بهبود معماری امنیت خدمات اساسی در محاسبات ابری

رحیم یزدانی[1]، محمود دی پیر[2]
[1]دانشجوی دکتری، دانشگاه عالی دفاع ملی، تهران، ایران
r.yazdani@sndu.ac.ir
[2]عضو هیئت‌علمی دانشگاه شهید ستاری، تهران، ایران
mdeypir@chmail.ir

چکیده

سازمان‌ها برای امن‌سازی دارایی‌های اطلاعاتی‌شان، بایستی از معماری امنیتی سازمان بهره ببرند. الگوهای امنیتی روش خوبی برای ساختن و آزمودن سازوکارهای جدید امنیتی است. به‌عنوان مثال الگوی امنیت سازمانی، نمونه‌ای از معماری مدل‌محور است که در پی حل مشکلات امنیتی سامانه‌های اطلاعاتی است. در این پژوهش کاربردی با رویکرد کیفی و روش پژوهش توصیفی تحلیلی، با مطالعه مبانی نظری و مصاحبه با خبرگان نمونه‌ای از الگوی امنیت سازمانی مدل‌محور درقالب Software as a Service امن، تبیین می‌شود تا سازمان‌ها موقع برون‌سپاری برای حفاظت از دارایی اطلاعاتی‌شان مورد بهره‌برداری قرار دهند. همچنین یکی از کاربردهای رایانش ابری، استفادهٔ مؤثر از منابع محاسباتی است؛ ولی مباحث امنیتی مرتبط با آنها مانعی برای سازمان‌ها و افراد است. در این پژوهش، به بررسی مشکلات امنیتی ابرهایی که سکو را به‌عنوان خدمت عرضه می‌کنند نیز پرداخته می‌شود. این مشکلات که در زمینهٔ کنترل دسترسی، حریم خصوصی، پیوستگی خدمات، حفاظت هم‌زمان از کاربر و ارائه‌دهنده است، احصا و طبقه‌بندی‌شده و اقدامات متقابل لازم مورد بحث قرار می‌گیرد.

واژگان کلیدی: الگوی امنیتی سازمانی، محاسبات ابری، معماری امنیت

۱- مقدّمه

در سال‌های اخیر برون‌سپاری به‌عنوان خدمت نرم‌افزاری برخط عمومیت پیدا کرده است. این نرم‌افزار برخط با نام SaaS [1]شناخته می‌شود که شامل یک برنامه کامل است و به‌صورت یک خدمت برحسب تقاضا فراهم می‌شود [۱]. تمرکز SaaS بر جداسازی مالکیت و کاربری نرم‌افزار است. این مدل خدمت برخط ارزان‌تر از حالتی است که سامانه‌های فناوری اطلاعات در اختیار خود سازمان باشد و با توجه به این که شرکت‌ها در پی صرفه‌جویی در هزینه‌های به‌روزرسانی، نیروی انسانی و زیرساخت‌های فناوری اطلاعات و پیاده‌سازی هستند و این مزایا در SaaS وجود دارد، لذا کاربرد بی‌شماری بر SaaS مترتب است؛ اما این محیط جدید تهدیدهایی را با خود به‌همراه دارد. نمونه‌هایی از راه‌حل‌ها (الگوی امنیت سازمانی SaaS امن) وجود دارند. هر سازمان موقع انتخاب هر کدام از نمونه‌ها، بایستی مخاطرات را بررسی کند؛ زیرا اتخاذ الگو تأثیر مستقیم بر امنیت دارد. الگوی امنیتی سازمانی مدل‌محور در قالب SaaS امن، کمک می‌کند که موقع برون‌سپاری، دارایی‌های اطلاعاتی سازمان‌ها (داده، برنامه‌های کاربردی، کد، پیکربندی) تضمین شود. چهار مدل در این راه حل وجود دارند [۷]: مدل مستقل محاسباتی[2] (CIM)، مدل مستقل سکو[3] (PIM)، مدل مشخصی از سکو[4] (PSM)، مدل وابسته تولید[5] (PDM).

در CIM، توصیفی از خط‌مشی‌های امنیتی ارائه می‌شود. در PIM، توصیف مفهومی از سازوکارهای امنیتی مطرح می‌شود که باید با سامانه آمیخته شود و مستقل از جزییات اجرایی و مشخصه‌های فنی است. در PSM، توصیف مؤلفه‌های معماری امنیتی مطرح است و به چگونگی ایجاد

[1]Software as a Service

[2]Computationally Independent Model
[3]Platform Independent Model
[4]Platform Specific Model
[5]Product Dependent Model

سازوکارهای امنیتی در داخل معماری می‌پردازد. در PDM، لازم است PSM در معماری فناورانه خاصی دیده شود. با این رویکرد ما از طرفی می‌توانیم عناصر امنیتی را در مدل‌های مختلف به‌طور مجزا مدیریت کنیم و از طرفی تبدیلات خودکار بین آنها انجام دهیم.

در بخش نخست پژوهش حاضر، الگوی امنیتی سازمانی مدل‌محور بیان و سپس این الگو در قالب SaaS امن تبیین می‌شود، تا سازمان‌ها از این الگو برای حفاظت از دارایی‌های اطلاعاتی‌شان موقع استفاده از SaaS بهره برند. در بخش دوم امنیت ابرهای PaaS از منظرهای مختلف شامل کنترل دسترسی، حریم خصوصی، پیوستگی خدمات همراه با حفاظت توامان از ارائه‌دهنده و کاربر بحث می‌شود. مشکلات امنیتی احصا شده و طبقه‌بندی می‌شود و اقدامات لازم پیشنهاد شده است.

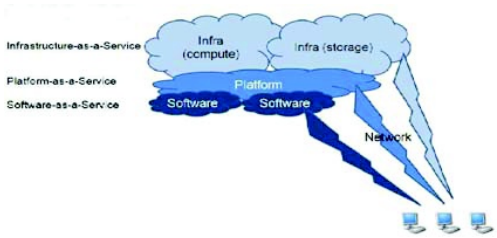
در بخش دوم پژوهش، مخاطرات امنیتی فنی ابرهایی که سکو را به‌عنوان یک خدمت عرضه می‌کنند (PaaS)[1] تعریف و طبقه‌بندی شده و راه حل‌های عملی پیشنهاد شده است. معماری‌های متمرکزشده ناشی از گستردگی اشیا بر روی میزبان‌های ابر چالش امنیتی مهمی ذکر شده است. درحالی که مواردی مانند شناوری منابع والاستیسیته سریع که منجر به مشکلات تعاملی منابع ناهمگن و آسیب‌پذیری میزبان‌ها و اشیا می‌شوند، مشکل امنیتی می‌باشند. البته برای کاهش مشکلات راه حل‌هایی ارائه شده است؛ مانند «رمزنگاری بخش‌های حساس» و «اجرای کدهای تحلیل کننده رخنه عملیاتی بر روی هر میزبان» که به‌عنوان یک لایهٔ امن بر روی سامانه عامل نشسته و یک واسط برنامه‌نویسی کاربردی استاندارد برای اشیای کاربر ارائه می‌دهد. همچنین به‌منظور دسترسی به شبکه وسیع در PaaS باید دو نیازمندی محرمانگی ارتباط و کنترل دسترسی (احراز هویت، مجازشناسی و قابل ردیابی) مد نظر قرار گیرد. بدین منظور راه حل‌های «امنیت لایه انتقال»، «خط مشی‌های سخت گیرانه کنترل دسترسی»، «خط مشی‌های همراه با اشیا» و «پروتکل گزارش‌گیری غیرقابل‌انکار» ارائه شده است.

پنج مشخصهٔ ضروری برای ابرها عبارتند از: خودسرویس مبتنی بر تقاضا (کاربر ابر نیازی به تراکنش انسانی با ارائه‌دهنده ابر ندارد) – دسترسی شبکه‌ای وسیع (دسترسی آسان و شبکه‌ای به‌منابع ابر)- سیال‌بودن منابع (منابع محاسباتی بین چندین کاربر به اشتراک گذاشته می‌شود)- الاستیسیته سریع (براساس تقاضا منابع ارائه شده به‌سرعت مقیاس پذیرند) – خدمات قابل اندازه‌گیری (نظارت بر استفاده از منابع).

در ابر PaaS، کاربر مجاز به ذخیره‌سازی داده یا اجرای برنامه کاربردی است. منابع بین چندین کاربر به اشتراک گذاشته می‌شود؛ درحالی که اشیای آنها ذخیره‌شده و یا درحال اجرا است. ابر از میزبان‌های متعددی تشکیل شده که میزبان اشیای کاربران هستند. منابع به‌طور الاستیسیته از طریق اختصاص اشیا به میزبان‌ها و مهاجرت اشیا بین میزبان‌ها به اشتراک گذاشته می‌شوند؛ لذا مخاطرات امنیتی ابرهای PaaS بررسی و راه حل‌های متناظر نشان داده شده است. برای این منظور جزییات مشکلات امنیتی ناشی از سیال‌بودن منابع و الاستیسیته سریع و دسترسی شبکه‌ای وسیع، احراز هویت آگاه از حریم خصوصی و پیوستگی خدمات بررسی و راه حل‌های متناسب با این مشکلات پیشنهاد شده است.

