# به سوی ارزیابی عمل‌کرد ارائه دهندگان سرویس ابر جهت امنیت داده های آن


**چکیده**

داده‌های امروزی بدلیل حفظ حریم شخصی و امنیت، هم از طرف تأمین کنندگان خدمات ابری و هم کاربران ، در همه ی سطوح شامل :سطح ذخیره شده، انتقال ، تقاضا و پردازش داده‌ها حساس هستند .پردازش ابری در حوزه سلامت، امنیت ملی، خدمات، بانکداری و زمینه‌های دیگر استفاده شده است و همانطور که در چندسال اخیر دیده ایم تعدادی از کمپانی ها اطلاعات محرمانه را در ابر) سرورهای خدمات ابری (ذخیره کرده اند .بنابراین اطلاعات و حفظ امنیت داده‌ها یک بحث حساس و حیاتی است که باید بصورت کامل و جامع در حوزه ی محاسبات ابری پیگیری شود .این پژوهش بر روی تحلیل  عمل‌کرد مدلهای امنیت داده در محاسبات ابری تمرکز دارد. این مقاله مدلهای امنیت داده‌های ابری را مبتنی بر فرایند کاری مدلسازی با نماد (BPMN) پیشنهاد کرده و با شبیه سازی نتایج، کارایی مباحث مربوط به امنیت داده‌ها را بعنوان بخشی از هرگونه ابتکار عمل سازمانی در زمینه ی مدیریت اجرایی کسب وکار (BPM) نشان داده است.



**کلید واژه ها:** ارائه دهنده خدمات ابری (CSP). مدیریت فرآیند کسب و کار (BPM). مدل سازی فرآیند کسب و کار (BPMN). پردازش ابری. امنیت داده ها

**۱. مقدمه**

محاسبات ابری در سالهای اخیر بعنوان یک زمینه ی بسیار تأثیر گذار و مهم در حوزه ی فناوری اطلاعات تلقی شده و توجه زیادی را به خود بدلیل کاهش هزینه‌های مدیریتی اش جلب کرده است .هزینه ای را که ایالات متحده آمریکا جهت محاسبات ابری قرار داده ، برای مدت ۵سال گذشته برآورد رشد ۴۰ درصدی را تا پایان سال و رسیدن به نرخ ۷ بیلیونی را داشته است)کافمن ۲۰۰۹ .(همچنین طبق گزارش ها این تخصیص هزینه تاعبور از مرز ۹۵بیلیون دلار در سال ۲۰۱۸ رسیده است)سوباشینی و کاویتا،۲۰۱۱ . (همچنین، پیش‌بینی می‌شد که دوازده درصد از بازار نرم افزار به سمت محاسبات ابری حرکت کند)آلزین، ساه،و پارادی ۲۰۱۳ .(با وجود رشد کنونی زمینه ی محسابات ابری و روند بازار نرم افزار، بنظر می‌رسد که این بازار از طریق محاسبات ابری از رشد دوازده درصدی خود هم عبور کرده بعلاوه، استفاده از ذخیره سازی و شبکه‌های اجتماعی از طریق ابر، انقلابی را در عرصه‌ی تعاملات اجتماعی فناوری اطلاعات و برقراری ارتباطات در میان مردم، به وجود آورده است.

در میان تعاریف مختلف از رایانش ابری، مشهورترین و شناخته شده ترین تعریف که بشکلی جامع راجع به اجزای آن توضیح میدهد، همان تعریف مؤسسه ی ملی فناوری استانداردها (NIST) است)مل و گرانس،۲۰۱۱.(برطبق این تعریف، محاسبات ابری یک مدل از فناوری اطلاعات برای استفاده آسان از منابع رایانشی مبتنی بر تقاضای کاربر، ذخیره سازی و خود تطبیق دهنده، چه نرم افزاری و چه سخت افزاری ، از طریق اینترنت بدون دردسرهایاحتیاج به منابع مدیریتی و تعامل بین تولید کننده و کاربر است .در این تعریف محاسبات ابری ۵ جزء اصلی از آن دیده می‌شود دسترسی از طریق شبکه، سلف سرویس براساس نیاز کاربر، مخزنی از منابع محاسباتی، محاسبه هزینه خدمات با توجه به اندازه استفاده و قابلیت ارتجاع خدمات با سرعت بالا)رونتری و کاستریلو ۲۰۱۴.(همچنین تعریف NIST بصورت عمومی شامل سه مدل خدماتی ) IaaS:زیرساخت بعنوان خدمات(، )PaaS بستر بعنوان خدمات (و )SaaS نرم‌افزار بعنوان خدمات (و چهار مدل گسترش یا استقرار) خصوصی،عمومی، انجمنی و ترکیبی (است.

با SaaS کاربر به نرم‌افزار و برنامه‌های کاربردی از طریق مرورگرها یا رابطهای برنامه نویسی، بدون کنترل مستقیم بر زیرساخت‌ها دسترسی پیدا می کند PaaS.بستر زیرساخت را مانند سیستم عامل(OS) فراهم می کند که کاربر

بتواند نرم‌افزار و برنامه ی کاربردی را روی آن اجرا و نصب نماید، اما کاربر نمی‌تواند به منابع سخت افزاری دسترسی داشته باشد .درIaaS ، کاربر با یک سخت‌افزار و شبکه ی زیرساختی تجهیز می‌شود که دسترسی فیزیکی به آن‌ها ندارد اما می‌تواند از آن‌ها برای اجرای سیستم عامل و برنامه‌های کاربردی خود بصورت مستقل استفاده نماید.

برطبقNIST ، درمدل استقرار خصوصی رایانش ابری ،عرضه کننده خدمات ابری (CSP) یک مدل خدماتی را تنها برای یک سازمان بامدیریت خود سازمان یا CSP یا یک شخص ثالث ایجاد می‌کند .در حالی که مدل استقرار انجمنی یک سرویس خدمات ابری را تنها برای یک گروه مشخص از کاربران عرضه می‌نماید، مدل عمومی سرویس را برای عموم عرضه می‌کند و چهارمین مدل، مدل ترکیبی، ترکیبی است از دو یا تعداد بیشتری از از مدل‌های استقرار قبلی. سه مولفه کاربردی در رایانش ابری خدماتی یا تحویل دهنده می باشند، حول ارای ُه کننده سرویس (CSP)هستند،و اینکه کاربر مشتری یا مالک نامیده می شود، می‌باشند) سود،۲۰۱۲.(

مدیریت CSP بر روی ابر ، نقش بسیار مهمی در تأمین منابع ذخیره سازی و محاسباتی دارد .کاربر یا مالک بصورت انفرادی یا سازمانی می تواند خدمات رایانش ابری را برای ذخیره سازی داده و یا پردازش آن‌ها خریداری و یا اجاره نماید.کاربر، شخصی است که از خدمات رایانش ابری بعنوان یک فرد ثبت نام شده، چه شخصی و چه از طریق یک سازمان استفاده می کند.

با این وجود رایانش ابری بدون چالش نیست .طبق گفته ی آرمبروست) ۲۰۱۰ (پردازش ابری مشکلات زیادی دارد . بعضی از آن‌ها مربوط به بازبینی ،محرمانگی و انتقال داده‌های قفل شده هستند .وسایر مشکلات شامل تدوام یا دردسترس بودن کسب وکار، عملکرد، غیر قابل پیش‌بینی بودن، مقیاس پذیری در امر ذخیره سازی، باگ و خطاهای موجود در سیستم‌های توزیع شده بزرگ و وسیع، و مجوزهای نرم‌افزاری است.ریسک‌های استفاده از رایانش ابری آنگونه که فوگارتی) ۲۰۰۹ (عنوان میکند ، شامل سازگاری، حفظ حریم خصوصی و قابلیت همکاری است .سازگاری به این معناست که داده‌ای ممکن است در یک CSP در CSP ی دیگر سازگار نباشد .سازمان مالک نمی‌تواند برروی حریم خصوصی اطلاعاتش کنترلی داشته باشد .همچنین آلزاین، پارادی، سوه و تام)۲۰۱۱(خاطر نشان کردند مسئله

ی حفظ حریم خصوصی و امنیت به خطراتی درمورد محتوایات داده ها، نفوذ به آن‌ها و در دسترس بودن خدمات مربوط برمی‌گردد.

بیشترین عیوب رایانش ابری که توسط تعداد زیادی از مولفین گفته شده و در بالا هم درموردشان بحث کردیم، و در جاهای دیگر هم می بینیم، مربوط به حفظ حریم شخصی و امنیت داده هاست .داده‌های امروزی بدلیل حفظ حریم شخصی و امنیت، هم از طرف تأمین کنندگان خدمات ابری و هم کاربران ، در همه ی سطوح شامل :سطح ذخیره شده، انتقال ، تقاضا و پردازش داده‌ها حساس هستند.پردازش ابری در حوزه سلامت، امنیت ملی، خدمات، بانکداری و زمینه‌های دیگر استفاده شده است و  تعدادی از کمپانی ها اطلاعات محرمانه را در ابر) سرورهای خدمات ابری ( ذخیره کرده اند )به عنوان مثال فلیندرز،۲۰۱۴ ;گیل ،۲۰۱۳ ;تاکسن ،۲۰۱۴.(بنابراین اطلاعات و حفظ امنیت داده‌ها یک بحث حساس و حیاتی است که باید بصورت کامل و جامع در حوزه ی محاسبات ابری پیگیری شود .این پژوهش بر روی تحلیل  عمل‌کرد مدلهای اخیر امنیت داده در محاسبات ابری تمرکز دارد.این مقاله در بخشهای مختلفی آمده است .بخش ۱ :مقدمه و معرفی این مقاله بخش ۲ :ارائه پیشینه و اصطلاحات مربوط به امنیت ابر و امنیت داده‌های ابری است .بخش ۳ :در مورد چگونگی تحقق امنیت در ابر بحث میکند .قسمت ۴ :یک ارزیابی مهم را روی روش‌ها و مدل‌های ایجاد امنیت داده‌ها ارائه می‌دهد .قسمت ۵ :مدل BPMN را برای عرضه کنندگان سرویسهای ابری-CSP) ۱و (۳-CSP ارائه می‌دهد و در نهایت در قسمت ۶ :مراحل شبیه سازی BPMN را براساس تنظیم عمل‌کرد پارامترها جهت شبیه سازی امنیت داده‌های ابری موجود در فرایندهای تجاری توضیح می‌دهد.

