بهبود امنیت در زیرساخت رایانش ابر با استفاده از پروتکل بلاکچین

محسن گرامی*
پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران
m.gerami@itrc.ac.ir

وحید یزدانیان
پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران
v.yazdanian@itrc.ac.ir

سیاوش نایب اصل
دانشگاه علوم تحقیقات، تهران، ایران
siavash.na94@gmail.com

تاریخ دریافت: ۱۴۰۰/۱۲/۲۱
تاریخ اصلاحات: ۱۴۰۱/۰۸/۲۰
تاریخ پذیرش: ۱۴۰۱/۰۹/۲۲

چکیده

امنیت در رایانش ابری امری بسیار حیاتی بوده، امنیت رایانش ابری مجموعه‌ای از امنیت کامپیوتر می‌باشد و امنیت شبکه در حالت کلی‌تر امنیت اطلاعات به حساب می‌آید و زمانی‌که یک وظیفه پردازشی از طریق بکارگیری الگوریتم زمان‌بندی به ماشین مجازی در ابر جهت پردازش تخلیه بار می‌شود این ماشین مجازی قادر نخواهد بود کاربر عادی موبایل را از حمله‌کنندگان تشخیص دهد در نتیجه حریم خصوصی نقض و امنیت داده انتقال یافته تضمین نمی‌شود، این در حالی است که فناوری بلاک‌چین به‌عنوان یک فناوری کلیدی برای تأمین امنیت به ویژه به لحاظ سه اصل اصالت، یکپارچگی و محرمانه‌بودن ظهور کرده است. بنابراین پس از تعیین راهبرد تخلیه بار می‌توان از بلاک‌چین در امنیت اطلاعات بهره برد و اطلاعات هر سرور در قالب یک بلوک کپسوله‌شده و تخلیه بار صورت می‌گیرد. با توجه به آنکه بلاک‌چین نیاز به منابع بالایی دارد در نتیجه بکارگیری آن در رایانش ابری نیازمند تدابیر خاص زمان‌بندی و تخصیص منبع است تا کمترین اثر منفی را بر روی کارایی داشته باشد در نتیجه جهت تخصیص منبع از یک راهکار زمان‌بندی فرااکتشافی و جهت افزایش امنیت از زنجیره بلاک‌چین استفاده می‌شود. در این تحقیق یک راهکار پیشنهادی ارایه می‌شود که همان ترکیب زنجیره بلاک‌چین و رایانش ابری به منظور افزایش امنیت و کارایی است. راهکار پیشنهادی پیاده‌سازی و مورد ارزیابی قرار می‌گیرد تا به نسبت سایر راهکارهای موجود، میزان افزایش کارایی آن بررسی شود.

واژگان کلیدی

رایانش ابری؛ امنیت رایانش ابری؛ بلاک‌چین؛ الگوریتم زمان‌بندی؛ موبایل؛ امنیت.

۱- مقدمه

دنیای فناوری اطلاعات و اینترنت که امروزه تبدیل به جزئی حیاتی از زندگی بشر شده، روز به روز در حال گسترش است. همسو با آن، نیازهای اعضای جوامع مانند امنیت اطلاعات، پردازش سریع، دسترسی پویا و آنی، قدرت تمرکز روی پروژه‌های سازمانی به جای اتلاف وقت برای نگهداری سرورها و از همه مهم‌تر، صرفه‌جویی در هزینه‌ها اهمیت زیادی یافته است. راه‌حلی که امروزه در عرصه فناوری برای چنین مشکلاتی پیشنهاد می‌شود، بکارگیری رایانش ابری است. رایانش ابری مدلی است برای داشتن دسترسی فراگیر، آسان و بنا به سفارشِ شبکه به مجموعه‌ای از منابع پردازشی پیکربندی‌پذیر (مثل: شبکه‌ها، سرورها، فضای ذخیره‌سازی، برنامه‌های کاربردی و سرویس‌ها) که بتوانند با کمترین کار و زحمت یا نیاز به دخالت فراهم‌کننده سرویس به سرعت فراهم شود [۶]. در واقع به کمک رایانش ابری شرکت‌ها، کاربران سرویس‌های فناوری اطلاعات، می‌توانند سرویس‌های مرتبط با فناوری اطلاعات خود را به‌عنوان سرویس خریداری نمایند. بر همین اساس، رایانش ابری راهی برای افزایش ظرفیت ذخیره‌سازی یا امکانات، بدون هزینه‌کردن برای زیرساخت جدید، آموزش پرسنل جدید، یا خرید مجوز نرم‌افزار جدید می‌باشد؛ در واقع شرکت‌ها یا افراد تنها برای آنچه مصرف می‌کنند هزینه خواهند کرد [۷]. بنابراین راهی مؤثر برای استفاده از منابع، مدیریت سرمایه و هزینه‌های پشتیبانی فناوری است.

امنیت رایانش ابری، زیرمجموعه‌ای از امنیت کامپیوتری، امنیت شبکه و در حالت کلی تر امنیت اطلاعات به حساب می‌آید. این مفهوم شامل مجموعه‌ای از سیاست‌ها، فناوری‌ها و کنترل‌ها جهت محافظت از داده‌ها، برنامه‌ها و زیرساخت‌های امنیتی در محاسبات ابری است. احراز هویت، محرمانگی"، یکپارچگی و حریم خصوصی داده‌ها جزو مسائل کلیدی مرتبط با امنیت رایانش ابری می‌باشند [۸]. احراز هویت جهت ایجاد ارتباط بین دو دستگاه و تبادل برخی کلیدهای عمومی و خصوصی از طریق گره‌ها برای جلوگیری از سرقت اطلاعات مورد نیاز است، که بحث حریم خصوصی اطلاعات هنوز بصورت کامل حل نشده است و به‌عنوان یک چالش و یا مسأله بسیار مهم مطرح می‌باشد. اخیراً بکارگیری بلاک‌چین به‌عنوان یک راه‌حل کارا به منظور تأمین امنیت در رایانش ابری پیشنهاد شده است. فناوری بلاک‌چین، اساساً یک پایگاه داده توزیع‌شده از

