
بسم الله الرحمن الرحيم

دانشگاه آزاد اسلامی

واحد تهران مرکزی

دانشکده فنی و مهندسی، گروه مهندسی کامپیوتر

پایان‌نامه برای دریافت درجه کارشناسی ارشد (M.Sc)

گرایش : نرم‌افزار

عنوان :

مدل‌سازی عملکرد لنفوسیت‌های سیستم ایمنی بدن و کاربرد آن در سیستم‌های تشخیص نفوذ

استاد راهنما :

دکتر رضا روانمهر

استاد مشاور :

دکتر رامین نصیری

پژوهشگر :

الناز باقری نوع پرست

تابستان ۹۲

تقدیم

تقدیم به اساتید عالیقدر جناب آقایان دکتر روانمهر و دکتر نصیری

تشکر و قدردانی

با تشکر از آقای دکتر روانمهر برای زحمات فراوان و راهنمایی‌های راه‌گشای ایشان

معاونت پژوهش و فناوری

به نام خدا

منشور اخلاق پژوهش

بایاری از خداوند سبحان و اعتقاد به این که عالم محضر خداست و همواره ناظر بر اعمال انسان و به منظور پاس داشت مقام بلند دانش و پژوهش و نظر به اهمیت جایگاه دانشگاه در اعتلای فرهنگ و تمدن بشری، ما دانشجویان و اعضاء هیات علمی واحدهای دانشگاه آزاد اسلامی متعهد می گردیم اصول زیر را در انجام فعالیت های پژوهشی مد نظر قرار داده و از آن تخطی نکنیم:

۱- اصل برائت: التزام به برائت جویی از هرگونه رفتار غیر حرفه ای و اعلام موضع نسبت به کسانی که حوزه علم و پژوهش را به شائبه های غیر علمی می آلایند.

۲- اصل رعایت انصاف و امانت: تعهد به اجتناب از هرگونه جانب داری غیر علمی و حفاظت از اموال، تجهیزات و منابع در اختیار.

۳- اصل ترویج: تعهد به رواج دانش و اشاعه نتایج تحقیقات و انتقال آن به همکاران علمی و دانشجویان به غیر از مواردی که منع قانونی دارد.

۴- اصل احترام: تعهد به رعایت حریم ها و حرمت ها در انجام تحقیقات و رعایت جانب نقد و خودداری از هرگونه حرمت شکنی.

۵- اصل رعایت حقوق: التزام به رعایت کامل حقوق پژوهشگران و پژوهیدگان (انسان، حیوان و نبات) و سایر صاحبان حق.

۶- اصل رازداری: تعهد به صیانت از اسرار و اطلاعات محرمانه افراد، سازمان ها و کشور و کلیه افراد و نهادهای مرتبط با تحقیق.

۷- اصل حقیقت جویی: تلاش در راستای پی جویی حقیقت و وفاداری به آن و دوری از هرگونه پنهان سازی حقیقت.

۸- اصل مالکیت مادی و معنوی: تعهد به رعایت کامل حقوق مادی و معنوی دانشگاه و کلیه همکاران پژوهش.

۹- اصل منافع ملی: تعهد به رعایت مصالح ملی و در نظر داشتن پیشبرد و توسعه کشور در کلیه مراحل پژوهش.

تعهد نامه اصالت پایان‌نامه کارشناسی ارشد

اینجانب الناز باقری نوع پرست دانش‌آموخته مقطع کارشناسی ارشد ناپیوسته به شماره دانشجویی ۹۰۰۷۹۷۵٤۸ در رشته مهندسی کامپیوتر نرم‌افزار که در تاریخ ۹۲/۰٦/۱۷ از پایان‌نامه خود تحت عنوان: مدل‌سازی عملکرد لنفوسیت‌های سیستم ایمنی بدن و کاربرد آن در سیستم‌های تشخیص نفوذ

با کسب نمره ۱۹/۲۵ و درجه عالی دفاع نموده‌ام، بدین‌وسیله متعهد می‌شوم:

۱- این پایان‌نامه حاصل تحقیق و پژوهش انجام‌شده توسط اینجانب بوده و در مواردی که از دستاوردهای علمی و پژوهشی دیگران (اعم از پایان‌نامه، کتاب، مقاله و غیره) استفاده نموده‌ام، مطابق ضوابط و رویه‌های موجود، نام منبع مورد استفاده و سایر مشخصات آن را در فهرست ذکر و درج کرده‌ام.