## ۲. پیش زمینه

امروزه رایانش ابری را می‌توان بر اساس به اشتراک گذاری منابع) اجاره ی چندگانه(، قابلیت ارتجاع، مقیاس پذیری ، و پرداخت هزینه زمانی که از آن استفاده می‌کنید، شناخت ) بعنوان مثال مل و گرانس،۲۰۱۱ و وینکلر،۲۰۱۱. (یکی از ویژگی‌های مدرن رایانش ابری مدل کسب وکار آن است که منابع مشابه در میان کاربران زیادی در شبکه میزبان و سطح برنامه ی کاربری به اشتراک گذاشته می شود .قابلیت ارتجاع به این موضوع اشاره دارد که کاربران رایانش ابری

می‌توانند نیازهای محاسباتی خود را تغییر داده و زمانی که نیازی به آن‌ها ندارند منابعی را به دیگران عرضه کنند . فناوری حاضر در مجاسبات ابری به مشتریان این امکان را می‌دهد تا سیستم‌ها ، پهنای باند و ظرفیت ذخیره سازی را با توجه به ویژگی‌های قابل قیاس در ابر اندازه‌گیری کرده و بسنجند .ویژگی‌های مهم دیگر در رایانش ابری بحث خودسازی و خود تأمینی توسط کاربر برای ظرفیت‌های محاسباتی، نرم افزاری، و فضای دیسک و شبکه است . بیشترین عرضه کنندگان خدمات رایانش ابری ، کاربر را تنها برای زمان و منابع استفاده شده شارژ می‌کنند که همان پرداخت به اندازه مصرف است.

معمول ترین خدمات رایانش ابری سه مدل ارایه و تحویلSaaS) ،PaaP،(IaaS، چهار مدل استقرار)خصوصی ، عمومی، انجمنی و ترکیبی (و چندین حوزه ی کاربردی) محاسبات، ذخیره سازی، دارایی، وب و (.. دارند.

طبق پیش‌بینی IDC در سال ۲۰۰۹،تخمین زده شده که خدمات رایانش ابری ، سالانه به رشد ۲۷٪ می رسدکه همراه با سرمایه‌گذاری ۴۲ بیلیون دلاری قبل از سال ۲۰۱۲ در مقایسه با خدمات قدیمی IT رشد با نرخ سالانه پنج درصد را به همراه دارد) .ماتر ، کوراسامی و لطیف ۲۰۰۹(، رشد سریع رایانش ابری به دلیل رشد نوآورانه در نرم‌افزار مثل مرورگرها، پروسه ها، امکانات ذخیره سازی، فناوری تصویر سازی، فناوری اینترنت با پهنای باند بالا، سرورها ، رابط های واسط کاربری (API)و دیگر موارد بود )وینکلر۲۰۱۱ .(درحال حاضر ، خدمات محاسبات ابری از طریق PC ها، تلفن‌های هوشمند، تبلت ها، بوسیله دستگاههایی در یخچال ها ، ماشین‌ها و حتی ساعت‌های مچی هوشمند در یک چشم به هم زدن در اختیار ما است.

بعضی از مشخصات اصلی که باعث استفاده از رایانش ابری می شودمربوط به سرمایه‌گذاری های کم اولیه و کمبود هزینه اجرایی، قابلیت اطمینان و نگهداری ، تکرار الگو، قابلیت ارتجاع منابع، عدم وابستگی مکانی، امکان به اشتراک گذاری منابع در مقیاس وسیع، اتوماسیون بهتر، دسترسی مبتنی بر تقاضا، کارایی پردازشی، و شفافیت فناوری) ماتر و همکاران ۲۰۰۹، وینکلر ۲۰۱۱، مودی،پاتل،بورسانیای، پاتل و راجاراجان ۲۰۱۳(می باشد. برای تحقق بهتر اتوماسیون، قابلیت اطمینان و کارایی، یک ابر براساس الگوهای تکراری طراحی می شود .وقتی که یک سرویس محاسباتی با انتزاعی کردن تکنولوژی از طریق رابط کاربری ایجاد می‌شود این تکنولوژی را شفاف می سازد.شفافیت

هزینه ی عرضه کننده ابر را کاهش می‌دهد که آن را  بوسیله بهره برداری و رقابت پذیری سودمند می‌کند .دستیابی بر اساس تقاضا و سلف سرویس،عرضه کننده را قادر می‌سازد که سرویس ابر را با اثر بخشی هزینه و بصورت سریع به مشتری تحویل دهد .همه ی این ویژگی‌ها برای درست بودن نیاز دارند به انتزاع بیشتر که پیچیدگی بیشتری راهم به همراه می آورد .این مبادله ی همه ی خصوصیت‌های خوب در رایانش ابری محسوب می شود .از آنجایی که پیچیدگی، زمینه ی حمله را وسیع‌تر می‌کند ، باعث به خطر افتادن امنیت در ابر می‌شود.

بنابراین رشد رایانش ابری با موانعی روبروست که شامل امنیت،حفظ حریم شخصی، اتصالات و دسترسی آسان، قابلیت اطمینان، قابلیت همکاری، عدم استقلال از CSP ها، ارزش اقتصادی، قلمرو فناوری اطلاعات و تغییرات در سازمان فناوری اطلاعات می‌باشد .ابر نمی‌تواند کارا ، قابل اطمینان و با هزینه مؤثر باشد، بدون یک شبکه که ممکن است برای کاربر پر هزینه باشد .سودمندترین مشخصه رایانش ابری برای اثر بخشی هزینه و سرعت، اتصالات و امنیت است .بحث امینت در ابر و بصورت مشخص، امنیت داده‌ها را در قسمت بعد پیگیری خواهیم کرد.

رایانش ابری درواقع به انتقال ، دستکاری و محاسبه و ذخیره سازی دیتا از طریق شبکه برای یک زیرساخت محاسباتی مدیریتی و محافظت شده خارج از سایت بوسیله یک شخص ثالث ، اشاره می‌کند .

پیکربندی رایانش ابری به صورتی است که بتواند برنامه‌های کاربردی را بصورت همزمان برای چندین کاربر و یا چندین مستاجر خود ،اجرا کند .تحت چنین شرایط محاسباتی، CSP باید بتواند امینت اطلاعات کاربر را، از طریق مواردی چون فایروال ، شبکه خصوصی تصویری (VPN) و شناسایی کاربر،کلید های عمومی و خصوصی ، کدگذاری و سایر اصول امنیتی تأمین کند .با توجه به مفهوم مخزن منابع مشترک با سایر ابرها ، داده ی کاربر می‌تواند در اختیار هم شخص و هم شخص ثالث قرار و هم ابری که در حال حاضر در حال استفاده است ، قرار گیرد) جولیش و هال ۲۰۱۲ .( بنابراین امنیت یک جز حیاتی در زمینه رایانش ابری برای اطمینان از داده ی موجود است و دسترسی مخصوص تنها برای کاربران معتبر می‌باشد ) اوربی،برادوا، وسامبومورتی۲۰۰۶. (

برخی از امتیازهای استفاده از رایانش ابری که در ادامه می‌آید و البته همه ی مزایای آن محسوب نمی‌شود، شامل کاهش هزینه‌های سرمایه گذاری اولیه)کریگر،۲۰۰۹ (،مدیریت های موجَز و مختصر)پرول،رپسلاگر،ایرکو

زارنکیو،۲۰۱۲ (،بهینه سازی استفاده از منابع) قابلیت ارتجاع)(آرمبروست و همکاران ،۲۰۱۲ ;کوسومانو،۲۰۱۲ (و بهره وری انرژی)کاتز،۲۰۰۹ (است.

آیر و هندرسون) ۲۰۱۰ (برخی از پتانسیل های رایانش ابری را بصورت خلاصه بیان کرده اند .محیط کاری تصویری، رابط کاربری تحت کنترل،دسترسی در هر شرایط، عدم وابستگی به مکان،قابلیت ارتجاع با سرعت بالا، استقلال در منابع ، قابلیت ردیابی و پیگیری، .هوبرگ، والژیسم و کرکما )۲۰۱۲ (سایر جنبه‌های رایانش ابری را مشخص نمودند :: افزایش مقیاس پذیری ،افزایش چابکی، کاهش روش پیچیدگی زیرساختهای فناوری اطلاعات، کاهش هزینه و بهیود تراز دلخواه برای کسب و کار و فناوری اطلاعات.

