سامانه‌های تشخیص نفوذ در رایانش ابری

مؤلفان:

مونا رافضـــــی

سیدامیر سیدحسینی

سرشناسه: رافضی، مونا، ۱۳۶۴ -

عنوان و نام پدیدآورندگان: سامانه‌های تشخیص نفوذ در رایانش ابری/ مونا رافضی، سیدامیر سیدحسینی.

مشخصات نشر: تهران - اندیشگان- ۱۳۹۵

مشخصات ظاهری: ۱۰۲ ص.: جدول، نمودار.

شابک: ۹۷۸-۶۰۰-۸۳۰۰-۴۱-۰

وضعیت فهرست نویسی: فیپا

یادداشت: کتابنامه: ص. [۹۷] - ۱۰۲.

موضوع: محاسبات ابری

شناسه افزوده: سیدحسینی، سیدامیر، ۱۳۶۳ -

رده‌بندی کنگره ۱۳۹۵ ۲ر۳م/QA ۷۶/۵۸۵

رده‌بندی دیویی ۰۰۴/۶۷

شماره کتابشناسی ملی: ۴۲۲۶۹۵

انتشارات اندیشگان با حمایت مالی کانون همیاری نور آفرینش

سامانه‌های تشخیص نفوذ در رایانش ابری

مونا رافضی، سیدامیر سیدحسینی

ناظر فنی

صدیقه صمدیان

نوبت چاپ: بهار ۱۳۹۵

شمارگان: ۱۰۰۰

قیمت: ۱۰۰۰۰۰ ریال

آدرس: تهران - میدان انقلاب اسلامی - خیابان کارگر شمالی بالاتر از نصرت - پلاک ۱۱۵۰

تلفن: ۶۶۵۶۹۸۹۱ و ۶۶۹۳۱۶۶۹ دورنگار: ۸۹۷۸۴۵۵۸

وب سایت: www.hamyari.co

فهرست مطالب

پیشگفتار

امروزه با پیشرفت فناوری اطلاعات و ارتباطات در حوزه اینترنت، مقوله جدیدی با عنوان رایانش ابری پا به‌عرصه وجود گذاشته است. رایانش ابری مدلی جهت ارائه دسترسی مناسب و دلخواه به‌مجموعه‌ای اشتراکی از منابع پردازشی قابل پیکربندی است که در هر زمان و مکانی به‌طور مناسب و از طریق شبکه امکان‌پذیر می‌باشد. شبکه‌ها، سرورها، محل‌های ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها می‌توانند مثال‌هایی از این منابع باشند که به‌سرعت در دسترس قرار می‌گیرد و با حداقل تلاش‌های مدیریتی و تعامل آزاد می‌شود.

با توجه به روند روز افزون تکنولوژی‌ها و تنوع نیاز کاربران در حوزه فناوری اطلاعات، جایگاه رایانش ابری کاربری بیشتری پیدا می‌کند. چرا که گسترش زیر ساخت محاسباتی در هر سازمان نیازمند صرف هزینه‌های زمان و نیروی انسانی بسیاری است که گاهی در توان عملیاتی یک سازمان نمی‌گنجد. از این رو سازمان‌ها برای پیشبرد اهداف خود تمایل به استفاده از چنین تکنولوژی‌هایی دارند.

پرداخت بر مبنای استفاده، مقیاس‌پذیری، استفاده از تکنولوژی اینترنت در هر زمان و مکان، سلف سرویس بودن بر مبنای تقاضا، کارایی بالا، پیاده‌سازی سریع، نگهداری و به‌روزرسانی آسان را می‌توان به‌عنوان مزایای کلیدی در رایانش ابری نام برد. همچنین می‌توان از مواردی نظیر بازیابی اطلاعات، عدم وجود کنترل کامل بر سرورهای ابر، مشکلات حقوقی توافقنامه سطح سرویس، معماری متفاوت، حسابرسی، بررسی و ارزیابی نحوه عملکرد محیط رایانش ابری، به‌عنوان عمده معایب در رایانش ابری نام برد.

با وجود صرفه‌جویی منابع در رایانش ابری که به‌کاربران وعده داده شده است و سایر مزایایی که در بالا به‌آن‌ها اشاره شد کاربران از تهدیدات امنیتی واهمه دارند. در این کتاب سعی ما بر این است تا پس از بررسی چالش‌های امنیتی موجود در رایانش ابری به‌مطالعه سیستم‌های تشخیص نفوذ در این حوزه بپردازیم. سیستم‌های تشخیص نفوذ می‌توانند به‌عنوان ابزاری گران‌بها در چالش‌های امنیتی سیستم‌ها و داده‌های ذخیره شده به‌کار روند که هدف اصلی آن‌ها تشخیص به‌موقع فعالیت‌های مخرب و جلوگیری از خرابی‌های بیشتر جهت حفاظت از سیستم‌ها می‌باشد.

