مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۳ ، پاییز ۱۳۹۵، ص ۴۱-۳۴

ISSN: 2745-3673
http://www.Rcsj.ir

مجلـه‌ی علمی پژوهش در علوم رایانه (سال دوم)
شماره ۳ / پاییز ۱۳۹۵ / ص ۴۱-۳۴

پردازش ابری، نگرانی ها و تهدیدات امنیتی و گذری بر راه حل های موجود در جهت رفع آن ها

زهرا شاه قلیان[۱]، مهدی خلیلی[۲]

[۱] دانشجوی کارشناسی ارشد، گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه پیام نور، تهران، ایران

[۲] استادیار، گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه پیام نور، تهران، ایران

نام و نشانی ایمیل نویسنده مسئول:

زهرا شاه قلیان

zahra.sh1990@gmail.com

چکیده

پردازش ابری پاسخ فناوری به نیازهای امـروزی افـراد جهـت انجـام کارهـای محاسـباتی سـنگین و دسترسی به حافظه های بزرگ بدون نیاز به سخت افزار و یا نرم افزارهای گـران اسـت. امـا همـواره شروع و ادامه فناوری های نوظهور نگرانی هایی را برای مصرف کنندگان به همراه مـی آورد. هرچـه از زمان استقاده از ابرها می گذرد و حجم اطلاعات آن ها بالاتر می رود تهدیدات امنیتـی پـیش رو نیز بیشتر می شود و نبود امنیت، خسارات جبران ناپذیرتری را به ارمغان می آورد. از این رو در ایـن مقاله مروری پس از بررسی فناوری پردازش ابری، به بررسی نگرانی های مصـرف کننـدگان ابرهـا و تهدیدات امنیتی پیش روی آنان پرداخته شده و در انتها گذری بر برخی از راه حل های امنیتی کـه تاکنون مطرح شده، داشته است.

واژگان کلیدی: پردازش ابری، نگرانی های امنیتی، تهدیدات امنیتی، امنیت، راه حل های امنیتی

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

با توسعه سریع فناوری های پردازش و ذخیره سازی، لزوم استفاده از منابع محاسباتی ارزان تر و قوی تر، بیشتر مورد توجه قرار می‌گیرد. پردازش ابری نمونه ای مناسب برای پاسخگویی به این نیازهاست. واژه ابر به اینترنت اشاره دارد و دلیل تشبیه در این است که اینترنت همانند ابری جزئیات فنی خود را از دید کاربرانش پنهان می سازد و لایه ای از انتزاع را بین این جزئیات و کاربران به وجود می آورد.

طبق تعریف موسسه ملی استاندارد و فناوری (NIST)[1] رایانش ابری، مدلی است برای فراهم کردن دسترسی آسان براساس درخواست کاربر از طریق شبکه به مجموعه‌ای از منابع محاسباتی قابل تغییر و پیکربندی (مانند: شبکه ها، سرورها، منابع ذخیره سازی، برنامه های کاربردی و خدماتی.). این دسترسی باید بتواند با کمترین نیاز به مدیریت منابع و یا نیاز به دخالت مستقیم ارائه دهنده، خدمات را به سرعت فراهم و عرضه کند[۱] .