### ۳. امنیت برای رایانش ابری

امنیت ابر در حالت عمومی شامل امنیت فیزیکی ، بازیابی و بازسازی در اثر خرابکاری و امنیت زیرساخت ها در سطح میزبان/نظارت‌گر ماشین مجازی)هایپروایزر (و شبکه) شانگ،۲۰۱۵ (،امنیت بستر چه در سطح روت و چه سطح سیستم عامل مهمان،مشابه امنیت نرم‌افزار که شامل امنیت کاربر،داده و امنیت اطلاعات و امنیت اپلیکیشن است ، می‌باشد . فایروال ،نظارت امنیتی ،متعادل کننده بار، BGPدر هایپروایزر امنیت را در سطح شبکه زیرساخت ها فراهم می کند .بعلاوه لایه‌های امنیتی برای زیرساخت ها ،API، NoSQL ، صف‌های پیغام و ذخیره سازی جهت امن کردن ابر در سطح بستر هستند .هویت و مدیریت دسترسی ،حسابرسی شبکه و سیستم مربوط به برقراری امنیت و نظارت کاربر است .کدگذاری یکی از لایه‌های اصلی امنیتی در معماری امنیتی SaaS است) شانگ،کو، راماشاندران۲۰۱۶.(

چندین موضوع و مسئله در مورد امینت ابر بررسی و پیگیری شد ) .آلزاین و همکاران،۲۰۱۳ دانیل و ویلسون ۲۰۰۳دیایوکوس،کاتساروس،پالیس ،واکالی، و مهرا ۲۰۰۹، مودی و همکاران ۲۰۱۳، سویاشینی و کاویتا ۲۰۱۱ .(بر اساس ویژگی برون سپاری رایانش ابری ،مباحث امنیتی مربوط به معماری از دیگر نگرانی‌های موجود در بحث امنیت است.چنین مواردی شامل حمله خارجی از فردی نامعتبر است که به داده‌های مهم مشتری از طریق عرضه کننده و کاربر و همچنین درحالت کلی رایانش ابری دسترسی دارد)سود۲۰۱۲ .(قرار گرفتن در موقعیت حمایت حکومتی و

مقررات سختگیرانه مانند سیستم‌های سازماندهی شده ی امنیت در ابر اعتماد سازمانها را افزایش داده و صاحبان کسب وکار را به سمت رایانش ابری سوق خواهد داد .

مودی و همکاران)۲۰۱۳ (مباحث امنیتی ابر را درقالب حملات ، تهدیدات و آسیب‌پذیری طبقه بندی کردند .حمله از متن رایانش ابری به عنوان عملی جهت تخریب منابع آن محسوب می‌شود . تهدید اشاره به رویدادی دارد که بصورت بالقوه با منابع ابر،سازش دارد یا می‌تواند سهواً یا عمداً به ابر آسیب امنیتی برساند .بعنوان مثال ایجاد اخلال در ذخیره سازی ابر نماید .آسیب‌پذیری در امنیت ابر به ابهامات موجود در سیستم امنیتی ابر اشاره داد که می‌تواند به یک نفوذگر این امکان را بدهد که به سیستم از طریق یک سری متدهای پیچیده دسترسی پیدا کند .کلید موارد کاملاً مشخص در ابر همانطور که سوباشینی و کاویتا) ۲۰۱۱ (گفته اند، امنیت شبکه، شناسایی افراد و مجوزدهی، مدیریت هویت و فرایند ثبت نام ، امنیت اپلیکیشن های تحت وب،آسیب پذیری مجازی سازی، در دسترس بودن، پشتیبانی، امنیت داده،محلی بودن داده‌ها ، اجزای داده، جدایی دادها،دسترسی داده، محرمانگی داده،نفوذ داده ها .طبق گفته محققین، بیشترین المانهای امنیتی ابر وابسته به امنیت داده هستند .فناوری ابر سه گونه از سرویسها را عرضه میکند:

نرم‌افزار به عنوان سرویس(SaaS)، بستر به عنوان سرویس(PaaS)، و زیرساخت به عنوان سرویس.(Iaas)

یک SaaS این گونه است که از اپلیکیشن های تحت وب در حال اجرا روی یک مرورگر وب استفاده می‌کند . تعمیرهای امنیتی در اپلیکیشن های وب می‌تواند موجب آسیب‌پذیری نرم‌افزارها و اپلیکیشن های عرضه شده توسط SaaSشود .آسیب‌پذیری های وابسته به برنامه‌های وب با شکاف های امنیتی نمی‌تواند از طریق فایروال شبکه IDS، IPSبصورت کامل پیگیری شوند .این بدلیل آن است که برنامه‌های وب تحت حملات خطرهای جدیدی قرار میگیرند که مقابله و پیشگیری در سطح برنامه و شبکه نمی تواند از امنیت آن‌ها پشتیبانی کند ). سوباشینی و کاویتا ۲۰۱۱(نسخه های گزارش شده از نفوذهای داده‌ای در سال ۲۰۰۸ نشان می دهد که ٪۵۰ نفوذهای امنیتی از طریق هک کردن برنامه‌های وب، که ۳۹ درصدشان از برنامه‌های کاربردی یا لایه خدماتی است، ۲۲ درصد از سیستم عامل یا بستر است، ۱۸ ٪بخاطر استفاده از موارد آسیب‌پذیر شناخته شده، ۵ ٪بدلیل استفاده از موارد آسیب‌پذیر شناخته نشده و ۵ ٪دیگر بخاطر استفاده از اعمال مخفیانه است).وید ، هیلندر و ولنتاین ۲۰۰۸ .(یک CSP باید ۷/۲۴ در

دسترس باشد .برای عرضه ی خدمات و شرکت داشتن در طول مدت زمان این می تواند با تغییر مداوم معماری در سطوح مختلف) اپلیکیشن، بستر یا زیرساخت (به منظور افزایش مقیاس پذیری و در دسترس بودن ، ایجاد می‌شود .با وجود اینکه حملات سرویس ها و خرابی سخت‌افزار یا نرم‌افزار در ابر همواره انکار می‌شود. موارد امنیتی اشاره شده توسط سوباشینی و کاویتا) ۲۰۱۱ (پشتیبانی می شوند CSP . ها باید سرویسهای پشتیبانی را برای همه ی دیتاهای حساس فراهم کنند تا بازیابی سریع را در زمان تخریب ممکن سازند . برای جلوگیری از دستیابی غیر مجاز به داده‌های پشتیبانی شده، داده‌ها باید کدگذاری شوند .داده‌های پشتیبانی شده می‌توانند یک مشکل امنیتی بالقوه را اگر به درستی مدیریت نشوند ، مخصوصاً موقع حذف شدن و انصراف یک کاربر از ادامه مشترک بودن خدمات ابر ، ایجاد کنند.

شبکه ، امنیت داده‌ها و اطلاعات در رایانش ابری بخش‌های ضروری IT هستند .در ابر امنیت به عنوان یک سرویس، شناخته می‌شود) . لینتیکوم۲۰۰۹، استینینگرو ندبال(۲۰۱۴این موارد بر اساس مشخصه هایی شامل احراز هویت، شناسایی، مجوزدهی،حریم شخصی ، یکپارچگی و ماندگاری دسته بندی می‌شوند) وینکلر،۲۰۱۱;آرم بروست و همکاران ۲۰۱۰ . (این به محافظت از داده‌ها ، برنامه‌ها، بستر، سرویس و زیرساخت مربوط است که در حالت عمومی با یک سری اصول ، فناوری و نظارت هایی می پردازد.حالت داده در ابر می‌تواند بصورت داده ی ذخیره شده)در حال استاحت (،داده ی در جریان)در حال استفاده(، داده در حرکت)در حال انتقال (باشد .امنیت داده باید بیشتر چالش های امنیتی رایانش ابری را پیگیری نماید).آکرنیم ۲۰۱۳ (در همه ی حالات داده اگرچه رایانش ابری از نظر تکنولوژی و اقتصادی سودمند است، امنیت باز هم به عنوان یک چالش اصلی در استفاده از آن هم برای عرضه کننده سرویس و هم برای مشتریان باقی می ماند ) به عنوان مثال مل و گریس۲۰۱۰ .(با این وجود، بدون استفاده از توسعه دهندگی سیستماتیک، سرویس های ابری با شکست روبرو هستند .دست آورد ما ، پیشنهاد و مدلسازی فرآیند کسب و کار به عنوان بخشی از مهندسی نیازهای وابسته به سرویس برای مطالعه هر فرآیندی در ابر قبل از اجرای واقعی است .در این مقاله ما این نتیجه را با بررسی دقیق امنیت داده‌ها ی ابر نشان داده‌ایم.

**۴. امنیت داده‌ها در ابر**

داده‌های امن داد و ستد و اعتماد بر فناوری  اطلاعات را ایجاد می کنند.این بخش مباحثی کلیدی را در مورد امنیت داده در ابر به عنوان موضوع اصلی این مقاله برای اعمال تجزیه و تحلیل داده‌های بزرگ جهت بررسی عمل‌کرد امنیت داده‌ها در ابر، عنو.ان می کند.

امینت داده چالشهای اصلی امنیتی ابر را بصورت عمومی از نظر معماری و تکنولوژی پوشش می‌دهد). شانتر و راماشاندران،۲۰۱۶ .(امنیت داده، همانطور که اوراکل درسال ۲۰۱۲ مشخص کرده، به معنی دستکاری) تغییر غیرمجاز داده ها(، سرقت و استراق سمع )به تاراج بردن اطلاعات شخصی مانند اطلاعات مربوط به کارتهای اعتباری، سرقت هویت ) بی‌اعتبار کردن هویت شخصی(، سرقت رمزهای عبور، دسترسی غیرمجاز به دیتابیس، مدیریت غیر مسئولانه سیستم، مدیریت ضعیف کاربر، ایجاد چند سرویس و لایه‌های برنامه کاربردی که مدیریت ابر را پیچیده می سازد، می باشد .

با وجود امتیازهای زیاد آن ، رایانش ابری در چالشی بزرگ‌تر بخاطر عدم امنیت که مربوط به داده ، اطلاعات ،میزبان و امنیت شبکه است می‌ماند ) ماتر و همکاران ، ۲۰۰۹ . (این عدم اطمینان منجر می‌شود که استفاده کنندگان از امنیت، و مخصوصاً امنیت داده  به عنوان نگرانی اصلی در مورد ابر یاد کنند .بنابراین یکی از فاکتورهای اصلی که مانع استفاده از ابر می شود مربوط به پردازش و ذخیره سازی داده‌های حساس در ابر ، مخصوصاً در حالت انجمنی ، ترکیبی یا عمومی ابر است .امنیت داده در ابر  با دو مسئله روبروست : کنترل محدود دیتا توسط صاحب داده طبق این حقیقت که داده‌ها در حیطه مفروظ صاحبانشان ذخیره نمی شود، و ویژگی اجاره ی چندگانه  ابر که خطر حساس بودن داده‌ها را افزایش می دهد .امنیت داده در اصل یک بحث جداگانه است . زمانی که داده در حال استراحت یا به عبارت دیگر در مخزن داده‌ها ذخیره شده است، زمانی که داده درحرکت است )جابجایی داده از جایی به جایی دیگر در ابر (و زمانی که داده در حال استفاده است .نگرانی‌های موضوع امنیت داده اغلب راجع به محرمانگی ، یکپارچگی، و در دسترس بودن در حالتهای مختلف آن شامل پردازش داده ویا استفاده است.