۲- ادبیات پژوهش

رایانش ابری فرایند محاسباتی است که در آن خدمات برروی یک شبکه و از طریق منابع محاسباتی تحویل داده و به‌کمک مجازی‌سازی با ایجاد یک لایهٔ انتزاعی بر روی کلیه منابع امکان مدیریت منابع حاصل می‌شود [۱]. برای مثال، اگر سازمانی نیاز به قدرت محاسباتی بالا داشته باشد، می‌تواند به‌راحتی آن را از طریق سرور مجازی در ابر به‌صورت برخط خریداری کند؛ به‌طوری که سرورها به‌سرعت با واسط برنامه‌نویسی کاربردی[2] قابل راه‌اندازی هستند [۸]. سه نوع اصلی از مدل‌های خدمات وجود دارند [۹]. شکل ۱ مدل خدمات رایانش ابری را نشان می‌دهد که شامل نرم‌افزار به‌عنوان یک خدمت (SaaS)، سکو به‌عنوان یک خدمت (PaaS) و زیرساخت به‌عنوان یک خدمت (IaaS) است.



(شکل ۱): مدل خدمات رایانش ابری [۹]

[1]Platform as a Service

[2]Application Programming Interface

مدل خدمات رایانش ابری از سه مدل سرویس‌دهی، چهار مدل استقرار و پنج ویژگی ضروری تشکیل شده است. سه مدل سرویس‌دهی عبارتند از: نرم‌افزار به‌عنوان سرویس، سکو به‌عنوان سرویس و زیرساخت به‌عنوان سرویس. چهار مدل استقرار عبارتند از: ابر خصوصی، ابر گروهی، ابر عمومی و ابر ترکیبی. همچنین پنج ویژگی شامل خدمات مستقیم در هنگام نیاز، دسترسی وسیع شبکه، کشش سریع، انعطاف پذیری سریع و اندازه‌گیری خدمات می‌باشند [۳].

مدل‌های تجاری از SaaS و نرم‌افزارهای کاربردی و پایگاه داده استفاده می‌کنند. زیرساخت و سکوهایی که این برنامه‌ها بر روی آن‌ها اجرا می‌شود، به‌وسیله ارائه‌دهندهٔ ابر مدیریت می‌شوند. SaaS به‌عنوان نرم‌افزار تقاضامحور نیز شناخته می‌شود و باعث کاهش هزینه‌های عملیاتی فناوری اطلاعات از طریق برون‌سپاری می‌شود. برای اتصال کاربر نهایی به برنامه‌های کاربردی ابرپایه، مرورگر وب یا برنامه کاربردی تلفن‌همراه لازم است، هم‌چنان که سرورها در محل راه دور برای ذخیره‌سازی داده‌ها و نرم‌افزار کاربر لازم است. SaaS یک مدلی است که در آن نرم‌افزار و دادهٔ مربوطه در ابر میزبان شده‌اند؛ و با استفاده از مرورگر وب (مانند جی‌میل به‌عنوان محصول SaaS عمومی) براساس تقاضا در اختیار کاربر قرار می‌گیرد. امروزه برنامه‌های کاربردی تجاری از SaaS برای حسابداری، همکاری و مدیریت ارتباط با مشتری استفاده می‌کنند.

PaaS نوع دیگری از مدل خدمت از رایانش ابری است که سکوی محاسباتی ارائه می‌دهد و برای نوشتن برنامه کاربردی قابل اجرا در ابر به‌کار می‌رود. در این مدل مشتریان یک نرم‌افزار را با استفاده از ابزارهای ارائه‌شده در ابر ایجاد و مدیریت توسعه و تنظیمات پیکربندی را نیز کنترل می‌کنند. هدف اصلی ارائه‌دهنده، ارائهٔ شبکه‌ها و سرورها و انباره‌ها و خدمات دیگر است. تفاوت PaaS با SaaS در این است که SaaS تنها برنامه‌های کاربردی ابر تکمیل‌شده را میزبان می‌کند؛ درحالی‌که PaaS سکو برای برنامه‌های تکمیل‌شده و در حال اجرا ارائه می‌دهد. درواقع محیطی است که توسعه‌دهنده می‌تواند برنامه کاربردی را ایجاد و گسترش دهد و نیازی به دانستن تعداد حافظهٔ لازم و تعداد پردازش‌گر مورد نیاز برای آن برنامه ندارد.

IaaS زیربنای رایانش ابری است که تحویل خدمات محاسباتی را به‌صورت اشتراکی برعهده دارد. به‌منظور پیاده‌سازی و عملیاتی‌سازی زیرساخت، بایستی منعطف و قابل اطمینان باشد. درواقع IaaS خدمتی ارائه می‌دهد که به سرور مجازی در چند دقیقه دسترسی داشته باشیم و از مؤلفه‌های زیرساختی مانند انباره، دیواره آتش، شبکه استفاده کنیم.

فناوری‌های متعددی برای ایجاد و مدیریت محیط ابر وجود دارند که بستگی به نوع خدمات قابل عرضه در ابر دارد. رایانش ابری به‌منظور الاستیسیته‌بودن به‌شدت بستگی به مجازی‌سازی و شبکه دارد. فناوری‌هایی مانند خدمات وب، معماری سرویس‌گرا [1]، واسط برنامه‌نویسی کاربردی برای دسترسی کاربران به منابع ابر به‌کار می‌روند[۱۰].

امن‌بودن ابر باعث بالارفتن پذیرش ابر می‌شود. از جمله تهدیدات رایانش ابری می‌توان به مواردی مانند دسترس‌پذیری، فقدان کنترل، چندمالکیتی، از دست رفتن داده، حملات بیرونی، حملات منع سرویس، سوء نیت‌های داخلی [۱۱] و خدشه‌دارشدن حریم خصوصی [۱۲] اشاره کرد. همچنین معماری کنونی رایانش ابری پاسخ‌گوی نیازهای پزشکی قانونی ابری نیست و روند پژوهش‌های پزشکی قانونی با چالش‌هایی مانند جمع‌آوری حجم زیاد داده از راه دور برای موارد بحرانی زمانی، عدم مقررات وحدت جهانی، بازسازی صحنهٔ جرم در محیط ابری، شناسایی محل و قلمرو دقیق داده، تحلیل خط‌زمانی پزشکی قانونی گزارش‌ها، بررسی و نظارت و سیاست‌گذاری گزارش روبه‌رو است [۲].

۳- نرم‌افزار به‌عنوان یک خدمت

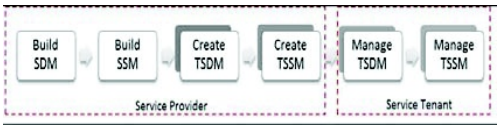
در اینجا دو معماری مدل‌محور را برای نرم‌افزار به‌عنوان یک خدمت بررسی می‌کنیم.

۳-۱- مهندسی امنیت مدل‌محور برای SaaS

شکل ۲، مهندسی امنیت مدل‌محور [2] (MDSE) پویا را برای کاربردهای ابرپایه SaaS که دارای چند مستأجر [3] (استفاده کننده متعدد از یک خدمت ابر) باشند نشان می‌دهد [۱۸]، این رویکرد امنیتی مستأجرپایه نیازمند تجمیع خدمات ابر با کنترل‌های امنیتی انتخاب‌شده توسط مستأجران بوده و بستگی به سکوی ابر دارد. ارائه‌دهندگان خدمات ابری ابتدا مدل توصیف خدمت [4] (SDM) و سپس مدل تعیین امنیت [5] (SSM) را در نظر می‌گیرند که شامل احصای تمام اجزای

[1] Service- Oriented Architecture
[2] Model-Driven Security Engineering
[3] Multi-tenancy
[4] Service Description Model
[5] Security Specification Model

امنیت ارائه‌شونده در خدمات ابری‌شان است. مستأجرین می‌توانند از این مدل‌ها برای به‌روزرسانی، حذف و یا اضافه‌کردن نمونه‌ها و توسعهٔ نیازهای امنیتی استفاده کنند. نیازمندی‌های امنیتی قابل اصلاح و به‌روزرسانی است.



(شکل ۲): فرآیند مهندسی امنیت مدل‌محور [۱۸]

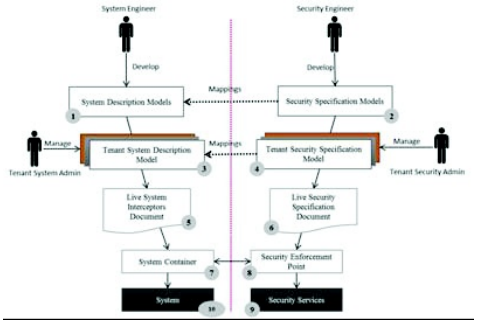
SDM: این مدل توصیف‌کننده خدمات قابل ارائه توسط ارائه‌دهندهٔ خدمات ابری است. این مدل شامل جزئیات برنامهٔ کاربردی هدف، شامل ویژگی‌های سامانه، معماری سامانه، طبقه‌های سامانه، رفتار سامانه و آرایش سامانه است که همگی در بحث امنیت دخیل هستند؛ زیرا از نگاه یک مهندس امنیت، در امنیت نهادهای سامانه، نیاز به مشخص‌بودن معماری، در امنیت وضعیت سامانه، نیاز به مشخص‌بودن رفتار سامانه و در امنیت گره‌های میزبان، نیاز به مشخص‌بودن آرایش سامانه است.

SSM: یک مجموعه از مدل‌های توسعه‌یافته و مدیریت‌شده توسط مهندسی امنیت ارائه‌دهندگان خدمات ابری است که نیازمندی‌های امنیتی لازم برای خدمات را نشان می‌دهند. این مدل شامل اهداف امنیت، مخاطرات امنیتی، نیازمندی‌های امنیتی، کنترل‌های امنیتی و معماری امنیتی است.

TSDM[1]: مدل توصیف خدمت مستأجر، توضیح‌دهنده ویژگی‌ها، معماری و طبقه‌های قابل دسترس برای هر کاربر است که از مستأجری به مستأجر دیگر به‌طور معمول متفاوت است و بستگی به مدل ارائه‌دهنده خدمات چندمستأجری دارد.