یکی از مهم‌ترین شاخص‌های استفاده ازخدمات ابری وجود این ویژگی است که فناوری ابرها به دور از کاربر است. بدین صورت که مسئولیت دارایی‌های فناوری اطلاعات و نگهداری از آن دارایی‌ها، به ارائه دهنده خدمات پردارش ابری منتقل می شود. کاربران پردازش ابری قادر به تمرکز بر روی ارزش دریافت شده از ابر، به عنوان یکی از راه های سنجش کیفیت پردازش ابری هستند. پردازش ابری می تواند انواع مختلف از حجم کارهای فراوان را در یک زمان انجام دهد[۲]. استفاده از رایانش ابری مزایای بسیاری از جمله: استقرار سریع، هزینه-های پایین تر، مقیاس پذیری، تأمین سریع، دسترس‌پذیری، انعطاف‌پذیری، هزینه اندک بازیابی اطلاعات، راه حل های ذخیره سازی، مدیریت در جهان تغییرات و ... را به ارمغان می‌آورد[۳]. با وجود این ویژگی های جذاب که ابرها وعده داده اند، نرخ مهاجرت به آن ها آهسته است که این مورد به علت چالش های امنیتی ذاتی همراه با این فناوری است. این چالش ها عبارتند از حریم خصوصی داده‌ها، شفافیت، مدیریت ریسک، انطباق و امنیت اطلاعات[۴, ۵].به نظر می‌رسد برای بسیاری از مشتریان، تنها امن بودن سیستم ملاک اعتماد به این فناوری است .گرچه امنیت مطلق چه درمحیط واقعی و چه در فضای مجازی دست نیافتنی است، ولی ایجـاد سطحی از امنیت که به اندازه‌ی کافی و متناسب با نیازها باشـد، تقریبا در تمامی شرایط محیطی امکان‌پذیر است. تنها با فراهم بودن چنین سطح مطلـوبی اسـت کـه اعتماد و اطمینان به فناوری‌های نو میسر می گردد. از این رو در این مقاله مروری سعی شده است پس از بررسی تکنولوژی ابرها، و بررسی نگرانی های موجود جهت استفاده از آن ها، به تحلیل تهدیدات امنیتی که ابرها در معرض آن هستند پرداخته شود. در انتها گذری بر برخی راه حل‌های موجود در جهت رفع این تهدیدات صورت گرفته است.

۱- پردازش ابری

ابرها سیستم‌هایی پویا و پیچیده با کاربران متعدد هستند. این پیچیدگی‌ها را می توان به مغز انسان تشبیه کرد که در آن سلول-های عصبی به طور مداوم برای ذخیره اطلاعات به سیناپس‌ها متصل می‌شوند[۶]. نسل‌های اخیر رایانش ابری تجمیع و ترکیبی از زیرساخت‌هایی شامل سرورها، نرم‌افزارهای کاربردی، داده ها و سکوهای سخت‌افزاری و نرم افزاری گوناگون هستند که می‌توانند بدون آگاهی دقیق از مکانی که در آن واقع شده‌اند، به استفاده از این زیر ساخت ها بپردازند[۷].این زیرساخت‌ها ما را قادر به توسعه و دریافت خدمات از طریق اینترنت یا یک شبکه خصوصی می‌کند. در رایانش ابری، مدیریت منابع و دخالت مستقیم تأمین‌کننده به حداقل می‌رسد و سرویس‌ها به سرعت فراهم و آزاد می شوند. طبقه‌بندی های رایانش ابری بر اساس مدل‌های سرویس‌دهی یا معماری ساخت و میزان توسعه آن‌ها می‌باشد . که دو دسته از مهمترین آن ها در ادامه آورده شده است.

۱-۱-۱ طبقه‌بندی بر اساس مدل‌های خدمات

این طبقه بندی شامل سه مدل پردازش ابری است که عبارتند از:

زیرساخت به عنوان یک سرویس[2](IaaS): استفاده از منابع محاسباتی زیرساختی از قبیل حافظه‌ها، شبکه‌ها، سرورها و دیگر منابع محاسباتی اساسی است که به منظور ارائه خدمات به کاربران نهایی استفاده می‌شود و به آن ها اجازه می‌دهد نرم افزارهایی همچون سیستم‌های عامل و سایر نرم‌افزارهای کاربردی را پیاده‌سازی و اجرا کنند. مصرف‌کننده می‌تواند بر سیستم های عامل، حافظه و برنامه‌های کاربردی مستقر، کنترل داشته باشد .

[1] National Institute of Standards and Technology
[2] Infrastructure as a service

ISSN: 2745-3673
http://www.Rcsj.ir

پلتفرم به عنوان یک سرویس [۳](PaaS):استفاده از ابزارها و منابعی است که به منظور ارائه خدمات به کاربران نهایی در یک زیرساخت ابری اجرا می‌گردد و در آن زبان‌های برنامه‌نویسی تولیدشده و سایر ابزارها توسط ارائه‌دهنده حمایت می‌شوند. مصرف‌کننده کنترلی بر زیرساخت های پایه‌ای شامل شبکه‌ها، سرورها، سیستم‌های عامل و حافظه ندارد، اما استقرار و اجرای نرم‌افزارهای کاربردی شخصی را تحت کنترل دارد.