داده درحال استراحت، داده‌ای است که در هارد دیسک روی کامپیوترهای کاربر ، سرور ها و دستگاه‌های ذخیره سازی پشتیبان ذخیره شده است . اگر داده ی به اشتراک گذاشته شود ویا در ابر ذخیره شده باشد، خطر امنیتی آن مشابه داده حالتهای دیگر است .همانطور که مالک کنترل کامل این داده را ندارد .وینکلر)۲۰۱۱ (بیان کرد که دو نیازمندی برای سازمان جهت انتخاب و ذخیره سازی ابر برای داده‌های حساس وجود دارد .یک محافظ مسئول است برای داده‌های شما با استفاده از بهترین اصول استاندارد موجود در صنعت، از تکنولوژی های امنیتی وابسته به نوع داده ی ذخیره شده، استفاده نماید.

داده درحال حرکت، داده‌ای است که درحال انتقال بین یک مخزن به یک جای مشابه دیگری است و یا از مخزن سازمان به مخزن ابر .زمانی که گفته می‌شود داده درحرکت است یا درحال انتقال است، که کاربر داده به یا از ابر را آپلود و دانلود می‌کند .

نام کاربری و رمز عبور کاربر که به سرویس ابر در جهت شناسایی یک کاربر کمک میکند، به عنوان داده‌های حساس در حرکت شناخته می‌شوند درحالی که بصورت رمزگذاری شده ذخیره نشده باشند) سوباشینی و کاویتا، ۲۰۱۱ .وینکلر ،۲۰۱۱ ; مودی و همکاران، ۲۰۱۳ .(مسایل مربوط به امنیت داده ی در حال انتقال مربوط به نگهداری از آن‌ها در مقابل دستکاری داده، حفظ محرمانگی دیتا و جلوگیری از مشاهده ی داده توسط یک شخص ثالث در حالی که داده در حال انتقال است، می باشد.رمزگذاری داده درحال انتقال احتمالاً تنها راهکار امنیتی برای این نوع داده است.

دیتای در حال استفاده داده‌ای است که درواقع در گیر پروسه پردازشی کاربر در ابر است .ممکن است داده‌ای برای پردازش باز باشد ، از یک مدل در حال اجرای در ابر تولید شده باشد، یا داده‌ای میانی است که نرم افزاری به عنوان وروردی اش جهت پردازش گرفته و یا موارد این چنینی باشد .هیچ راهکار امنیتی شناخته شده‌ای برای داده ی درحال استفاده بدلیل آنکه نمی‌توان چنین داده‌ای را کدگذاری نمود وجود ندارد . تنها راه امنیتی برای چنین داده‌ای استفاده از آن در محیطی امن مانند محیطهایی که امکان دسترسی به کنترل و فایروال دارند، می باشد.

بیشترین تحقیقات روی امنیت داده‌ها مربوط به تکنیک های اصلی رمزگذاری و رمزگشایی هستند .دیر زمانی است که ما به قدر کافی در مورد فرایند ایمن سازی در محیط ها ی ابری واقعی ، با جزییات و اینکه چگونه آن‌ها کار

خواهند کرد نمیدانیم . بنابراین ، ما روش اصولی تری را جهت حل مبحث امنیت داده ها پیشنهاد کرده ایم .به عنوان مثال سود)۲۰۱۲ (تکنیکهای معمول و قابل استفاده در رایانش ابر را در مورد امنیت داده‌ها جمع‌بندی می کندو طراحی امنیتی جدیدی را پیشنهاد. و عمل‌کرد آن را تحلیل می‌کند . سود)۲۰۱۲ (همچنین عنوان می کند که یک راهکار امنیتی که حریم ، شناسایی و یکپارچگی داده را حفظ می نماید ، از بهترین روشهای قابل استفاده برخوردار است .طراحی امنیتی پیشنهاد شده شامل تقسیم‌بندی دیتا به بخش‌های مختلف، ۱۲۸ بیتی SSL رمز گذاری شده، سازنده ایندکس ، تأیید پیام مالک و احراز هویت اطلاعات کاربر در مرحله آزمایشی) بوسیله کاربر و ابر ( است.

پراساد و همکارانش) ۲۰۱۱ (راهکار شناسایی سه بعدی را ارایه دادند .که قابل استفاده بودن داده را با غلبه یافتن بر مشکلاتی مانند انکار سرویس و تراوش داده ، تهیه می‌کند . راهکار معرفی شده نیازی به رمز گذاری ندارد .در نتیجه اگر نام کاربری و رمز عبور تصدیق شود، کاربر می‌تواند به راحتی به داده ی موجود در ابر دسترسی پیدا کند .

کامارا و لوترد)۲۰۱۰ (مدلی امنیتی مطرح کردند که از مفهوم رمزگذاری ایندکس استفاده میکند و مناسب برای حفظ تمامیت با استفاده از رمزنگاری است .در این روش ، زمانی که داده از سیستم کاربر به ابر یا سیستم دیگر منتقل شده است ، یک کلید رمز گشایی در سمت دریافت‌کننده جهت رمزگشایی آن برای شناسایی کاربر ذخیره می‌شود . مشکل این متد آن است که جستجوی داده ی رمز گذاری شده پیچیده و ناکاراست .یک مدل امنیتی رمز گذاری داده که توسط وانگ و همکارانش) ۲۰۱۰ (مطرح گردید قابل جستجو و مناسب است . اما مشکل استفاده از چنین متدی در ابر این است که کاربر به داشتن اطلاعات قبلی راجع به داده ی رمزگذاری شده احتیاج دارد .بعلاوه هیچ مدرکی دال بر محرمانگی ، یکپارچگی، و ایمن بودن در مقابل حمله را نشان نمیدهد .

درواقع این روش به عنوان یک روش مناسب جهت ایجاد امنیت در نظر گرفته می شود.

پوپا و همکاران) ۲۰۱۰ (چیزی را که مدل امنیتی ذخیره سازی قطعی ابر نامیده می‌شود،عنوان کردند . این روش از رمزگذاری و سایر ابزارهای مهندسی برای ایجاد یک مدل امن قیاس پذیر و کارا استفاده میکند که کاربر را قادر می سازد محرمانگی، یکپارچگی، توانایی نوشتن سریال و بروز بودن و سوءرفتار ابر را شناسایی کند.

در این مقاله، روش بر اساس مدل سازی فرآیند کاری (BPMN) امنیت داده را در دوفاز ارائه میکند :۱ زمانی که داده درحال انتقال است ).به عنوان مثال در حال انتقال به ابر است (و درحال استراحت می‌باشد ) به عنوان مثال وقتی در ابر ذخیره می‌شود (. و ۲ . زمانی که به داده از ابر دسترسی پیدا می‌کنیم . در فاز دوم روش دسترسی به داده را برای کاربر ارائه می‌دهد، اگر آن‌ها از همه ی دروازه های امنیتی که توسط این روش همانطور که در بالا اشاره شد می باشند، عبور کرده باشند .

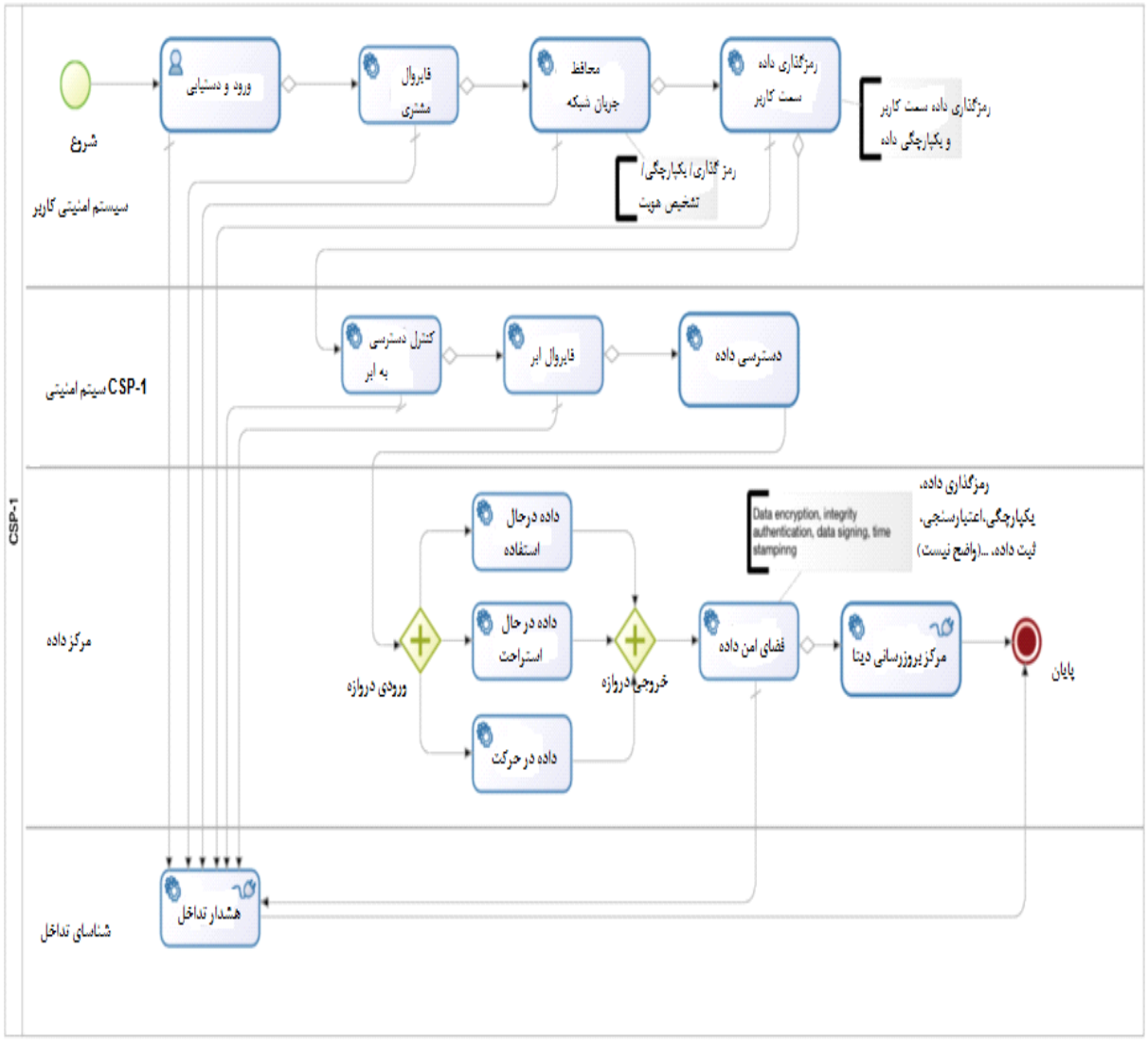
## ۵. مدل فرایند کار(BPM)