ساختار توزیع شده و باز در رایانش ابری و سرویس‌های آن موضوعی جذاب و پتانسیلی برای حملات سایبری توسط مهاجمان است. معماری سرویس در رایانش ابری شامل سه لایه است که به‌یکدیگر وابسته‌اند و شامل زیرساخت، بستر و برنامه‌های کاربردی می‌باشد. هر لایه می‌تواند آسیب‌پذیری‌های مشخصی داشته باشد که توسط برنامه‌نویسی‌های مختلف یا خطاهای پیکربندی کاربر یا سرویس دهنده به وجود می‌آید. سیستم رایانش ابری می‌تواند با تهدیدات مختلفی مواجه شود که صحت، محرمانگی و دسترس‌پذیری منابع داده و زیرساخت‌های مجازی‌سازی شده را به‌خطر می‌اندازد. مشکل زمانی بدتر می‌شود که ابر با محاسبات و ظرفیت ذخیره‌سازی بالا توسط نفوذگر داخلی مورد تهاجم قرار گیرد.

کمبود کنترل کامل در زیرساخت نگرانی اصلی برای مشتریان سرویس‌های ابری می‌باشد. واضح است که بخش سیستم‌های تشخیص نفوذ حفاظت از اطلاعات کابر در رایانش ابری است. با توجه به ماهیت پیچیده و بازبودن محیط‌های رایانش ابری سیستم‌های تشخیص و جلوگیری از نفوذ سنتی ناکارآمد هستند بنابراین باید از ترکیبی از سیستم‌های مختلف استفاده کرد. در این کتاب سعی بر آن است تا ده‌بندی‌های مختلفی از سیستم‌های تشخیص نفوذ معرفی و نیازمندی‌های ضروری که باید سیستم‌های تشخیص نفوذ در محیط ابری به‌کار گرفته شوند و روش‌ها و تکنیک‌هایی که این نیازمندی‌ها را پوشش می‌دهد، بررسی شود.

مقدمه

دنیای فناوری اطلاعات و اینترنت که امروزه تبدیل به‌جزئی حیاتی از زندگی بشر شده، روز به‌روز در حال گسترش است. همسو با آن، نیازهای اعضای جوامع مانند امنیت اطلاعات، پردازش سریع، دسترسی پویا و آنی، قدرت تمرکز روی پروژه‌های سازمانی به‌جای اتلاف وقت برای نگهداری سرورها و از همه مهم‌تر، صرفه‌جویی در هزینه‌ها اهمیت زیادی یافته است. راه‌حلی که امروزه در عرصه فناوری برای چنین مشکلاتی پیشنهاد می‌شود فناوری است که این روزها با نام رایانش ابری[1] (محاسبات ابری، پردازش ابری) پرداخته می‌شود.

رایانش ابری مدلی است برای داشتن دسترسی فراگیر، آسان و بنا به‌سفارش شبکه به‌مجموعه‌ای از منابع پردازشی پیکربندی‌پذیر (نظیر: شبکه‌ها، سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها) که بتوانند با کمترین کار و زحمت یا نیاز به‌دخالت فراهم‌کننده سرویس به‌سرعت فراهم شده یا آزاد (رها) گردند.

به‌طور خلاصه به‌وسیله‌ی رایانش ابری شرکت‌ها، کاربران سرویس‌های فناوری اطلاعات، می‌توانند سرویس‌های مرتبط با فناوری اطلاعات خود به‌عنوان سرویس بخرند؛ به‌جای خرید سرورها برای سرویس‌های درونی یا برونی، یا خرید مجوز نرم‌افزارها، شرکت‌ها می‌توانند آن‌ها را به‌عنوان سرویس بخرند.

رایانش ابری راهی برای افزایش ظرفیت ذخیره‌سازی یا امکانات، بدون هزینه کردن برای زیرساخت جدید، آموزش پرسنل جدید، یا خرید مجوز نرم‌افزار جدید می‌باشد؛ در واقع شرکت‌ها یا افراد تنها برای آنچه مصرف می‌کنند پول خواهند داد. بنابراین راهی مؤثر برای استفاده از منابع، مدیریت سرمایه و هزینه‌های پشتیبانی فناوری است.

ساختار کاملاً باز و توزیع شده در رایانش ابری و سرویس‌های آن موجب می‌شود تا هدفی جذاب برای مهاجمان باشد. این ساختار شامل پارادایم‌های سرویس‌گرا و توزیع شده مِش چندگانه، اجاره چندگانه، دامنه‌های چندگانه و ساختارهای مدیریتی خودمختار چند کاربره می‌باشد که مستعد تهدیدات امنیتی و آسیب‌پذیری بیشتری‌اند.

معماری سرویس در رایانش ابری از ترکیب سه لایه وابسته به‌هم به‌نام‌های زیرساخت[2]، سکو

---

1. Cloud Computing
2. Infrastructure

یا بستر[1] و برنامه[2] تشکیل شده است که با خطاهای پیکربندی متفاوتی که توسط کاربر یا فراهم کننده سرویس ایجاد می‌شود.

یک سیستم رایانش ابری می‌تواند با چندین تهدید متفاوت رو به‌رو شود که شامل تهدیدات یکپارچگی (صحت)، محرمانگی و دسترس‌پذیری منابع، داده و زیرساخت‌های مجازی سازی شده که به‌عنوان بستری برای حملات جدید می‌باشد. یکی از روش‌های شناسایی حملات استفاده از سیستم‌های تشخیص نفوذ می‌باشد و هدف از این کتاب بررسی راهکارهای مختلف ارائه شده در مورد سیستم‌های تشخیص نفوذ در محیط رایانش ابری می‌باشد.

1. Platform
2. Application