نرم‌افزار به عنوان یک سرویس[۴](SaaS): استفاده از نرم‌افزارهای کاربردی به منظور ارائه خدمات به کاربران نهایی در یک زیرساخت ابری است. برنامه‌هایی که از دستگاه‌های مختلف از جانب مشتری با یک رابط (مانند یک مرورگر وب) در دسترس هستند. مصرف‌کننده کنترلی بر زیرساخت‌های پایه ای از جمله شبکه، سرورها، سیستم عامل و حافظه ندارد[۸].

۱-۱-۲ طبقه بندی بر اساس معماری ابر

این طبقه‌بندی شامل چهار مدل پیاده سازی برای معماری ابر را به شرح زیر ارائه می دهد :

ابر خصوصی[۵] : زیر ساخت‌های ابری که در مالکیت یا اجاره یک سازمان خصوصی است . در واقع تمامی منابع اصلی ابر، برای استفاده خصوصی به یک سازمان خاص واگذار می‌گردد و به وسیله آن سازمان یا شخص ثالث اداره می شود.

ابر عمومی[۶]: زیرساخت‌های ابری که متعلق به سازمان فروش خدمات ابر است، اما برای عموم مردم یا گروه های صنعتی بزرگ قابل دسترس است.

ابر گروهی[۷]: این ابر مشابه ابر خصوصی است، با این تفاوت که زیر ساخت‌های آن بین اعضای یک گروه و یا چندین سازمان خصوصی به اشتراک گذاشته می‌شوند و به وسیله سازمان‌ها یا شخص ثالث اداره می‌شوند.

ابر ترکیبی[۸]: این ابر ترکیبی از دو یا چند زیرساخت ابری(خصوصی، عمومی، گروهی) است که با استانداردسازی یا فناوری اختصاصی محدود شده است. هدف اصلی ابر ترکیبی، معمولا اختصاص منابع اضافی در مورد تقاضاهای بالا است[۹].

۲- نگرانی های امنیتی در پردازش ابری

حداکثر ظهور پردازش ابری نگرانی‌های امنیتی را برای کاربران ابرها به وجود آورده است که عبارتند از :

دسترسی شبکه: ارزش پردازش ابری زمانی است که حداقل نیاز شما از اتصال به شبکه و پهنای باند را در هر زمانی که به آن نیاز دارید فراهم نماید. اگر اینگونه نباشد موقعیت عدم دسترسی، خود تهدیدی برای کاربران خواهد بود.

بقاء ارائه دهنده ابر: از آنجا که ارائه‌دهندگان ابر در دنیای کسب و کار نسبتا جدید هستند مسأله تعهد و بقای آن‌ها باید مورد توجه قرار گیرد. کاربران می خواهند مطمئن باشند ابری که از آن استفاده می کنند در طی سال های آتی از بین نخواهد رفت و به ارائه خدمات خود ادامه می دهد.

بازیابی و تداوم کسب و کار: لازم است کاربران مطمئن باشند که خدماتی که دریافت می کنند تداوم داشته باشد، حتی اگر ارائه‌دهندگان محیط ابر در معرض خطر باشند.

حوادث امنیتی : وقتی که یک حادثه در حال وقوع است، کاربر باید به موقع توسط ارائه‌دهنده از حادثه باخبر شود و در صورت نیاز توسط ارائه‌دهنده در قبال خطرات حمایت شود. ممکن است ارائه‌دهنده حمایت کافی برای کاربران نداشته باشد.

شفافیت: ارائه‌دهندگان ابر، جزییات خط مشی داخلی و یا پیاده‌سازی خود را در اختیار قرار نمی دهند. از این‌رو کاربران باید به ادعاهای امنیتی آنان اعتماد کنند. با تمام این تفاسیر، لازم است ارائه‌دهنده ابر، برخی از موارد امنیتی، حریم خصوصی و یا چگونگی مدیریت حوادث را شفاف سازد.