مدل فرایند کاری نمادگذاری (BPMN) برای طراحی سیستم مؤثر بوده استد ومی‌تواند در مهندسی ایمن سازی جهت محاسبه ی زمان و منابع مورد نیاز بدست گیری مجدد کنترل مرکز داده ی به خطر افتاده استفاده شود و این بسیار برای همه ارائه دهندگان سرویس و کاربران حیاتی و ضروری بود .آن‌ها آزمایشی را مبنی بر نفوذ اطلاعات در مقیاس بزرگ انجام دادند تا قدرت امنیت سیستم و سرویسشان را قبل از استفاده واقعی ، به دست آوردند BPMN . می‌تواند برای هر سازمانی مناسب باشد .بونیتا سافت نرم‌افزار BPM برای نشان دادن اینکه چگونگی مؤثر بودن BPMNبرای ابر و برای اجرای آزمایش شبیه سازی مجازی می‌تواند مناسب باشد .بونیتا سافت یک محیط نرم‌افزاری برای مدلسازی مدیریت فرایند کاریBPM و شبیه سازی فرایند توسعه نرم افزار است.

BPMNبرای شبیه سازی مدلهای امنیتی داده برای سه تأمین کننده سرویس ابری-CSP ,CSP-2,CSP-3 ) . ( ۱استفاده می‌شود . عرضه کنندگان سرویسهای ابری برای این منظور درنظر گرفته شده‌اند تا بتوانند طراحی امنیت داده را در CSP ها کنترل نمایند .اطلاعات ۲-CSP از وقتی که آن‌ها اطلاعاتشان را برای انتشارات آکادمیک ارسال نکردند ، فاش شد .بعد از تصدیق و تأیید اخلاقی و توافق از دو عرضه کننده دیگر سرویس ، هر دو ,۳-CSP ۱-CSPبرای باقی این مقاله مانند.

### ۵.۱. مدل امنیت داده:۱-CSP

CSP-1عنوان میکند که امنیت و سطح بالای سرویسهای را مثل زیرساخت، پردازشی، ذخیره سازی، شبکه ، سرویسهای دیتا بیس ارسال می‌کند CSP-۱ .بر این باور است که امنیت اطلاعات مهم است و یک نیاز اساسی سرویس برای حفظ یکپارچگی و اطلاعات مهم در مقابل حذف سهوی یا عمدی ، تراوش ، تداخل، و یکپارچگی داده و سرقت.مدل امنیتی داده در ابر استCSP-۱ . بر اساس مسئولیت مشترک بین عرضه کننده و کاربراست . مشتری‌های CSP-۱ مسئول نگهداری از محرمانگی ، یکپارچگی و در دسترس بودن داده هایشان در ابر هستند و باید لزومات مشخصی را برای حفظ اطلاعات در هنگام ورود به SLA تدارک ببینند .مسیر موجود در SLA شامل بهترین اصول می‌شود) اما نه اینکه چگونه(، که می‌تواند به یک کاربر کمک کند قدرت یابد CSP-1. از سیستم مدیریت امنیت اطلاعات(ISMS) استفاده میکند و نشان می دهد که استراتژی امنیت ابر و پروسیجرهایی برای امنیت داده در CSP-1 به مشتری مربوط است.




شکل ۱ . مدل امنیتی CSP-1را همانطور که در یونیتاساقت مدلسازی شده است، نشان می دهد.

در مشخصه مسئولیت مشترک امنیت در CSP-1 اکثریت مسئولیت پذیری را برای امن کردن داده در CSP-1 همانطور که در شکل ۱ در مسیر سیستم امنیتی کاربر می بینید ، به عهده ی کاربر گذاشته است .عرضه کننده سیستم به مشتری اجازه می‌دهد تا مدل امنیتی خود را با استفاده از معماری امنیتی CSP-1 و مشخصات به عنوان شالوده آن طراحی کند . مسئولیت اصلی این عرضه کننده، ایمن کردن زیرساخت و سرویسهاست .امنیت امکانات ، سخت‌افزار، شبکه،زیرساخت مجازی را تأمین میکند. و به عنوان مثال این وظیفه ی کاربر است تا عکسهای ماشین، سیستم عامل، داده و اپلیکیشن ها، گواهی ها، و پیکربندی و موارد دیگری از عرضه کننده ی ابر را ایمن سازد .برای

CSP-1سرویسهای ذخیره سازی، مشتری  مسئولیت کامل برای امینت داده و تنظیم قوانین فایروال خودش و به دست آوردن کنترل برای دستیابی به سرویسها را دارد.

همانطور که در شکل ۱ مشخص شده ،  CSP-1 از مدیریت دسترسی و تشخیص هویت (IAM) در مدل امنیتی اش استفاده می‌کند تا کاربران ، اعتبارات)شامل رمز عبور، کلیددستیابی و گواهی های سرویس های مخصوص در ابر ( را مدیریت نماید .یک کاربر که به سیستم مشتری دسترسی دارد می تواند، برای CSP-1  ثبت نام نماید تا حسابی با نام کاربری و پسوورد ساخته شود.این کاربر ابتدا به سیستم کاربری وارد می شود )ورود و دستیابی به سیستم امنیتی کاربر (و از روال های امنیتی) فایروال مشتری، حفاظت ترافیک شبکه و رمزگذاری سمت کاربر (قبل از ورود به کنترل دسترسی به ابر،عبور می کند .در کنترل دسترسی به ابر ، کاربر می‌تواند از نام کاربری و پسوورد ابر برای دسترسی به آن و استفاده از کنسول مدیریتی مبتنی بر مرورگر از منابع آن استفاده نماید .مشتری می‌تواند کلید دسترسی برای همه کاربران را ایجاد کند که اجازه دسترسی به CSP-1  را  با IAM بوسیله یک خط فرمان واسط کاربری ایجاد میکند . بنابریان مشتری می‌تواند حسابهای  CSP-1 را با استفاده از IAM برای هرکاربر با نام کاربری جدا، رمز عبور و کلیدهای دسترسی به دست آورد .این به کاربران امکان وصول به کنسول ابر را ازطریق یک URL مشخص که به کاربر تعلق گرفته است را می دهد.

هنگامی که کاربر در حال عبور از راه کنترل دسترسی به ابر است )سیستم امنیتی ابر که در شکل ۱ آمده (می‌تواند به داده دسترسی پیدا کند اما برای داشتن امکان خواندن و نوشتن، کاربر باید از مراحل نظارتی دیگری جهت امنیت عبور کند مانند کلید رمز گذاری .برای رمز کردن دیتا جهت انتقال و  نگهداری و رمزگشایی به منظور استفاده از آن، مرکز داده و قسمتهای تشخیص نفوذ برای همه ی مدلها یکسان هستند .و در جایی دیگر از این مقاله در موردشان بحث شده است.

یک نمونه CSP-1  جدید می‌تواند از طریق پروتکلهای سیستم از راه دور امن ، مثل پوسته امن (SSH)یا پورتکل دسکتاپ از راه دور  (RDP)ایجاد و مورد استفاده قرار بگیرد . قبل از دسترسی و تشخیص نمونه بصورت ازراه دور باید درلایه بستر احراز هویت شود و سپس مکانیزم شناسایی میتواند نصب گردد .جهت اجراز هویت، CSP-1  ، از