۲- این پایان‌نامه قبلا برای دریافت هیچ مدرک تحصیلی (هم‌سطح، پایین‌تر یا بالاتر) در سایر دانشگاه‌ها و موسسات آموزش عالی ارائه نشده است.

۳- چنانچه بعد از فراغت از تحصیل، قصد استفاده و هرگونه بهره‌برداری اعم از چاپ کتاب، ثبت اختراع و غیره از این پایان‌نامه داشته باشم، از حوزه معاونت پژوهشی واحد مجوزهای مربوطه را اخذ نمایم.

٤- چنانچه در هر مقطع زمانی خلاف موارد فوق ثابت شود، عواقب ناشی از آن را بپذیرم و واحد دانشگاهی مجاز است با اینجانب مطابق ضوابط و مقررات رفتار نموده و در صورت ابطال مدرک تحصیلی‌ام هیچگونه ادعایی نخواهم داشت.

نام و نام خانوادگی : الناز باقری نوع پرست

تاریخ و امضاء :

بسمه تعالی

در تاریخ : ۹۲/۰۶/۱۷

دانشجوی کارشناسی ارشد خانم الناز باقری نوع پرست از پایان‌نامه خود دفاع نموده و با نمره ۱۹/۲۵ بحروف نوزده و بیست و پنج صدم و با درجه عالی مورد تصویب قرار گرفت.

امضاء استاد راهنما

فهرست مطالب

عنوان **صفحه**

فهرست جدول‌ها

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فهرست علایم و نشانه‌ها

عنوان	علامت اختصاری
میزان تطابق	α
پهنای باند اختصاص‌یافته به هر گره	β
درصد احتمال شکست سیستم	δ
درصد احتمال نفوذ کل	γ
احتمال اولیه فرضیه	h
اندیس معیارها در هر کلاس	i
اندیس کلاس معیارها	j
تعداد الگوی کارکردها و فراخوانی‌های سیستمی منطبق	k
درصد انحراف معیار رفتارهای سخت‌افزاری	C_H
درصد انحراف معیار رفتارهای نرم‌افزاری	C_S
درصد انحراف معیار رفتارهای کاربری	C_U
نمونه‌های آموزشی	D
شناسه فرمون	$ID_{Fermonea}$
درصد احتمال نفوذ هر الگوی کارکردها و فراخوانی‌های سیستمی	P_k
احتمال اولیه مشاهده	$P(D)$
احتمال قبل از مشاهده داده‌های آموزشی	$P(h)$
احتمال ثانویه فرضیه	$P(h\|D)$
میزان حساسیت درخواست	S
نمره کل وزن‌دار برای هر کلاس معیار	S_j
نمره بدون وزن برای هر معیار در هر کلاس	U_{ij}
نمره واقعی معیار	W_{ij}

فصل ۱- مقدمه

۱-۱- پیشگفتار

از آنجا که در دنیای امروز، فن‌آوری شبکه‌های ارتباطی و کاربردهای آن منجر به ایجاد تحولات چشمگیری در فرایندهای اقتصادی، اجتماعی و فرهنگی شده است؛ به طوری که برخی از روال‌های مرسوم قبلی منسوخ و جای خود را به شیوه‌های مرسوم هزاره سوم یا به اصطلاح مجازی داده است. از این رو شبکه‌های کامپیوتری نقشی اساسی در پیشبرد این فرایندها ایفا می‌کنند.

مقوله ارتباطات شبکه‌ای به همان اندازه که جذاب و موثر است، در صورت عدم رعایت اصول امنیت به همان میزان و یا شاید بیشتر، نگران‌کننده و مسئله‌آفرین خواهد بود؛ و پول و تجارت الکترونیک، خدمات به کاربران خاص، اطلاعات شخصی، اطلاعاتی عمومی و نشریات الکترونیک همگی در معرض دستکاری و سوءاستفاده‌های مادی و معنوی قرار خواهند گرفت. از این رو بحث امنیت در سال‌های اخیر به میزان قابل توجهی تکامل یافته است و سالانه هزینه‌های هنگفتی صرف آن می‌شود. این حوزه، موضوعات تخصصی گوناگونی از جمله تامین امنیت سیستم‌ها و زیرساخت‌ها، تامین امنیت برنامه‌های کاربردی و پایگاه‌داده‌ها، تست امنیت، حسابرسی و بررسی سیستم‌های اطلاعاتی، برنامه‌ریزی تداوم تجارت و بررسی جرائم الکترونیکی، و غیره را در بر می‌گیرد.

