تاریخ دریافت مقاله: ۹۶/۰۱/۳۰
تاریخ پذیرش مقاله: ۹۶/۰۳/۰۹

بهبود امنیت مدیریت داده‌ها در رایانش ابری با استفاده از الگوریتم فاخته

شیرین جباری*
مدرس، گروه کامپیوتر، آموزشگاه فنی و حرفه‌ای سماء، دانشگاه آزاد اسلامی، بندرعباس، ایران
پست الکترونیکی: shirinjabari90@gmail.com

علی‌اصغر صفایی
استادیار گروه انفورماتیک پزشکی،دانشکده علوم پزشکی، دانشگاه تربیت مدرس تهران ایران
پست الکترونیکی: aa.safaei@modares.ac.ir

چکیده

رایانش ابری، مدلی است که به ارائه دسترسی آسان، توزیع‌شده و فراگیر به منابع محاسباتی تجمیعی و مشترک قابل پیکربندی، می‌پردازد. به دلیل فراگیر شدن رایانش ابری و افزایش حجم داده‌ها نیاز است که کار تحلیل داده‌ها در مقیاس بزرگ انجام شود، زیرا امروزه یکی از حیاتی‌ترین نیازهای یک سرویس‌دهنده ابری این است که کار تحلیل داده‌ها برای تمامی سطوح کاربران فراهم شود. بنابراین نیاز به داشتن یک سیستم مدیریت داده کارآمد برای یک سرویس‌دهنده ابری بسیار حائز اهمیت است. یکی از انواع بسترهای ابری ابرهای خصوصی هستند. مدیریت منابع، به‌ویژه در ابرِ خصوصی می‌تواند بر روی طراحی امنیتی ابر تأثیر متقابل و به‌سزائی داشته باشد. اصولا محاسبات ابری در کنار مزایا و فوایدی که فراهم می‌کند با چالش‌های نگران‌کننده‌ای به‌ویژه در زمینه امنیت مواجه و روبرو است. تامین امنیت و حفظ حریم خصوصی در رایانش ابری نیازمند سیاست‌ها و راهکارهایی است تا بستر ابری مورد نظر مورد اطمینان کاربر واقع شود. امنیت و حریم خصوصی غالباً بزرگ‌ترین مانع در راه پذیرش فناوری رایانش ابری محسوب می‌شود. در این مقاله با توجه به اهمیت موضوع و جهت بهبود امنیت در محاسبات ابری و مدیریت داده‌ها بر بستر رایانش ابری یک روش مبتنی بر الگوریتم تکاملی فاخته (که یکی از بهترین و کارآمدترین الگوریتم‌های تکاملی است) ارائه شده است. در روش پیشنهادی، پیشینه امنیتی ارائه‌دهندگان و مصرف‌کنندگان در سیستم ثبت می‌شود و این اطلاعات به‌عنوان پارامترهای ورودی الگوریتم فاخته استفاده می‌شود. نتایج به‌دست آمده از ارزیابی عملی به خوبی بیانگر بهبود در معیارهای امنیت داده‌ها در روش پیشنهادی نسبت به روش‌های مشابه پیشین می‌باشد.

کلید واژه: محاسبات ابری، بهبود امنیت داده‌ها، الگوریتم فاخته، الگوریتم‌های تکاملی

۱- مقدمه

با پیشرفت فناوری اطلاعات کاربران نیازمند آن هستند بتوانند کارهای محاسباتی سنگین خود را بدون الزام به تهیه و تدارک سخت‌افزارها و نرم‌افزارهای گران‌قیمت برای خودشان، بلکه از طریق بهره‌مندی از خدمات ارائه شده

* نویسنده مسئول

توسط سازمان‌های ارائه دهنده این گونه خدمات، انجام دهند. رایانش ابری آخرین پاسخ فناوری به این نیازها بوده است. در واقع رایانش ابری توانایی ارتقای بهره‌وری و صرفه‌جویی در منابع و افزایش توان محاسباتی را فراهم می‌کند، به‌طوری‌که توان پردازشی به ابزاری با قابلیت دسترسی همیشگی تبدیل می‌شود. اگرچه رایانش ابری مزایای زیادی دارد، ولی امنیت در رایانش ابری چالشی بزرگ و لذا بسیار حائز اهمیت است. با ظهور محاسبات ابری به‌عنوان یک طرح محاسباتی جدید، سازمان‌ها آن را به‌عنوان انتخابی حیاتی برای سرویس‌های اصلی فناوری خارجی جهت شکست هزینه در نظر می‌گیرند. با این حال، چالش‌های امنیت فناوری تبادل اطلاعات در ابر باید به‌طور مناسبی مرتفع شوند. حفظ امنیت و حریم خصوصی نیاز به سیاست‌ها و راهکارهایی دارد تا مورد اطمینان کاربر واقع شود. این‌که کاربران و سازمان‌ها داده‌های خود را در محلی غیر از سازمان خود نگهداری و پردازش می‌کنند برای عده زیادی قابل پذیرش نیست و نمی‌توان مطمئن بود که افراد غیرمجاز قادر به دسترسی به داده‌ها نیستند[۱]. این نگرانی از دو جهت بررسی می‌شود، یکی جلوگیری از خواندن اطلاعات خصوصی توسط دیگران مانند مشتریان دیگر، که یک نگرانی روشن و آشکار است که در سناریوهای مانند سرقت یا سایر حملات مخرب مستقیم نمایان است. و مسئله دیگر، موضوع خواندن اطلاعات خصوصی ارائه دهنده سرویس است[۲]. در حقیقت چالش بنیادی همان تامین امنیت و حفظ حریم خصوصی خواهد بود.

شرکت‌های بزرگ به طور مرتب گزارش‌هایی از شکستن هزینه‌ها را ارائه می‌کنند که ممکن است به‌عنوان تلاشی برای کاهش ناکارامدی تفسیر شود. شرکت‌های تجاری در تمام دنیا تمایل به شکستن هزینه‌ها دارند. در میان حوزه‌های هدف در محاسبات ابری تبادل اطلاعات جایگاه انتخابی بالایی برای دستیابی به این اهداف را دارد و به شرکت‌های تجاری اجازه بهره‌برداری از بهترین برنامه‌های تجاری و زیرساخت‌های فناوری اطلاعات در کاهش هزینه‌ها را می‌دهد. محاسبات ابری جذابیت زیادی برای تجارت دارد که ناشی از انتخاب‌های انعطاف‌پذیر آن است. به‌رغم این مزایا بیشتر سازمان‌ها از پیوستن به دنیای محاسبات ابری خودداری می‌کنند تا خطرات اصلی شناخته شوند، به درستی درک و به‌طور موثری مدیریت شوند. تشکل‌های صنایع مختلف گزارش‌هایی می‌دهند مبنی بر این‌که تهدیدهای مرتبط با محاسبات ابری بیشتر از مزایای آن است. نگرانی‌های امنیتی موضوع پایه‌ای مرتبط با محاسبات ابری است که به دنبال آن قابلیت دسترسی، کارایی و فقدان تعامل استاندارد نیز وجود دارد.

