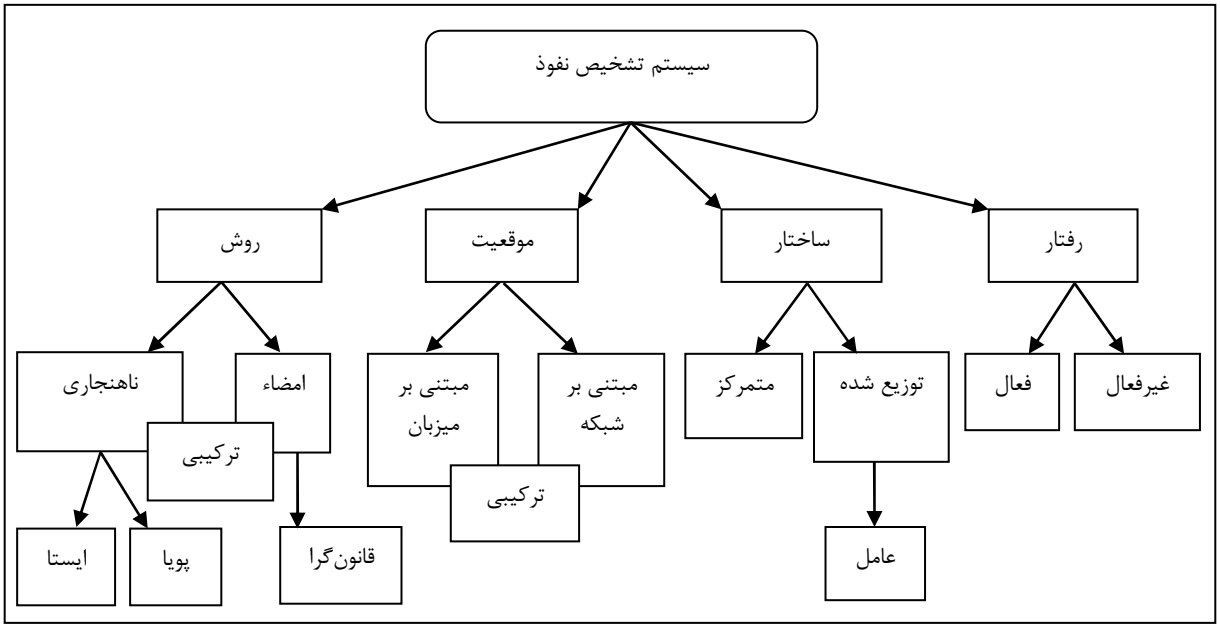
در ادامه، طبقه‌بندی سیستم‌های تشخیص نفوذ بر اساس روش تشخیص شرح داده شده است.

۳-۱- طبقه‌بندی سیستم‌های تشخیص نفوذ براساس روش تشخیص

روش‌های تشخیص، هسته و پایه اصلی فناوری‌های تشخیص نفوذ هستند. در واقع این روش‌ها، موتور اصلی تشخیص فعالیت‌های بداندیشانه و مخرب در منابع اطلاعاتی هستند. به‌طور کلی روش‌های تشخیص نفوذ به دو دسته اصلی تشخیص مبتنی بر امضاء (تشخیص سوء استفاده[5]) و تشخیص مبتنی بر ناهنجاری تقسیم می‌شوند. در ادامه، این دو روش شرح و توضیح داده شده‌اند.

۳-۱-۱- تشخیص مبتنی بر امضاء

سیستم‌های تشخیص نفوذ مبتنی بر امضاء، به‌عنوان سیستم‌های تشخیص نفوذ مبتنی بر دانش نیز شناخته می‌شوند. این سیستم‌ها اشاره به یک پایگاه داده از حملات قبلی، امضاءها و آسیب‌پذیری‌های سیستم دارند. معنی کلمه امضاء، زمانی که درباره سیستم‌های تشخیص نفوذ صحبت می‌شود، به عنوان یک مدرک ثبت‌شده از یک نفوذ یا یک حمله است. هر نفوذ، یک اثر انگشت یا یک ردپا به‌جای می‌گذارد، این اثر انگشت یا ردپا، امضاء یا الگو نامیده می‌شود و می‌تواند جهت شناسایی حملات مشابه در آینده مورد استفاده قرار گیرد[۱۳].



شکل ۱– طبقه‌بندی سیستم‌های تشخیص نفوذ [۱۲]

1- Signature Based 2- Anomaly Based 3- Host-based IDS 4- Network_Based IDS 5- Misuse Detection

سیستم تشخیص نفوذ مبتنی بر امضاء، یک پایگاه داده که شامل تعدادی امضاء حملات شناخته‌شده است را آماده می‌کند. داده‌های ممیزی جمع‌آوری شده توسط IDS[1] با محتوای پایگاه داده مقایسه شده و اگر با آن انطباق داشته باشد، یک هشدار صادر می‌شود. رخدادهایی که با مدل حملات مطابقت نداشته باشند، به‌عنوان بخشی از فعالیت‌های قانونی در نظر گرفته می‌شوند[۱۴].

این روش برای حملات شناخته‌شده بسیار مؤثر است و تعداد کمی هشدار غلط تولید می‌کند. با این حال، این روش قادر نیست حملات جدید را تشخیص دهد. هنگامی که الگوی حملات کمی تغییر داده شود، این روش نسخه‌های تغییریافته از حملات قدیمی را تشخیص نمی‌دهد. بنابراین، این روش تنها در تشخیص حملات ازپیش‌شناخته‌شده، مؤثر است[۱۵].

تکنیک‌های مختلفی مانند سیستم‌های خبره، تحلیل امضاء[2]، داده‌کاوی[3] و تحلیل حالت انتقال[4] در تشخیص مبتنی بر امضاء، استفاده می‌شوند. در جدول (۱)، مزایا و معایب سیستم‌های تشخیص نفوذ مبتنی بر امضاء آورده شده است.

۳-۱-۲- تشخیص مبتنی‌بر ناهنجاری

در سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری، نمایه‌های طبیعی (یا رفتارهای طبیعی) در سیستم نگهداری می‌شوند. سپس سیستم، داده‌های گرفته‌شده را با این نمایه‌ها مقایسه کرده و رفتار هر فعالیتی که از این نمایه‌ها انحراف داشته باشد را به‌عنوان یک نفوذ تلقی می‌کند و با اطلاع‌رسانی به مدیر امنیتی سیستم یا اتخاذ یک پاسخ مناسب در برابر آن اقدام می‌کند[۱۶].