* نویسنده مسئول

اسناد و یا دفتر کل عمومی " از همه تراکنش‌ها یا رویدادهای دیجیتال" است، که توسط اجزای تشکیل‌دهنده‌اش (عضوها) به شکل مشترک اجرا می‌شود. هر تراکنش در دفتر کلی عمومی با توافق اکثریت اجزای سیستم ثبت می‌گردد. اطلاعاتی که یکبار وارد سیستم شده باشد، هرگز از بین نمی‌رود و همچنین زنجیره‌ی بلوکی برای هر تراکنش منحصر به فردی که ایجاد شده باشد، اطلاعات قطعی و قابل بازبینی را ثبت می‌کند. بطورکلی فناوری زنجیره‌ی بلوکی از ترکیب شبکه‌ای همتا به همتا و مفهوم کلید عمومی و امضای دیجیتال و همچنین پروتکل‌های اجماع تشکیل شده است که در آن پایگاه داده به صورت خودگردان تغییرات اطلاعات را بررسی و مدیریت می‌کند. در این شبکه نیازی به وجود مدیر نیست و در واقع کاربران، کار مدیریت آن را انجام می‌دهند. در ادامه با توجه به اهمیت ویژگی‌های بلاک‌چین، به بررسی پژوهش‌های انجام‌شده در این زمینه پرداخته می‌شود و مزایای اصلی آن بیان می‌گردد. در این تحقیق یک راهکار پیشنهادی ارایه می‌شود که همان ترکیب زنجیره بلاک‌چین و رایانش ابری به منظور افزایش امنیت و کارایی است. راهکار پیشنهادی پیاده‌سازی و مورد ارزیابی قرار می‌گیرد تا به نسبت سایر راهکارهای موجود، میزان افزایش کارایی آن بررسی شود. نهایتاً به جمع‌بندی مطالب ارایه‌شده در این پژوهش پرداخته می‌شود، همچنین پیشنهادهایی برای پژوهش‌های آتی بیان می‌گردد.

۱-۱- بیان مسأله

حفاظت از داده‌ها و حفظ حریم خصوصی چالش‌های کلیدی برای رایانش ابری است [۹]. با استفاده از فناوری زنجیره بلوکی، مشکل مدیریت هویت در رایانش ابری می‌تواند کاهش یابد. اعتماد یکی دیگر از ویژگی‌های مهم رایانش ابری است، که در آن ادغام زنجیره بلوکی می‌تواند نقش داشته باشد. اهمیت اعتماد در بسترهای رایانش ابری به‌عنوان یکی از اهداف اصلی برای اطمینان از موفقیت آن شناخته شده است. تکنیک‌های یکپارچگی داده‌ها یکی دیگر از گزینه‌ها برای اطمینان از دسترسی به داده‌ها در یک زمان هستند زیرا از زنجیره‌ی بلوکی بیش از حد به مقدار زیادی از داده‌های تولیدشده توسط رایانش ابری اجتناب می‌کنند. در بلاک‌چین هر بلاک شامل یک سری داده، هش کد مربوط به آن بلاک و هش کد مربوط به بلاک قبلی می‌باشد. داده‌هایی که در هر بلاک ذخیره می‌شوند به نوع بلاک‌چین بستگی دارند. عنصر دیگری که در بلاک موجود است، هش می‌باشد. هش به مانند اثر انگشت برای انسان است. هنگامی‌که یک بلاک به وجود می‌آید هش آن محاسبه شده و به واسطه تغییر در بلاک هش آن نیز تغییر می‌کند. هر یک از هش‌ها مجموعه‌ای از اعداد و حروف هستند که براساس اطلاعات ذخیره‌شده در بلاک‌ها ایجاد می‌شود. عنصر سومی که در هر بلاک وجود دارد؛ هش بلاک قبلی است که از عوامل تأثیرگذار در به‌وجود آمدن زنجیره بلاک‌ها می‌باشد. تغییر در داده‌های بلاک موجب تغییر در هش آن بلاک می‌شود که این امر خود به خود هشی که در بلاک بعدی به‌عنوان هش بلاک قبلی ذخیره شده را تغییر می‌دهد و این تغییر در شبکه خود را نشان می‌دهد و عدم مطابقت این دو هش با یکدیگر مانع از تغییر داده‌های بلاک می‌شود. با تغییر اطلاعات یک بلاک هش آن بلاک نیز تغییر می‌کند و در نتیجه تمام بلاک‌های بعد از آن نامعتبر می‌شوند [۱۰]. بر همین اساس در این تحقیق از طریق ترکیب بلاک‌چین و رایانش ابری یک راهکار بهینه به منظور افزایش امنیت در فرایند تخلیه بار از دستگاه‌های موبایل به محیط ابری با کمترین تأثیر منفی بر روی کارایی ارایه می‌شود. با توجه به آنکه بلاک‌چین نیاز به منابع بالایی دارد در نتیجه بکارگیری آن در رایانش ابری نیازمند تدابیر خاص زمان‌بندی و تخصیص منبع است تا کم‌ترین اثر منفی را بر روی کارایی داشته باشد در نتیجه جهت تخصیص منبع از یک راهکار زمان‌بندی فرااکتشافی و جهت افزایش امنیت از زنجیره بلاک‌چین استفاده می‌شود.

۱-۲- سؤالات تحقیق

- به چه صورت می‌توان بلاک‌چین را جهت بهبود امنیت در زیرساخت رایانش ابری بکار برد؟
- بکارگیری بلاک‌چین جهت تأمین امنیت در زیرساخت رایانش ابری چه تأثیری بر روی پارامترهای کیفیت سرویس از جمله توافقنامه سطح سرویس دارد؟
- چگونه می‌توان از زمان‌بند در جهت تخصیص منبع برای بلاک‌چین استفاده نمود؟
- به چه صورت می‌توان فرایند تخلیه‌بار از دستگاه‌های موبایل به محیط ابری را بهبود و به کمک بلاک‌چین تأمین امنیت نمود؟