روش‌های امنیتی در طول دهه‌ها با استفاده از راهبردهای مختلفی جهت کاهش انواع آسیب‌پذیری‌ها تکامل یافته است. این آسیب‌پذیری‌ها می‌تواند به معماری و زیرساخت ابر مربوط باشد و یا این‌که مرتبط با رفتار یک کاربر و یا یک برنامه کاربردی باشد. در این راستا روش‌های مختلفی توسط پژوهشگران برای برقراری امنیت در زیر ساخت ابر پیشنهاد گردیده است که هر یک دارای مزایایی می‌باشند. با وجود ارائه این روش‌ها، مشکل اصلی موجود این است که بسیاری از روش‌ها برای پوشش آسیب‌پذیری‌ها و ارتقای امنیت ابر متحمل هزینه‌های زیادی می‌گردند که بسیاری از آن‌ها در عمل امکان‌پذیر نمی‌باشد. بنابراین نیاز به روشی که بتوان مشکلات امنیتی را به خوبی مرتفع نماید و در عین حال هزینه محاسباتی کم و زمان پردازش مناسبی را داشته باشد احساس می‌گردد.

در این مقاله، یک چارچوب امنیتی برای ابر و رویکردی برای پوشش آسیب‌پذیری‌ها و بهینه‌سازی هزینه با استفاده از الگوریتم فاخته ارائه شده است. هدف چارچوب پیشنهادی، کاهش یک مجموعه مشخص از آسیب‌پذیری‌ها با استفاده از مجموعه‌ای انتخابی از روش‌هایی است که هزینه را کمینه و پوشش حملات را بیشینه می‌کند. نتایج نشان می‌دهد که ارائه دهندگان محاسبات ابری و سازمان‌هایی که پیاده‌سازی ابر را در خودشان انجام می‌دهند می‌توانند به‌طور موثری پوشش امنیت و هزینه را با این رویکرد متوازن کنند. در این

مقاله ابتدا با استفاده از مطالعات انجام گرفته قبلی اطلاعات لازم در این خصوص جمع‌آوری شده و توسط سازوکاری مبتنی بر الگوریتم فاخته به دنبال ارایه روشـــی برای تامین امنیت ساختار ابر هستیم.

روش جســـتجوی فاخته (CS) یک روش بهینه‌ســـازی فـــرا ابتکاری اســـت که رویکـــردی تکاملی در جســـتجوی راه‌حل بهینه دارد و در ســـال ۲۰۰۹ توسط Yang و Deb [۳] پیشنهادشده است. این روش از رفتار جالب‌توجه گونه‌هایی از پرندۀ فاخته در پرورش تخم الهام گرفته است و آن را با پرواز له‌وی[1] که نوعی گشـــت تصادفی است ترکیب می‌کند. برخی از گونه‌های فاخته به‌جای ساختن لانه، تخم‌های خود را در لانۀ پرنده‌ای از گونه‌هـــای دیگر می‌گذارند و آن‌ها را با تقلید از شـــکل تخم‌ها و جوجه‌های پرنـــدۀ میزبان وادار به مشارکت در بقای نســـل خود می‌کنند. روش جستجوی فاخته (CS) یـــک الگوریتم فرا ابتکاری اســـت که تقلیدی از راهبرد تولید مثل هوشمندانه فاخته است. این پرنده به دقت لانـــه میزبان را از دیگر پرندگان انتخاب می‌کند و تخم خود را در میان تخم‌های موجود می‌گذارد. پرنده میزبان اشتباهی از تخم فاخته مراقبت می‌کند. با این حال برخی ممکن اســـت تخم را تشخیص دهند و آن را از بین ببرند یا به خارج از لانه بفرستند[۴]. از رفتار هوشمندانه این پرنده برای توسعه یک الگوریتم بهینه سازی جدید تقلید شده است.

۲- پیشینه پژوهش

پیدایش مفاهیم اساســـی محاسبات ابری به دهه ۱۹۶۰ بازمی‌گـــردد. زمانی که جان مک کارتی اظهار داشـــت که «تقریباً تمام» محاســـبات ممکن است روزی به‌عنوان مثال از صنایع همگانی سازمان‌دهی شـــود. ویژگی‌های امروز محاسبات ابری شـــامل مواردی چون تدارک قابل ارتجاع، ارائه به‌صورت یک صنعـــت همگانی، برخط بودن و توهم دسترســـی به عرضه نامحدود به همراه مقایسه با صنعت برق و شکل‌های مصرف عمومی و خصوصی و دولتی و انجمنی هســـتند که این ویژگی ها را پارک هیل داگلاس در کتابی با عنوان «مشـــکل صنعت همگانی رایانه » در ســـال ۱۹۶۶ مورد بررســـی قرار داد. واژه ابر درواقع برگرفته از صنعت تلفن است به این‌گونه که شرکت‌های ارتباطات راه دور کـــه تا دهه ۱۹۹۰ تنها خطوط نقطه‌به‌نقطه اختصاصی ارائه می‌کردند، شروع به ارائه شبکه‌های خصوصی مجازی با کیفیتی مشـــابه و قیمت‌های کمتر نمودند. نماد ابر برای نمایش نقطه مرزی بین بخش‌هایی که در حیطه مســـئولیت کاربر است و آن‌هایی که در حیطه مسئولیت عرضه‌کننده اســـت، به‌کار گرفته می‌شد. محاســـبات ابری مفهوم ابر را به‌گونه‌ای گســـترش می‌دهد که کارسازها را نیز علاوه بر زیرساخت‌های شبکه در برگیرد[۱].

در مقاله[۴] ارتباط بین مشتریان و ارائه دهندگان ابر از طریق رابط‌های برنامۀ کاربردی (API) انجام می‌شود. وظیفه API، تامین و مدیریت سرویس‌هایی است که قرار است در ابر ارائه شود. APIهای ضعیف می‌توانند سازمان‌های ارائه دهنده را در معرض تهدیدات امنیتی مختلفی مانندد‌سترسی ناشناس، مجوز نامناسب و... قرار دهند.