در این روش، برای تشخیص حملات جدید و همچنین مهاجمان داخلی مراحل زیر باید دنبال شود:

مرحله اول: شناسایی رفتارهای نرمال و پیدا کردن قوانین ویژه برای آن‌ها (توصیف رفتار عادی به‌وسیله یادگیری خودکار)

مرحله دوم: ابتدا باید نمایه‌هایی از رفتارهای عادی سیستم، شبکه، کاربران و گروه‌های کاربری ایجاد شود.

با بررسی ترافیک ورودی، رفتارهایی که از این نمایه‌ها پیروی می‌کنند، جزء رفتارهای عادی به‌حساب می‌آیند و فعالیت‌هایی که انحراف بیش از حدّ از مقادیر تعریف‌شده برای این نمایه‌ها دارند به‌عنوان رفتارهای ناهنجار و تلاش‌های نفوذ شمرده می‌شوند[۱۷].

مهم‌ترین روش‌های تشخیص ناهنجاری عبارت‌اند از: تشخیص ناهنجاری آماری، تشخیص مبتنی بر داده‌کاوی، تشخیص مبتنی بر دانش و تشخیص مبتنی بر یادگیری ماشین. مزایا و معایب سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری در جدول (۲)، آورده شده است.

جدول ۱- مزایا و معایب سیستم‌های تشخیص نفوذ مبتنی‌بر امضاء

مزایا	معایب
هشدارهای اشتباه کمی دارند.	ناتوانی در تشخیص حملات ناشناخته و جدید که نمونه امضائی برای آن‌ها تولید نشده است.
ساده بودن روش تشخیص حملات.	ناتوانی در برابر حملاتی که از چند مرحله تشکیل شده‌اند و مبتنی بر یک سری رخدادهای متوالی هستند.
توانایی در تشخیص مؤثر تمامی الگوهای شناخته‌شده حملات.	الگوی‌های نفوذ باید مرتب به‌روز شود.
تحلیل‌های انجام‌شده، عمیق و مفصل است و موجب می‌شود فهم مشکل و اقدامات پیش‌گیرانه توسط مدیر امنیتی ساده‌تر شود.	نیاز به پایگاه داده، مجموعه‌ای از تمام الگوهای شناخته‌شده حملات است و کارایی سیستم به شدت به این پایگاه داده وابسته است.
	در سرعت‌های بالا، کارا و قابل اجرا نیستند، زیرا باید تمامی بسته‌های اطلاعاتی را از لحاظ تطابق با تمامی الگوهای حمله مقایسه کنند.

جدول ۲- مزایا و معایب سیستم‌های تشخیص نفوذ مبتنی‌بر ناهنجاری

مزایا	معایب
قادر به تشخیص حملات جدید که تا به حال رخ نداده‌اند، هستند.	انتخاب یک مجموعه مناسب از پارامترها و ویژگی‌های سیستم، برای اندازه‌گیری و تشخیص حملات براساس آن‌ها، مشکل و نیازمند تجربه زیادی است.
این سیستم‌ها وابستگی کمی به مکانیزم‌های مربوط به سیستم‌عامل دارند.	دارای نرخ بالای هشدارهای غلط هستند؛ زیرا در مرحله یادگیری، پوشش دقیق تمام جنبه‌های رفتار یک سیستم امکان‌پذیر نیست. همچنین رفتار یک سیستم ممکن است با گذشت زمان تغییر کند.
از آن‌جا که الگوهای رفتارهای هنجار می‌توانند برای هر سیستم تشخیص نفوذ منحصر به‌فرد باشند، سیستم تشخیص نفوذ در برابر حملات نفوذ مقاوم‌تر است.	نگهداری فایل‌های نمایه، سربار قابل توجهی دارد. همچنین بیشتر اوقات نیاز به مجموعه آموزشی برای ایجاد نمایه‌های طبیعی است.
سیستم‌های تشخیص ناهنجاری می‌توانند اطلاعاتی تولید کنند که در تعریف امضاء برای سیستم‌های تشخیص مبتنی بر امضاء مورد استفاده قرار می‌گیرد.	در مواردی که دامنه عملکرد سیستم وسیع باشد و یا رفتار عادی به‌مرور زمان تغییر کند، ایجاد نمایه رفتار عادی سیستم، کاری دشوار و زمان‌گیر خواهد بود.

1- Intrusion Detection System 2- Signature Analysis 3- Data Mining 4- State Transition Analysis

۴- وب‌سرویس

در این بخش به معرفی وب‌سرویس‌ها، معماری و مؤلفه‌های تشکیل‌دهنده وب‌سرویس، پرداخته شده است.

۴-۱- تعریف وب‌سرویس

طبق تعریف کنسرسیوم جهانی وب[1]، یک وب‌سرویس، نوعی سیستم نرم‌افزاری است که جهت تعامل ماشین با ماشین در سطح شبکه طراحی شده و دارای یک تعریف قابل پردازش توسط ماشین به‌نام WSDL است. دیگر سیستم‌ها طبق این توصیف از قبل مهیاشده ،با سرویس‌دهنده تعامل دارند و پیام های خود را تحت پروتکل SOAP منتقل می‌کنند. وب‌سرویس، حاصل ترکیب دو فناوری قدرتمند XML و HTTP[2] است[۱۸].