۲- امنیت در رایانش ابری

یکی از چالش‌های اصلی در برابر رایانش ابری، امنیت می‌باشد. چندین دلیل برای این امر وجود دارد. اول اینکه در هسته اکثر زیرساخت‌های رایانشی، چندین فناوری مختلف از جمله شبکه‌های بی‌سیم، توزیع‌شده، نظیر به نظیر و پلات‌فرم مجازی‌سازی فعال شده است. در این حالت فقط تأمین امنیت تمامی این فناوری‌ها یک چالش نیست بلکه نحوه هماهنگ‌سازی مکانیزم‌های مختلف امنیتی در چنین زیرساخت ناهمگنی نیز یک چالش اساسی است و پیچیدگی‌های خاص خود را دارد [۱۱]. دوم اینکه، رایانش ابری بزرگ‌تر از مجموع بخش‌هایش می‌باشد به‌عبارت دیگر حتی اگر از امنیت کلیه فناوری‌های موجود اطمینان حاصل شود نمی‌توان در مورد امنیت کلی سیستم مطمئن بود. سوم اینکه اگر یک مشکل امنیتی در یک بخش بخصوصی از رایانش ابری اتفاق بیافتد می‌تواند تمامی بخش‌های دیگر را نیز تحت تأثیر قرار دهد در واقع این مشکل امنیتی به سایر برنامه‌ها ارث‌بری خواهد شد. در جدول ۱ یک دسته‌بندی از تهدیدات موجود در بخش‌های مختلف زیرساخت‌های رایانشی نشان بیان شده است.

جدول ۱- دسته‌بندی تهدیدات موجود در بخش‌های مختلف زیرساخت‌های رایانشی [۱۱]

منبع	تهدید
زیرساخت شبکه	منع سرویس، حمله مرد میانی، rogue gateway
مرکز داده لبه	صدمه فیزیکی، نشت حریم خصوصی، افزایش امتیاز، دستکاری سرویس
زیرساخت هسته	نشت حریم خصوصی، دستکاری سرویس
زیرساخت مجازی‌سازی	منع سرویس، سوءاستفاده از منابع، نشت حریم خصوصی، افزایش امتیاز، دستکاری ماشین مجازی
دستگاه‌های کاربر	تزریق اطلاعات، دستکاری سرویس

۳- پیشینه پژوهش

مقاله [۱۲] مروری می‌باشد و در آن به مشکلات و چالش‌های پیش‌روی فناوری بلاک‌چین پرداخته شده است. بر همین اساس در ابتدا توضیحات کاملی در مورد نحوه عملکرد بلاک‌چین و تأمین امنیت در آن ارایه شده است. سپس در ادامه یک دسته‌بندی کلی در مورد مشکلات امنیتی که می‌تواند در بلاک‌چین بوجود بیاید انجام شده، بر این اساس، چالش‌های امنیتی موجود در بلاک‌چین را می‌توان بصورت زیر در نظر گرفت:

- حملات مربوط به اکثریت که در این حالت کاربری که قدرت پردازشی بالاتر از ۵۱٪ را در اختیار داشته باشد می‌تواند داده مربوط به تراکنش را تغییر داده و یا از تأیید بلوک و همچنین استخراج بلوک جلوگیری به عمل آورد.
- مشکلات مربوط به انشعاب: یکی از مشکلات مهم در بلاک‌چین است که این حالت در اثر به‌روزرسانی‌های نرم‌افزاری و ایجاد نسخه جدید بوجود می‌آید. به‌عنوان نمونه گره قدیمی در مقایسه با گره جدید نیازمندی‌های مربوط به تأیید یا تصدیق آن بسیار سخت‌گیرتر می‌باشد و در این حالت در بخش جدید تأیید اما در نسخه قدیمی مورد تأیید قرار نمی‌گیرد.
- مقیاس‌پذیری بلاک‌چین: با رشد بلاک‌چین، داده‌های مربوط به آن نیز بزرگ و بزرگ‌تر می‌شود در نتیجه بارگذاری و همچنین پردازش آن نیز سخت و سخت‌تر خواهد شد. بر همین اساس زمان بسیار زیادی جهت همگام‌سازی داده نیاز خواهد بود و امکان دارد در حین فرایند همگام‌سازی، داده دوباره تغییر نماید که در نتیجه می‌تواند مشکلاتی را برای کاربر بوجود آورد.
- مشکلات مربوط به جامعیت.

در مقاله [۱۳] یک راهکار توزیع شده و سیستم احراز هویت اعتماد بر پایه بلاک‌چین و رایانش ابری پیشنهاد شده است. این سیستم از سه لایه فیزیکی، لبه بلاک‌چین و همچنین شبکه بلاک‌چین تشکیل شده است. بر همین اساس الگوریتمی به نام PBFT ارایه گردیده و هدف آن ایجاد یک راهکار چندمنظوره به کمک بلاک‌چین جهت ذخیره‌سازی داده‌ها و گزارشات احراز هویت است. در این الگوریتم از رایانش به منظور ارایه سرویس احراز هویت لبه‌ای استفاده می‌شود. همچنین از یک رمزنگاری نامتقارن به منظور جلوگیری‌کردن از حملات بین گره‌ها و ترمینال‌ها بهره برده شده است. در انتها راهکار پیشنهادی مورد ارزیابی قرار گرفته و این نتیجه حاصل شده که از طریق بکارگیری آن می‌توان میزان تأخیر را به شکل قابل توجهی کاهش داد.

در پژوهش [۱۴] یک راهکار احرازهویت مبتنی بر بلاک‌چین و همچنین مدیریت کلید با استفاده از زیرساخت رایانش ابری ارایه شده است. در این تحقیق بیان شده است، با وجود رمزنگاری‌های مختلفی که در زیرساخت رایانش ابری جهت تأمین امنیت انجام گرفته مشکلات مربوط به عدم پشتیبانی پروتکل‌های موجود از قابلیت ناشناسی و مدیریت کامل کلید می‌باشد. بر همین اساس راهکار پیشنهادی قادر است با بهره‌گیری از زنجیره بلاک‌چین یک پروتکل امنیتی جهت احراز هویت و همچنین مدیریت کلید ارایه دهد. این راهکار بخوبی از قابلیت ناشناسی پشتیبانی می‌کند و نیازی به رمزنگاری‌های پیچیده جهت پیاده‌سازی ندارد. در انتها نیز از طریق ارزیابی‌هایی که انجام‌گرفته این نتیجه حاصل شده است که روش پیشنهادی بخوبی توانسته هزینه ارتباطی و محاسباتی را در رایانش ابری کاهش دهد.