در مقاله [۵] امکان بهره‌برداری از ابرداده ذخیره شده در پایگاه داده‌های ابر به منظور بررسی حریم خصوصی داده‌هـــای پیرامون کاربران که با اســـتفاده از ســـرویس ذخیره‌ســـازی ســـاده ارائه دهنده ابرذخیره می‌شود، بیان شده است .و پس از آن، یک چارچوب مبتنی بر پایگاه داده طراحی مجدد و بازســـازی پویا از ابرداده برای حفاظت از اطلاعات حریم خصوصی کاربران ابر پیشنهاد شده است. این مقاله در همان زمان، دسترسی بدون تغییر به فایل‌های پایگاه داده برای ارائه دهنده ابر را با استفاده از بازسازی پویا ابرداده که برای ترمیم شمای پایگاه داده اصلی مورد نیاز است تضمین نمود.

در مقالـــه [۶] حمـــلات با توجه به میزان خســـارت و همچنین ســـطح حملات آن‌ها در محیط ابری دســـته‌بندی می‌شوند. براین اساس، برای هرحمله یک ریسک خطر تهیه وبه آن‌ها داده شد و براساس آن روشی برای مقابله با آن

1- Levy Flight

در نظرگرفته شده است. مشکل این سیستم تهیه این قوانین و همین‌طور تعیین ریسک‌های مربوط به آن‌ها می‌باشد. حتی دربرخی موارد نمی‌توان برای هر کاربری همه موارد را به کاربرد و یا میزان ریسک همسانی را به آن‌ها داد. همچنین تهیه این قوانین نیازبه داشتن آگاهی‌هایی اززمینه کاربرد کاربر و برنامه‌های آن‌ها دارد که خود باعث انجام پردازش‌هایی سنگین و پیچیده و گاه زمان‌برمی‌گردید؛ اما در نوع خود دارای مزیت‌هایی است. از آن جمله این‌که بیشتر به مباحث درون شبکه‌ای، به‌ویژه منابع، پرداخته است و از انجام پردازش‌هایی برروی عوامل خارجی پرهیز می‌کند و این یعنی صرفه‌جویی در انجام پردازش‌های مازاد؛ اما همین خود باعث نقص درسیستم می‌باشد.

در مقاله [۷] یک رویکرد شاخص بر اساس شبه شناسه کارآمد برای اطمینان از حفظ حریم خصوصی و دستیابی به ابزار داده‌های بیش از مجموعه داده‌های افزایشی و توزیع در ابر، پیشنهاد شده است. شبه شناسه، نشان‌دهنده گروهی از داده‌های ناشناخته است که برای بهره‌وری نمایه می‌شود. دراین مقاله بهره‌وری حفظ حریم خصوصی در مقیاس بزرگ مجموعه داده‌های افزایشی درابر نیز، بررسی می‌شود.

مقاله [۸] رویکردهای مقابله با تهدیدات را به دو دسته کلی تقسیم نموده است: کنترل دسترسی و اقدام متقابل و پاسخ. سازوکار کنترل دسترسی، اطمینان ازدسترسی کاربران مجاز و جلوگیری دسترسی‌های غیرمجاز به سیستم‌های اطلاعاتی است. واقعه اقدام متقابل و پاسخ، یافتن مشکلات ایجاد شده و پیداکردن واکنش مناسب در برابر مشکلات است. همچنین در این مقاله، مسائل امنیتی مطرح شده که کاربران باید از آن‌ها اطلاع داشته باشند، به شرح زیراست: دسترسی ممتازکاربر، پیروی از مقررات، موقعیت داده‌ها، تفکیک داده‌ها، بازیابی، پشتیبانی تحقیقاتی، مدت زمان زنده ماندن.

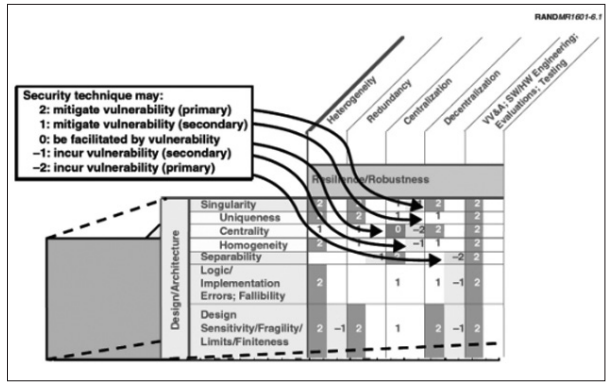
در مقاله [۹] اقداماتی برای مقاومت در برابر فریب کاری‌های فروشنده‌ها در نظر گرفته شده است که خریداران می‌توانند برنامه‌های خود را با خواسته‌های بسیار کم قبل از مهاجرت به بُن‌سازهٔ ابر سفارش دهند. موقعیت‌های بین خریداران و فروشندگان به‌عنوان یک مدل ریاضی به نام مدل بازی استراق سمع و مقاومت مذاکره (ERN) مدل‌سازی می‌شود. راهبرد بازی خریداران و فروشندگان، بازی ERN را با رویکرد اقتصادی و محاسباتی بر اساس عامل‌های هوشمند تجزیه و تحلیل می‌کند.

در مقاله [۱۰] درمورد یکی از مسائل مهم در رایانش ابری، تحت عنوان نظارت امنیتی از سه منظرنگاه می‌شود: نیازمندی‌های نظارت کاربر، روش‌های فنی برای نظارت امنیت و قابلیت‌های ارائه دهنده خدمات ابر در حال حاضر برای رفع نیازهای نظارتی. همچنین مسائل مربوط به نظارت خاص به دو دسته تقسیم می‌شوند: زیرساخت‌های نظارت امنیت و نظارت امنیت اطلاعات. با وجود تعدادی از روش‌های موجود برای مقابله با نگرانی‌های نظارت کاربردر زمینه نظارت داده‌ها، ارائه‌دهندگان ابر تا کنون تنها در زیرساخت‌های نظارت امنیت متمرکز شده است.

در مقاله [۱۱] به بررسی پذیرش خدمات محاسبات ابری در سازمان‌های دولتی، با تمرکز بر ویژگی‌های کلیدی که بر قصد رفتاری تاثیر می‌گذارد، می‌پردازد. این مطالعه براساس مدل پذیرش فناوری با ترکیب عواملی از جمله در دسترس بودن، امنیت و قابلیت اطمینان، گسترش داده می‌شود. مدل تحقیق تجربی با بررسی ادراک کاربران مشغول به کار درموسسات دولتی تایید شده است. نتایج مدل‌سازی نشان می‌دهد که نیت و رفتار کاربران تا حد زیادی ازویژگی‌های درک شده از ابر با خدمات فراهم شده تاثیر گرفته است. این یافته‌ها باعث ارتقاءدولت ازخدمات عمومی ابر، افزایش آگاهی کاربر از طریق افزایش قابلیت‌ها و درخواست تجدید نظر و تامین امنیت می‌شود.