فقدان کنترل فیزیکی: چون در ابرها کاربران کنترل فیزیکی روی داده ها و نرم افزار های کاربردی خود ندارند، طیف وسیعی از نگرانی‌ها برای آن‌ها پیش می‌آید.

---

[3]Platform as a service
[4]Software as a service
[5]Private cloud
[6]Public cloud
[7]Community cloud
[8]Hybrid cloud

ISSN: 2745-3673
http://www.Rcsj.ir

حریم خصوصی داده‌ها : در ابر گروهی و عمومی ممکن است داده‌ها در یک سیستم باقی نمانند و این خود موجب نگرانی‌های متعدد کاربران می‌شود.

کنترل داده‌ها : داده های کاربران و سازمان ها ممکن است به طرق مختلف به داده های سایرین ملحق گردد. یک ارائه دهنده ابر، دامنه کنترل محدودی در IaaS و حتی کمتر از آن در PaaS دارد. از این رو لازم است کاربر به ارائه دهنده برای ایجاد کنترل مناسب، اعتماد کند.

خطرات جدید، آسیب‌پذیری‌های جدید: پردازش ابری قشرهای جدیدی از خطرات و آسیب‌پذیری‌ها را به همراه می‌آورد. با وجود اینکه ما می‌توانیم حدس‌هایی راجع به این خطرات داشته باشیم اما سوءاستفاده‌های واقعی تا حد زیادی تابعی از روش پیاده‌سازی ابر است. اگرچه همه‌ی نرم‌افزارها، سخت‌افزارها و تجهیزات شبکه در معرض این آسیب‌های جدید هستند، یک ابر می‌تواند با استفاده از لایه-های امنیتی و درک مناسب فرآیندهای عملیاتی، از آن‌ها محافظت کند.

الزامات قانونی و مقررات: اگر داده‌هایی که شما نیاز به پردازش آن‌ها دارید موضوعی است که محدودیت‌ها و الزامات قانونی دارد ممکن است استفاده از ابرهای عمومی مشکل یا غیرواقعی باشد. در حالیکه ما انتظار داریم ارائه -کنندگان یک ابر آن را تضمین و برای آن گواهی صادر کنند تا نیاز بازارهای تحت نظارت را پاسخگو باشد، ممکناستبه دست آوردن این گواهینامه‌ها به دلیل بسیاری از عوامل غیرفنی به چالش کشیده شود[۱۰].

۳- مفاهیم امنیت

تعریف امنیت: امنیت، حالت فراغت نسبی از تهدید یا حمله و یا آمادگی برای رویارویی با هـرتهدیـد و حملـه را گویند. برای افزایش امنیت اقداماتی چون حفاظت، حراست، کنترل، تقویت، مهار و بیمه انجام می‌شود.

امنیت اطلاعات: حفاظت اطلاعات و سیستم‌هـای اطلاعـاتی از هرگونه فعالیـت‌هـای غیرمجـاز به منظور دسترسی، استفاده، افشاء، خواندن، نسخه‌برداری یاضبط، خـراب‌کـردن، تغییـر و دستکاری اطلاعات را گویند. امنیت اطلاعات به محرمانگی، یکپارچگی و در دسترس بودن داده‌ها بدون در نظرگرفتن فرم اطلاعات مربوط می شود[۱۱].

محرمانگی :محرمانگی یعنی جلوگیری از افشای اطلاعات به افراد غیرمجاز.

یکپارچگی: جلوگیری از تغییر داده‌ها بطور غیر مجاز و تشخیص تغییر درصورت دستکاری غیر مجاز اطلاعات.

قابل دسترس بودن: اطلاعات باید زمانی که مورد نیاز توسط افراد مجاز هستند دردسترس باشند. این بدان معنی است که باید از درست کارکردن و جلوگیری از اختلال درسیستم‌های ذخیره و پـردازش اطلاعات وکانال‌های ارتباطی مورد استفاده برای دسترسی به اطلاعات، اطمینان حاصل کرد.