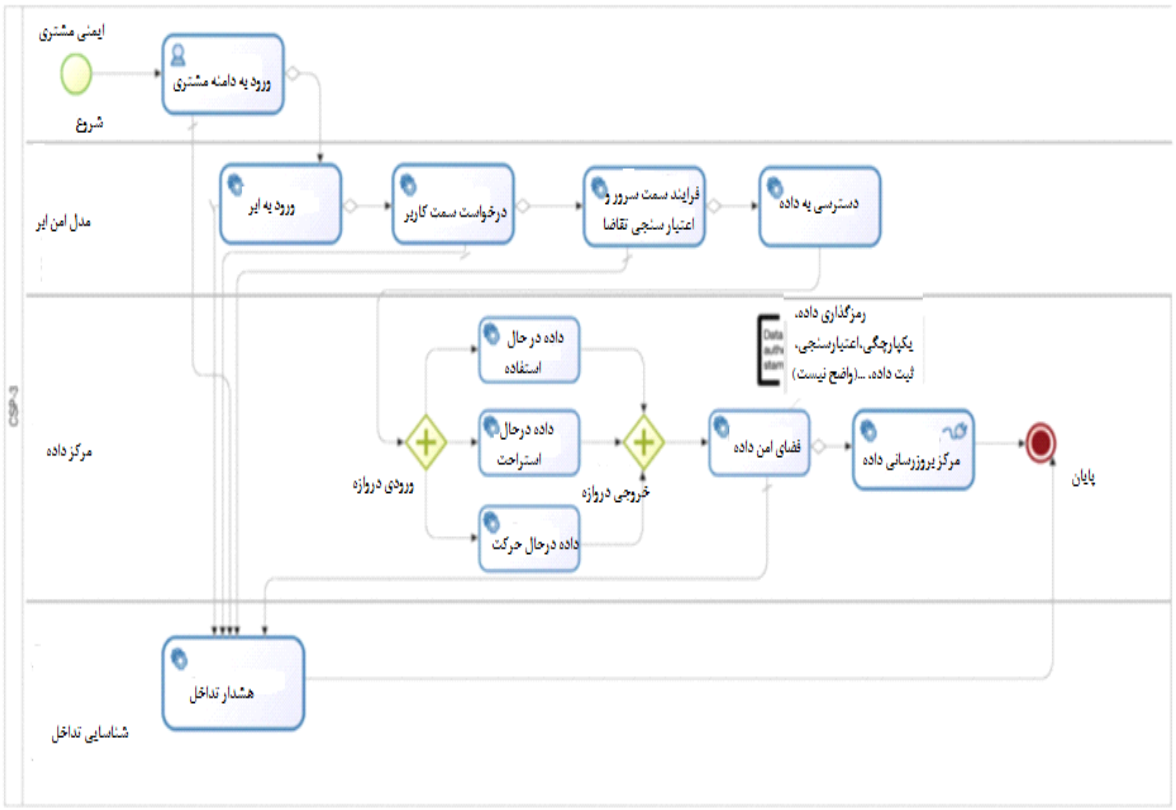
صنعت استاندارد RSA مربوط به جفت کلید های متقارن) کلیدهای خصوصی و عمومی را ارائه می دهند (استفاده میکند .که هرکدام از کاربران می توانندچند جفت کلید ، )برای شروع نمونه‌هایی با جفت کلیدهای متفاوت (داشته باشند .کلیدهای عمومی و خصوصی می‌توانند در یک محیط امن توسط کاربر با استفاده از ابزارهای استانداردی مانند openSSlایجاد شوند .این در مسئولیت مشتری است که کلیدها ، مخصوصاً کلیدهای خصوصی تولید و مدیریت کند . اما کلیدها می‌توانند در یک محیط ابر به وسیله CSP-1 تولید شوند و وقتی که یک نمونه برای اولین بار ساخته شود به کاربر داده شوند . در چنین مواردی کلیدها باید توسط کاربر دانلود و ذخیره شوند .اگر کلیدها گم شوند باید توسط کاربر مجدداً تولید گردند .این جفت کلیدها مربوط به ابر یا اعتبارات کاربر نمی باشند .اما برای آن هستند که به کاربر اجازه استفاده از یک نمونه مشخص را می دهند .در این مدل این‌ها از طریق کنترل دسترسی، مدلسازی و تشکیل می‌شوند.

در توافق مشترک مسئولیت پذیری در قبال امنیت ، CSP-1 پشتیبانی داده و ابزارهای ریکاوری را فراهم می‌کند . اما کاربر باید از ابزراها و تشخیص درست برای اصل بازسازی پس از تخریب استفاده نماید .

### ۵.۲. مدل امنیتی داده۳-CSP

استراتژی امنیت CSP-۳ در چندین مرحله ی ذخیره سازی داده ، دستیابی و انتقال با استفاده از اصول امنیتی به کارگیری داده، امنیت ساختاری کمپانی ، مدیریت داده، کنترل دسترسی ، امنیت پرسنل، امنیت زیرساختی و محیطی و فیزیکی، سیستم‌ها و توسعه ی نرم‌افزار و نگهداری و قدرت بازسازی تخریب و تداوم کاری است.در این قسمت امنیت نهادهایی که مربوط به امنیت داده در CSP-۳ هستند و در شکل ۲ نشان داده شده‌اند ، مورد بحث قرار می گیرند . عموما امنیت در CSP-۳ شامل چندین موضوع می‌شود که اصولی امنیتی را که باید بوسیله همه ی استعمال کنندگان در سطوح مختلف امنیتی برای تطبیق با حساب ها، داده‌ها و امنیت فیزیکی وهمچنین اصولی را که کارمندان باید اجرا کنند،به کار می‌گیرید . وقتی پرسنل CSP-۳ که از سیستم و اپلیکیشن یکپارچه استفاده می‌کنند ، باید طبق اصول کمپانی در استفاده درست از داده مربوط به فرایندهای کاری و خروجی های حاصل از تخلف کدهای اجرایی

که وابسته به داده مشتری است ، باشند .اصول امنیتی در زمانهای مشخص مورد ارزیابی قرار میگیرد و کارکنان، درمورد امنیت داده ، آموزش معمول و رسمی می بینند .امنیت CSP-۳ در چندین مورد دسته بندی شده است، مثل امنیت فیزیکی ، امنیت داده، امینت اطلاعات، امنیت پرسنل و غیره که هرکدام از تیمی از افراد تشکیل شده تا مباحث امنیتی را در دپارتمانهای مربوط به خود کنترل کنند . مشتری CSP-۳ و دارایی‌های کاربر و اطلاعات بوسیله این قوانین و روشهای امنیتی نظارت و مدیریت می گردند .




شکل۲. مدل امنیتی داده CSP-3 نشان می دهد

هر داده مشتری، سازماندهی شده یا نشده، در CSP-۳ در بین چندین سخت‌افزار همگن به اشتراک گذاشته شده است .مخزن داده ی CSP-۳ نیاز به شناسایی و احراز هویت دارد تا در دسترس اجزای دیگر قرار گیرد .احراز هویت بین یک سرویس تا یک سرویس دیگر براساس یک پروسیجر امنیتی است که وابسته به زیزساخت شناسایی هویت است . همانطور که در شکل CSP-۳ نشان داده شده است ، مدل امنیتی روی مسیر امنیتی ابر در شکل ۲، یک کاربر ورود پیدا کرده به محدوده ابر، باید دوباره جهت حدمات ابر لاگ‌این کند. وقتی که برای خدمات ابر وارد شدید

یک کاربر می‌تواند  از طریق یک اپلیکیشن سمت کاربر تقاضای داده معتبر را بدهد .همزمان اپلیکیشن سمت کاربر ، با فراخوانی سیستم مجازی ،نرم‌افزار سمت سرور را فراخوانی میکند تا تقاضا را تکمیل نماید  . نرم‌افزار سمت سرور فراخوانی سیستم را زمانی معتبر می‌داند که فراخوانی سیستم تنها از سمت کاربری معتبراز اپلیکیشن نرم‌افزار سمت کاربر باشد .اگر که فراخوان معتبر بود، اپلیکیشن سمت سرور یک فراخوانی سیستمی را برای لایه ذخیره سازی جهت دریافت داده مورد نظر ایجاد میکند .آنگاه تقاضا که اعتبار سنجی شده است توسط لایه ذخیره سازی هم شناسایی می‌شود واگر تقاضا کننده سمت سرور اول در نرم‌افزار سمت سرور دوم معتبر باشد پردازش می‌گردد و آنگاه می‌توان به داده موردنظر در مخزن دسترسی پیدا کرد .

داده  CSP-۳ در مقابل دسترسی نامعتبربا استفاده از چندین کنترل دسترسی ) اعتبار سنجی و شناسایی ( که در سیستم امنیتی موجودند، محافظت می‌شود . یکی از این کنترل های دسترسی از یک پسورد و آی دی یکتای کاربر استفاده میکند . یوزر و آی دی به CSP-۳  کمک می‌کند تا بر اعمال کاربرمانند اعمال روی شبکه ابر، دسترسی به ابر یا داده مشتری نظارت کرد . کلمه و عبارتهای ورودی که نیاز به تغییر دوره ای دارند جهت  اجراز هویت یک کاربر برای دسترسی به اپلیکیشنهای سمت کاربر است.سیستم ابر، کاربر را مجبور میکند تا کلمه های عبور و عبارتهای ورودی اش را تغییر دهد .با تغییر کلمه های عبور در حین زمان انقضای آنها، محدود سازی استفاده مجددشان و با پیروی از قوانین مشخص  پسورد هایی را که از قدرتشان مطمئن است می سا.زد CSP-۳ .از تکنیک های اعتبار سنجی دومرحله ای استفاده میکند ، شامل گواهی ها و تعبیه کنندگان کلمه عبور .اعبتار سنجی دومرحله ای برای دستیابی به سرویس ابر، منابع و یا استفاه از اپلیکیشن ها ی شخص ثالث که از اپ ابر استفاده میکنند ضروری است .کنترل دسترسی بر اساس نقش کاربر در ابر و نحوه ی مشتری بودن است .برای دستیابی مستقیم بیشتر به داه ، یک کاربر بایداجراز هویت مجددی را برای دسترسی مطمئن توسط یک صاحب سیستم داده مدیر یا مجریان تقاضا کند .