TSSM[2]: مدل تعیین امنیت مستأجر است، که شامل اهداف، نیازمندی‌ها، معماری، طراحی و کنترل‌های امنیتی است که مستأجرین خدمات دارند و می‌خواهند در دارایی‌هایشان که در ابر مستقرند اعمال شود. کنترل‌هایی مانند احراز هویت، مجازشناسی، بازرسی، رمزنگاری در این مدل قرار دارند.

شکل ۳ نمای کلی از رویکرد MDSE را همراه با تراکنش‌های اصلی و ذی‌نفعان اصلی در مباحث «مهندسی امنیت چندمستأجری» و «مدیریت امنیت مستأجر» نشان می‌دهد. بعد از احصای مدل‌های امنیت و برنامه کاربردی، سکوی MDSE چنین تغییرات مدل‌شده را با استفاده از جداکننده‌ها و رویکرد برنامه‌نویسی جنبه‌محور AOP[3] محقق می‌کند؛ به‌طوری که امنیت را به نهادهای برنامهٔ کاربردی (مؤلفه‌ها، طبقه‌ها و روش‌ها) تزریق می‌کند.



(شکل ۳): نمای کلی از رویکرد MDSE [18]

MDSE دو مرحله نگاشت دارد. نگاشت نخست، نگاشت نهادهای SSM به نهادهای SDM خدمت است که توسط ارائه‌دهندگان خدمات در زمان طراحی، اجرا در نظر گرفته و مدیریت می‌شود. هر موقع ارائه‌دهنده خدمات مشکل امنیتی یا نیازمندی امنیتی را کشف کرد، آن را مستقیم به مدل تعیین امنیت خدمت اعمال کرده و سپس به مدل توصیف خدمت نگاشت می‌کند که این نگاشت به‌طورمستقیم بر روی مدل‌های مستأجر تأثیر می‌گذارد. نگاشت دوم، نگاشت نهادهای TSSM به نهادهای TSDM خدمت است که توسط مستأجر خدمت در زمان اجرا مدیریت می‌شود. مدل MDSR از نگاشت چندبه‌چند بین نهادهای SDM مستأجر و SSM مستأجر پشتیبانی می‌کند.

[1]Tenant Service Description Model
[2]Tenant Security Specification Model
[3]Aspect-Oriented Programming

۳-۲- الگوی امنیت سازمانی با معماری مدل‌محور در قالب SaaS امن

چهار مدل در الگوی امنیتی سازمان با معماری مدل‌محور در قالب SaaS امن، وجود دارند [۷] که عبارتند از: مدل مستقل محاسباتی، مدل مستقل سکو، مدل مشخصی از سکو و مدل وابسته تولید.

در مدل مستقل محاسباتی (CIM)، توصیفی از خط‌مشی‌های امنیتی ارائه می‌شود که مستقل از مشخصه‌های فنی است. خط مشی‌های امنیتی باید به دارایی‌های اطلاعاتی و قلمروهای امنیتی اعمال شود. موقع ساخت سامانه‌های امن، CIM برای تعریف نیازمندی‌های امنیتی کمک می‌کند.

در مدل مستقل سکو (PIM)، توصیف مفهومی از سازوکارهای امنیتی مطرح می‌شود که باید با سامانه آمیخته شود و مستقل از جزئیات اجرایی و مشخصه‌های فنی است. موقع طراحی سامانه‌های امن، PIM می‌تواند کمک کند تا از الگوهای امنیت سازمان در تحلیل روش‌های امنیتی استفاده کرد.

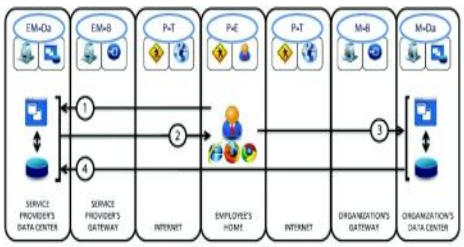
در مدل مشخصی از سکو (PSM)، توصیف مؤلفه‌های معماری امنیتی مطرح است که مستقل از فناوری است. PSM مربوط به چگونگی ایجاد سازوکارهای امنیتی در داخل معماری است. الگوهای امنیتی توصیف‌شده در PIM، در مؤلفه‌های امنیتی معماری لحاظ می‌شوند. ISO27000 خطوط راهنمایی در این زمینه ارائه کرده است. PSM کمک می‌کند تا از الگوهای امنیت سازمان در طراحی روش امنیتی استفاده کنیم.

در مدل وابسته‌تولید (PDM)، لازم است PSM در معماری فناورانه خاصی دیده شود. یک مؤلفه معماری ممکن است به محصولات فناورانه مختلفی مربوط باشد. محصولات فنی بایستی از طرف سازندگان خوش‌نام در صنعت امنیت باشد. بسته به فناوری‌های مورد استفاده، راه‌حل‌های نهایی ممکن است متفاوت باشند.

با این رویکرد ما از طرفی می‌توانیم اجزای امنیتی را در مدل‌های مختلف به‌طور مجزا مدیریت کنیم و از طرفی تبدیلات خودکار بین آنها انجام دهیم. به‌عنوان‌مثال اگر CIM داشته باشیم، ممکن است خط‌مشی‌های امنیتی مورد نیاز برای تضمین دارایی‌های اطلاعاتی را بدون درنظرگرفتن الگوهای امنیتی مدیریت کنیم. علاوه‌بر آن ممکن است خط‌مشی‌های امنیتی موجود در CIM را به‌طور خودکار تبدیل تا الگوهای امنیتی مورد استفاده در PIM را اتخاذ کنیم.

SaaS امن به‌عنوان یک الگوی امنیت سازمانی

در اینجا یک الگوی امنیت سازمانی معرفی می‌شود که سازمان‌ها می‌توانند موقع برون‌سپاری برخط، برای حفاظت از دارایی‌های اطلاعاتی‌شان (حفاظت از محرمانگی داده‌های برون‌سپاری) از آن استفاده کنند. [۷]. کارمندان یک سازمان از منزل (قلمرو عمومی کارمند (P-E)[1] به برنامه‌های کابردی برخط دسترسی دارند. ارائه‌دهنده خدمات، برنامه کاربردی را در مرکز داده قرار داده است. (قلمرو داده مدیریت‌شده خارجی (EM-D)[2]). دسترسی کارمند به ارائه‌دهنده خدمات از طریق اینترنت است (قلمرو انتقال (P-T)[3]) (مسیر شماره یک). ارائه‌دهنده خدمات یک گیت‌وی (دروازه) بین اینترنت و مرکز داده دارد (قلمرو استحکامات مدیریت‌شدهٔ خارجی (EM-B)[4]). به‌منظور اجازه‌دادن به کارمند با استفاده از اعتبار دسترسی، وقتی کارمند تلاش می‌کند که به برنامه‌های کاربردی برخط دسترسی داشته باشد، ارائه‌دهنده خدمات، مرورگر کارمند را به دروازهٔ سازمان (قلمرو استحکامات مدیریت‌شده (M-B)[5]) هدایت می‌کند (مسیرهای شماره ۲ و ۳). در همان لحظه کارمند در سامانهٔ سازمان (قلمرو داده مدیریت‌شده (M-Da)[6]) معتبر می‌شود تا برگه‌ای برای دسترسی به ارائه‌دهنده بگیرد. بعد از گرفتن برگه، دسترسی امکان‌پذیر می‌شود (مسیر شماره ۴). شکل ۴ روندنمای این الگو را نشان می‌دهد.



(شکل ۴): روندنمای مفهومی [۷]

سطح حساسیت دارایی اطلاعات (داده) که این الگو در پی حفاظت از آن است، در جدول ۱ آمده است. داده مشمول برون‌سپاری بایستی به‌صورت واضح توسط کارمند

[1]Public Employee realm
[2]Externally Managed Data realm
[3]Public Transport realm
[4]ExternallyManaged Bastion realm
[5]Managed Bastion realm
[6]Managed Data realm

ذخیره شده باشد (P-E). مرکز داده سازمان (M-Da) می‌تواند داده را به‌صورت واضح ذخیره کند؛ اما این داده‌ها مرتبط با برنامه‌های کاربردی برون‌سپاری شده نیست. مابقی قلمروها بایستی داده را مخفی کنند. داده ممکن است از ارائه‌دهندهٔ خدمات حذف شود؛ ولی مسیرهای ارتباطی باید امن باشند. مرکز داده سازمان (M-Da) ممکن است داده را به‌صورت واضح انتقال دهد؛ اما این داده‌ها مرتبط با برنامه‌های کاربردی برون‌سپاری نیستند.

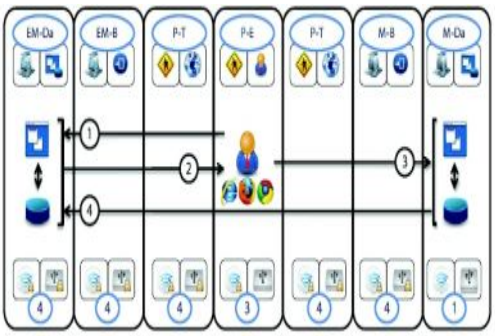
این الگو باید موقعی استفاده شود که کارمندان سازمان از برنامه‌های کاربردی برون‌سپاری‌شدهٔ برخط برای ذخیره‌سازی دارایی‌های اطلاعاتی دارای سطح حساسیت استفاده می‌کنند.