۴-۲- معماری وب‌سرویس

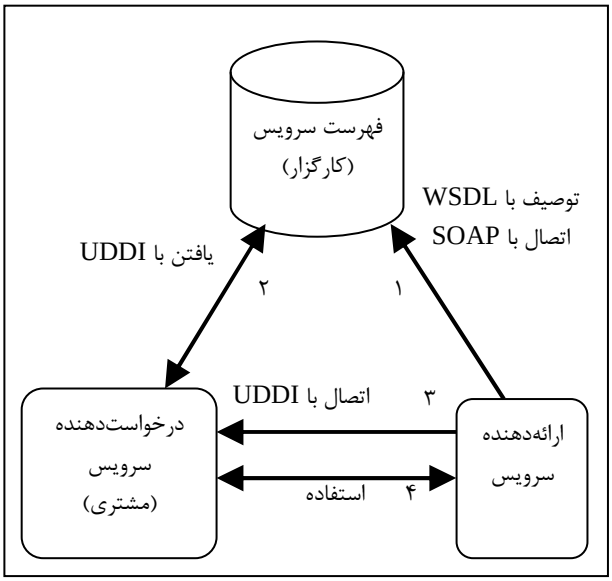
معماری وب‌سرویس عمدتاً مبتنی‌بر تعامل بین سه نقش: ارائه‌دهنده سرویس، درخواست‌کننده سرویس و فهرست[3] سرویس است. تعامل، مستلزم برخی عملیات مانند انتشار، یافتن و اتصال است. در مجموع چهار مرحله رویداد برای وب‌سرویس‌ها وجود دارد که عبارت‌اند از:

- ارائه‌کننده سرویس، توصیفی از سرویس تعریف نموده و آن را در فهرست سرویس منتشر می‌کند.
- کارگزار سرویس، سرویس‌های بهینه را با برآورد مشخصات فهرست، می‌یابد.
- کارگزار سرویس، سرویس را به درخواست‌کننده سرویسی که آن سرویس را پیدا کرده، منتقل می‌کند.
- هنگامی که سرویس یافت شد، جهت اتصال این سرویس به درخواست‌کننده سرویس، با ارائه‌دهنده سرویس مذاکره صورت می‌گیرد.

درخواست‌کننده سرویس، ممکن است یک کلاینت، یک دستگاه، یک برنامه یا یک وب‌سرویس دیگر باشد. وب‌سرویس‌ها دارای سه رفتار عملیاتی به نام انتشار، یافتن و اتصال هستند. عملکرد وب‌سرویس در گرو رخ دادن این سه رفتار است. معماری و عملکرد وب‌سرویس‌ها در شکل (۲) نشان داده شده است[۱۹].

۴-۳- اجزاء وب‌سرویس

مؤلفه‌های تشکیل‌دهنده وب‌سرویس که شامل SOAP، WSDL و UDDI هستند، در ادامه معرفی شده‌اند.



شکل ۲- معماری وب‌سرویس [۱۹]

۴-۳-۱- WSDL

زبان توصیف وب‌سرویس، زبانی مبتنی‌بر XML است که برای تعریف وب‌سرویس و توصیف چگونگی دسترسی به وب‌سرویس استفاده می‌شود. یکی از خواص وب‌سرویس‌ها، توصیف خود آن‌ها است. وب‌سرویس دارای اطلاعاتی است که نحوه استفاده از خود را توضیح می‌دهد. این توضیحات در WSDL نوشته می‌شود. WSDL متنی به زبان XML است که به برنامه‌ها می‌گوید این وب‌سرویس چه اطلاعاتی به‌عنوان ورودی لازم دارد و چه اطلاعاتی را برمی‌گرداند[۱].

۴-۳-۲- SOAP

SOAP یک پروتکل سبک‌وزن برای تبادل اطلاعات در محیط‌های توزیع‌شده و غیرمتمرکز است. این پروتکل، مبتنی بر XML و شامل سه بخش: ۱) یک پوشش که چارچوبی برای توصیف پیام و چگونگی پردازش آن را تعریف می‌کند؛ ۲) یک مجموعه‌ای از قوانین رمزنگاری برای بیان نمونه‌هایی از انواع داده‌های تعریف‌شده و ۳) قراردادی برای نمایش و فراخوانی و پاسخ از راه دور می‌باشد.

SOAP به‌طور بالقوه می‌تواند در ترکیب با انواع پروتکل‌های دیگر استفاده شود. SOAP دارای فرمت ویژه‌ای برای تبادل اطلاعات وب‌سرویس‌ها از طریق پروتکل HTTP است. وقتی یک برنامه شروع به ارتباط با وب‌سرویس می‌کند، پیام‌های SOAP وسیله‌ای برای ارتباط و انتقال دیتا بین آن‌دو هستند. یک پیام SOAP به وب‌سرویس فرستاده می‌شود و یک تابع را در آن به اجرا درمی‌آورد. وب‌سرویس نیز از محتوای پیام SOAP استفاده کرده و عملیات خود

1- W3C
2- Hyper Text Transport Protocol
3- Registry

را آغاز می‌کند. در انتها نیز نتایج را با یک پیام SOAP دیگر به برنامه اصلی می‌فرستد[۱].

UDDI -۳-۳-۴

UDDI استانداردی طراحی‌شده برای ارائه یک فهرست راهنمای قابل جستجو برای وب‌سرویس‌ها است. بنابراین، مکان و موقعیت کارگزار سرویس را نمایش می‌دهد. در بسیاری موارد، UDDI مانند یک دفترچه تلفن طراحی شده است. شرکت‌ها می‌توانند وب‌سرویس خود را معرفی کنند، با وب‌سرویس دیگران آشنا شوند و آن را در سیستم‌های خود استفاده کنند[۱].

۵- معرفی چند معماری سیستم تشخیص نفوذ در وب‌سرویس‌ها

در این بخش به بررسی چند نمونه از سیستم‌های تشخیص نفوذی که برای استفاده در وب‌سرویس‌ها طراحی شده‌اند، پرداخته شده است.