**۶. شبیه سازی BPMN برای امنیت:**

این بخش راجع به شبیه سازی مدل های امنیتی با استفاده از BPMN است BPMN .یک زبان تصویری است که برای شناسایی فرایندها و نیازمندی ها و تخصیص های فرایند شناسایی استفاده شده تا کارایی یک سیستم را ارزیابی نماید .شبیه سازی یک فرایند کمک میکند تا عمل‌کرد کار با توجه به ورود اتفاقات منتظره و غیرمنتظره در فرایند ارزیابی شود . بنابراین ، استفاده شبیه سازی BPMN در مدلهای امنیتی ابر، به ارزیابی عمل‌کرد وکارایی فرایند های مختلف و وظایف داخل مدل برای سناریوهای منتظره و غیر منتظره کمک میکنند)شانگ و راماشاندران،۲۰۱۶ ;شانگ و همکاران، ۲۰۱۶ .(

همانگونه که در بخش ۲ گفته شد، دلیل اینکه BPMN برای شبیه سازی مدل امنیتی انتخاب شده این است که میتواند زمان اجرای فرایند ایمن سازی و محافظت از مرکز داده را ارایه دهد .بعلاوه نکته مهم دیگر که ارزش اشاره درمورد مدلسازی فرایند کاری ( BPMN ) دارد، آن است که به شناسایی فرایند کسب و کار کمک میکند تا بصورت عمومی روی سیستم به صورت بالقوه تأثیر داشته باشد و بطور مشخص به سرمایه گذاران وتحلیلگران کسب وکار اجازه می دهد تا مهمترین فرایندهای کاری را اولویت بندی کنند .

همانطور که در بخشهای قبلی گفته شد، مدلهای معماری امنیتی داده ابر شامل سرمایه گذارانی هستند در ادامه آمده اند:

۱. مشتری( مصرف کننده خدمات سرویس) که کاربران رادر ابر ثبت نام میکنند.

۲. ارایه دهنده سرویس ابر که شامل قسمتها ی زیر است:

- سیستم امنیتی ابر/ سستم مدیریت ابر
- مرکز داده و مخزن منابع
- شناسایی حمله و فرایند جلوگیری از تداخل

مشتری رایانش ابری می‌تواند کامپیوترها و اپلیکشن های طراحی شده جهت دستیابی و استفاده از خدمات رایانش ابری باشد .بعضی از کامپیوترها رابط کاربری را از طریق پایانه ها ومروگرهای وب در اختیار کاربر قرار می‌دهند . CSPبخشی است که سرویسهای ابر را با استفاده از مدلهای ارسال خدمت از طریق اینترنت عرضه میکند.

### ۶.۱. چگونه BPMN می‌تواند برای ایجاد امنیت مفید باشد.

این بخش توضیح می‌دهد که چگونه استفاده از BPMN می‌تواند برای امنیت کسب وکارها مفید و مناسب باشد . در این مقاله کاربر به مخزن داده ابر از طریق لاگ‌این به دامنه کاربر و استفاده از اعتبارات ابر که برای کاربر فراهم شده است دسترسی پیدا میکند .مدلهای امنیتی CSP-۱ و CSP-۳ از این دست می باشند.در نمونه اول وقتی که تقاضا به ابر فرستاده می‌شود از میان سنجش های امنیتی و مدیریتی عبور می کنند .در نمونه دوم ارسال برای تقاضای داده نیست اما تنها ورود به سیستم مشتری و دسترسی به ابر با استفاده از اعتبارات مشتری وجود دارد .هنگامی که تقاضای داده کاربر درسیستم ابر نمونه اول یا در نمونه دوم در است ، از میان چندین آزمون امنیتی شامل تیم مدیریتی ابر در سیستم امنیتی ، مخازن امن در مراکز داده عبور میکنند .اگر تقاضا یا گواهی از یکی از لایه‌های امنیتی در هرکدام از لایه‌های سیستم امنیتی داده در ابر عبور کرد،به بخش شناسایی حمله و سیستم جلوگیری از تداخل منتقل میشود.

مرکز داده یک بخش مهم ازCSP هااست . مخصوصاً آن‌هایی که بخش ذخیره سازی یک سرویس را فراهم میکنند . مرکز داده به سرور ها، سرویسهای ذخیره سازی داده و اپلیکیشنهای درون ابر وصل است . کارایی دادو ستد ابر وابسته به مرکز داده ، حمایت و عمل‌کرد آن است . ار آنجایی که مرکز داده که نقشی حیاتی را در کار ابر ایفا می کند، مهم است که مطمئن شویم بصورتی کارا مدیریت می شود، سرویسش به دقت طراحی شده است تا عمل‌کرد روبه روشد راهدایت نماید و نیازهای اپلیکیشن را فراهم سازد . مرکز داده درهمه ی معماری های امنیتی ، با یک تصمیم مبنی بر حالات دیتا ) در استفاده، در حرکت و در استراحت (شروع می‌شود . زمانی که کاربر از دروازه ی

وضعیت عبور کرد، او به یک داده تبدیل می‌شود که در یک حالت قرار دارد .قبل از رهاسازی کامل داده و رفتن به انتهای دسترسی داده، باید از مخزن امنیتی عبور کندکه میتواند شامل رمزگذاری و بروزرسانی مرکز داده شود .

بخش شناسایی تداخل سیستم امنیتی ابر، مرکز داده و مشتریان و یاکربران را از وجود یک حمله نفوذی یا تداخل آگاه می سازد .اگر هر تداخلی بخواهد اتفاق بیفتد، سیستم باید ایمیلی را تهیه و به بخش‌های مسئول ارسال نماید .

در همه ی مدلهای امنیتی برای تحلیل ، کلیدهای اجزا که وابسته به این کاردر معماری رایانش ابری هستند ،شامل مشتریان ابر ، کاربران )CSP تیم مدیریت امنیت، حالت داده، مخزن امنیتی و بروزرسانی داده در مرکز داده و شناسایی تداخل (و تستهایی که فرایند شناسایی تداخل در آن عمل میکند، میشود.فرایندهایی که نیاز به شبیه سازی دارند با استفاده از BPMN بصورت خلاصه به این شرح اند:

۱. کاربری که میتواند مشتری یا عضو کارکنان باشد و یک تقاضا را به CSP از طریق دامنه اینترنت مشتری و یا ازخارج ارسال میکند.در بونیتاسافت BPMN ، این یک عامل برای شروع شبیه سازی فرایند با ارسال یک پیغام تقاضای داده بصورت مستقیم به ابر یا از طریق سیستم مشتری که به تقاضا رسیدگی میکند و پیام تقاضا را به ابر می‌فرستد با نیمی از سمت کاربر می باشد .یک عامل در بونیتاسافت جایی برای کاربر است که وظایفی را دریک پروسه انجام میدهد.

۲. پیغام تقاضای داده که وارد سیستم ابر شده است، از تعدادی آزمونهای امنیتی عبور می‌کند که وابسته به مدل امنیتی آن عرضه کننده ی مشخص ابر است .به عنوان مثال :

• ارسال کننده هویت ، توسط مکانیزم های کنترل دسترسی و فایروال چک می شود. مدیریت هویت مؤکد شده تا سطح دسترسی درست را تنها به یک شخص معتبر اعطا کند.

• شناسایی تداخل و فرایند جلوگیری بوسیله ی شناسایی حملات و تداخل ها و نفوذ با استفاده از ارایه فناوری های بروز جهت جلوگیری از حملات مانند Dos ، ضد کلاهبرداری، اسکن کردن پورت ها ، شناسایی آسیب‌پذیری ها، حملات مبتنی بر الگو، دستکاری پارامترها، تزریق کد XSS، تزریق SQL و مسموم سازی کوکی ها، اتفاق می افتد.

• از میان فرایندهای رمز گذاری عبور میکند. رمز گذاری به محض اینکه رفتار موجودیت بصورت غیر نرمال باشد نگرانی‌های اولیه را نشان میدهد .

• وضعیت‌ها را براساس دستیابی به داده در مرکز داده بروزرسانی میکند.

• اگر تداخلی اتفاق بیفتد در هر مرحله یک پیام باید برای نمایش ارسال شود. برای شناسایی اینکه کدام نوع حمله امنیتی بوده ، یک پیغام هشدار به CSP، به مشتری و کاربر بسرعت هرچه تمامتر ارسال می‌شود.

۳. مرکز داده ابر ، داده از وضعیتهای داده‌ای و سایر مخازن امن در همه مدلهای امنیتی مورد نظر گذر میکند. در این نمونه مراحل به جزییات در زیر آمده است:

• دیتا از مرحله تصمیم گیری وضعیت عبور میکند که این مرحله به فرایند شبیه سازی امکان عبور از مراحل مختلف را بسته به حالت داده( در استفاده ، در استراحت، در جریان) در ابر می دهد.

• داده باید از حفاظت های دیگری هم بگذرد که اعمالی جداگانه در مرکز داده هستندبا فرایندهای امنیتی مشخص ( فضای داده امنیتی و بروزرسانی مرکز داده) که کمک میکند تا کنترلهای امنیتی در محلی قبل از اتمام بررسی شوند.

• در نهایت دسترسی داده بنا به هویت عاملی که فرایند را آغاز کرده است بروز رسانی می شود.

۴ . مسیری دیگر از مدلهای امنیت بخش شناسایی تداخل است . این بخش به توجه بیشتری نیاز دارد. از سه مسیر در فرایند شبیه سازی، بخش تأمین کننده امنیت ابر،بخش مرکز داده و بخش امنیت مشتری. اگر هر مورد مشکوکی راجع به امنیت شناسایی شد، در هرکدام از وظایف این سه مورد، آژیر خطر امنیت به صدا در می‌آید و دو طرف را بسرعت مطلع می سازد.

## ۷. نتیجه گیری

بصورت خلاصه BPMN می‌تواند برای کسب و کار، مناسب باشد .بدلایلی که در ادامه می آید .اول اینکه آن‌ها می‌توانند مشکلاتی را که بخاطر یک نفوذ امنیتی رخ داده است، کدام بخش از سرویس امنیتی در خطر است و زمان بازیابی دیتا را برای بازگرداندن سیتم به حالت عادی ، شناسایی کنند . . ثانیاً می‌توانند انگیزه‌های لازم برای طراحی

سرویس امنیتی را فراهم کنند که به سازمان اجازه می دهد سرویس امنیتی فعلی خود را بررسی نمایند، محدوده ی عنوان شده طراحی توسط طراحی سیستم و ارزیابی فضاهای رشد پیشنهادی را شناسایی کنند .مثالهای دو ارائه دهنده سرویس در این مقاله نشان می‌دهند که BPMN می‌تواند راه حلی سودمند برای طراحی امنیتی و برقراری اطمینان از امنیت داده باشند.