جهت تضمین امنیت لازم است که از اطلاعات انتقالی در سطح شبکه (پیام‌ها) در مقابل دسترسی، تغییر و انتشار غیرمجاز حفاظت گردد. همچنین خود اتصال باید به صورتی امن بنا شده و در طی انتقال اطلاعات امن بماند. جلوگیری از ترافیک غیرقانونی، یکی از اهداف ارتباطات امن است که از دست‌یابی بیگانگان به اطلاعاتی چون اهداف و رفتار کاربران شبکه جلوگیری می‌کند. مدیران امنیتی جهت دست‌یابی به این هدف، از روش‌های گوناگونی بهره می‌برند. اگرچه این روش‌ها در موارد بسیاری پرکاربرد هستند اما محدودیت‌هایی نیز دارند. برای مثال دیواره‌های آتش ممکن است به گونه‌ای تنظیم شده باشند که انواع مشخصی از ترافیک را بلوکه کنند اما نفوذگران همچنان قادر به یافتن راهی برای استفاده از ترافیک غیرقانونی جهت نیل به اهدافشان هستند. از این رو نیاز به تشخیص نفوذ بوجود می‌آید تا در صورت عبور نفوذگر از سدهای دفاعی، بتوان در اولین فرصت و به محض شروع عملیات مخرب نفوذگر، به تشخیص نفوذ پرداخت و در مقابل آن واکنش نشان داد.

۱-۲- تاریخچه

از آنجا که شبکه‌های مبتنی بر سیستم‌های کامپیوتری به طور فزاینده نقش حیاتی در جامعه مدرن را بر عهده دارند، به هدف مجرمانی چون هکرها و یا نفوذگرها تبدیل شده‌اند. این نفوذگرها با استفاده از روش‌های مختلف از جمله استفاده از بدافزارها سعی در دستیابی به اهداف بدخواهانه خود دارند. با توجه به بررسی‌های گروه پاسخ‌گویی حوادث رایانه‌ای، در چند سال اخیر میزان حملات اینترنتی به بیش از دو برابر رسیده است. این در حالی است که گزارش سایت بین‌المللی ثبت رکوردهای هک جهان [۱] نشان می‌دهد که در حدود یک میلیون و پانصد حمله در سال ۲۰۱۰ به وب‌سایت‌ها و شبکه‌ها صورت پذیرفته است. این سرعت گسترش حمله به همراه پیچیدگی آن، بر نیاز به مکانیزم‌های واکنشی پیچیده و بروز امنیتی تاکید دارد. از این رو در صنعت فناوری اطلاعات اولین عاملی که موفقیت یک سیستم را تضمین می‌کند تشخیص نفوذ و برقراری امنیت است.