۵-۱- تشخیص نفوذ در سرویس‌های وب به‌وسیله تحلیل محتوای پیام‌های XML

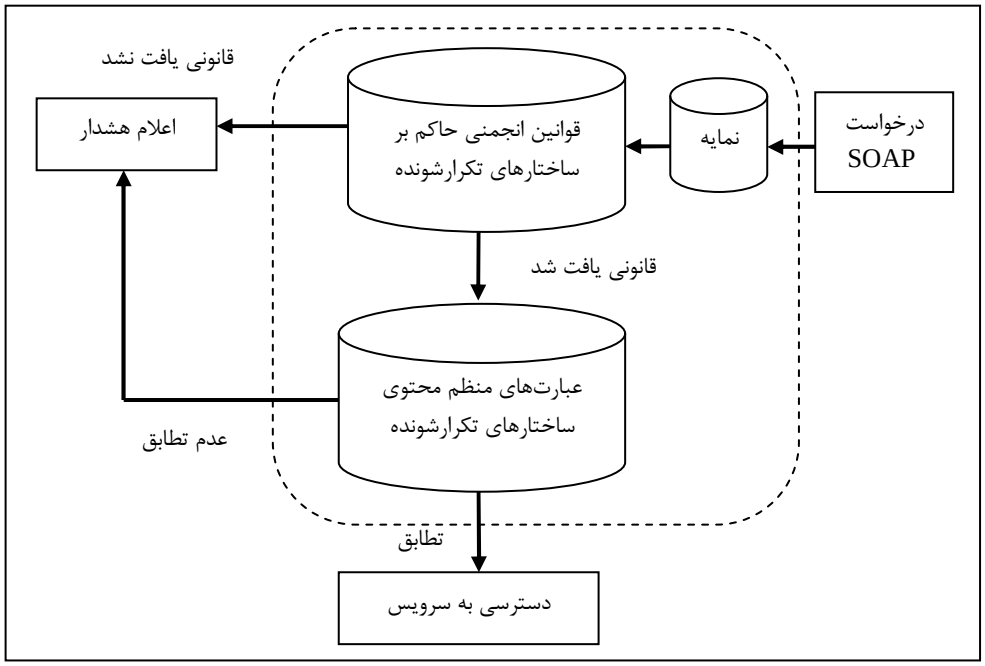
در [۴] با به‌کار بردن روش‌های داده‌کاوی بر روی پیام‌های SOAP، ناهنجاری‌های سرویس‌های وب شناسایی شده است. در این فن، همچنین از قوانین انجمنی مبتنی بر درخت برای استخراج دانش در فاز آموزش استفاده شده است. از دانش به‌دست آمده در فاز آموزش برای تشخیص هرگونه سوءاستفاده در فاز آزمون، بهره‌برداری می‌شود. به علت وقوع حمله‌های جدید، این کار دانشگاهی به دنبال یک سیستم تشخیص ناهنجاری است تا قادر به تشخیص حمله‌های جدید باشد. از طرفی، تنها داده‌های حالت نرمال در این کار در نظر گرفته شده است و از رویکرد تشخیص ناهنجاری نیمه‌نظارت‌شده استفاده شده است.

۵-۱-۱- چارچوب روش پیشنهادی

برای تشخیص ناهنجاری نیمه‌نظارت‌شده در پیام‌های SOAP یک سرویس وب، باید یک نمایه نرمال از درخواست‌ها و پاسخ‌های سالم SOAP آن سرویس را برای فاز آموزش تهیه نمود. از آن‌جایی که ساختار پیام‌های SOAP بر پایه XML است، از روش‌های کشف دانش برای تشخیص ناهنجاری در آن‌ها استفاده شده است. برای کشف دانش از فایل‌هایی با ساختار XML، باید دو مرحله کاوش ساختار و کاوش محتوی در نظر گرفته شود. البته کاوش محتوی با توجه به نتایج به‌دست‌آمده از مرحله کاوش ساختار انجام می‌شود. فن داده‌کاوی مورد نظر برای کاوش ساختار، کشف قواعد انجمنی است.
برای کاوش ساختار از طریق کاوش قواعد انجمنی، باید دو زیر مرحله کاوش الگوهای تکرارشونده و کشف قواعد انجمنی انجام شود. با کاوش الگوهای تکرارشونده از اسناد XML، یک دانش نسبی و تقریبی از ساختار و همچنین محتوی اسناد به‌دست می‌آید. در این روش کاوش، به‌طور مستقیم با اسناد XML کار می‌شود و داده‌ها به پایگاه داده‌های رابطه‌ای یا قالب‌های میانی دیگری نگاشت نمی‌شوند. در نهایت، قواعد انجمنی در قالب XML ذخیره می‌شوند. زیرمرحله کاوش الگوهای تکرارشونده، یک دانش نسبی از محتوی اسناد به ما می‌دهد. امّا هدف نهایی فن پیشنهادی برای کاوش محتوی آن است که قواعد انجمنی استخراج‌شده علاوه‌بر آن‌که قواعد حاکم بر ساختارهای تکرارشونده را به ما می‌دهد، بتواند قالب محتوی هر یک از این ساختارها را نیز به‌صورت عبارت‌های منظم بیان کند. از آن‌جایی که کاوش قواعد انجمنی مبتنی بر درخت هنوز یک مسئله باز است، در این‌جا فرض می‌شود که قالب محتوی ساختارهای تکرارشونده را یک شخص ماهر به‌صورت عبارت‌های منظم در فاز آموزش می‌نویسد. در حالت‌هایی که تعداد قوانین تولیدشده به میزانی باشد که احتمال کند شدن فرایند یافتن یک قانون وجود داشته باشد، می‌توان روی قوانین انجمنی کشف‌شده، نمایه تعریف کرد تا دسترسی به آن‌ها سریع‌تر شود.
پس از طی این دو مرحله، نمایه تشریح کننده وضعیت نرمال پیام‌های SOAP آماده است و می‌توان از آن به‌عنوان مبنای تشخیص ناهنجاری‌ها در فاز آزمون استفاده کرد. در شکل (۳) فرایندهای دخیل در فاز آزمون این معماری نشان داده شده است.