(جدول ۱): سطح حساسیت دارایی‌های اطلاعاتی

قلمرو امنیتی	سیاست‌گذاری امنیتی	سطح حساسیت
داده مدیریت‌شده خارجی	کانال امن و ذخیره‌سازی مخفی	۴
استحکامات مدیریت شده خارجی	کانال امن و ذخیره‌سازی مخفی	۴
انتقال عمومی	کانال امن و ذخیره‌سازی مخفی	۴
کارمند	کانال امن و ذخیره‌سازی آشکار	۳
استحکامات مدیریت‌شده	کانال امن و ذخیره‌سازی مخفی	۴
داده مدیریت‌شده	کانال آشکار و ذخیره‌سازی آشکار	۱

در این جا، هر کدام از مدل‌ها را بررسی می‌کنیم:

مدل CIM: نیاز داریم خط‌مشی‌های امنیتی متناسب با سطح حساسیت دارایی‌های اطلاعاتی را اعمال کنیم. همچنان که در شکل ۵ دیده می‌شود، ما از طریق رمزنگاری کانال‌ها و ذخیره‌سازی پنهانی داده، از شنود داده توسط نفوذگر جلوگیری می‌کنیم.



(شکل ۵): مدل CIM [۷]

مدل PIM: در اینجا سیاست‌های امنیتی CIM را به‌عنوان الگوهای امنیتی تحقق می‌بخشیم. نوع کانال‌هایی که می‌توان در PIM پیدا کرد، عبارتند از: کانال واضح (تک‌خط) — کانال امن (جفت‌خط). علاوه‌بر این این کانال‌ها، نمایش منطقی از پیام‌ها را نشان می‌دهند. نوع پیام‌ها عبارتند از: پیام درخواست و جواب پیام ضبط (خط‌چین).

ما سری عملیات روندنمای PIM را که در شکل ۶ نشان داده شده است، بیان می‌کنیم:

۱- کارمند از طریق مرورگر، درخواست مسیر امن برای دسترسی به برنامه‌های کاربردی برخط می‌کند (کانال امن ۱)

۲- ارائه‌دهنده سرویس سازمان آن کارمند را چک می‌کند

۳- ارائه دهنده سرویس مرورگر کارمند را به سازمان ارجاع می‌دهد تا برگه دسترسی صادر شود

۴- مرورگر کارمند درخواست مسیر امن برای دسترسی به سامانه‌های سازمان می‌کند (مسیر امن ۲)

۵- کارمند برگه اعتبارش را به سازمانش ارائه می‌کند (هویت ۲)

۶- سازمان بررسی می‌کند که کارمند آیا همان کسی است که ادعا می‌شود (احراز هویت). درصورت مثبت‌بودن کارمند برگهٔ امضاشده برای دسترسی کارمند ارائه می‌دهد

۷- سامانه‌های سازمان مرورگر، کارمند را همراه با برگه امضاشده، به سامانه‌های ارائه‌دهندهٔ خدمات ارجاع می‌دهد. بررسی‌کردن کنترل دسترسی انجام می‌شود درصورتی که برگهٔ امضاشده همان تولید شده قبلی باشد

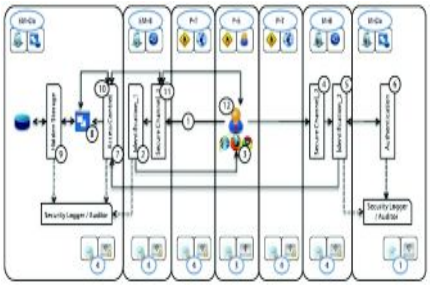
۸- درصورت معتبربودن برگه، کارمند قادر به دسترسی به برنامهٔ کاربردی‌اش خواهد بود

۹- برنامهٔ کاربردی باید داده را رمزگشایی کند به‌طوری که قابل نشان‌دادن به کارمند باشد (ذخیره سازی مخفی)

۱۰- قبل از نمایش برخط برنامه کاربردی به کارمند، ارائه‌دهنده خدمات دوباره بررسی می‌کند که آیا کارمند مجوز دسترسی به داده‌ها و برنامه‌ها را دارد یا نه؟ (کنترل دسترسی)

۱۱-ارائه‌دهنده خدمات، برنامه‌های کاربردی کارمند را از طریق مسیر امن نشان می‌دهد.

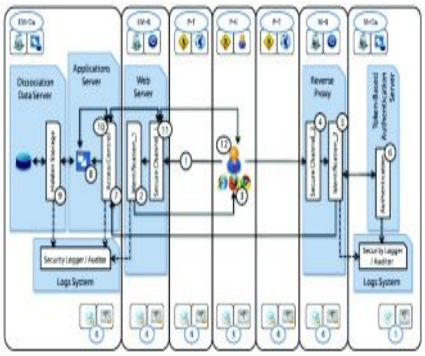
۱۲-ارائه‌دهنده خدمات یک کوکی در مرورگر کارمند ذخیره می‌کند. از این منظر کارمند ممکن است بدون احراز هویت مجدد دسترسی داشته باشد.



(شکل ۶): دیاگرام PIM [۷]

به‌منظور بررسی حملات ممکنه، سازوکارهایی برای شناسایی، احراز هویت، کنترل دسترسی و ذخیره‌سازی نهانی، باید تمام فعالیت‌ها با الگوهای امنیتی ثبت و بازرسی شوند.

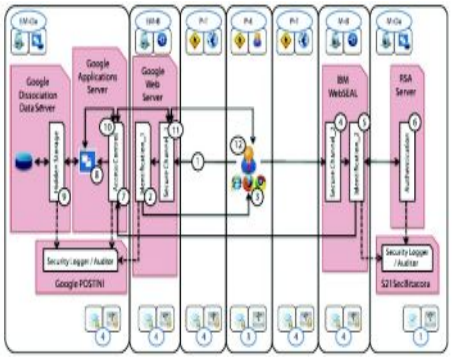
مدل PSM: در این جا دنبال تبدیل الگوهای امنیتی PIM به مؤلفه‌های معماری هستیم. هم چنان که در شکل ۷ نیز دیده می‌شود، الگوهای امنیتی کانال امن ۱ و شناسایی ۱ به وب‌سرور تبدیل می‌شوند. درحالی‌که کانال امن ۲ و شناسایی ۲ به Reverse Proxy تبدیل می‌شوند، الگوی امنیتی به Log System تبدیل می‌شود. همچنین الگوی امنیتی کنترل دسترسی و برنامه‌های کاربردی به Application Server تبدیل می‌شوند. درنهایت الگوی امنیتی Storage Hidden و داده به Dissociation Data Server تغییر می‌یابد.



(شکل ۷): دیاگرام PSM [۷]

به‌منظور جلوگیری ازحملهٔ مهاجم برای دسترسی به برنامه‌های کارمند، نیاز داریم به اطمینان‌یافتن از راست‌بودن احراز هویت. برای این منظور، لازم است یک سامانه احراز هویت همراه با سطح حساسیت بالا استفاده شود؛ به‌عنوان‌مثال می‌تواند سرور احراز هویت توکن‌پایه، یا اثبات بیومتریک و.... باشد.

مدل PDM: در این جا دنبال تبدیل مؤلفه‌های معماری به محصولات فناورانه هستیم. که در شکل ۸ دیده می‌شود.



(شکل ۸): دیاگرام PDM [۷]

فناوری‌های انتخابی در PDM مورد نظر در جدول ۲ آمده است. دیده می‌شود که، سربار محاسباتی معماری امنیتی سازمان افزایش نمی‌یابد، حتی به‌دلیل زیرساخت فناوری اطلاعات برون‌سپاری‌شده نیز می‌تواند کاهش یابد.

(جدول ۲): موارد قابل بررسی

	موارد قابل بررسی	تحلیل
سربار محاسباتی	ذخیره‌سازی	۰
	حافظه اولیه	۰
	پردازشگر	۰
	پهنای باند	۰
پیچیدگی	مدیریت امنیت	۱
	مدیریت لاگ	۱
	کاربر نهایی	۰
	بسط حجیم	۰
	مدیریت سامانه	۰
	هزینه نصب	۰
	مخاطره باقیمانده	۰

تهدیدات، مرتبط هستند با محرمانگی دارایی‌ها، جامعیت و دسترس‌پذیری [۱۳]. نکات زیر سازوکارهای امنیتی را برای جلوگیری با کاهش تهدیدات (تهدیدکنندگان محرمانگی، جامعیت و دسترس‌پذیری) برجسته می‌کند [۷]:

- مهاجم ممکن است دادهٔ مورد دسترس کارمند را بخواند. در این صورت وب‌سرور ارائه‌دهندهٔ خدمات و پروکسی معکوس سازمان می‌توانند از طریق کانال‌های امن مانع این کار شوند.
- ممکن است مهاجم پس از دزدی هویت کارمند، به برنامهٔ کاربردی کارمند دسترسی داشته باشد، در این احراز، توکن پایه پیشنهاد می‌شود.
- ممکن است مهاجم از یک آسیب‌پذیری برای دستیابی به برنامه کاربردی کارمند استفاده کند. برای جلوگیری از این حالت، ارائه‌دهنده باید مدام وصله انجام دهد.
- برای جلوگیری از افشاگری کاربر فنی باید از تفکیک‌سازی سرور داده در ارائه‌دهنده خدمات استفاده کرد.

این الگو درحالتی‌که دسترسی کارمند به برنامه‌های کاربردی‌اش، به‌جای منزل از دیگر طرق سازمان نیز باشد قابلیت اجرا دارد.