۳- چارچوب کلی روش پیشنهادی

ایده به‌کار گرفته شده در این مقاله، حل آسیب‌پذیری‌های موجود با انتخاب راه‌حل‌های امنیتی برای آن، از طریق الگوریتم جستجوی فاخته است. از آنجایی که پیداکردن راه‌حل‌های



شکل ۱: نمایی از داده‌های مورد استفاده

امنیتی برای پوشش آسیب‌پذیری‌های مختلف به دلیل وجود راه‌حل‌های فراوان و همچنین اثر مثبت یا منفی هر راه‌حل بر روی آسیب‌پذیری‌های دیگر در عمل امری غیرممکن به نظر می‌رسد، استفاده از الگوریتم فاخته برای این کار روشی امیدبخش به نظر می‌رسد. از آنجایی که فضای جستجوی مسئله بسیار بزرگ می‌گردد، پیدا کردن راه‌حل‌های بهینه با بررسی تمامی راه‌حل‌ها امکان‌پذیر نمی‌باشد. در این شرایط الگوریتم فاخته با توجه به همگرایی سریع جواب مناسبی را در زمان مناسب پیدا خواهد نمود. برای رفع مشکلات امنیتی ابر می‌بایست نگاشت مناسبی در میان الگوریتم جستجوی فاخته و مفاهیم امنیتی ابر قرار گردد. علاوه بر این باید تابع سازگاری مناسبی تعریف گردد تا تخم‌ها را با هدف افزایش امنیت ابر و رفع کامل آسیب‌پذیری‌ها، در میان بهترین لانه‌ها توزیع نماید. در ادامه این فصل نحوه نگاشت مفاهیم الگوریتم فاخته به آسیب‌پذیری‌های موجود و راهکارهای امنیتی بیان می‌گردد و یک تابع سازگاری مناسب نیز برای این مسئله تعریف می‌گردد.

گام‌های روش پیشنهادی به شرح زیر می‌باشند.

گام۱: جمع‌آوری داده‌های مرتبط با آسیب‌پذیری‌ها و اثر هر یک از راه‌حل‌های امنیتی بر روی آن‌ها

گام ۲: نگاشت مراحل الگوریتم فاخته به مسئله امنیت زیر ساخت ابر

گام ۳: تعریف یک تابع هدف برای الگوریتم جستجوی فاخته با توجه به مسئله امنیت زیرساخت محاسبات ابری

گام ۴: آزمایش و ارزیابی روش معرفی شده

۳-۱- جمع آوری داده‌ها

برای جمع‌آوری داده‌ها از داده‌های معرفی شده در [۱۱] استفاده شده است که در آن از یک طرف، روش‌های امنیتی برای اطمینان بخشی به سیستم در مقابل حملات و خرابی‌ها می‌باشند تا به‌صورت فعال حملات یا خرابی را تشخیص و به آن پاسخ دهد؛ فعالیت‌های مشکوک در دسترسی به منابع حساس را مسدود کند یا به صورتی بازدارنده از حملات جلوگیری کند. از طرف دیگر، ویژگی‌های آسیب‌پذیری که مربوط به طراحی و معماری سیستم، و دیگر ویژگی‌های مرتبط به ساختار و رفتار سیستم است دسته‌بندی شده‌اند. در این داده‌ها تعداد ۳۰ راه‌حل امنیتی و ۱۹ خطر امنیتی و آسیب‌پذیری بیان شده‌اند. شکل (۱) نمایی از این داده‌ها را نشان می‌دهد. در این داده‌ها مقادیر عددی بیان‌کننده اثر روش‌های امنیتی برای کاهش آسیب‌پذیری‌های مختلف است. مقدار ۱ و ۲ هنگامی که تکنیک امنیتی آسیب‌پذیری را کاهش می‌دهد استفاده می‌شود که ۱ به معنی کاهش ثانویه و ۲ کاهش اولیه آسیب‌پذیری است. صفر وقتی که آسیب‌پذیری‌ها اثری مثبت دارند و تکنیک امنیتی را اثربخش نشان نمی‌دهد استفاده می‌شود. شماره ۲- و ۱- منعکس کننده رخ دادن آسیب‌پذیری جدید هنگام پیاده‌سازی تکنیک امنیتی است.

۳-۲- نگاشت الگوریتم فاخته به راهکار امنیت ابر

الگوریتم با مجموعه‌ای از آسیب‌پذیری‌ها و راه‌حل‌های امنیتی شروع می‌شود. این کار معادل با گام اول الگوریتم فاخته است. برای نگاشت این مفاهیم امنیتی چون آسیب‌پذیری و راه‌حل امنیتی به الگوریتم جستجوی فاخته بدین صورت عمل می‌گردد که هر یک از راه‌حل‌ها به‌عنوان لانه‌های الگوریتم فاخته و آسیب‌پذیری‌ها به‌عنوان تخم‌های مورد نظر در نظر گرفته می‌شوند. اگر لانه‌ای برای تخمی مناسب باشد و پرنده میزبان آن تخم را بیرون نینداخته و از آن مراقبت کند، بدین معنی است که راه‌حل امنیتی برای آسیب‌پذیری منتسب شده به آن مناسب می‌باشد. این کار معادل با گام دوم الگوریتم فاخته است.

علاوه بر این برای بررسی میزان کیفیت هر لانه از یک

تابع سازگاری هدف استفاده می‌شود که در اینجا از معادله ارایه شده در بخش بعد که یک تابع سازگاری برای امنیت شبکه ابر معرفی می‌کند، استفاده می‌شود. این کار معادل با گام سوم الگوریتم فاخته است.

۳-۳- تعیین تابع هدف الگوریتم فاخته برای ارتقای امنیت زیر ساخت ابر

اهداف این نگاشت به‌صورت زیر بیان می‌شود:

۱-بیشینه‌کردن پوشش آسیب‌پذیری‌ها و کمینه‌کردن آسیب‌پذیری‌های باقی مانده که به‌صورت زیر می توان نشان داد:

$$m_v = \text{Max} \sum_{ij=1}^{nm} \tau_{ij} \quad (۱)$$

در اینجا τ_{ij} نتیجه را بعد از به کار بردن روش امنیتی برای کاهش آسیب‌پذیری v_i را نشان می‌دهد.