در مقاله [۱۵] یک چارچوب مبتنی بر بلاک‌چین به منظور افزایش کیفیت ارایه سرویس در اینترنت‌اشیاء و برقراری توازن از طریق بهره‌گیری از رایانش ابری ارایه شده است. در این تحقیق یک معماری جدید به منظور مانیتورکردن و امنیت سیستم‌های اینترنت‌اشیاء پیشنهاد شده است و این عملیات براساس یک نمونه از خانه هوشمند بیان شده است. در این خانه هوشمند از یک WSN به منظور مانیتورکردن تمام فعالیت‌هایی که در خانه هوشمند رخ می‌دهد، استفاده شده است. در ادامه WSN اطلاعات را به بلاک‌چین ارسال می‌کند. این عمل باعث جمع‌آوری اطلاعات خانه هوشمند و در نتیجه ذخیره‌سازی ایمن آنها در بلاک‌چین می‌شود. بخش کنترل‌کننده هوشمند وظیفه مدیریت گره‌های IoT و تمامی گره‌های WSN مربوطه را بر عهده دارد. از Raspberry Pi هم به منظور اجرای دستورات هوشمند در زنجیره اصلی بلاک‌چین استفاده می‌شود. در واقع در این راهکار بخش مربوط به رایانش لبه‌ای واحد اصلی پردازشی می‌باشد و جهت بهینه‌سازی عملیات پردازش Raspberry Pi مورد استفاده قرار می‌گیرد. این بخش قابلیت پردازش محاسبات بسیار پیچیده را در زمان قابل قبولی فراهم می‌کند. در انتها با ارزیابی‌های انجام‌گرفته نشان داده شده است که راهکار از طریق برقراری توازن، توانسته است میزان انرژی و دما را در زیرساخت رایانشی کاهش دهد.

در تحقیق [۱۶] یک راهکار مبتنی بر یادگیری ارایه شده است تا علاوه بر ایجاد توازن در منابع بتوان قابلیت پشتیبانی بلاک‌چین را نیز به رایانش ابری اضافه نمود. با توجه به محدودیت دستگاه‌های هوشمند در IoT در این راهکار وظایف پردازشی به دستگاه‌های پردازش ابری تخلیه می‌شوند. اما در طی فرایند تخلیه بار از دستگاه‌های موبایل به رایانش ابری امکان نفوذ به اطلاعات و همچنین تغییر در داده‌ها وجود دارد بر همین اساس

یک راهکار مبتنی بر زنجیره بلاک‌چین به منظور ایمن‌کردن فرایند تخلیه بار ارایه شده است در واقع در این راهکار از بلاک‌چین در رایانش ابری و به منظور تضمین جامعیت داده‌ها مورد استفاده قرار می‌گیرد. در ادامه طی شبیه‌سازی‌هایی که انجام‌شده این نتایج حاصل شده که روش پیشنهادی میانگین بهره‌وری و همچنین کارایی منابع را بالا برده است.

در تحقیق [۱۷] از بلاک‌چین به‌عنوان یک راهکار جهت افزایش امنیت و کارایی در به اشتراک‌گذاری داده در رایانش لبه‌ای و شبکه خودرویی استفاده شده است. در این پژوهش به اهمیت رایانش لبه‌ای به‌عنوان یک قدرت پردازشی عظیم و همچنین فضای ذخیره‌سازی مناسب جهت بکارگیری در شبکه‌های خودرویی استفاده شده است. با توجه به آنکه پردازش سیستم‌های خودران پایین می‌باشد در نتیجه می‌توان وظایف پردازشی آنها را به رایانش لبه‌ای ارسال کرد اما با توجه به اعتماد پایین به این نوع راهکار در این پژوهش از بلاک‌چین جهت تأمین امنیت داده‌ها در طی فرایند ارسال و ذخیره‌سازی آنها در رایانش لبه‌ای استفاده شده است. این راهکار بطور مؤثری می‌تواند از دسترسی به داده‌های اشتراکی بدون فرایند احراز هویت جلوگیری به‌عمل آورد.

در مقاله [۱۸] به‌عنوان یک سرویس ذخیره‌سازی برای دفترکل بلاک‌چین از رایانش ابری در لبه شبکه استفاده شده است. دلیل بهره‌گیری از این راهکار در نیاز به فضای ذخیره‌سازی برای بلاک‌چین است که توسط موبایل و یا دستگاه‌های هوشمند پشتیبانی نمی‌شود. بر همین اساس از دستگاه‌های موجود در اینترنت‌اشیاء در جهت استفاده از منابع پردازشی آنها استفاده می‌شود. اما از طرفی با توجه به محدودیت فضای ذخیره‌سازی که این دستگاه‌ها دارند نیاز به یک روش جایگزین جهت ذخیره‌سازی دفترکل است که برای این منظور و جهت جلوگیری از مشکلات محرمانگی داده (به دلیل مکان ذخیره‌سازی داده‌ها) از قابلیت رایانش ابری به‌عنوان یک راهکار استفاده می‌شود. همچنین در این تحقیق یک معماری به منظور کاهش نیاز دستگاه‌های IoT به حافظه ارایه شده است. در انتها این نتیجه حاصل شده که معماری پیشنهادی مبتنی بر معماری بلاک‌چین و رایانش لبه‌ای و ابری در مقایسه با معماری‌های سنتی موجود، بخوبی می‌تواند کارایی پردازنده و منابع را افزایش دهد.

در مقاله [۱۹] محدودیت‌های راه‌های موجود برای بهبود امنیت ابر را در این مطالعه بررسی شده است. به‌طورکلی، یک بلاک‌چین به‌عنوان رکورد عمومی برای تراکنش‌ها در نظر گرفته می‌شود و در برابر تهدیدات سایبری در طول تراکنش‌های مربوط به ارز مجازی محافظت می‌کند. در نتیجه، سوابق ذخیره‌شده در فضای ابری و قابل دسترسی از طریق اینترنت‌اشیاء، اتخاذ پروتکل‌های بسیار امنی را که قادر به مقاومت در برابر حملات سایبری هستند، ضروری می‌سازد. در این تحقیق یک راهبرد اعتبارسنجی داده مبتنی بر SDN ارائه شده است که در آن فقط کاربران مجاز می‌توانند به سوابق تراکنش دسترسی داشته باشند.