۴- سکو به‌عنوان یک خدمت:

PaaS به‌دلیل استفادهٔ مجدد از سکوها و سخت‌افزارها، قابلیت بالایی در صرفه‌جویی دارد. Paas محیطی برای توسعه، آزمون و میزبانی SaaS ارائه می‌دهد. در طراحی مؤلفه‌های پایه‌ای سکو باید به داشتن انعطاف بیشتر برای مدیریت‌کردن منابع و مشتری‌پسندکردن خدمات و تعامل‌پذیری توجه شود. انواع مختلفی از PaaS وجود دارند [۶]:

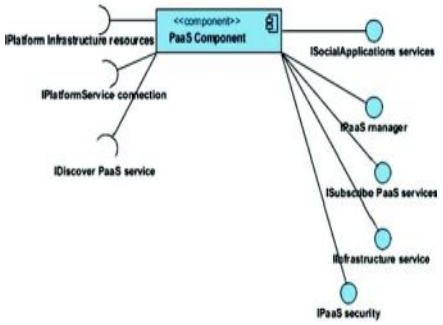
۱-سکوهایی با کارکرد اجتماعی مانند فیس‌بوک که رابط‌هایی برای نوشتن کاربران ارائه می‌دهد.

۲- سکوهای محاسباتی مانند ابر آمازون که خدمات پهنا، خدمات ذخیره‌سازی و خدمات پردازشی ارائه می‌دهد. توسعه‌دهندگان می‌توانند برنامه‌های کاربردی‌شان را بارگذاری کرده و در موقع نیاز آن را اجرا کنند.

۳-سکوهای وب مانند گوگل.

۴-سکوهای کسب‌وکار مانند فورث دات کام که زیرساخت‌های اختصاصی حرفه مانند پایگاه داده، تجمیع و خدمات رابط کاربر ارائه می‌دهد.

مدل مؤلفه‌ایی ابر paas در شکل ۹ آمده است.



(شکل ۹): مدل مؤلفه‌ای ابر PaaS [۶]

در این مدل هر رابط نشان‌گر مجموعه‌ای از معیارهای طراحی است. مجموعهٔ ارائه‌دهندهٔ رابط‌های برنامه کاربردی با نام خدمات Isocial نشان داده شده است، درحالی‌که IpaaS برای تجمیع داده و خدمات است. Isubscribe اتصال PaaS را با دیگر SaaSهای مرتبط انجام می‌دهد. Iinfrastructure نظارت بر زیرساخت سکو را انجام می‌دهد و همچنین Sec. IpaaS امنیت خدمات و داده را تضمین می‌کند. Iplatform تا Idiscover به‌عنوان خدمات مورد نیاز حرفه شناخته می‌شوند، درحالی‌که Isocial تا .IpaaS Sec، به‌عنوان خدمات ارائه‌شده به سامانه‌ها و کاربران شناخته می‌شوند.

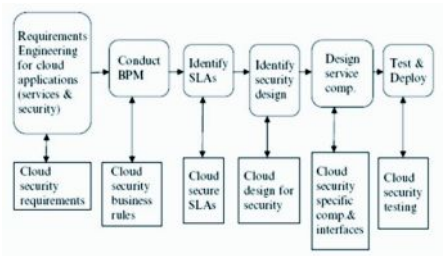
۴-۱- مؤلّفه‌های امنیت در ابر:

سکو به‌عنوان خدمت، یک لایه از نرم‌افزار را به‌صورت بسته‌بندی‌شده و به‌عنوان یک خدمت فراهم می‌کند؛ به‌طوری که بتوان از آن برای ایجاد سرویس‌های سطح بالاتر استفاده کرد [۱]. محاسبات ابری ترکیبی از محاسبات مستقل (خودمدیریتی) و مدل کلاینت سروری محاسبات توزیع‌یافته و محاسبات شبکه‌ای عظیم (مجازی، توزیع‌یافته، محاسبات موازی) و قدرت محاسباتی تعاملی (پردازش‌های تعاملی به‌همراه مدیریت منابع سازمانی) و معماری شبکه‌ای توزیع‌یافته بدون نیاز به هماهنگی متمرکز) است.

شکل ۱۰ نشان‌گر مدل فرایند توسعه ابر با محوریت امنیت است؛ به‌طوری که در حین تعیین نیازمندی، این امر بخشی از رویکرد مهندسی نرم‌افزار به برنامه‌های کاربردی ابر است. فرایند توسعه ابر شامل مراحل مهندسی نیازمندی‌ها[1] (RE)، هدایت مدیریت پردازش حرفه از طریق استاندارد[2] (BPMN) برای مدل‌سازی فرایند حرفه و زبان

[1]Requirements Engineering
[2]Business Process Modelling Notations

اجرایی فرایند حرفه (BPEL) جهت تعیین چارچوب کاری سطح خدمات[1] و تعیین توافق سطح خدمات[2] (SLA)، ایجاد امنیت در خدمات طراحی و آزمون و توسعه است. همچنین می‌توانیم از مدل‌های چرخهٔ حیات توسعهٔ نرم‌افزار[3] (SDLC) برای احصای ویژگی‌های وظیفه‌ای و غیروظیفه‌ای هر خدمت نرم‌افزاری و وب‌سرویس‌ها بهره برد. مهم این است که در مرحلهٔ طراحی از یک سری قواعد طراحی برای ترکیب عناصر SaaS استفاده کرد. هم‌چنین می‌توان در طراحی SaaS به نیازمندی‌های خدماتی توجه کرد [۶]:



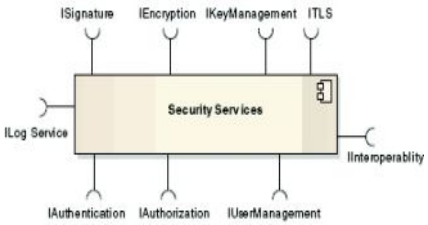
(شکل ۱۰): مدل فرایند توسعه در برنامه‌های کاربردی ابر [۶]

مؤلفه‌های ابر SaaS، PaaS و IaaS است که در SaaS، موضوعاتی مانند وب‌سرویس‌ها، امنیت آنها، میزان سطح خدمات، داده‌هایی که تحت عنوان خدمت عرضه می‌شوند، امنیت داده‌ها، امنیت خدمات، دسترس‌پذیری و تاب‌آوری (انعطاف‌پذیری) آن‌ها مورد توجه‌اند، درحالی‌که در PaaS موضوعاتی مانند سخت‌افزاری که تحت عنوان خدمت عرضه می‌شود، میزان خطای قابل قبول سکو، مدیریت منابع، امنیت خدمات، دسترس‌پذیری و تاب‌آوری آن‌ها مورد توجه‌اند و در مؤلفه IaaS، موضوعات سامانه‌های کاربردی، مقیاس‌پذیری پویا، امنیت خدمات زیرساختی و امنیت خدمات، دسترس‌پذیری و تاب‌آوری آن‌ها مورد توجه‌اند.

در هرکدام از مؤلفه‌های مذکور ابر، امنیت یک بخش کاملی از برنامه‌های کاربردی، شبکه‌ها، سرورها، منابع و معماری است. شکل ۱۱ چارچوبی برای خدمات امنیتی در ابر ارائه می‌دهد. این مؤلفه نرم‌افزاری پایه برای هر خدمت ابری است که امنیت نرم‌افزاری در دل آن قرار دارد. رابط‌های لازم عبارتند از [۶]:

Isignature, Iencryption, Ikeymanagement, ITLS, Iinteroperability, Ilogservice, Iauthentication, Iauthorisation,Iusermanagement

[1]Business Process Execution Language
[2]Service Level Agreements
[3]Software Development Life Cyle



(شکل ۱۱): مدل مؤلفه‌ای برای خدمات امنیتی ابر [۶]

خدمات امنیتی اجازه می‌دهد که مشتری بعد از دسترسی به خدمات، مدیریت چرخهٔ حیات کاربر (ایجاد و اصلاح و حذف)، دسترسی مجاز به خدمات، محرمانگی تضمینی [۴] و جامعیت (رمزنگاری، امضا، کنترل دسترسی)، مدیریت کلید رمزنگاری، قدرت ایجاد طرح تونل امن (TLS) بین کلاینت و سرور را داشته باشد. یکی از مشخصه‌های کلیدی در محاسبات ابر، تعامل‌پذیری است؛ زیرا خدمت ابر پایه می‌تواند از طریق دیگر برنامه‌های کاربردی ابر یا از کلاینت‌های سکوهای نامتجانس مورد استفاده قرار گیرد.

۴-۲- معماری ذخیره‌سازی امن در ابر:

سکوهای تجاری متعددی همانند Amazon S3 و Azure Microsoft در طی سال‌های اخیر برای ذخیره‌سازی توسعه یافته‌اند [۱۹]. فرایندهای احراز یا اطلاعات مجازشناسی از طریق پست الکترونیکی تبادل می‌شود. گرچه رفتار سکوها ممکن است متفاوت باشند و طرح‌های زیادی برای امن‌سازی ذخیره‌سازی داده شده است [۱۴]؛ ولی یک راهبرد ساده می‌تواند جامعیت را تضمین کند. هم‌چنان‌که در شکل ۱۲ دیده می‌شود، وقتی مالک، داده‌ای را به فضای ذخیره‌سازی در ابر بارگذاری می‌کند، ارسال داده به ارائه‌دهنده با MD5_1 صورت می‌گیرد. اگر داده از طریق اینترنت ارسال شود، یک درخواست غیرقابل انکار استفاده می‌شود. وقتی ارائه‌دهنده داده‌ای را همراه با MD5 دریافت می‌کند داده را متناظر با MD5_1 ذخیره می‌کند. وقتی ارائه‌دهنده خدمات درخواست بازبینی از طرف کاربر دریافت می‌کند در این صورت ارائه‌دهنده داده را همراه با MD5 به کاربر خواهد فرستاد. بر روی سکو Azure، موقع بارگذاری‌کردن، MD5_1 به‌وسیله مالک ارسال می‌شود و موقع دریافت‌کردن، MD5_2 محاسبه شده توسط Amazon's AWS، ارسال می‌شود. برای حفظ جامعیت، داده بارگذاری‌شد MD5_1 در دادگان نگه داشته می‌شود و آن را موقع درخواست برای کاربر می‌فرستد [۲]. چرخه در هر

بخش مجزا امن است. جامعیت و محرمانگی داده درحین ارسال، توسط پروتکل لایه دریچه امن (SSL) تضمین می‌شود.