۲- کمینه‌کردن هزینه کاهش آسیب‌پذیری هزینه محاسبه شده با استفاده از معادله زیر:

$$cv_j = \lambda CLv_j + \mu CSv_{ij} \; ; \; \lambda + \mu = 1 \quad (۲)$$

که CLv_j هزینه پرداختی یک فقدان[2] است اگر آسیب‌پذیری v_i دلیل اصلی این اتفاق باشد. CSv_{ij} هزینه راه‌حل[3] مورد نیاز برای کاهش آسیب‌پذیری v_i است؛ هزینه پرداختی یک فقدان و هزینه راه‌حل مورد نیاز برای کاهش آسیب‌پذیری بسته به هر کاربرد و با توجه به شرایط هر سازمان فعال در زمینه ارتباطات و فناوری اطلاعات متفاوت بوده و توسط کاربر بیان می‌گردد. λ و μ ضرایب انتخابی توسط سازمان است که مطابق با سطح امنیت مورد نیاز یا تحمل‌پذیری خطر امنیتی است.

$$m_c = \text{Min} \sum_{j=1}^{m} (cvj)$$
$$m_c = \text{-Max} \sum_{j=1}^{m} (-cv)_j \quad (۳)$$

۳-کمینه‌کردن ریسک حملات پراکسی است (استفاده همسایه آسیب‌پذیر و وجود خطر حمله). این کار با بیشینه‌کردن فاصله بین گره آسیب‌پذیر و گرهی که به‌طور بالقوه قربانی است (چه بر روی همان ماشین فیزیکی باشند یا بر روی ماشین‌های دیگر درشبکه) صورت می‌گیرد و می توان به‌صورت زیر نمایش داده می‌شود.

$$\varepsilon = \text{Max} \sum_{j=1}^{n} (h_j + n_j) \quad (۴)$$

در اینجا h_j فاصله میزبان (فاصله بین گره با v_j و گره قربانی در زیر شبکه مشابه) است. N_j فاصله شبکه است (فاصله بین گره با v_j و گره قربانی وقتی خارج از زیر شبکه است). فاصله توسط تعداد گام‌ها و تعداد وسیله‌های امنیتی بین دو میزبان اندازه‌گیری می‌شود.

تابع سازگاری برای سطح امنیت شبکه ابر به‌صورت زیر است:

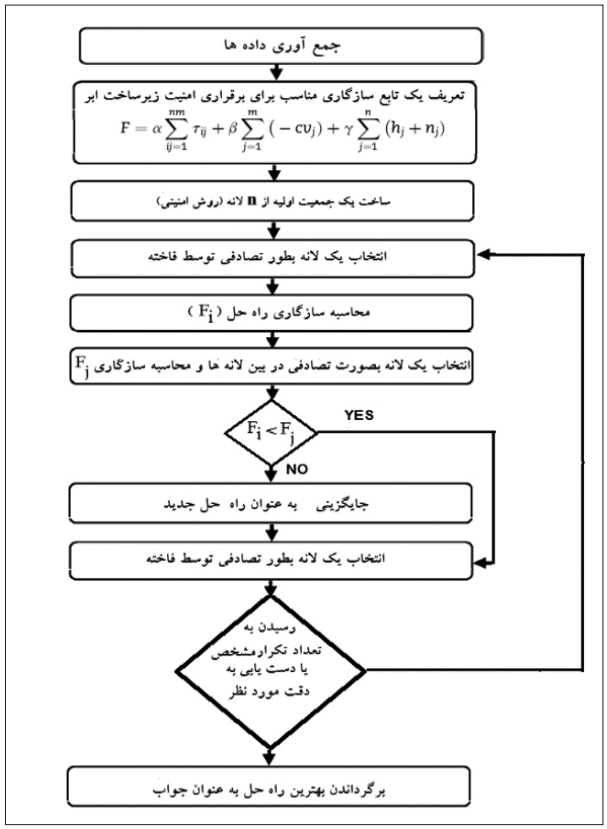
$$F = \alpha \sum_{ij=1}^{nm} \tau_{ij} + \beta \sum_{j=1}^{m} (-cv_j) + \gamma \sum_{j=1}^{n} (h_j + n_j) \quad (۵)$$

در اینجا α، β و γ ضرایب مثبت و $\alpha + \beta + \gamma = 1$ است. α، β و γ برای توازن سطح امنیتی، تحمل‌پذیری خطر امنیتی و هزینه است. اگر موسسه‌ای دارای ساختار محدودی باشد و بخواهد که هزینه را کمینه کند و در عین حال پوشش حداکثری آسیب‌پذیری‌های امنیتی را داشته باشد ممکن است $\beta > \gamma + \alpha$ انتخاب شود. در غیر این‌صورت، باید $\beta < \gamma + \alpha$ انتخاب شود. وقتی β صفر است، ملاحظات مالی هیچ ارتباطی به روش‌های امنیتی پذیرفته شده برای کاهش آسیب‌پذیری‌های شناخته شده ندارد.

معادله ۵ شامل ۵ متغیر مستقل است: سطح امنیتی مورد نیاز که با انتخاب $\alpha + \beta + \gamma$ نشان داده می‌شود؛ هزینه که هزینه پیاده‌سازی روش امنیتی را نشان می‌دهد؛ مقدار امنیت یک روش که با (امنیتی که مقدار و آسیب‌پذیری باقی مانده) نشان داده می‌شود؛ فاصله بین گره‌ها/ میزبان (تعداد گام‌ها) که مکان VMها را بر روی ماشین فیزیکی در شبکه‌ای مشابه را نشان می‌دهد؛ و فاصله بین شبکه‌ها (تعداد گام‌ها) که تعداد گام‌های بین ماشین مجازی آسیب‌پذیر میزبان شبکه را نشان می‌دهد. در نهایت سطح پوشش آسیب‌پذیری را هنگامی که یک مجموعه از روش‌های امنیتی به‌کار برده می‌شود متغیر وابسته است.

برتری جستجوی فاخته در این ویژگی است که از یک جهش برداری ترکیبی، تقاطع با جایگشت و انتخاب راه‌حل از میان بهترین راه‌حل‌ها استفاده می‌کند. در این روش و

2- Cost Of Loss
3- Cost Of Solution



شکل ۲: روندنمای روش پیشنهادی

بر اساس نگاشت بیان شـــده در مراحل قبل، از تابع هدف معادله (۵) برای ارزیابی جواب های پیشـــنهادی اســـتفاده می‌کند.