۴- تهدیدات امنیتی خدمات پردازش ابری

حجم داده‌های بزرگ و استفاده از ماشین‌های مجازی در فناوری ابرها چالش‌های امنیتی جدیدی را مطرح می کند. این چالش‌ها شامل آسیب‌پذیری، دسترسی فیزیکی، حریم خصوصی و کنترلی، یکپارچگی، شفافیت، مدیریت ریسک، انطباق، محرمانگی، احرازهویت، تأییداطلاعات و...می باشد [۵].همچنین ممکن است تأمین‌کننده خدمات ابری نیز از این اطلاعات سوءاستفاده کند یا در اثر فشـارهای دولت آن را افشا کند. واضح است که این خطرات امنیتی پیامدهای وخیمی را درپی دارنـد[۱۰].

دسته‌بندی تهدیدات امنیتی

تهدیدات امنیتی در حالت کلی در دو دسته داخلی و خارجی طبقه‌بندی می‌شود:

تهدیدات داخلی

این نوع تهدیدات از درون سازمان های ارائه‌دهنده سرویس به وجود می‌آیند. به این معنی که مشتریان داده‌های حیاتی خود را در فضای ابر ذخیره می‌کنند، حال در صورتی که کارکنان سازمان به علت داشتن دسترسی به این داده‌ها، از آن اطلاعات سوءاستفاده کنند این نوع تهدید رخ می دهد.

ISSN: 2745-3673
http://www.Rcsj.ir

تهدیدات خارجی

علاوه بر تهدیدات داخلی تهدیدات خارجی هم می‌تواند باعث بروز خسارت های جبران‌ناپذیری به سیستم و فرآیندهای آن شود. نقاط ضعف سازمان ارائه‌دهنده می تواند راهی برای مهاجمان خارج از سازمان باز کرده و باعث حملات مخربی شود، به طور مثال مهاجمان می توانند از ضعف رابط برنامه‌نویسی نرم افزار(API)[9] و کانالهای ارتباطی استفاده کرده وسازمان را مورد حمله قرار دهند. برای حفاظت سازمان در برابر چنین تهدیداتی، استفاده از فایروالها و سیستم‌های تشخیص و پیشگیری از نفوذ بسیار ضروری است[۱۲].

کلیه تهدیدات امنیتی ابرها در این دو دسته جای می گیرد. همانطور که طبق گزارش سال ۲۰۱۰ اتحادیه امنیت ابری (CSA)[10] هفت خطر امنیتی که ابرها تهدید می کند عبارتند از: سوءاستفاده از پردازش ابری، همکار خیانت‌کار، رابطهای کاربری نا امن، سرقت اطلاعات و یا سرویس‌های کاربران، از دست دادن یا افشاء اطلاعات، نتایج استفاده مشترک از تکنولوژی وخطرات ناشناخته[۱۳].