از منظر ذخیره‌سازی ابر، امنیت داده نه‌تنها درحین بارگذاری‌کردن و دریافت‌کردن، بلکه در حین نگهداری نیز باید باشد. پیوندی برای ردیابی داده ذخیره‌شده در ابر وجود ندارد.

شکل ۱۲: جامعیت در سکو [۸]

نیازمندی‌های امنیتی مانند احراز هویت، مجازشناسی، دسترس‌پذیری، محرمانگی، مدیریت و به‌اشتراک‌گذاری کلید، ممیزی و تشخیص نفوذ، قابلیت بهره‌برداری، نحوهٔ اجرا که در سامانه‌های ذخیره‌ساز توزیع‌یافته مطرح است، بایستی در ذخیره‌سازی ابر نیز مد نظر قرار گیرد. در معماری پیشنهادشده توسط آقای کامار[15]،موضوعات محرمانگی، جامعیت، دسترس‌پذیری، قابلیت اعتماد، بازیابی، خدمات به اشتراک‌گذاری داده همگی ارائه می‌شود. برای این منظور معماری از چهار مؤلفه مولدتوکن[1] (TG) به‌منظور تولید شاخص‌هایی که ارائه‌دهنده را قادر به جستجوی داده می‌کند، پردازش‌گر داده[2] (DP) تا دادهٔ به‌وسیلهٔ روش AES رمز شود، مولد گواهی[3] (CG) برای اعمال خط‌مشی کنترل دسترسی، بازبینی داده[4] (DV) برای بررسی جامعیت بهره می‌برد. در این معماری ارائه‌دهندهٔ ذخیره‌سازی ابر در قبال دسترس‌پذیری و اعتمادپذیری مسئولیت دارد. DP متولی محرمانگی و جامعیت، CG متولی اشتراک‌گذاری داده، TG متولی بازیابی داده است. مدل اثبات بازیافتی[5] (POR) و مدل مالکیت داده[6] (PDP) برای اثبات عمل ذخیره‌سازی است.

آقای پوپا [۱۶]، یک معماری برای ذخیرهٔ امن در ابر نشان داده است که در آن خواص امنیتی ذخیره‌سازی ابر به چهار دسته تقسیم شده است: محرمانگی، جامعیت، پیوستگی در نوشتن، تازگی در خواندن، با پیام امضاشده و زنجیرهٔ درهم‌ساز، ویژگی پیوستگی در نوشتن ارائه می‌شود؛ درحالی که با ممیزی مکرر داده، موضوع تازگی در خواندن تضمین می‌شود.

۴-۳- مشکلات امنیتی PaaS در ابر و راه‌حل‌های عملی

۴-۳-۱- منابع مشکلات و طبقه‌بندی مشکلات:

چالش‌های امنیتی متمایزی در PaaS وجود دارند که به‌طورکلّی ناشی از گستردگی در ابر است [۱۷]:

- منابع مشکلات

چالش‌های امنیتی معماری‌های متمرکزشده به‌طور معمول ناشی از گستردگی اشیای کاربر بر روی میزبان‌های ابر است. دسترسی اشیا به‌منابع و دفاع اشیا در قبال بدافزارها یا در قبال ارائه‌دهندگان خراب، خطرپذیری‌های ممکنه را کاهش می‌دهد. سنجش دسترسی، خدمات شبکه، حفظ حریم خصوصی کاربر، پیوستگی خدمات در ارتباطات ابری مقوله‌های مهم هستند.

- طبقه‌بندی مشکلات

مشکلات امنیتی ناشی از ابر عبارتند از: شناوری منابع، الاستیسیته سریع که منجر به مشکلات تعاملی منابع ناهمگن و آسیب‌پذیری میزبان‌ها و اشیا می‌شوند. محرمانگی و کنترل دسترسی (احراز هویت، مجازشناسی و قابلیت ردیابی)، توازن بارپویا [۵]، حریم و پیوستگی خدمات در ابر لازم هستند.

۴-۳-۲- موضوعات مرتبط با شناوری منابع و الاستیسیته سریع [۱۷]):

۴-۳-۲-۱- مشکلات

- فقدان تعامل

اگر دسترسی اشیا به منابع از روش استانداردی اقدام نشود، منابع محاسباتی متنوع منجر به رخنهٔ امنیتی می‌شود؛ لذا برخی منابع لنگ خواهند زد. برای حفظ تعامل‌پذیری، از رابط‌های عمومی برای اشیا جهت دسترسی به منابع می‌توان بهره برد.

[1] token generator
[2] data processor
[3] credential generator
[4] data verifi er
[5] proof of retrievability model
[6] provable data possession model

- میزبان‌های آسیب‌پذیر

اگر اشیای کاربر در میزبان‌های چندکاربری به‌هم متصل توزیع شده باشند، نه‌تنها اشیا بلکه میزبان‌ها باید از حملات ممکنه در امان باشند. چنین حفاظتی به‌وسیله ارزیابی درخواست‌های دسترسی به‌منابع هر شئ بر روی میزبان امکان‌پذیر است.

اگر رخنهٔ امنیتی در میزبان رخ دهد، مهاجم به منابع میزبان و همهٔ اشیای تحت مالکیت آن میزبان دسترسی خواهد داشت؛ لذا محافظت میزبان ضروری است. اتخاذ اقدامات امنیت شبکه، مسئولیت‌پذیری ارائه‌دهنده را نشان می‌دهد.

- اشیای آسیب‌پذیر

در ابرهای PaaS، به سه دلیل امنیت اشیا ممکن است دچار خدشه شود: دسترسی‌داشتن ارائه‌دهنده به هر شئ کاربر که در میزبان‌های آن مستقر شده‌اند، حمله‌کردن کاربرها به اشیای یکدیگر، وقتی که مالکیت میزبان‌هایشان یکی است و حملهٔ شخص ثالث به شئ کاربر.

دلیل نخست چاره‌ای به‌جز اعتماد بین کاربر و ارائه‌دهنده ندارد. برای جلوگیری از حملات نوع دوم، استفاده از سازوکارهای ارزیابی دسترسی منابع توصیه می‌شود. حملات نوع سوم به‌وسیلهٔ خود اشیا قابل دفاع است (با استفاده از کدگذاری امن)

۴-۳-۲-۲- راه حل

مشکلات مذکور با دو اقدام برطرف می‌شود [۱۷]. برای مشکلات فقدان تعامل‌پذیری و میزبان‌های آسیب‌پذیر، روش "مبنای محاسباتی اعتمادی[1] (TCB)" و برای مشکل اشیای آسیب‌پذیر، رمزنگاری بخش‌های حساس اشیا، راه حل مناسب است.

- TCB

مبنای محاسباتی اعتمادی مجموعه‌ای از کدهای اجرایی و پرنده‌های پیکربندی است که امن فرض می‌شوند. TCB بعد از تحلیل رخنه‌های امنیتی، به‌عنوان یک لایه بر روی سیستم عامل نشسته و یک واسط برنامه‌نویسی کاربردی استاندارد برای اشیای کاربر ارائه می‌دهد. البته به‌منظور حداقل‌سازی پیچیدگی کد منبع TCB، بایستی کمینه باشد، لذا TCB لایهٔ نرم‌افزاری باریک و مقاوم است. در ساخت TCB، طبقه‌بندی منابع و نقش منابع و ارزیابی درخواست‌های دسترسی منابع مد نظر قرار می‌گیرند. برای دسترسی به هر نوع منبع به‌وسیلهٔ یک شئ چکیده‌سازی می‌شود؛ لذا موقعی که منبع مورد دسترسی قرار می‌گیرد، چکیده باید ارائه شود.

با نصب TCB بر روی هر میزبان، تعامل‌پذیری به‌راحتی صورت گرفته و تخصیص منابع از طریق TCB خواهد بود؛ لذا اشیا از یک واسط برنامه‌نویسی کاربردی استانداردشده برای دسترسی به منابع استفاده می‌کنند. به‌دلیل بررسی‌شدن تخصیص منابع از طریق TCB، از حملات ممکنه از اشیا به میزبان‌ها ممانعت به‌عمل می‌آید؛ لذا میزبان‌ها محافظت می‌شوند.

- اشیای رمزشده:

ارائه‌دهنده در قبال جامعیت و حریم خصوصی اشیای کاربر روی میزبان مسئولیت دارد؛ درصورتی که ارائه‌دهنده سوءنیت داشته باشد یا یکی از میزبان‌هایش به‌وسیله شخص مورد سوء استفاده قرار گیرد، در این صورت شئ قابل خواندن، اصلاح و حذف‌شدن است. روش رمزنگاری از اصلاح جلوگیری می‌کند؛ ولی مانع حذف‌کردن یا منع خدمت[2] نمی‌شود. روش‌های رمزنگاری متقارن و نامتقارن، چکیده‌ساز و امضا از محتوا حفاظت می‌کنند. امضا برای آشکارکردن تغییرات داده شده استفاده می‌شود. الگوریتم رمزنگاری متقارن سریع، مانع خوانده‌شدن محتوای اشیا می‌شوند. کلیدهای متقارن با کلیدهای نامتقارن کاربر مجاز رمز می‌شوند و فایل به شئ پیوست می‌شود. یک میدان انبار کلید برای نگه‌داشتن کلیدهای مختلف کاربران و یا نقش‌ها در سناریوهای دسترسی مختلف لازم است. اگر یک مجموعه کلید، به شئ پیوست شود، امنیت انبار کلید یک مشکل جدید خواهد بود. انبار کلید به‌منظور حذف سوء استفاده می‌تواند رمز شود. در آن صورت اشیا باید یک میدان اضافی برای تعیین این که چه کسی می‌تواند انبار کلید را رمزگشایی کند، لازم دارند. همچنانکه در جدول ۳ نیز مشخص شده است این لایه،لایه خط‌مشی کنترل دسترسی بوده و این رویکرد به مدیریت کنترل دسترسی برای هر شئ مجزا کمک می‌کند، لذا کاربران دربارهٔ نیازمندی‌های کنترل دسترسی، تصمیم می‌گیرند که به چه کسی اعتماد کنند و چه چیزی برای حفظ حریمشان باید مخفی باشد.