امنیت یک حوزه ی پیچیده است که شامل جنبه‌های مختلفی از قبیل رمزگذاری، فایروال، کنترل دسترسی ، مدیریت هویت، احراز هویت، شناسایی، مدیریت مرکز داده و شناسایی تداخل است .تکنیکهای مختلف و توصیه‌هایی نیازمندند تا تحویل یک سیستم را قدرتمند و قابل اطمینان سازند تا بتواند در مقابل حملاتی چون تزریقSQL ، نادیده گرفتن سرویس ، ویروسها و تروجان ها، ضد کلاهبرداری، اسکن کردن پورتها، تزریق کدهای XSS ، حمله فیشینگ ودسترسی نامعتبر، مقاومت کند . بنابراین دستیابی کامل و همه جانبه نیازمند سرویس های امنیتی مختلف است تا همه ی کاربران را در مقابل هک شدن و دستیابی نامعتبر محافظت کند. یکی از این موارد با استفاده از یک فریم وورک می باشد که نه تنها شامل توصیه‌هایی برای اصول امنیتی ، آموزش و بهترین سرمشق هاست، بلکه شامل راه حل های امنیتی برای هر جنبه کلیدی امنیت است که در بالا گفته شد .به عنوان مثال به تصویر کشیدن امنیت توسط فری وورک (CCAF) (Cloud Computing Adoption می‌تواند لایه‌های چندگانه و سرویسهای امنیتی چند منظوره را فراهم سازد .این شامل هماهنگی همه ی سه بخش اصلی راه حل امنیتی می‌شود که میتواند حملات را کم کند .همانگونه که با آزمون نفوذ در قیاس بزرگ و هک های اخلاقی نشان داده شده ، استفاده از دیتابیسهای NoSQLمی‌تواند کمترین آسیب‌پذیری را از طریق تزریق SQL که توسط تستی بر مقیاس بزرگ توسط هک کردن اخلاقی اجرا شد، نشان دهند)شانگ و همکاران ،۲۰۱۶.(

بنابراین استفاده از دست آورد فریم وورک مربوط به سرمایه گذاراها است زیرا سرویسها و همه ی انواع داده هایشان باید محافظت شوند BPMN .می‌تواند بعداً در ورژن دو CCAF مورد استفاده قرار گیرد که از این طریق BPMN می‌تواند هرزمان برای شناسایی طراحی امنیت و ارزیابی عملکرد مورد استفاده قرار گیرد BPMN .میتواند زمان

،اثرات و ضعف لینکها را شبیه سازی ) بنابراین نقاط آسیب پذیر (و به مدیر سیستم گزارش کند تا در برابر حملات وقتی که سرویسها در معرض حملات شناخته شده هستند،دفاع نماید.

BPMNمی تواندبه صورت کامل با ورژن دوم CCAF ادغام شود تا یک سیستم امنیتی قابل اطمینان ، چابک و محکم را برای سرمایه گذاران ایجاد کند.

## ۸. نتیجه‌گیری و چشم انداز آینده

این مقاله در ابتدا با لحنی عمومی در مورد ابر و امنیت داده شروع می‌شود و اعمال موجود را ارزیابی می کند .استفاده از BPMN به عنوان سرویسی برای تأمین امنیت داده و طراحی امنیت عنوان می شود .دو نمونهCSP در این مقاله عنوان می‌شود و جزییات طراحی امنیتی آن‌ها تشریح میگردد .طبق یک طراحی منطقی، همه ی داده‌ها در خلال نفوذ امنیتی، استفاده از BPMN ایمن می‌مانند BPMN .می‌تواند مشخص کند که کدام بخشهای سرویس امنیتی تحت حمله است و بنابراین می‌توان زمان و منابع را برای اجرای روال بازسازی حفظ کند BPMN .می‌توان برای حمایت از امنیت داده همانطور که با مثالهایی از دو ارایه دهنده سرویس نشان داده شد مؤثر باشد .کار بعدی شامل شبیه سازی مقیاس بزرگ و ارزیابی ها ی عملکرد BPMN برای این دو ارائه دهنده سرویس است .بعلاوه سرویسهای امنیتی جدید، طراحی خواهند شد تا سطوح بالاتری از امنیت را به نمایش گذارند که می‌تواند منجر به دست یابی یک عمل‌کرد خوب در شناسایی مشکلات شوند ، عملیات قرنطینه سازی را برای فایلهای آسیب دیده انجام داده و این داده‌ها را در خارج از سیستمهای ایمنی ذخیره سازند BPMN .با نسخه ی دوم CCAF ادغام خواهد شد تا برای کسب و کارها سرویس امنیتی چابک و مطمئنی را فراهم سازد

## References


Ackermann, T. (2013). IT security risk management: perceived IT security risks in the context of cloud computing. Springer Gabler.

AlZain, M. A., Soh, B., & Pardede, E. (2013). A survey on data security issues in cloud computing: from single to multi-clouds. Journal Of Software, 8, 1068–1078.

Alzain, M. A., Pardede, E., Soh, B., & Thom, J. A. (2011). Cloud Computing security: from single to multi-clouds. Proceedings of the HICSS, 5490–5499.

Armbrust, M., Stoica, I., Zaharia, M., Fox, A., Griffith, R., Joseph, A. D., et al. (2010). A view of cloud computing. Communications of the ACM, 53, 50–58.

Chang, V. (2015). Towards a big data system disaster recovery in a private cloud. Ad Hoc Networks, 35, 65–82.

Chang, V., Kuo, Y. H., & Ramachandran, M. (2016). Cloud computing adoption framework: a security framework for business clouds. Future Generation Computer Systems, 57, 24–41.

Chang, V., & Ramachandran, R. (2016). Towards cloud data security proposed and demonstrated by cloud computing adoption framework. IEEE Transactions on Service Computing, 9(1), 138–151.

Creeger, M. (2009). CTO roundtable. Communications of the ACM, 52, 50.

Cusumano, M. (2010). Cloud computing and SaaS as new computing platforms. Communications of the ACM, 53, 27–29.

Daniel, E. M., & Wilson, H. N. (2003). The role of dynamic capabilities in e-business transformation. European Journal of Information Systems, 4, 282–296.

Dikaiakos, M. D., Katsaros, D., Pallis, G., Vakali, A., & Mehra, P. (2009). Cloud computing. IEEE Internet Computing, 12, 10–13.

K. Flinders, K. (2014). Banks could lower costs with cloud computing, but there are risks too. Available from: http://www.computerweekly.com Accessed 25.05.14.

Fogarty, K. (2009). Cloud Computing definitions and solutions Available from: http://www.cio.com/article/print/501814 Accessed 25.05.14.

Gill, P. S. (2013). Cloud computing and enterprise systems: applications in the auto industry. The International Journal of Technology, Knowledge and Society, 9, 1832–3669.

Hoberg, P., Wollersheim, J., & Krcmar, H. (2012). The business perspective on Cloud Computing: A literature review of research on Cloud Computing. Proceedings of the AMCIS,

Iyer, B., & Henderson, J. C. (2010). Preparing for the future–understanding the seven capabilities of cloud computing. pp. 117-131. MIS Quarterly Executive.

Julisch, K., & Hall, M. (2010). Security and control in the cloud. Information Security Journal: A Global Perspective, 19, 299–309.

Kamara, S., & Lauter, K. (2010). . pp. 136–149. Cryptographic cloud storage Lecture Notes in Computer Science (6054) Springer.

Katz, R. (2009). Tech titans building boom. IEEE Spectrum, 40–54.

Kaufman, L. M. (2009). Data security in the world of cloud computing. IEEE Security and Privacy, 7, 61–64.

Linthicum, D. (2009). Defining the Cloud Computing Framework: Refining the concept. Available from: http://cloudcomputing.sys-con.com/node/811519 Accessed 23.03.14.

Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud security and privacy. O'Reilly Media Inc.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. NIST Special Publication [800-145]

Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of cloud computing. Journal of Supercomputing, 63, 561–592.

Overby, E., Bharadwaj, A., & Sambamurthy, V. (2006). Enterprise agility and the enabling role of information technology. European Journal of Information Systems, 15, 120–131.

Popa, R. A., lorch, J. R., Molnar, D., Wang, H. J., & Zhuang, L. (2010). Enabling security in cloud storage SLAs with cloud proof. Technical Report. Microsoft Research.

Prasad, P., Ojha, B., Shahi, R., & R.and Lal, R. (2011). 3-Dimensional security in cloud computing. Computer Research and Development (ICCRD), 3, 198–208.
Pröhl, T., Repschläger, J., Erek, K., & Zarnekow, R. (2012). IT- Service management in Cloud Computing. In HMD—Praxis der Wirtschaftsinformatik. pp. 6–14. Springer.
Rountree, D., & Castrillo, I. (2014). The basics of cloud computing: understanding the fundamentals of cloud computing in theory and practice (1st ed.). Elsevier Inc.
Sood, S. K. (2012). A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35, 1831–1838.
Stieninger, M., & Nedbal, D. (2014). Characteristics of cloud computing in the business context: a systematic literature review. Global Journal of Flexible Systems Management, 15, 59–68.
Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34, 1–11.
Toxen, B. (2014). The NSAand snowden: securing the all-seeing eye. Communications of the ACM, 57, 41–55.
Wade, H. B., Hylender, C. D., & Valentine, J. A. (2008). Verizon Business 2008 data breach investigation report Available from: http://www.verizonbusiness.com/ resources/ Accessed 20.03.14.
Wang, C., Cao, N., Li, J., Ren, K., & Lou, W. (2010). Secure ranked keyword search over encrypted cloud data. Journal of the ACM, 43, 431–473.
Winkler, V. J. R. (2011). Securing the cloud: cloud Computer security techniques and tactics. Elsevier Inc.