در مقاله [۲۰] بیان شده است که قراردادهای هوشمند و بلاک‌چین با اجازه‌دادن به ایجاد فناوری‌های ابری/ مه‌آلود کاملاً غیرمتمرکز که هزینه‌ها را با تولید نتایج قابل پیش‌بینی بدون نیاز به هیچ واسطه‌ای کاهش می‌دهند، این فرصت را داشته‌اند تا شکل فعلی بازارهای ابری را تغییر دهند. علاوه بر این، بسیاری الزامات فعلی را برای ایجاد راه‌حل‌های ابری غیرمتمرکز کاملاً یکپارچه توصیه می‌کنند که به فروشندگان بزرگ اجازه می‌دهد از این نوع راه‌حل‌ها پیروی کنند و از سخت‌افزار اختصاصی اجتناب کنند. این تحقیق نشان می‌دهد که تجزیه و تحلیل معین نه تنها با کشف ناسازگاری‌های پیاده‌سازی و راه‌حل‌های جایگزین برای مسائل توسعه در این زمینه، بلکه از طریق ارزیابی قوانین از پیش تعیین‌شده و پیشنهاد امکانات بزرگ برای قابلیت همکاری، به پیشرفت سیستم‌های ابری کمک می‌کند.

۳-۱- مرور تحقیقات داخلی

در تحقیق انجام‌شده در [۱] یک مدل پیشنهادی جهت امنیت اینترنت‌اشیاء و رایانش ابری با استفاده از الگوریتم AES و RSA ارایه شده است. در این تحقیق، هر دو فناوری رایانش ابری و اینترنت‌اشیاء با تمرکز بر مسائل امنیتی بررسی شده است. به‌طور خاص، این دو فناوری به منظور بررسی ویژگی‌های مشترک و کشف مزایای آن‌ها ترکیب شده‌اند. در نتیجه، تأثیر رایانش ابری در اینترنت‌اشیاء بررسی شده است. بر همین اساس با توجه به زمان اجرای پایین الگوریتم‌های متقارن از جمله AES، عملیات رمزنگاری داده اصلی به کمک آن انجام می‌شود، سپس جهت ایجاد امضای دیجیتال از الگوریتم RSA بهره برده شده است. در نهایت، چالش‌های امنیتی ادغام هر دو فناوری رایانش ابری و اینترنت‌اشیاء بررسی و مدل امنیتی جهت ادغام امن فناوری‌های مذکور ارائه خواهد شد.

در تحقیقی که در [۲] انجام شده است، بر روی ارایه یک الگوریتم کارا جهت احراز هویت کاربران در رایانش ابری تمرکز شده است. الگوریتم پیشنهادی شامل دو مرحلهٔ ثبت‌نام و احراز هویت متقابل می‌باشد و دارای دو نقش سرور و کاربر است. در فاز ثبت‌نام، کاربر درخواست ثبت‌نام خود را به سرور می‌فرستد سپس بعد از تعیین یک شناسه برای کاربر، سرور یک کلمه عبور برای وی در نظر می‌گیرد. در مرحله احراز هویت نیز مقادیر پارامترهای مربوط به احراز هویت در قالب یکسری روابط ریاضی تعیین می‌شود و چنانچه این روابط برقرار باشند، کاربر برای سرور احراز هویت می‌شود.

در مقاله [۳] بر روی استفاده از فناوری بلاک‌چین جهت بالابردن امنیت در داده‌های ابری تمرکز شده است. در این تحقیق بیان شده است که با توجه به رشد سریع رایانش ابری، هنوز هم نگرانی‌های امنیت اطلاعات به‌طور کامل رفع نشده است که می‌تواند مانع رشد آن شود. این در حالی است که فناوری بلاک‌چین به‌عنوان یک فناوری کلیدی برای تأمین امنیت به ویژه به لحاظ سه اصل اصالت، یکپارچگی و محرمانه‌بودن ظهور کرده است. در ادامه این تحقیق به بررسی امنیت در سرویس‌های

ابری و نقش و کمک بلاک‌چین به‌عنوان یک سرویس در بالابردن امنیت آن پرداخته شده است. همچنین ویژگی‌ها و چالش‌های بکارگیری بلاک‌چین در محیط ابری نیز مورد بررسی قرار گرفته است. در ادامه و به منظور تأمین امنیت رایانش ابری به کمک بلاک‌چین یک چارچوب ذخیره‌سازی ابری جدید و ایمن، با کنترل دسترسی، از طریق استفاده از فناوری بلاک‌چین اتریوم پیشنهاد شده است. این روش پیشنهادی، ترکیبی از رمزنگاری مبتنی بر خصیصه سیاست رمز- متن و بلاک‌چین اتریوم است. چارچوب ذخیره‌سازی پیشنهادی غیرمتمرکز است به عبارتی هیچ‌گونه شخص ثالث مطمئنی، در سیستم وجود ندارد.

در تحقیق [۴] به بررسی دلایل پذیرش بلاک‌چین به‌عنوان یک ضرورت در تجارت الکترونیک پرداخته شده است. در این مقاله بیان شده است که برنامه‌های مبتنی بر بلاک‌چین، اکثر صنایع تجارت الکترونیک را برای معاملات مالی، قراردادها و فرایندهای توسعه تجارت، پذیرفته‌اند. همچنین این فناوری قادر است یک دسترسی هوشمند را به داده‌ها، بدون تغییر و بصورت کاملاً ایمن فراهم کند. در نتیجه اگر شرکت‌ها و ارائه‌دهندگان خدمات، سعی نکنند که امروز از بلاک‌چین استفاده کند، همین فناوری بعداً و در آینده نزدیک به تهدیدی تبدیل خواهد شد. همچنین خاصیت زنجیره بلاک‌چین گستردگی بسیار زیاد آن بوده و همه اتفاقات حول محور آن و در یک سلسله مراتب تجمیع می‌شود، ضمن اینکه اگر کسی بخواهد در این زنجیره دستکاری یا خللی ایجاد کند، مشخص می‌شود. در نتیجه با تسهیل کارکردهای کلیدی بلاک‌چین در صورت موفقیت پذیرش، می‌تواند مکمل و رقیب روش‌های سنتی باشد. از طرف دیگر، خدمات فراگیر قادر به بهبود تجربه کاربر از طریق تحویل کارآمد محتوا و واکنش‌های سریع به خواسته‌های آنها خواهند بود.