در طول دو دهه گذشته، راهبردها و روش‌های بسیاری جهت برقراری امنیت در این سیستم‌ها توسعه یافته‌اند[۲]. اولین تحقیقات در تشخیص نفوذ به وسیله کامپیوتر در دهه ۸۰ صورت پذیرفته است[۳]. بیشتر سیستم‌های تشخیص نفوذ قدیمی، متمرکز و با معماری یکپارچه بودند. اطلاعات در یک ماشین جمع‌آوری شده و از طریق جستجوی فایل‌های تاریخچه وقایع و یا جریان ترافیک شبکه، در آن ماشین تحلیل می‌شدند، که نواقصی را در مورد ساختار و تکنولوژی تشخیص از جمله سربار سرویس‌دهنده[1] و هشدارهای بی‌شمار به همراه داشتند. از این رو ظرفیت تحمل کاذب مثبت و درستی پاسخ به خروجی در این سیستم‌های تشخیص نفوذ قابل بحث است[۲]. برخی بر این باورند که سیستم‌های تشخیص نفوذ سنتی نه تنها یک لایه امنیتی اضافی را به سیستم‌ها افزوده‌اند، بلکه به همراه آن، پیچیدگی مدیریت امنیت را نیز به کار اضافه کرده‌اند. بنابراین، روش‌های توزیع‌شده تشخیص نفوذ بوجود آمدند. در حال حاضر سیستم‌های تشخیص نفوذ توزیع‌شده، جهت جمع‌آوری داده‌ها عمدتا از عامل‌های توزیع‌شده استفاده می‌کنند و سپس این اطلاعات به مرکز پردازش ارسال و در آنجا تجزیه و تحلیل می‌گردد. با این حال، این مدل دارای مشکلاتی از جمله عدم توانمندی تشخیص در زمان اجرا و نیز تبدیل پردازشگر مرکزی به گلوگاه و به نقطه شکست سیستم[2] توزیع‌شده می‌باشد، که در نتیجه، تاخیر در دریافت و پردازش اطلاعات، و تشخیص نفوذ را به همراه دارد. به منظور غلبه بر کاستی‌های روش‌های تشخیص نفوذ فعلی، سیستم‌ها نیازمند مدیریتی

[1] Server
[2] Single Point of Failure

غیرمتمرکز هستند که به صورت گسترده در سطح شبکه به تشخیص نفوذ و برقراری امنیت (قطع یک ارتباط، کشتن یک پردازش و غیره) بپردازد.

۱-۳- شیوه‌های نوین

ایده‌ی محاسبات خودمختار[1] ابتدا در سال ۱۹٤۰ توسط نوربرت وینر[2] ارائه گردید[٤]. سال ۲۰۰۱ پال هورن[3] با الهام از عملکرد اعضای بدن ایده محاسبات خودمختار را مطرح نمود[٥]. هدف از محاسبات خودمختار ارائه سیستمی با قابلیت خود-مدیریتی[4] است به نحوی که عناصر یک مجموعه بتوانند با تعامل با یکدیگر و بدون نیاز به عنصر مرکزی امور واگذارشده را بدون دخالت عنصر خارجی انجام دهند. با توجه به اینکه سیستم ایمنی زیستی یکی از سیستم‌های خودمختار در بدن انسان است که بدون دخالت مغز به برقراری ایمنی در بدن می‌پردازد[٦]، می‌توان با الهام از عملکرد عناصر خودمختار این سیستم به خصوص لنفوسیت‌ها[5]، به طراحی سیستمی امنیتی در سیستم‌های توزیع‌شده پرداخت.

۱-٤- هدف از انجام تحقیق

هدف از این تحقیق، ارائه یک سیستم پیشنهادی با الهام از سیستم ایمنی زیستی بر اساس عامل‌های[6] خودمختار می‌باشد که این عامل‌ها با همکاری یکدیگر به برقراری امنیت در شبکه می‌پردازند. از طرفی این عامل‌ها قابلیت یادگیری و بروزرسانی دانش خود را داشته و با توجه به تعاملاتی که با یکدیگر دارند قادر به تبادل دانش می‌باشند. بدین‌ترتیب در سیستم پیشنهادی نیاز به مدیریت متمرکز، بروزرسانی سیستم امنیتی و همچنین نگهداری تاریخچه عملیات[7] رفع ناهنجاری (جهت بکارگیری در رفع ناهنجاری‌های مشابه) برطرف می‌گردد.

۱-٥- نوآوری تحقیق

با الهام از عملکرد لنفوسیت‌های سیستم ایمنی بدن، می‌توان مدلی چند-عاملی را جهت تشخیص نفوذ در سیستم‌های توزیع‌شده ارائه نمود، به نحوی که عامل‌های آن بتوانند با تعامل با یکدیگر و بدون نیاز به عنصر

[1] Autonomic Computing
[2] Norbert Wiener
[3] Paul Horn
[4] Self Management
[5] Lymphocyte
[6] Agent
[7] Log

مرکزی به تشخیص نفوذ در سطح سیستم‌های توزیع‌شده بپردازند. بدین‌ترتیب سربار اضافی به یک سیستم مرکزی تحمیل نشده و با توجه به امکان تبادل اطلاعات و کسب دانش عامل‌ها، نیاز به بروزرسانی این سیستم بوجود نمی‌آید.