۵- راه‌حل‌های امنیتی

تاکنون در دنیا تحقیقات بسیاری در زمینه امنیت ابری انجام شده است. چندین گروه و سازمان تمایل به توسعه راه حل های امنیتی و استاندارد سازی ابرها دارند. در اینجا به ذکر برخی از سازمان هایی که استانداردهایی را ارائه داده اند می پردازیم. اتحادیه امنیت ابر (CSA) ارائه‌دهندگان راه حل امنیت ابری در سازمان‌های غیرانتفاعی را گردهم آورده است تا بهترین شیوه ها را برای تأمین امنیت داده‌های ابری در آینده مورد بحث قرار دهد[۵].موسسه ملی استاندارد و فناوری ایالت متحده، افزون بر ارائه معماری محیط رایانش ابری، معماری مجزایی برای امنیت رایانش ابری ارائه کرده است. معماری مرجع امنیتی رایانش ابری ارائه شده، چارچوبی است که ضمن تعیین مجموعه مؤلفه‌های امنیتی، مسئولیت بازیگران ابری در هر الگو ارائه سرویس را نیز بیان می کند[۱۴]. آژانس امنیت شبکه و اطلاعات اروپا (ENISA)[11] مزایا، ریسک ها و توصیه هایی را در زمینه پردازش ابری منتشر ساخته که قابل استفاده سازمان هایی است که مایل به اتخاذ پردازش ابری بودند[۱۵]. علاوه بر این استاندارد ها گروه هایی نیز طرح های امنیتی خود را به این شرح ارائه داده اند : راج و همکارانش برای تضمین امنیت داده‌ها، ایزوله‌سازی منابع را پیشنهاد دادند. این امر به صورت ایزوله‌سازی حافظه نهان پردازنده در ماشین های مجازی صورت می‌گرفت[۱۶]. بلار و همکارانش یک طرح رمزگذاری را جهت حفظ محرمانگی و جامعیت داده‌ها ارائه دادند[۱۷].برنزمد و همکارانش نشان دادند که وجود توافق‌نامه‌های سطح خدمات ابر می‌تواند جنبه های امنیتی را توسعه دهد[۱۸]. رانگ و همکارانش نیز طرح رمزگذاری دیگری را جهت به اشتراک‌گذاری امن داده‌ها بر روی ابر پیشنهاد دادند[۱۹]. یوم و همکارانش پیشنهاد دادند که اگر کاربری تصدیق ارائه‌دهنده ابر را برای ورود دریافت کرد تا زمان اعتبار آن تصدیق به شخص دیگری برای احراز هویت آن تصدیق داده نشود[۶].چانگ و همکارانش یک (CCAF)[12] امنیتی مناسب برای ابرهای کسب و کار ارائه دادند[۲۰].با تمام این تفاسیر همچنان با گسترش ابرها لزوم به ارائه راه‌هایی برای گسترش راه حل‌های امنیتی ابرها مورد نیاز است اما با ارائه این راه حل ها در کنار هم متذکر می شویم که استفاده هم زمان و هم جهت از چند روش می تواند امنیت بیشتری را برای ابرها به ارمغان آورد. البته لازم است طرح ها به گونه ای انتخاب و در هم ادغام شوند که برای ایجاد امنیت در راستای هم گام بردارند. این تفکر می تواند موضوعی برای تحقیقات آتی در زمینه امنیت ابرها گردد.

[9] Application Programming Interface
[10] Cloud security alliance
[11] European Union Agency for Network and Information Security
[12] Cloud Computing Adoption Framework

ISSN: 2745-3673
http://www.Rcsj.ir

۶- نتیجه گیری

پردازش ابری مدلی برای دسترسی آسان به منابع شخصی خود در هر زمان و مکان، بدون نیاز به نرم افزار یا سخت افزاری خاص است. ابرها مزایای بسیاری ارائه می‌دهند که می‌تواند برای انتخاب و استفاده از آن‌ها توسط کاربران کافی باشد. به دلیل این مزایا با گذشت زمان تعداد افراد و سازمان‌هایی که اطلاعات و محاسبات خصوصی خود را به ابرها می‌سپارند بیشتر شده است؛ اما همواره این استفاده ها با نگرانی‌هایی همراه بوده که برخی از آن‌ها مربوط به تهدیدهای داخلی و برخی مربوط به تهدیدهای خارجی ابرها می باشد. ارائه‌دهندگان ابر تلاش می‌کنند با اعتمادسازی بین کاربران نگرانی‌های آنان را در مورد تهدیدات کاهش دهند. اعتماد سازی شاید بتواند نگرانی هایی که ناشی از تهدیدات داخلی است را کاهش دهد اما نگرانی‌هایی که مربوط به تهدیدات خارجی ابرهاست نشأت گرفته از ضعف سازمان‌ها و زیرساخت‌های آن می باشد که پیگیری ها و دوراندیشی های بیشتری می طلبد. در این مقاله پس از تعریف جامع و دسته بندی درست از رایانش ابری به بررسی‌های این تهدیدات در دو دسته داخلی و خارجی پرداختیم و هفت خطر امنیتی راکه اتحادیه امنیت ابری(CSA) در سال ۲۰۱۰منتشر ساخته است، را برشمردیم و سپس گذری بر راه حل‌های امنیتی که در قالب استانداردها و طرح ها ارائه شده اند داشتیم و با کنار هم قرار دادن این راه‌حل‌ها سعی بر متذکر شدن این نکته شدیم که تجمیع مناسب چند طرح می‌تواند بهبود قابل توجهی در امنیت ایجاد نماید. انتخاب طرح های مناسب برای تجمیع، تفکری است که می تواند در آینده مورد توجه قرار گیرد..