۴- مراحل روش پیشنهادی

همان‌طـــور که در بخش قبل بیان گردید روشـــی نوین بـــرای شناســـایی و رفـــع آســـیب‌پذیری‌های موجود در محیـــط پردازش ابـــری بیان گردیـــد. بعـــد از جمع‌آوری داده‌ها می‌بایســـت نگاشت مناسبی را بین مفاهیم مرتبط با آسیب‌پذیری در محیط ابر و همچنین پارامترهای الگوریتم جســـتجوی فاخته، ایجاد نمود. روش پیشـــنهادی مراحل متفاوتی را داشته که شکل (۲) روندنمای روش پیشنهادی را بیان می دارد.

همان‌طور که از روندنما مشـــخص است ابتدا یک تابع ســـازگاری مناسب برای مسئلهٔ پوشش آسیب‌پذیری‌ها بر اساس معیارهای ارائه شـــده در بخش قبل بیان می‌گردد.

نگاشت مفاهیم امنیتی ابر به پارامترهای الگوریتم جستجوی فاخته بدین‌صورت اســـت که هر یک از آسیب‌پذیری‌ها را به‌عنوان تخم‌های فاختـــه و راه‌حل‌های امنیتی را به‌عنوان لانه‌های الگوریتم جستجوی فاخته قرار می‌دهیم. الگوریتم جســـتجوی فاخته بر اساس تابع هدف ارائه شده در بخش قبل تکرار می‌گردد تا جایی که آسیب‌پذیری‌های موجود به خوبی توسط راه‌حل‌های امنیتی مرتفع گردد. شبه کد روش پیشنهادی به‌صورت زیر بیان می‌گردد:

```
Cuckoo search
Begin
 Objective function f(x) = α∑_{ij=1}^{nm} τ_ij + β ∑_{j=1}^{m}(−cv_j) + γ ∑_{j=1}^{n} (h_j + n_j)
 Generate initial population of n host nests x_i (i= 1.2,….., n)
 While ( t < MaxGeneration ) or (stop criterion)
     Get a cuckoo randomly
     Evaluate its quality / fitness F_i
     Choose a nest among n (j) randomly
     If (F_i < F_j),
         Replase j by the new solution;
End
    A fraction (p_a) of worse nestes is abandoned and new onse are built;
    Keep the best solutions (or nests with quality solutions);
    Rank the solutions and find the current best
 End While
 post process results and visualization
 End
```

۴- ارزیابی عملی عملکرد چارچوب پیشنهادی

٤-۱- تنظیم‌های ارزیابی

بـــرای پیاده‌ســـازی روش پیشـــنهادی از نرم‌افـــزار MATLAB R2010a استفاده گردیده است. این شبیه‌سازی بـــر روی سیســـتمی کامپیوتری بـــا پردازنـــده corei7 با میـــزان حافظ اصلی ۴ گیگابایت و بر روی سیســـتم عامل ویـــندوز ۷ اجـــرا شـــده اســـت. MATLAB R2010a برای پیاده‌سازی الگوریتم جستجوی فاخته جهت یافتن راه‌حلی بهینه بـــرای آســـیب‌پذیری‌هایی که شناســـایی شـــده‌اند اســـتفاده شـــده اســـت. برای انجام آزمایش‌هـــا برای هر i و j، $2 \le \tau_{ij} \le -2$، $7 \le cv_j \le 1$، $9 \le h_j \le 0$ و $255 \le n_j \le 1$ درنظر گرفته شـــده است. بنابراین مجموعه ممکن (فضای جواب) یک مجموعه چهارتایی (τ_{ij}, cv_j, h_j, n_j) است که مقدار τ_{ij} حداقل ۲- و حداکثر ۲، مقدار cv_j به حداقل ۱ و حداکثر ۷ نرمال شده است، h_j حداقل صفر و حداکثر ۹ و n_j حداقل ۱ و حداکثر ۲۵۵ است. برخی بسط‌ها به پارامترهای استفاده شده حساس نیست و پارامترهای $n = 15$ و $pa = 0.25$ برای

بیشتر مسائل بهینه‌سازی مناسب است. برای شبیه‌سازی مسئله نیاز به یک سری داده‌ها جهت انجام آزمایش‌ها است که برای این کار از مجموعه آسیب‌پذیری‌ها و نتیجه اجرای راهکارهای امنیتی بر روی آن‌ها که در [۱۷] بیان گردیده‌اند استفاده شده است .

٤-۲- معیار ارزیابی

با توجه به عملکرد روش پیشنهادی، جواب‌ها در یکی از دو دسته زیر قرار می‌گیرند:

• جواب صحیح مثبت (TP)[4]: آسیب‌پذیری‌هایی در این دسته قرار می‌گیرند که روش پیشنهادی به درستی آن‌ها را مرتفع ساخته است. یعنی این‌که یک روش امنیتی در ابر برای مرتفع ساختن و پوشش یک آسیب‌پذیری بیان گردیده است و نتیجه روش ارائه شده بیانگر این است که این روش نیز به خوبی آن آسیب‌پذیری را مرتفع ساخته است.

• جواب اشتباه مثبت (FP)[5]: آسیب‌پذیری‌هایی در این دسته قرار می‌گیرند که روش پیشنهادی نتوانسته به درستی آن‌ها را مرتفع سازد. یعنی این‌که یک روش امنیتی در ابر برای مرتفع ساختن و پوشش یک آسیب‌پذیری بیان گردیده است و نتیجه روش ارایه شده بیانگر این است که این روش آن آسیب‌پذیری را مرتفع نساخته و آن آسیب‌پذیری به قوت خود باقی است.

برای ارزیابی از معیار دقت استفاده می‌گردد که بیانگر تعداد جواب‌های صحیح به کل جواب‌های موجود می‌باشد.

$$\text{Precision}=\frac{\text{تعداد جواب صحیح مثبت } (TP)}{\text{تعداد جواب اشتباه مثبت } (FP)+\text{تعداد جواب صحیح مثبت } (TP)}$$

در این مقاله برای ارزیابی و اعتبارسنجی روش پیشنهادی از سازوکار معروف اعتبارسنجی ضربدری استفاده می‌گردد. اعتبارسنجی ضربدری، که گاهی تخمین گردشی نیز نامیده می‌شود، یک روش ارزیابی است که مشخص نتایج یک تحلیل آماری بر روی یک مجموعه داده تا چه اندازه قابل تعمیم و مستقل از داده‌های آموزشی است.