۱-٦- ساختار گزارش

در فصل آتی، ابتدا به تعریف امنیت و مولفه‌های موثر در تامین آن پرداخته شده و سپس مفاهیمی چون نفوذ، نفوذگر و اهداف نفوذ به سیستم‌ها و شبکه‌ها مورد بررسی قرار می‌گیرد. سپس انواع نفوذ و کدهای مخربی که ممکن است در انواع نفوذ مورد استفاده قرار گیرد بررسی می‌گردد. همچنین مروری کلی بر روی انواع دسته‌بندی سیستم‌های تشخیص نفوذ، معیارهای ارزیابی این سیستم‌ها و پیشینه تحقیق انجام می‌گیرد. فصل سوم، مفاهیم پایه محاسبات خودمختار و خصوصیات یک سیستم خودمختار را ارائه می‌دهد. همچنین در این فصل سیستم ایمنی زیستی به عنوان یک سیستم خودمختار معرفی می‌گردد. سپس، سیستم ایمنی مصنوعی که از سیستم ایمنی زیستی الهام گرفته شده به همراه الگوریتم‌های آن توضیح داده می‌شود. از آنجا که الگوریتم‌های سیستم ایمنی مصنوعی به تنهایی قادر به ارائه خصوصیات یک سیستم خودمختار نمی‌باشند، سیستم‌های چند-عاملی -که قادر به ارائه برخی از این خصوصیات هستند- به همراه کاربرد آنها در سیستم‌های تشخیص نفوذ در این فصل مورد بررسی قرار می‌گیرند. در فصل چهارم، مروری مختصر بر کلونی مورچگان و شبکه بیزین انجام می‌گیرد. و در نهایت در فصل پنجم مدل پیشنهادی ارائه، شبیه‌سازی و ارزیابی می‌گردد. فصل ششم به نتیجه‌گیری کلی و معرفی پیشنهادات می‌پردازد.

فصل ۲- ادبیات تحقیق

۲-۱- مقدمه

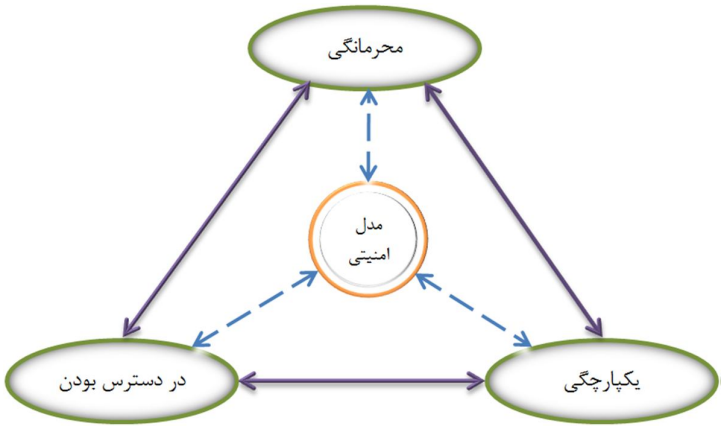
پیشرفت‌های کنونی تکنولوژی‌های مدرن منجر به استفاده از سیستم‌های کامپیوتری در طیف وسیعی از امور از جمله عملیات تجاری، و جمع‌آوری و به‌اشتراک‌گذاری اطلاعات در دانشگاه‌ها و شرکت‌ها از طریق اینترنت شده است. امروزه بسیاری از عملیات بانکی از طریق شبکه صورت می‌گیرد، عده‌ای از شرکت‌ها و کارخانه‌ها محصولات خود را در سایت‌های اینترنتی عرضه می‌کنند و بسیاری از ارتباطات از طریق مکاتبات الکترونیکی صورت می‌پذیرد. داده‌هایی که از این طریق در انواع کسب‌وکارها مبادله می‌شود، عموما داده‌هایی هستند که حفظ امنیت آنها منجر به پابرجا ماندن آن کسب‌وکار می‌گردد و در صورتی که این اطلاعات مورد سوءاستفاده قرار گیرند، می‌توانند زیان‌های جبران‌ناپذیری را برای صاحبان آن به همراه بیاورند. از این رو در این فصل به ارائه توضیحات بیشتر درباره امنیت، نفوذ و راه‌های مقابله با آن پرداخته می‌شود.