در مقاله [۵] یک روش مبتنی بر رمزنگاری متقارن به منظور تأمین امنیت داده‌های ذخیره‌شده در ابر ارایه شده است. این راهکار بر از طریق بهبود رمزنگاری‌های متقارن ارایه شده است. بطوریکه از طریق بکارگیری آن بتوان تا حدودی مشکلات و معایب راهکارهای موجود را برطرف نمود. راهکار امنیتی پیشنهادی به اینصورت است که ترکیبی از الگوریتم رمزنگاری متقارن بلوفیش به همراه الگوریتمی مشابه با عملکرد جانشینی و کلاسیک Playfair مورد استفاده قرار گرفته است. دلیل استفاده از الگوریتم بلوفیش، نیاز به حافظه پایین، سرعت بالا و همچنین عملکرد عالی آن در جلوگیری از سوء استفاده بیان شده است. بر همین اساس داده‌های اصلی موجود در مراکز داده به کمک این الگوریتم رمزنگاری می‌شود. نتایج ارزیابی هم بیانگر آن است که زمان شکست این الگوریتم به نسبت سایر رمزنگاری‌های متقارن بالاتر می‌باشد.

۴- شکاف تحقیقاتی و نوآوری

هنگامی‌که یک وظیفه پردازشی از طریق بکارگیری الگوریتم زمان‌بند به یک ماشین مجازی در رایانش ابری جهت پردازش، ارسال می‌شود این ماشین مجازی قادر نخواهد بود که کاربرهای عادی را از حمله‌کننده‌ها تشخیص دهد. در نتیجه می‌تواند حریم خصوصی نقض و امنیت داده انتقال‌یافته تضمین نشود. برای این منظور و رفع این چالش الگوریتم‌های رمزنگاری مختلفی مبتنی بر رمزنگاری متقارن و نامتقارن پیشنهاد شده است، اما با توجه به آنکه این دسته از روش‌های رمزنگاری قابلیت توزیع‌پذیری چندانی ندارند در نتیجه بکارگیری آنها در محیط‌های توزیع‌شده و مقیاس‌پذیری مانند رایانش ابری دارای مشکلات متعددی است که افزایش سربار شبکه و کاهش کارایی از مهم‌ترین آنها می‌باشد. در نتیجه نیاز به روش‌های نوینی است که با محیط‌های توزیع‌شده از جمله رایانش ابری سازگار باشد. بر همین اساس در این پژوهش از بلاک‌چین برای رفع این مشکل استفاده می‌شود. در نتیجه ابتدا از یک راهکار زمان‌بندی مبتنی بر الگوریتم PSO بهبود یافته استفاده می‌شود تا از طریق آن بتوان به کمک قابلیت بررسی منبع، بهترین گره‌های پردازشی را جهت زمان‌بندی انتخاب کرد، سپس اطلاعات مربوط به راهبرد زمان‌بندی، بجای یک کنترلر مرکزی توسط سایر مراکز پردازشی ارزیابی می‌گردد. این اطلاعات می‌تواند در قالب یک بلوک، کپسوله‌شده و از بلاک‌چین به منظور رمزنگاری این اطلاعات زمان‌بندی یا مهاجرت از جمله مقدار هش بلوک قبلی، اطلاعات کاربر، اطلاعات وظیفه و سایر موارد استفاده کرد.

۵- راهکار پیشنهادی

از آنجاکه محیط ابری دارای گره‌های پردازشی قوی می‌باشد در نتیجه براحتی می‌توان از آن به منظور فرایندهای پردازشی سنگین و پیچیده بهره برد. بر همین اساس از طریق تخلیه‌ی وظایف پردازشی دستگاه‌های قابل حمل به این زیرساخت، علاوه بر کاهش زمان اجرا می‌توان در مصرف انرژی این دستگاه‌ها هم صرفه‌جویی به‌عمل آورد [۲۱]. اما در طی فرایند انتقال، ضعف و مشکلات مختلفی مربوط به امنیت و جامعیت داده در اثر نشت و یا نقص عملیات انتقال ممکن است رخ دهد. در واقع هنگامی‌که یک وظیفه پردازشی از طریق بکارگیری الگوریتم زمان‌بند به یک ماشین مجازی در ابر جهت پردازش، تخلیه‌بار می‌شود این ماشین مجازی قادر نخواهد بود که کاربرهای عادی موبایل را از حمله‌کننده‌ها تشخیص دهد. در نتیجه می‌تواند حریم خصوصی نقض و امنیت داده انتقال‌یافته تضمین نشود. بر همین اساس در این پژوهش از بلاک‌چین برای رفع این مشکل استفاده می‌شود. در نتیجه پس از تعیین راهبرد تخلیه‌بار، اطلاعات مربوط به مهاجرت، بجای یک کنترلر مرکزی توسط سایر مراکز پردازشی ارزیابی می‌گردد. اطلاعات هر سرور می‌تواند در قالب یک بلوک، کپسوله‌شده و از بلاک‌چین به منظور رمزنگاری اطلاعات تخلیه‌بار از جمله مقدار هش بلوک قبلی، اطلاعات کاربر، اطلاعات وظیفه و سایر موارد استفاده گردد. سایر ماشین‌ها به جز ماشینی که سرویس مورد نظر را برای دستگاه موبایل ارایه داده است جهت اعتبارسنجی رکورد مربوط به عملیات تخلیه‌بار باهم رقابت خواهند کرد. پس از آنکه اطلاعات مربوط به سرویس توسط تمام

ماشین‌ها مورد بررسی قرار گرفت، می‌توان مطمئن شد که امنیت و جامعیت در طی فرایند تخلیه‌بار بطور کامل اعمال شده است و در نتیجه عملیات تخلیه‌بار شروع می‌شود. در ادامه این پژوهش نحوه انجام عملیات زمان‌بندی مورد بررسی قرار می‌گیرد و سپس نحوه تأمین امنیت و جامعیت آن به کمک بلاک‌چین بررسی می‌شود.