4- True Positive
5- False Positive

شکل ۳: دقت روش پیشنهادی به ازای تعداد آسیب‌پذیری‌های مختلف

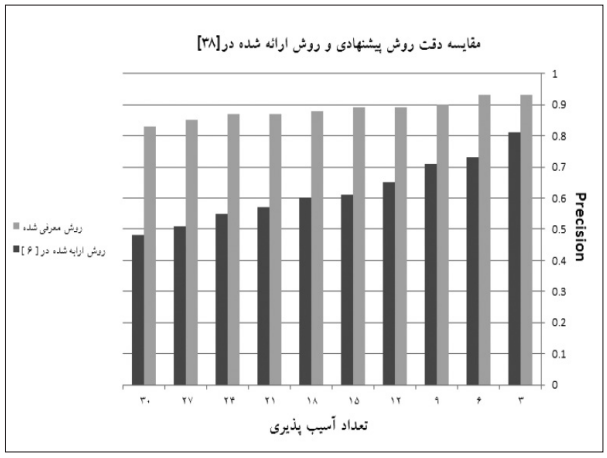
٤-۳- نتایج ارزیابی

برای ارزیابی روش پیشنهادی می‌بایست مقایسه‌های مختلفی را بر روی فاکتورهای متفاوت کیفیتی انجام داد تا بتوان از کیفیت روش پیشنهادی اظمینان حاصل نمود. برای ارزیابی روش پیشنهادی از دو فاکتور دقت تشخیص آسیب‌پذیری‌ها و سپس زمان اجرای روش پیشنهادی استفاده می‌گردد که در ادامه به بیان هر یک می‌پردازیم.

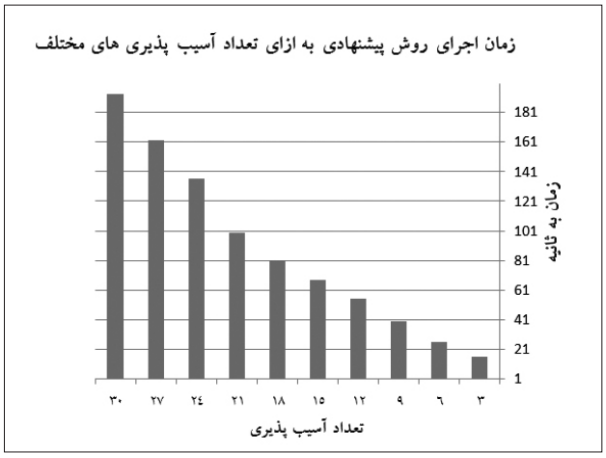
۴-۳-۱- دقت تشخیص

روش پیشنهادی برای تعداد آسیب‌پذیری‌های متفاوت مورد ارزیابی قرارگرفته است. در این روش هر چقدرکه تعداد آسیب‌پذیری‌ها افزایش پیدا می‌کند متعاقب آن فضای جستجوی مسئله نیز به همان اندازه رشد پیدا کرده و تعداد حالات مورد مقایسه آن نیز افزایش پیدا می‌کند. به روشنی مشخص است که با داشتن یک مجموعه از راه‌حل‌های ثابت و از پیش تعیین شده، هر چقدر که تعداد آسیب‌پذیری‌ها کمتر باشد روش پیشنهادی به خوبی قادر خواهد بود آن آسیب‌پذیری‌ها راکاهش دهد. در مقابل هر چقدر که تعداد آسیب‌پذیری‌ها افزایش پیدا می‌کند می توان انتظار داشت که دقت نیز در پی آن کاهش پیدا کند. شکل (۳) بیانگر این مسئله است.

یکی از روش‌های انجام شده در گذشته که به کار انجام شده در این مقاله از جهاتی نزدیک است، روش انجام شده در تحقیق [۶] می‌باشد. برای ارزیابی کیفیت روش و پیشنهادی و همچنین نشان دادن مزیت و برتری روش



شکل ۴: مقایسه دقت روش پیشنهادی و روش ارائه شده قبلی



شکل ۵: زمان اجرای روش پیشنهادی به ازای تعداد آسیب‌پذیری‌های مختلف

پیشنهادی مقایسه‌ای بین این دو روش از نظر دقت نتایج خروجی، انجام شده است که نمودار ارایه شده در شکل (۴) این امر را به خوبی نشان می‌دهد.

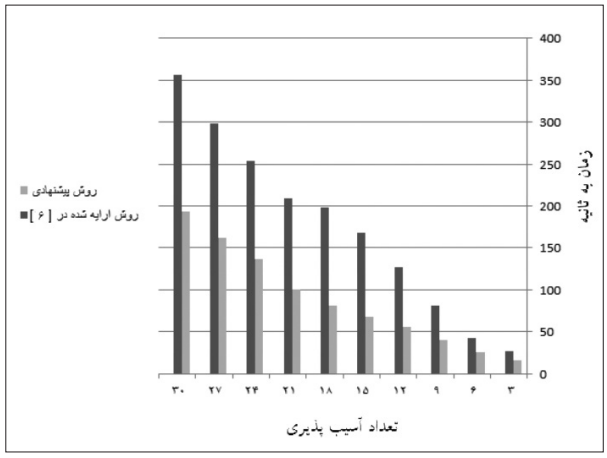
همان‌طور که از نمودار شکل(۴) مشخص است روش پیشنهادی برای تعداد متفاوت آسیب‌پذیری با روش ارائه شده قبلی [۶] از نظر دقت مورد مقایسه قرار گرفته است که در تمامی این حالات روش پیشنهادی دارای دقت بالاتری می‌باشد که این امر بیان‌گر کیفیت مناسب روش پیشنهادی نسبت به روش انجام شده قبلی می‌باشد. از آنجایی که روش پیشنهادی این مقاله از الگوریتم جستجوی فاخته استفاده می‌کند، این روش به خوبی قادر خواهد بود تا از قابلیت جستجوی تصادفی فضای مسئله و انتساب تصادفی راه‌حل‌ها به آسیب‌پذیری‌های موجود بهره ببرد، به‌طوری‌که این امرمنجر به دقت تشخیص بالا و پوشش مناسب آسیب‌پذیری‌ها می‌گردد.

۴-۳- ۲- زمان اجرا

مشکل عمده روش‌هایی که دارای مرتبه زمانی نمایی این است که با افزایش اندازه مسئله زمان اجرای مسئله نه به‌صورت خطی بلکه به صورت نمایی و با سرعت رشد بسیار بالا افزایش می‌یابد. این یعنی این‌که اگر اندازه مسئله‌ای x برابر شود تعداد فضای حالات 2^x برابر خواهد شد.