۵-۲- تشخیص نفوذ در سرویس‌های وب مبتنی‌بر سری‌های زمانی

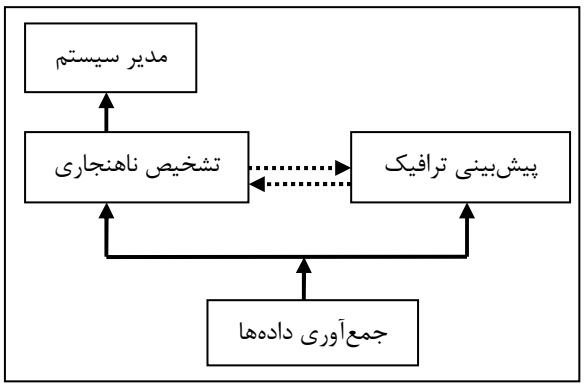
در [۵] روشی برای تشخیص نفوذ در وب‌سرویس‌ها، مبتنی بر سری‌های زمانی ارائه شده است. روش‌های سنتی تشخیص نفوذ، هر نمونه داده را به‌عنوان یک رکورد تک‌متغیره یا چندمتغیره به‌صورت مستقل تحلیل کرده و از جنبه ترتیبی داده صرف‌نظر می‌کنند. امّا اغلب ناهنجاری‌ها تنها با تحلیل دنباله‌ای از نمونه‌های داده قابل تشخیص خواهند بود؛ از این‌رو، توسط روش‌های تشخیص ناهنجاری سنتی تشخیص داده نمی‌شوند. بنابراین، تحلیل یک سری زمانی و دنباله‌ای از داده‌ها بسیار مهم و راه‌گشا است. مدل سری زمانی از یک زمان‌سنج دوره‌ای همراه با یک شمارنده رخدادها یا اندازه‌گیر منابع استفاده کرده و ترتیب و زمان ورود مشاهدات و مقادیر آن‌ها را ذخیره می‌کند. اگر احتمال وقوع یک مشاهده جدید در یک زمان کم باشد و مشاهده جدیدی رخ دهد، آن یک ناهنجاری تلقی می‌شود. هنگام سروکار داشتن با مقدار زیادی از داده که ممکن است رفتار آن‌ها در طول زمان تغییر کند، مدل سری زمانی می‌تواند مورد استفاده قرار گیرد. همچنین در مواردی که حمله‌ها به‌صورت توزیع‌شده هستند، این روش بسیار مفید خواهد بود.



شکل ۳- فاز آزمون تحلیل محتوای پیام‌های SOAP [۴]

۵-۲-۱- معماری پیشنهادی

هدف این پژوهش، ارائه روشی برای تشخیص ناهنجاری است. معماری مورد نظر در شکل (۴) نشان داده شده است. واحد تشخیص ناهنجاری، ورودی را که معمولاً سری زمانی ثبت شده‌ای از مجموعه داده‌ها است از واحد جمع‌آوری داده دریافت کرده و با واحد پیش‌بینی ترافیک مقایسه کرده و سپس خروجی مورد نظر را تولید می‌کند. این خروجی، ناهنجاری‌های تشخیص‌داده‌شده در ورودی داده‌شده است. در ادامه، مؤلفه‌های این معماری شرح داده شده است.



شکل ۴- معماری سیستم تشخیص نفوذ مبتنی بر سری‌های زمانی [۵]

- **واحد جمع‌آوری داده**، داده‌ها را از پورت‌ها و ورودی‌های مختلف **می‌خواند** و با تنظیم یک زمان‌سنج، آن‌ها را در قالب مجموعه دادهٔ سری زمانی که در آن، نمونه‌ها ثبت شده‌اند، ذخیره می‌کند.

همچنین این واحد، اطلاعات ذخیره‌شده را با توجه به متد وب‌سرویس مقصد، برچسب‌گذاری کرده و با توجه به تعاریف انجام‌شده توسط فرد خبره، داده‌های ذخیره‌شده را به داده‌های ممیزی بر اساس ساختار مورد نیاز تبدیل می‌کند.

- **واحد پیش‌بینی ترافیک**، مقدار مورد انتظار برای هر نقطه از زمان در سری زمانی را مشخص می‌کند.
- **واحد تشخیص ناهنجاری**، سری‌های زمانی ثبت‌شده را دریافت کرده و در تعامل با واحد پیش‌بینی ترافیک، سعی بر تشخیص ناهنجاری دارد. این واحد با استفاده از مدل مشخص‌شده و مقایسه آن با مقادیر پیش‌بینی‌شده، ناهنجاری را تشخیص خواهد داد و اگر مقداری به نظر ناهنجار آید، پیام هشداری به مدیر سیستم داده خواهد شد.

۵-۳- چارچوب جلوگیری و تشخیص نفوذ فعال برای وب‌سرویس‌ها

در [۲۰] یک سیستم تشخیص و جلوگیری از نفوذ برای حفاظت از سرویس‌های‌وب در برابر حملات SOAP/XML/SQL ارائه شده است. در این مقاله سیستم تشخیص و جلوگیری از نفوذ از روش‌های انطباقی مانند فنون داده‌کاوی مبتنی بر عامل، به همراه منطق فازی در لایه کاربرد استفاده کرده است. عامل‌ها به‌عنوان حسگر با استفاده از روش‌های داده‌کاوی برای تشخیص انحراف نمایه‌های طبیعی به‌کار می‌روند. همچنین با استفاده از منطق فازی، ناهنجاری‌ها برای تشخیص حملات و کاهش هشدارهای اشتباه تحلیل می‌شوند. در این

روش، رفتار معمول کاربر مانند آدرس IP مبداء، آدرس IP مقصد، شناسه کاربر و تقاضا و پاسخ‌های تکرارشونده کاربر در قالب یک نمایه برای او نگهداری می‌شود.