[1] Trusted computing base

[2] Denial of Service

مشخصه واحد شئ (آشکار و امضاشده توسط مالک شئ)
سیاست کنترل دسترسی (آشکار و امضاشده توسط مالک شئ)
انبار کلید/گواهی (شامل چند بخش که هر بخش به‌وسیله یکی از کلیدهای عمومی اشخاص مجاز رمز می‌شود)
محتوای شئ (شامل چند بخش که هر بخش به‌وسیله یکی از کلیدهای ذخیره شده در میدان قبلی رمز می‌شود)

(جدول ۳): ساختار اشیاء [۱۷]

۴-۳-۳- موضوعات مرتبط با دسترسی به شبکه وسیع

۴-۳-۳-۱- نیازمندی‌ها

برای سامانهٔ شبکه‌ای، دو نیازمندی متصور است: محرمانگی و کنترل دسترسی (احراز هویت، مجازشناسی و قابل ردیابی) به نهادهای کنترلی.

- محرمانگی ارتباط

ارتباط محرمانه یک عامل اصلی در سامانه رایانه‌ای شبکه شده و در ابرهای PaaS است. به‌دلیل تعامل و قابل دسترس‌بودن به‌وسیله مالک، لازم است با مالک ارتباط داشته باشند. مسیرهای ارتباطی قابل شنودند؛ لذا محرمانگی در ارتباط لازم است

- احراز هویت:

احراز هویت نخستین عنصر در کنترل دسترسی است. اثبات هویت در حین تراکنش لازم است. سازوکارهای موجود کافی هستند و نیاز به ابداع سازوکار جدید نیست.

- مجازشناسی

سازوکارهای مجازشناسی تعیین می‌کنند که براساس خط مشی‌های از پیش تعریف شده چه کسی می‌تواند به اشیا دسترسی داشته باشد. امروزه سامانه‌های مجازشناسی، کنترل دسترسی به محتواهای ثابت را انجام می‌دهند. کنترل دسترسی نقش‌پایه و کنترل دسترسی متحد که به مدیریت‌کردن چند حوزه توسط متولیان کمک می‌کنند، ممکن است نتوانند همهٔ مشکلات ابر PaaS را به‌دلیل مهاجرت اشیا و پیکربندی مجدد میزبان‌ها، پوشش دهند.

میزبانی که اشیای بی‌شماری را در یک زمان معین میزبان می‌کند، باید خط مشی‌های هر شئ را جهت اعمال به آنها بدانند. طبیعت پویای ابرهای PaaS، اجازهٔ به‌روزنگهداشتن این خط مشی‌ها را به‌صورت محلی نمی‌دهد. همچنین میزبان ممکن است درخواست‌هایی را برای فراخوانی خط‌مشی هر شئ هدایت کند. در این صورت هر کاربر نیاز دارد پایگاه داده مرکزی را برای خط مشی‌های اشیایش مدیریت کند. این رویکرد متمرکز ممکن است برای کاربر ابر سخت باشد.

هر شئ می‌خواهد نیازمندی‌های کنترل دسترسی خودش را داشته باشد؛ زیرا هر شئ ممکن است در هر میزبانی مستقر شود. برای مثال وقتی یک شئ به یک میزبان جدید منتقل می‌شود، خط‌مشی‌هایی که در میزبان قبلی بودند، باید در میزبان جدید نافذ باشند. یک روش عملی عبارت از انجام خط‌مشی‌ها همراه با اشیا است. خروجی این خط‌مشی‌ها در طرف میزبان، نقاط اجرایی خط‌مشی[1] (PEP) هست که کارش اجرای خط‌مشی‌ها است.

- قابلیت ردیابی:

با نگه‌داشتن رکوردهای اتفاقات انجام‌شده در یک سامانه قابلیت ردیابی امکان‌پذیر است. یک ابر PaaS نیاز به سازوکار گزارش‌گیری انکارناپذیر مجتمع دارد و این گزارش‌گیری باید امن و حفاظت‌شده در قبال سایر تراکنش‌ها باشد

۴-۳-۳-۲- راه حل

محرمانگی و احراز هویت در ارتباطات، به‌راحتی توسط "امنیت لایهٔ انتقال[2] (TLS)" در جایی که زیرساخت کلید همگانی[3] (PKI) وجود داشته باشد، قابل انجام است. برای توزیع آسان و سفارشی‌سازی مقیاس اشیا، خط‌مشی‌های کنترل دسترسی می‌تواند همراه با اشیا باشد. احراز هویت همراه با PEPها و همراه با خط‌مشی‌های کنترل دسترسی پیوست‌شده به اشیا به میزبان‌ها اعمال می‌شود. درنهایت یک پروتکل ابداعی گزارش‌گیری انکارناپذیر معرفی می‌شود تا اتفاقات در ابر ردیابی شوند.

۱) TLS

کانال‌های محرمانه بایستی از طریق TLS به‌منظور جلوگیری از استراق سمع و احراز هویت امن شکل گیرد لازم است که گواهی‌ها به اشیا نه به میزبان‌ها مرتبط باشند؛ زیرا میزبان می‌توانند اشیای زیادی را مستقر کند که بایستی از طریق کانال‌هایشان ارتباط داشته باشند. یک احراز هویت دوطرفه لازم است.

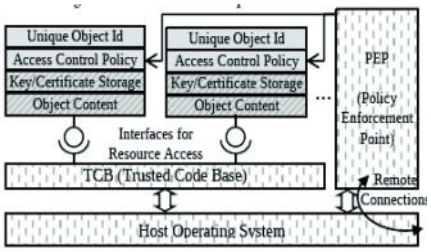
[1] policy enforcement points
[2] Transport Layer Security
[3] public key infrastructure

۲) خط‌مشی‌های سخت کنترل دسترسی

خط‌مشی‌های کنترل دسترسی چه به‌صورت محلی و چه به‌صورت متمرکز برای طبیعت پویای ابر مناسب نیستند. خط‌مشی‌های کنترل دسترسی که به اشیا پیوست می‌شوند، عملی است. این خط‌مشی‌ها سه برتری دارند: تنظیمات فقط برای اشیا است؛ اتصال جدید لازم نیست؛ درحین مهاجرت اشیا پیکربندی مجدد لازم نیست. علاوه‌بر این، خط‌مشی‌های پیوستی، به‌جای این‌که همهٔ کنترل دسترسی‌های اطلاعاتی را به‌طور متمرکز نگه‌داشته باشند، حامل برخی تصمیم‌گیری‌ها هستند که با طبیعت PaaS سازگارند.

۳) PEP

PEPها همچنانکه در شکل ۱۳ مشاهده می شود به منظور حفاظت هاست ها و اشیاء از حملات ممکنه،دسترسی به اشیا را مطابق با خط‌مشی‌های پیوستی مدیریت می‌کنند.PEP مجموعه‌ای از مؤلفه‌های نرم‌افزاری است که متولی خواندن خط مشی‌های پیوستی و مقایسه آن‌ها با درخواست‌های دسترسی است. تصمیمات در PEP میزبان‌ها و بعد از هر درخواست دسترسی گرفته می‌شود. درحین فرایند تصمیم‌گیری، PEP میزبان‌ها باید پروتکل گزارش‌گیری غیرقابل‌انکار داشته باشد. درحین تصمیم، PEP یک میزبان خط‌مشی شئ را خوانده و تعیین می‌کند که آیا طرف اتصال حداقل‌های احراز را دارد یا نه؟ اگر داشته باشد PEP اجازهٔ اتصال و دسترسی به شئ را طبق خط‌مشی می‌دهد وگرنه محرز نمی‌شود. PEP تسخیرشده یا بدخواه یک خطر امنیتی عمده است.



(شکل ۱۳): نمای کلی مؤلفه‌ها ودواجاره‌ای [۱۷]

۴) پروتکل لاگ‌گیری (گزارش‌گیری) غیرقابل‌انکار

گزارش‌گیری غیرقابل‌انکار راه حل مشکل جامعیت گزارش را آسان کرده است. زیرا به‌موجب آن عملکردهای تقلبی اضافه نمی‌شوند و عملکردهای صحیح قابل اصلاح و حذف‌کردن نیستند. البته گزارش‌ها در هر طرف باید مرتبط باشند. چنین پروتکلی با استفاده از تابلوی اعلانات برخط که یک ذخیره‌ساز فقط خواندنی عمومی، امکان‌پذیر است. درخواست‌های دسترسی و پاسخ‌های آن‌ها به‌طورمستقیم به‌طرف‌ها ارسال نمی‌شود. به‌جای آن، تابلوی اعلانات مذکور همانند یک میانجی عمل می‌کند و طرفین مطابق پیام اعلامی تابلو عمل می‌کنند. این پروتکل از درخواست و پاسخ‌های جعلی ممانعت می‌کند. از اقدامات رمزنگاری برای حفظ حریم پیام‌های منتشره در تابلو استفاده می‌شود.