همان‌طور که از شکل (۵) مشخص است زمان اجرای الگوریتم روش پیشنهادی در این تحقیق به‌صورت تقریبا خطی و نه نمایی رشد کرده است . این امر بیانگر کیفیت بالای روش پیشنهادی می‌باشد که در عمل نشان دهنده مقیاس پذیری بالای این روش می‌باشد. به‌طوری که می‌توان مسایلی با اندازه بزرگ را در زمین اجرای مناسب و خطی حل نمود و زمانی که با آسیب‌پذیری‌های زیادی روبرو هستیم الگوریتمی ارایه داد که دارای پیچیدگی زمانی مناسبی باشد. همچنین برای نشان دادن مزیت و برتری روش پیشنهادی مقایسه‌ای نسبت به روش انجام شده در [۶] مقایسه ای بین این دو روش از نظر زمان پردازش نتایج خروجی، انجام شده است که نمودار ارایه شده در شکل (۶) این امر را به خوبی نشان می‌دهد.

همان‌طور که از نمودار شکل(۶) مشخص است روش پیشنهادی برای تعداد متفاوت آسیب‌پذیری با روش ارائه شده قبلی [۶] از حیث زمان اجرا مورد مقایسه قرار گرفته است که در تمامی این حالات روش پیشنهادی دارای زمان اجرای کمتری می‌باشد که این امر بیان‌گر کیفیت مناسب روش پیشنهادی نسبت به روش انجام شده قبلی می‌باشد. کاهش چشم‌گیر زمان اجرای روش پیشنهادی به علت جستجوی تصادفی فضای مسئله توسط جستجوی فاخته و همگرایی سریع به جواب بهینه می‌باشد که باعث کارایی این الگوریتم از نظر پیچیدگی زمانی گردیده است.



شکل ۶: مقایسه زمان اجرای روش پیشنهادی و روش ارایه شده در [۶]

۵- نتیجه گیری و کارهای آتی

برای کاهش مباحث انتزاعی و شناسایی راه‌حلی بهینه، در نظر گرفتن هزینه مربوطه لازم است و تحمل آسیب‌پذیری رویکردی سیستماتیک‌تر را می‌پذیرد که در این مقاله از الگوریتم جستجوی فاخته برای بهینه‌سازی استفاده شد. برای نگاشت این مفاهیم امنیتی چون آسیب‌پذیری و راه‌حل امنیتی به الگوریتم جستجوی فاخته بدین صورت عمل می‌گردد که هر یک از راه‌حل‌ها به‌عنوان لانه‌های الگوریتم فاخته و آسیب‌پذیری‌ها به‌عنوان تخم‌های مورد نظر در نظر گرفته می‌شوند. اگر لانه‌ای برای تخمی مناسب باشد و پرنده میزبان آن تخم را بیرون نینداخته و از آن مراقبت کند، بدین معنی است که راه‌حل امنیتی برای آسیب‌پذیری منتسب شده به آن مناسب می‌باشد. روش پیشنهادی از لحاظ فاکتورهای متفاوتی همچون دقت و زمان اجرا نیز طی ارزیابی‌های متفاوت و به ازای مقادیر مختلف مورد ارزیابی قرار می‌گیرند . برای بیان کیفیت روش پیشنهادی مقایسه‌هایی نیز با روش انجام شده قبلی صورت گرفت. شبیه‌سازی‌ها بیانگر کیفیت بالای روش پیشنهادی نسبت به این روش از نظر دو فاکتور دقت و زمان اجرا می‌باشد. برای کارهای آتی می‌توان از این الگوریتم به نحوی استفاده کرد که کاربر بتواند پارامترهای کیفیتی دیگر چون اولویت دادن به برخی از آسیب‌پذیری‌ها را اضافه کند که در آن روش پیشنهادی می‌تواند به پوشش برخی از آسیب‌پذیری‌های حیاتی نسبت به سایر آسیب‌پذیری‌ها اهمیت بیشتری قائل شود.

منابع

[1] Zhang, Xuyun, et al. “An efficient quasi-identifier index based approach for privacy preservation over incremental data sets on cloud.” Journal of Computer and System Sciences 79.5 (2013): 542-555.

[2] Michael, M. J., A view Of Cloud Computing, Communications Of The ACM,April, 2010.

[3] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. InSecurity and Privacy, 2007. SP ’07. IEEE Symposium on, pages 321–334, 2007

[4] S. Jarecki and X. Liu. Efficient Oblivious Pseudorandom Function with Applications toAdaptive OT and Secure Computation of Set Intersection. In Theory of Cryptography,volume 5444 of Lecture Notes in Computer Science, pages 577–594. Springer Berlin Heidelberg,2009. ISBN 978-3-642-00456-8.

[5] D. X. Song, D. Wagner, and A. Perrig. Practical techniques for searches on encrypteddata. In Proceedings of the 2000 IEEE Symposium on Security and Privacy, SP ’00, pages44–, Washington, DC, USA, 2000. IEEE SocietyISBN:0-7695-0665-8. URLhttp://dl.acm.org/citation.cfm?id=882494.884426.

[6] J. Trostle and A. Parrish. Efficient Computationally Private Information Retrieval fromAnonymity or Trapdoor Groups. In Proceedings of Conference on Information Security,pages 114–128, Boca Raton, USA, 2010.

[7] B. R.Waters, D. Balfanz, G. Durfee, and D. K. Smetters. Building an encrypted and searchableaudit log. In Proceedings of NDSS’04, 2004.

[8] Shin, Dong-Hee. “User centric cloud service model in public sectors: policy implications of cloud services.” Government Information Quarterly 30.2 (2013): 194-203.

[9] Bose, Ranjit, Xin Luo, and Yuan Liu. “The Roles of Security and Trust: Comparing Cloud Computing and Banking.” Procedia-Social and Behavioral Sciences 73 (2013): 30-34.

[10] Zissis, Dimitrios, and Dimitrios Lekkas. “Addressing cloud computing security issues.” Future Generation Computer Systems 28.3 (2012): 583-592.

[11] D. Zissis and D. Lekkas, “Securing e-Government and e-Voting with an open cloud computing architecture,” Government Information Quarterly,vol. 28, pp. 239-251, 2011.

[12] J.R. Winkler, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Technical EditorBill Meine, Elsevier Publishing, 2011.

[13] Y. Jadeja and K. Modi, “Cloud computing - concepts, architecture and challenges,” in Computing, Electronics and Electrical Technologies(ICCEET), 2012 International Conference on, 2012, pp. 877-880.

[14] Michael, M. J., A view Of Cloud Computing, Communications Of The ACM,April, 2010.

[15] A. Behl ,“Emerging Security Challenges in Cloud Computing”, word congress on Information and Communication Technologies, PP. 217-222,2011.

[16] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Elsevier, Network and ComputerApplications, Vol. 34, p.1-11, 2010.