۶- زمان‌بندی

در این پژوهش به منظور ایجاد توازن و انتخاب سرورهای پردازشی جهت میزبانی از درخواست‌های تخلیه‌بار از یک زمان‌بند مبتنی بر الگوریتم بهینه‌سازی ازدحام ذرات[1] استفاده خواهد شد که در کنار آن از زنجیره بلاک‌چین به منظور تأمین محرمانگی و جامعیت بهره برده شده است. در این راهکار به منظور انتخاب یک سرور پردازشی جهت اجرای وظایف تخلیه‌شده از یک مانیتور منبع استفاده خواهد شد که به کمک آن وضعیت منابع سرورها مورد بررسی قرار می‌گیرد و براساس آن تصمیمات مربوط به درخواست تخلیه‌بار از یک دستگاه به سرور موردنظر تعیین و انجام می‌گیرد. این راهبرد انتخاب براساس میزان منابع در دسترس و همچنین عدم بوجودآمدن سربار در یک سرور در صورت پذیرش میزبانی، می‌باشد. در ادامه نحوه فرموله‌سازی راهکار مورد بررسی قرار گرفته است.

۷- فرموله‌سازی راهکار

به منظور بررسی وضعیت منابع در دسترس سرورهای پردازشی که وظیفه اجرای دستورات تخلیه‌بار شده را بر عهده دارند از رابطه ۱ استفاده می‌شود. در این فرمول میزان مصرف پردازنده و حافظه در ماشین‌های پردازشی موجودر در زیرساخت ابری طبق [۲۲] و بصورت زیر مدل می‌شود:

$$W_j = \frac{|L_j^{\,p} - L_j^{\,m}|}{U_j^{\,p} + U_j^{\,m}} \qquad (۱)$$

$L_j^{\,p}$: مقدار پردازنده باقی مانده برای ماشین فیزیکی j ام

$L_j^{\,m}$: مقدار حافظه باقی مانده برای ماشین فیزیکی j ام

$U_j^{\,p}$: مقدار پردازنده مصرف شده برای ماشین فیزیکی j ام

$U_j^{\,m}$: مقدار حافظه مصرف شده برای ماشین فیزیکی j ام

W_j: مصرف منابع سرور j ام

این پارامترها به دلایل زیر انتخاب و لحاظ شده‌اند:

- تأثیر استفاده از تمامی منابع (پردازنده و حافظه)
- حفظ تعادل هر سرور از نظر مصرف منابع
- توازن بار بر روی شبکه با توجه به میزان مصرف حافظه، پردازنده‌های ماشین مجازی، حافظه و پردازنده‌های باقی مانده برای ماشین‌های فیزیکی

۸- بهینه‌سازی ازدحام ذرات

بهینه‌سازی ازدحام ذرات یک الگوریتم هوشمند براساس ازدحام است [۲۳] که از رفتار اجتماعی حیوانات؛ مانند پرندگان که جهت یافتن منبع غذا تلاش می کنند یا دسته‌ای از ماهیان که از خود در برابر صیادان حفاظت می‌کنند؛ نشأت گرفته شده است. در این الگوریتم، جمعیت برابر با تعداد ذره‌ها در فضای مسأله است. ذرات به صورت تصادفی مقداردهی اولیه می‌شوند. هر ذره یک مقدار سازگاری خواهد داشت و به‌وسیله تابع سازگاری که بایستی در هر نسل بهینه شود، ارزیابی خواهد شد. به عبارت دیگر این راهکار معادل یک پرنده در الگوی حرکت جمعی پرندگان می‌باشد. هر ذره یک مقدار شایستگی دارد که توسط یک تابع شایستگی محاسبه می‌شود. هرچه ذره در فضای جستجو به هدف نزدیک‌تر باشد، شایستگی بیشتری دارد. همچنین هر ذره دارای یک سرعت است که هدایت حرکت ذره را برعهده دارد. هر ذره با دنبال‌کردن ذرات بهینه در حالت فعلی، به حرکت خود در فضای مسأله ادامه می‌دهد. به این شکل است که گروهی از ذرات در بهینه‌سازی ازدحام، آغاز کار به صورت تصادفی به‌وجود می‌آیند و با به‌روزکردن نسل‌ها سعی در یافتن راه‌حل بهینه می‌نمایند. در واقع هر ذره بهترین مکان (pbest) و بهترین موقعیت تا به حال خود را از بین گروه کاملی از ذرات gbest پیدا می‌کند. pbest هر ذره بهترین نتیجه تا بحال بدست‌آمده به‌وسیله ذره است، درحالیکه gbest بهترین ذره به نسبت معیار سازگاری در کل جمعیت می‌باشد. در هر نسل سرعت و موقعیت ذرات به ترتیب توسط روابط ۲ و ۳ بروزرسانی خواهد شد. سرعت و موقعیت اولیه در واقع پارامتر ورودی می‌باشد [۲۳].

```
v[ ] = v[ ] + c1 * rand() * (pbest[ ] - position [ ]) + c2 *
rand() * (gbest[ ] - position[ ])                    (۲)
position[ ] = position[ ] + v[ ]                     (۳)
```

سمت راست معادله (۲) از سه قسمت تشکیل شده که قسمت اول، سرعت فعلی ذره است و قسمت‌های دوم و سوم تغییر سرعت ذره و چرخش آن به سمت بهترین تجربه شخصی و بهترین تجربه گروه را به عهده دارند. اگر قسمت اول این معادله در نظر گرفته نشود، آنگاه سرعت ذرات تنها با توجه به موقعیت فعلی و بهترین تجربه ذره و بهترین تجربه جمع تعیین می‌شود. به این ترتیب، بهترین ذره جمع، در جای خود ثابت می‌ماند و سایرین به سمت آن ذره حرکت می‌کنند. در واقع حرکت دسته‌جمعی ذرات بدون قسمت اول معادله (۲)، پروسه‌ای خواهد بود که طی آن فضای جستجو به تدریج کوچک می‌شود و جستجویی محلی حول بهترین ذره شکل می‌گیرد. در مقابل اگر فقط قسمت اول معادله (۲) در نظر گرفته شود، ذرات راه عادی خود را می‌روند تا به دیواره محدوده برسند و به نوعی جستجویی سراسری را انجام می‌دهند. بر همین اساس از طریق بکارگیری الگوریتم بهینه‌سازی ازدحام ذرات وضعیت منابع سرورها بصورت پویا مورد بررسی قرار می‌گیرد و براساس آن می‌توان یک راهبرد بهینه را جهت تخلیه بار تعیین نمود.