۲-۲- امنیت[1]

اگر بخواهیم به طوری کلی به مفهوم امنیت بنگریم می‌توانیم آن را حفاظت از افراد یا اشیاء در برابر خطر، آسیب، از دست دادن، و سوءاستفاده تعریف کنیم. مفهوم امنیت در شاخه‌های علمی مختلفی کاربرد دارد، اما امروزه به خاطر حساسیت بیشتر برخی از این شاخه‌ها از جمله علوم اجتماعی، علوم سیاسی و فناوری اطلاعات، شکل پررنگ‌تری به خود گرفته است. در شاخه فناوری اطلاعات، امنیت به معنای امنیت منابع موجود در کامپیوترها و شبکه‌ها است. به عبارت دیگر، حفاظت، پشتیبانی و نگهداری از منابع سخت‌افزاری و نرم‌افزاری (اطلاعات مهم، برنامه‌های حساس، نرم‌افزارهای مورد نیاز)، امنیت نامیده می‌شود. از این رو حفاظت از منابع که شامل برقراری ویژگی‌های یکپارچگی[2]، محرمانگی[3]، و دردسترس‌بودن[4] منابع ارائه‌شده توسط سیستم کامپیوتری می‌باشد[۷ و ۸]، یکی از ابعاد مورد توجه در علوم کامپیوتر به شمار

[1] Security
[2] Integrity
[3] Confidentiality
[4] Availability

می‌آید. همانطور که در شکل ۲-۱ [۹] نشان داده شده است، این سه ویژگی به عنوان اهداف عمومی[۱۰] مدل‌های امنیتی تحت عنوان سه‌گانه CIA شناخته می‌شوند.



شکل ۲-۱ سه‌گانه CIA

محرمانگی به معنای جلوگیری از افشای غیرمجاز اطلاعات حساس است، به طوری که تنها افراد با حق دسترسی مجاز بتوانند به این اطلاعات دست یابند. محرمانگی مهمترین ویژگی سه‌گانه CIA است، زیرا که این ویژگی بیشتر از سایرین مورد تهدید و حمله قرار می‌گیرد[۹]. از جمله مکانیزم‌های حفاظت از محرمانگی، رمزنگاری[۱] و کنترل‌دسترسی[۲] می‌باشند[۱۱]. منظور از رمزنگاری تبدیل اطلاعات به فرمی است که به غیر از کاربر مجاز، شخص دیگری نتواند از آن اطلاعات استفاده کند، حتی اگر به آن دسترسی داشته باشد. برای مثال در تراکنش‌های آنلاین بانکی، لازم است که جزئیات حساب کاربر مانند رمزعبور به صورت رمزنگاری‌شده از میان رسانه‌های اشتراکی شبکه منتقل شود تا در طول مسیر انتقال مورد تجاوز و سوءاستفاده قرار نگیرد[۹]. کنترل‌دسترسی نشان می‌دهد که تنها افراد و یا ابزارهای مجاز با سطوح دسترسی مختلف، اجازه دسترسی و استفاده از منابع سخت‌افزاری و نرم‌افزاری مختلفی را در سطح شبکه دارند که این اجازه دسترسی و استفاده بر اساس سطح دسترسی آنها مشخص شده است.

یکپارچگی به اصل امانت‌داری و صیانت از اطلاعات اشاره دارد به طوری که از تغییرات غیرمجاز و نامناسب اطلاعات جلوگیری نموده و صحت و تمامیت اطلاعات را حفظ نماید. یکپارچگی در زمینه امنیت اطلاعات نه تنها یکپارچگی خود اطلاعات، بلکه یکپارچکی منابع اطلاعاتی را در بر می‌گیرد[۱۱]. به بیان دیگر، یکپارچگی از تغییرات غیرمجاز در داده، سیستم‌ها و اطلاعات جلوگیری می‌کند تا صحت اطلاعات و عملکرد سیستم‌ها تضمین شود[۹]. مکانیزم‌های حفاظت از یکپارچگی به دو دسته مکانیزم‌های پیشگیری و

[1] Cryptography
[2] Access Control