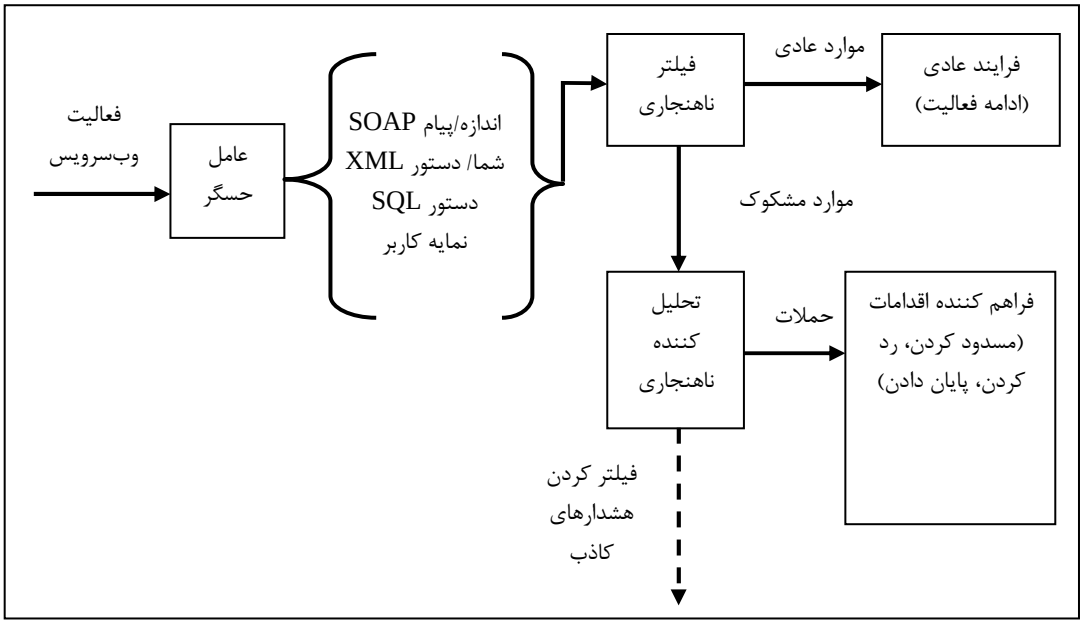
سایر اطلاعات، شامل پارامترهای SOAP، قاب زمانی تقاضا و پاسخ و اندازه پیام‌ها نیز نگهداری می‌شوند. در این مرحله، عامل‌ها که نقش یک حسگر را دارند با به‌کارگیری فنونی مانند خوشه‌بندی، کاوش قواعد انجمنی و ترتیبی، به شناسایی ناهنجاری‌ها و انحراف‌های صورت‌گرفته از نمایه نرمال کاربر می‌پردازند. برای کاهش هشدارهای اشتباه، ناهنجاری‌های شناسایی‌شده در مرحله قبل، دستخوش یک مرحله تحلیل دیگر با استفاده از منطق فازی شده، که طی این مرحله، حمله‌های واقعی تعیین می‌شوند. به ازای شناسایی یک حمله، اعمال جبرانی گوناگونی مانند بلوکه کردن، ردکردن و پایان دادن به عمل صورت می‌گیرد. معماری پیشنهادی این مقاله در شکل (۵) نشان داده شده است.

۵-۴- مقایسه بین معماری سیستم‌های تشخیص نفوذ

برای مقایسه بین معماری سیستم‌های تشخیص نفوذی که در این مقاله به آن‌ها اشاره شد، ابتدا عواملی که برای مقایسه سیستم‌های تشخیص نفوذ مؤثر هستند را تعریف نموده و سپس هر یک از معماری‌ها با این عوامل سنجش می‌شوند. همان‌گونه که در جدول (۳) مشاهده می‌شود، این عوامل عبارت‌اند از: روش تشخیص نفوذ، الگوریتم تشخیص نفوذ، آموزش و یادگیری سیستم، نرخ هشدارهای کاذب، پاسخ‌دهی سیستم.

۶- راهکار پیشنهادی برای توسعه سیستم‌های تشخیص نفوذ در سرویس‌های وب

با توجه به معماری‌های معرفی‌شده در جهت اهداف مقاله و عواملی که برای مقایسه این معماری‌ها در نظر گرفته شد، رویکرد مورد نظر برای توسعه سیستم‌های تشخیص نفوذ در سرویس‌های وب به شرح ذیل پیشنهاد می‌شود.



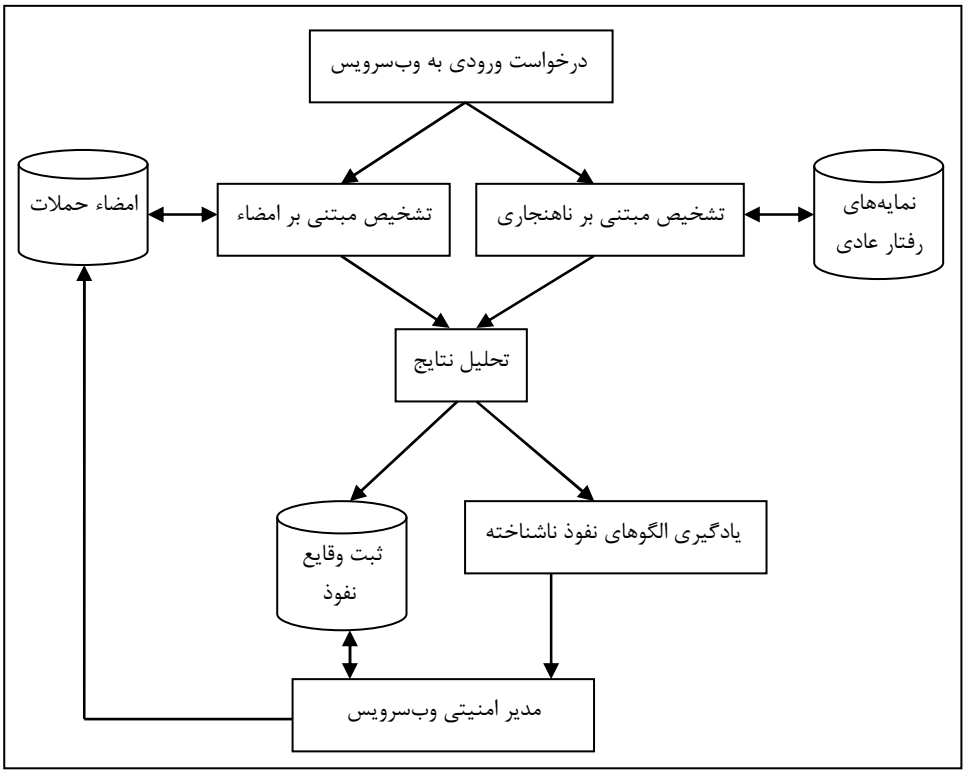
شکل ۵- چارچوب جلوگیری و تشخیص نفوذ فعال برای وب‌سرویس‌ها [۲۰]

جدول ۳- مقایسه بین معماری سیستم‌های تشخیص نفوذ

عوامل مقایسه / معماری	روش تشخیص	الگوریتم تشخیص	آموزش سیستم	نرخ هشدار کاذب	پاسخ‌دهی
تشخیص نفوذ به وسیله تحلیل محتوای پیام‌های XML	تشخیص ناهنجاری	داده کاوی	برنامه‌ریزی شده	بالا	فاقد پاسخ‌دهی
تشخیص نفوذ مبتنی بر سری‌های زمانی	تشخیص ناهنجاری	داده کاوی - مدل سری زمانی	برنامه‌ریزی شده	بالا	فاقد پاسخ‌دهی
چهارچوب جلوگیری و تشخیص نفوذ فعال	تشخیص ناهنجاری	داده کاوی- منطق فازی	برنامه‌ریزی شده	بالا	فاقد پاسخ‌دهی