۴-۳-۴- احراز هویت آگاه از حریم خصوصی

به‌طور معمول اطلاعات بیشتر از نیاز، در حین احراز درخواست می‌شود. گواهی‌های پراکسی خطرپذیری آشکارسازی ویژگی‌های اضافی را از بین می‌برد. این گواهی، الکترونیکی بوده که تنها خصوصیات لازم را شامل می‌شود. دو نیازمندی در حین احراز هویت الکترونیکی آگاه از حریم باید لحاظ شود: نخست این که میزبان‌ها و اشیا نباید خصوصیات بیشتر از مقدار لازم را درخواست کنند. این امر بستگی به خط‌مشی‌های کنترل دسترسی تعریفی برای میزبان‌ها (به‌وسیله ارائه‌دهنده) و اشیا (به‌وسیله کاربر) دارد. درصورت درخواست بیش از حد مجاز استدلال لازم است. دوم این که گواهی‌های موثق قابل پیکربندی که داده‌های هویت مالک را آشکار می‌کند آسان باشد.

متولیان گواهی وکالتی[1] (PCA) می‌توانند تولید پویای گواهی اعتبارنامه‌هایی که بر پایهٔ اسناد صحیح بوده را اجرا کنند. PCA مرجعی برای حل اختلاف بین اسناد صحیح و گواهی‌های پراکسی است. آن‌ها نه‌تنها گواهی‌های پراکسی منتشره و اسناد صحیح را نگه می‌دارند بلکه گواهی‌های پراکسی را جهت عدم انکار امضا می‌کنند. PCAها می‌توانند ارائه‌دهندهٔ مستقل خدمات در ابر یا ناشر اصلی اسناد صحیح باشند. با استفاده از PCA سلسله‌مراتبی چندگانه، مقیاس‌پذیری امکان‌پذیر می‌شود.

۵- نتیجه‌گیری و پیشنهاد

الگوهای امنیتی، روشی برای ساخت و ارزیابی سازوکارهای امنیتی جدید است، ولی آنها آن چنان که بایسته است، درعمل به‌کار گرفته نمی‌شوند، زیرا طراحان در انتخاب آن‌ها و اعمال صحیح‌شان مشکل دارند. سازمان‌ها قبل از استفاده از SaaS باید از تهدیدات اطلاع داشته باشند. سازمان‌ها

[1] Proxy certificate authorities

می‌توانند با اتخاذ الگوی امنیت سازمانی بحث‌شده داده‌های برون‌سپاری‌شده را از تهدیدات حفاظت کنند.

همچنین با بررسی نقاط ضعف امنیتی در ابر PaaS که در این پژوهش بحث شد، راه حل‌های امن‌سازی پیشنهاد شده است؛ درصورت تحقق پیش‌فرض‌های مذکور، در قبال حملات امنیت برقرار خواهد شد.

پیشنهاد می‌شود با توجه به این که در کشور ما نیز ایجاد زیرساخت مفهوم رایانش ابری مورد توجه قرار گرفته است، لازم است الگوی امنیت سازمانی در قالب IaaS،SaaS،PaaS متناسب با شرایط سازمان‌های ارائه‌دهندهٔ خدمات ابری و کاربران در کشورمان، مورد تحقیق قرار گیرد تا PaaS امن و IaaS امن محقق شود. باید توجه شود که در شبکهٔ ملی اطلاعات امن (تحقق امنیت در تاروپود شبکهٔ ملی اطلاعات) تحقق این موضوعات امکان پذیر خواهد بود.

۶- منابع

[۱] اکبری محمدکاظم، سرگلزایی جوان مرتضی، "محاسبات ابری - ارائه معماری‌ها، ابزارها، سرویس‌ها و مسائل مرتبط"، مرکز تحقیقات رایانش ابری، ۱۳۸۹.

[۲] نجفی دیارجان هاله، ابراهیمی آتانی رضا، زیبافر سجاد، «مروری برپزشکی قانونی ابری»، دو فصل‌نامه علمی ترویجی امنیت فضای تولید و تبادل اطلاعات، ۱۳۹۳، جلد ۳، شماره ۱، صفحات ۵۹ – ۷۹.

[۳] محمدی واحد، نیارکی اصلی راهیه، «چالش‌های امنیتی حفظ حریم خصوصی محاسبات ابری درکاربردهای تجارت الکترونیکی»، ۱۳۹۲، دانشگاه گیلان، دانشکده فنی، پایان نامه کارشناسی ارشد.

[۴] صدرالساداتی سید محسن، محمدجواد کارگر، «چالش‌های امنیتی در رایانش ابری و ارائه راهکاری جهت بهبود امنیت آن در راستای توسعه خدمات عمومی دولت الکترونیک»، همایش ملی مهندسی کامپیوتر و توسعه پایدار، ۱۳۹۲، موسسه آموزش عالی خاوران مشهد.

[۵] نسرین عرب، ابوطالبی مجید، «ارائه یک راهکار توازن بار پویا در محیط محاسبات ابری با استفاده از الگوریتم‌های تکاملی»، ۱۳۹۱، یازدهمین کنفرانس سراسری سامانه‌های هوشمند، انجمن سامانههای هوشمند ایران، دانشگاه خوارزمی.

[6] Mahmood,Z.; Hill, R. "Cloud Computing for Enterprise Architectures", Springer, London, UK (2011), ISBN: 978-1-4471-2235-7

[7] Moral-García S.; Moral-Rubio S.; Eduardo Fernández; Fernández-Medina E., "Enterprise security pattern: A model-driven architecture instance", Computer Standards & Interfaces (2014), Volume 36, Issue 4, Jun 2014, PP 748–758

[8] Balduzzi,M.;Zaddach, J.; Balzartti,D. "A Security Analysis of Amazon's Elastic Compute Cloud Service ", Proceedings of the 27th Annual ACM Symposium on Applied Computin,, (2012), pp1427-1434

[9] Rani D.,"A Comparative Study of SaaS, PaaS and IaaS in Cloud computing ", International Journal of Advanced Research in Computer Science and Software Engineering, (2014), Volume 4, Issue 6, June 2014, pp 458-462

[10] Vitti P.A.F.; Santos D.R.D,"Current Issues in Cloud Computing Security and Management", in Proceedings of the 8th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE2014), 2014

[11] Rachana S. C., Guruprasad2 H.S., "Emerging Security Issues and Challenges in Cloud Computing", International Journal of Engineering Science and Innovative Technology (IJESIT), (2014) Volume 3, Issue 2, PP485-491

[12] Keshtkar M. A.; Ghoreyshi,S. M. " Security-Aware Dispatching of Virtual Machines in Cloud Environment",ACSIJ Advances in Computer Science: an International Journal, (May 2013), Vol. 2, Issue 2, No.3, pp48-52

[13] Archana T. A.,"SURVEY ON CLOUD COMPUTING SECURITY TECHNIQUES", IJRET: International Journal of Research in Engineering and Technology, (Jan 2014), Volume: 03 Issue: 01,pp240-242

[14] Kokane M.; Jain P.,"Data Storage Security in Cloud Computing", International Journal of Advanced Research in Computer and Communication Engineering, (March 2013),Vol. 2, Issue 3, pp1388-1394

[15] Kamara S.; Lauter K. "Cryptographic cloud storage". Financial Cryptography and Data Security. LNCS, (2009) vol. 6054, pp. 136–149.

[16] Popa, R.A.; Lorch, J.; Molnar, D., et al." Enabling security in cloud storage SLAs wi th Cloud", in Proceedings of the 2011 USENIX conference on USENIX annual technical

conference, ser. USENIXATC'11. USENIX Association, 2011

[17] Sandıkkaya, M. T.; Harmancı A. E. "Security Problems of Platform-as-a-Servic e (PaaS) Clouds and Practical Solutions to the Problems ",31st International Symposium on Reliable Distributed Systems (2012),pp463-468

[18] Almorsy, M., Grundy, J.C., Ibrahim, A., Adaptable, Model-driven Security Engineering for SaaS Cloud-based Applications, Automated Softw-are Engineering, Volume 22, Issue 2, April 2014, pp 187-224

[19] Microsoft Azure Services Platform: http://-www.microsoft.com/azure/default.mspx (4/3/2009)

رحیم یزدانی چهاربرج دانشجوی دکترای رشته امنیت فضای سایبر در دانشگاه عالی دفاع ملی است. ایشان مدرک کارشناسی ارشد خود را در رشته مخابرات از دانشگاه تربیت مدرس و مدرک کارشناسی خود را در رشته الکترونیک از دانشگاه ارومیه دریافت کرده است. علاقه‌مندی پژوهشی وی در زمینه های مخابرات و امنیت فضای سایبر است. ایشان تاکنون مقالاتی را در این زمینه ها منتشر کرده و پروژه هایی نیز در این حوزه ها انجام داده است.

محمود دی پیر مدرک دکترای خود را در رشتهٔ کامپیوتر-سامانه‌های نرم‌افزاری و مدرک کارشناسی ارشد خود را در رشتهٔ کامپیوتر نرم‌افزار هر دو از دانشگاه شیراز دریافت کرده است. مقطع کارشناسی خود را نیز در همین رشته از دانشگاه هوایی شهید ستاری دریافت کرده است. هم اکنون عضو هیئت علمی دانشکده رایانه و فناوری اطلاعات دانشگاه هوایی شهید ستاری است. زمینه‌های پژوهشی ایشان شامل داده کاوی و امنیت فضای سایبر است و دارای مقالات متعددی در مجلات و کنفرانس‌های معتبر ملی و بین المللی است. نامبرده در پروژه‌های پژوهشی و صنعتی متعددی مشارکت داشته است.