.

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[1] Mell, P. and T. Grance, *Effectively and securely using the cloud computing paradigm.* NIST, Information Technology Laboratory, ۲۰۰۹: p. .۳۱۱-۳۰٤

[2] Hurwitz, J., et al., *Cloud computing for dummies.* ۲۰۱۰: John Wiley & Sons.

[3] Viega, J., *Cloud computingand the common man.* Computer, ۲۰۰۹. ٤۲(۸): p. .۱۰۸-۱۰٦

[4] Armbrust, M., et al., *Above the clouds: A berkeley view of cloud computing.*.۲۰۰۹

[5] Subashini, S. and V. Kavitha, *A survey on security issues in service delivery models of cloud computing.* Journalof network and computer applications, ۲۰۱۱. ۳٤(۱): p. .۱۱-۱

[6] Habiba, U., et al., *Cloud identity management security issues & solutions: a taxonomy.* Complex Adaptive Systems Modeling, ۲۰۱٤. ۲(۱): p. .۱

[7] Klyuev, V. and V. Oleshchuk, *Semantic retrieval :an approach to representing, searching and summarising text documents.* International Journal of Information Technology, Communications and Convergence, ۲۰۱۱. ۱(۲): p. .۲۳٤-۲۲۱

[8] Hashemi, S. and S.Y. Hashemi, *Cloud computing for E-learning with more emphasis on Security Issues.* computing, ۲۰۱۳. ٦: p. .۸

[9] Mell, P. and T. Grance, *The NIST definition of cloud computing.*.۲۰۱۱

[10] Winkler, V.J., *Securing the Cloud: Cloud computer Security techniques and tactics*. ۲۰۱۱: Elsevier.

[11] Jansen, W. and T. Grance ,*Sp* ۱٤٤-۸۰۰. *guidelines on security and privacy in public cloud computing.*.۲۰۱۱

[12] Behl, A. *Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation*. in *Information and communication technologies (WICT), ۲۰۱۱ world congress on*. ۲۰۱۱. IEEE.

[13] Sood, S.K., *A combined approach to ensure data security in cloud computing.* Journal of Network and Computer Applications, ۲۰۱۲. ۳۵(٦): p. .۱۸۳۸-۱۸۳۱

[14] Liu, F., et al., *NIST cloud computing reference architecture.* NIST special publication, ۲۰۱۱. ۵۰۰(۲۰۱۱): p. .۲۹۲

[15] Popović, K. and Ž. Hocenski. *Cloud computing security issues and challenges*. in *Proceedings of the ۳۳rd International Convention. IEEExplore, Opatija*. .۲۰۱۰

[16] Raj, H., et al. *Resource management for isolation enhanced cloud services*. in *Proceedings of the ۲۰۰۹ACM workshop on Cloud computing security*. ۲۰۰۹. ACM.

[17] Bellare, M., O. Goldreich, and S. Goldwasser. *Incremental cryptography and application to virus protection*. in *Proceedings of thetwenty-seventh annual ACM symposium on Theory of computing*. ۱۹۹۵. ACM.

[18] Bernsmed, K., et al. *Security SLAs for federated cloud services*. in *Availability, Reliability and Security (ARES), ۲۰۱۱Sixth International Conference on*. ۲۰۱۱. IEEE.

ISSN: 2745-3673
http://www.Rcsj.ir

[19] Zhao, G ,.et al. *Trusted data sharing over untrusted cloud storage providers*. in *Cloud Computing Technology and Science (CloudCom), ۲۰۱۰IEEE Second International Conference on*. ۲۰۱۰. IEEE.

[20] Chang, V., Y.-H. Kuo, and M. Ramachandran, *Cloud computing adoption framework: A security framework for business clouds.* Future Generation Computer Systems, ۲۰۱٦. ٥٧: p. -۲٤ .٤١