۶-۱- راهبرد اصلی طراحی

همان‌طور که در شکل (۶) نشان داده شده است، ادغام روش‌های تشخیص مبتنی‌بر امضاء و مبتنی بر ناهنجاری، به‌عنوان راهبرد اصلی طراحی سیستم‌های تشخیص نفوذ در سرویس‌های وب باید مورد استفاده قرار گیرد. بیشتر سیستم‌های تشخیص نفوذ رایج، از یکی از این دو روش تشخیص نفوذ استفاده می‌کنند. سیستم تشخیص نفوذ ترکیبی، مرکّب از هر دو روش تشخیص مبتنی‌بر امضاء و مبتنی بر ناهنجاری است. این سیستم، پایگاه داده امضاءهای خود را با حملاتی که توسط تشخیص مبتنی بر ناهنجاری کشف شده‌اند، به‌روزرسانی می‌کند. با استفاده از سیستم تشخیص نفوذ ترکیبی می‌توان از ویژگی‌های مثبت هر دو روش تشخیص نفوذ برای رسیدن به دقّت تشخیص بالا و کاهش هشدارهای غلط استفاده نمود. با این روش ترکیبی، حملات دارای امضاء به‌خوبی شناسایی شده و از طرف دیگر حملات ناشناخته نیز قابل تشخیص خواهند بود. در جدول (۴)، روش‌های تشخیص نفوذ با یکدیگر مقایسه شده‌اند.



شکل ۶- راهکار پیشنهادی برای توسعه سیستم‌های تشخیص نفوذ در وب‌سرویس‌ها

جدول ۴- مقایسه بین روش‌های تشخیص نفوذ

ویژگی	مبتنی‌بر امضاء	مبتنی‌بر ناهنجاری	ترکیبی
دقت تشخیص	بالا (برای حملات شناخته شده)	پایین	بالا
قابلیت تشخیص حملات جدید	خیر	بله	بله
اعلام هشدار غلط	پایین	بالا	متوسط
هشداردهی به موقع	سریع	آهسته	نسبتاً سریع
بروزرسانی الگوها	متناوب	غیرمتناوب	غیرمتناوب

۶-۲-آموزش و یادگیری سیستم

آموزش و یادگیری سیستم تشخیص نفوذ، یکی از عوامل مؤثر در دقّت تشخیص سیستم است. آموزش و یادگیری، برای خودکار ساختن شناسایی الگوی رفتاری حملات و در نتیجه، امضاء حملات جدید در سیستم‌های تشخیص نفوذ کاربرد دارد. هنگامی که یک نفوذ جدید به سیستم، توسط واحد تشخیص، ناهنجاری تشخیص داده شد، با استفاده از فرایند یادگیری، رفتار این نفوذ به‌عنوان یک امضاء جدید متعلق به این نفوذ تعریف خواهد شد. با استفاده از این عامل، سیستم قادر خواهد بود که پس از ایجاد امضاء یک حمله جدید، پایگاه داده امضاء حملات را به‌روزرسانی نماید. به این وسیله سیستم تشخیص سوء استفاده، از تکرار عمل بدخواهانه نفوذگر به سیستم با صرف کمترین هزینه پردازشی جلوگیری می‌کند.

۶-۳- بانک ثبت وقایع نفوذ

بانک ثبت وقایع نفوذ، امکان نگهداری رکورد کاملی از درخواست‌های نفوذی SOAP را فراهم می‌کند. در این بانک، رکوردهایی از فعالیت واحدهای تشخیص ناهنجاری و تشخیص سوءاستفاده ذخیره می‌شوند. این رکوردها حاوی اطلاعات افراد مشکوکی هستند که فعالیت خراب‌کارانه یا بدخواهانه آن‌ها کشف شده است. این بانک سابقه نفوذگران در ارتباط با سرویس‌های وب و متدهای آن‌ها را در خود نگهداری می‌کند.

۶-۴- استفاده از فرایند پاسخ‌دهی

وظیفه اصلی فرایند پاسخ‌دهی این است که نحوه استدلال سیستم تشخیص نفوذ را برای مدیر امنیتی وب‌سرویس توضیح دهد. با استفاده از این فرایند، سیستم تشخیص نفوذ می‌تواند برای مدیر امنیتی توضیح دهد که چگونه به این نتیجه رسیده است که درخواست ورودی، یک درخواست نفوذ است. استفاده از امکانات پاسخ‌دهی سیستم‌های خبره در تشخیص نفوذ پیشنهاد می‌شود. مشخصه بارز سیستم‌های خبره، توانایی آن‌ها در توضیح فرایند استدلال‌شان است.

به‌کارگیری فرایند پاسخ‌دهی برای طراح سیستم، این مزیت را دارد که خطاهای ممکن در سیستم را تشخیص دهد و برای مدیر امنیتی وب‌سرویس نیز این مزیّت را دارد که روش استدلالی سیستم را به‌طور شفاف دنبال کند. در نتیجه، مدیر امنیتی وب‌سرویس- زمانی که منطق استدلال تشخیص نفوذ را مشاهده کند- به نتیجه ارائه‌شده توسط سیستم تشخیص نفوذ، بیشتر اعتماد خواهد کرد. همچنین با استفاده از فرایند پاسخ‌دهی، می‌توان تا حدود زیادی از هشدارهای کاذب سیستم تشخیص نفوذ جلوگیری نمود. زیرا با سؤالاتی که مدیر امنیتی وب‌سرویس از سیستم می‌پرسد، می‌تواند به نقاط ضعف سیستم پی ببرد.

۷- نتیجه‌گیری

سرویس‌های وب، مؤلفه‌های نرم‌افزاری مبتنی بر شبکه‌ای هستند که از پروتکل SOAP که مبتنی بر XML است برای تعاملات خود استفاده می‌کنند و وابسته به هیچ سکّو یا زبان برنامه‌نویسی خاصی نیستند. ویژگی خودتوصیف‌گری در این کاربردها امکان ترکیب سرویس‌های مختلف برای ایجاد کاربردهای توزیع‌شده را ممکن می‌سازد. سرویس‌های وب به‌عنوان یک پیاده‌سازی از معماری سرویس‌گرا، نه‌تنها در اینترنت بلکه در ارتباط‌های میان سازمان‌ها در سال‌های اخیر بسیار مورد توجه قرار گرفته‌اند. از سوی دیگر، قرارگرفتن در معرض حملات بدخواهانه و نفوذگران، قابلیت اطمینان استفاده از این سرویس‌ها را با نگرانی‌هایی همراه می‌کند. بنابراین، ایجاد راهکارهایی برای حفظ بقای چنین سیستم‌هایی در مقابل حملات و نفوذگران و رعایت مباحث پدافند غیرعامل در سرویس‌های وب از اهمیت زیادی برخوردار است.

امروزه سیستم‌های تشخیص و پیشگیری نفوذ برای تکمیل سطوح دفاعی سازمان‌ها در فضای سایبر کاملاً شناخته‌شده هستند. ولی متأسفانه، چنین سیستم‌هایی برای تحلیل وقایع سرویس‌های وب کارایی لازم را ندارند. چرا که سرویس‌های وب در سطحی بالاتر از حدّ تشخیص این سیستم‌ها فعال هستند. کارهای بسیار محدودی را می‌توان یافت که به چنین راه‌حلی درخصوص سرویس‌های وب اشاره کرده باشند. در این مقاله، راهکاری مناسب برای توسعه سیستم‌های تشخیص نفوذ در سرویس‌های وب ارائه گردید. راهکار مذکور، حاصل بررسی وب‌سرویس‌ها، روش‌های تشخیص نفوذ و سه معماری سیستم تشخیص نفوذ در این زمینه است. راهکار پیشنهادی، حاصل ادغام روش‌های تشخیص نفوذ مبتنی بر امضاء و مبتنی‌بر ناهنجاری در سرویس‌های وب است. همچنین با استفاده از فرایند پاسخ‌دهی و آموزش سیستم تشخیص نفوذ می‌توان کارایی سیستم در برابر حملات ناشناخته را افزایش و نرخ هشدارهای غلط در سیستم تشخیص نفوذ را کاهش داد.

مراجع

۱. حسنی آهنگر، محمدرضا؛ اخضمی، مصطفی؛ اتکاپذیری در وب‌سرویس‌ها با رویکرد پدافند غیرعامل؛ فصل‌نامه علمی- ترویجی پدافند غیرعامل؛ سال سوم، شماره چهارم، ص ۱ تا ۱۰، (۱۳۹۱).

۲. آقاجانی، زهرا؛ یک معماری چندلایه برای سرویس‌های وب تحمل‌پذیر نفوذ؛ پایان‌نامه کارشناسی ارشد، دانشگاه علم و صنعت ایران، (**۱۳۸۷**).
۳. جان‌محمدی، پرژک؛ ارائه راهکار تشخیص نفوذ توزیع‌شده با استفاده از زیرساخت گرید؛ پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی زنجان، (**۱۳۹۰**).
۴. قاسم‌اصفهانی، ریحانه؛ ارائه فنی برای تشخیص نفوذ در سرویس‌های وب به‌وسیله تحلیل محتوای پیام‌های XML؛ پایان‌نامه کارشناسی ارشد، دانشگاه علم و صنعت ایران، (**۱۳۸۵**).
۵. شیرانی، پریا؛ ارائه روشی برای تشخیص نفوذ در سرویس‌های وب مبتنی بر سری‌های زمانی؛ پایان‌نامه کارشناسی ارشد؛ دانشگاه علم و صنعت ایران، (**۱۳۹۱**).

6. Gomez, j, others; A Pareto-based multi-objective evolutionary algorithm for automatic rule generation in network intrusion detection Systems; Springer-Verlag, (**2012**).
7. Sharma, Amit; The Role and Use of Data Mining Techniques for Intrusion Detection Systems; International Journal of Research in IT & Management(IJRIM), Volume 2, Issue 2,p 425-430,(**2012**).
8. Srinivasu, Pakkurthi, Avadhani, P.S; Approaches and Data Processing Techniques for Intrusion Detection Systems; IJCSNS International Journal of Computer Science and Network Security, Vol.9 No.12, p 181-186, (**2009**).
9. Gareffa, Vincent, Matthew, Schwartz; Intrusions What You Need to Know; (**2008**).
10. Mohamed, M.A.; Development of Hybrid-Multi-Stages Intrusion Detection Systems; IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.3,p 69-77;(**2010**).
11. K Ranganath, Shaik, Shafia; Integrated Conditional Random Fields with the Layered Approach for Intrusion Detection; International Journal of Engineering Inventions ISSN: 2278-7461, Volume 1, Issue 4,p 68-76,(**2012**).

The Role of Intrusion Detection Systems in Web Services Security

S. Bejani[1]
M. R. Hasani Ahangar[2]
M. Akhzami[3]

Abstract

Web services play an important role in the development of service-oriented architecture and distributed architectures. Web services allow the reuse of software code and thus reduce the cost of programming and communication, they have received much attention in recent years, due to the use of the Internet as a medium of data transmission and autonomy of hardware and software platforms. On the other hand, Web services have specific security challenges. This is especially important when the organizations are dependent on the service in the form of Web services. In this case, with the weakness of the current security systems to protect Web services, these organizations are defenseless against all types of known and unknown threats that threaten Web services.Nowadays, intrusion detection systems, are well-known to complete the levels defense in cyberspace. The main purpose of this article is to conduct research on intrusion detection techniques and architectures of Web services to support passive defense issues in organizations that make use of Web services.The comparison between the architectures of intrusion detection, to achieve a high level of understanding of intrusion detection techniques in the web services, will help to improve current intrusion detection systems in the level of Web service, or to make specific intrusion detection systems for these services along with other security tools.

Key Words: *Intrusion Detection System, Web Service, Signature Based Intrusion Detection, Anomaly Based Intrusion Detection, Passive Defense*

1 . Instructor and Academic Member of the Computer Faculty, Imam Hossein Comprehensive University (sbejani@ihu.ac.ir)
2 . Assistant Professor and Academic Member of the Computer Faculty, Imam Hossein Comprehensive University (mrhassani@iust.ac.ir)
3 . M.S Candidate of Computer, Imam Hossein Comprehensive University (mostafa_akhzami@yahoo.com) - Writer in Charge