1. Particle Swarm Optimization (PSO)

قدم‌های الگوریتم PSO تغییر یافته، در شکل ۱ لیست شده است. این الگوریتم با مقداردهی اولیه مکان و سرعت ذره آغاز به‌کار می‌کند. در این مسأله ذرات وظایفی هستند که واگذار می‌شوند و اندازه (بُعد) ذرات، تعداد وظایف موجود هستند. مقدار تخصیص داده‌شده به هر بُعد از ذرات شاخص‌های منابع پردازشی هستند. به این ترتیب هر ذره، نگاشت یک منبع به یک وظیفه را نشان می‌دهد.

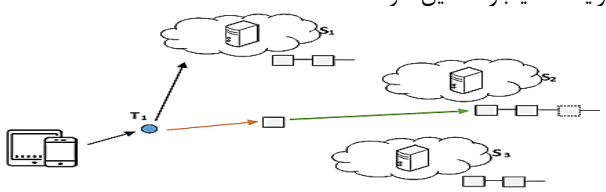
```
1: Calculate average resource wastage cost using equaption 3-1
2: Compute PSO({ti})
3: Repeat
4: For all "ready" tasks {ti} ∈ T do
5:    Select tasks {ti} for resources {pj} according to the solution provided by PSO
6: End for
7: Dispatch all the mapped tasks
8: Wait for polling time
9: Update the ready task list
10: Update the average resource wastage
11. Start blockchain for offload confirmation
12: Compute PSO({ti})
13: until there are unscheduled tasks
```

شکل ۱- زمان‌بندی اکتشافی مبتنی بر PSO تغییر یافته

ذرات سرعت‌شان را با استفاده از رابطه (۲) محاسبه می‌کنند و موقعیت مکانی‌شان را به‌روزرسانی می‌کنند. همچنین به منظور دریافت وضعیت منابع پردازشی از رابطه (۱) استفاده می‌شود. این ارزیابی تا زمانیکه به تعداد مشخصی از تکرار رسد، ادامه پیدا می‌یابد. در انتها یک راهبرد زمان‌بندی انتخاب می‌شود که براساس آن تعیین می‌شود چه وظایفی به چه ماشینی تخلیه شوند این اطلاعات در قالب یک بلوک ذخیره و با استفاده از بلاک‌چین که در ادامه تشریح شده است مورد تأیید قرار می‌گیرد.

۹- تضمین جامعیت و امنیت به کمک بلاکچین

هنگامی‌که راهبرد تخلیه‌بار به پایان رسید (نحوه تخلیه‌بار و سرور کاندید تعیین گردید) سایر ماشین‌ها موجود در زیرساخت ابری که به‌عنوان استخراج‌کننده[1] عمل می‌کنند برای ثبت‌کردن راهبرد تخلیه‌بار باهم رقابت می‌کنند. درواقع هنگامی که یک وظیفه پردازشی به یک ماشین مجازی جهت پردازش، تخلیه‌بار می‌شود این ماشین قادر نخواهد بود که کاربرهای عادی موبایل را از حمله‌کننده‌ها تشخیص دهد [۲۴]. بر همین اساس می‌تواند حریم خصوصی کاربران نقض و امنیت داده انتقال‌یافته تضمین نشود. در نتیجه پس از تعیین نحوه تخلیه‌بار (از طریق بکارگیری الگوریتم بهینه‌سازی ازدحام ذرات)، کلیه اطلاعات مربوطه در قالب یک بلوک، ثبت می‌شود تا از طریق آن بتوان فرایند تخلیه‌بار را ردیابی و تأیید کرد. هر بلوک شامل تصمیم‌گیری مربوط به تخلیه‌بار، دستگاه اصلی موبایل، داده مربوط به وظیفه و مقدار اثبات کار (PoW[2]) می‌باشد. مالک PoW باید قادر باشد تابع هش را که در برگیرنده اطلاعات بلوک‌های قبلی در زنجیره بلاک‌چین جاری است را حل نماید و همچنین بلوکی که اطلاعات مربوط به راهبرد تخلیه‌بار جاری را ذخیره می‌کند نیز باید ثبت شود. بر همین اساس اولین ماشین که بتواند مقدار PoW را محاسبه کند این حق را دارد که اطلاعات تخلیه‌بار را ثبت کند. در ادامه این سرور اطلاعات مربوط به بلوک تخلیه‌بار را برای سایر سرورها به منظور بررسی، ارسال سراسری[3] می‌کند. فقط هنگامی‌که اطلاعات بلوک توسط سایر استخراج‌کننده‌ها تأیید شود، این بلوک به زنجیره بلاک‌چین جاری اضافه خواهد شد و در نتیجه فرایند مهاجرت به سرور موردنظر انجام می‌گیرد. بر همین اساس درصورتیکه بلاک‌چین توسط کلیه سرورها نگه داشته شود هر بلوک اطلاعاتی باید به اجماع حداکثر سرورها دست پیدا کند، در غیراینصورت اجرا نخواهد شد. این بدان معناست که هرگونه دسترسی غیرمجاز و تأییدنشده رد خواهد شد و در نتیجه جامعیت و محرمانگی داده تضمین می‌شود. به‌عنوان مثال در شکل۲ به کمک راهبرد زمان‌بندی؛ تعیین شده است که وظیفه T1 باید به سرور S1 تخلیه‌بار شود. سایر سرورها به منظور ذخیره‌سازی اطلاعات تخلیه‌بار باهم رقابت می‌کنند. در این حالت سرور S2 به این حق دست می‌یابد که بتواند اطلاعات مهاجرت را ثبت کند. در نتیجه S2 یک پیام سراسری برای تأیید اطلاعات ارسال می‌کند. اگر سایر سرورها به یک اجماع بر روی اطلاعات تخلیه‌بار دست پیدا کنند، این اطلاعات در قالب یک بلوک ثبت و به بلاک‌چین جاری اضافه می‌شود. همچنین قبل از آنکه یک وظیفه مهاجرت داده شود اطلاعات مربوط به وابستگی‌های بلوک، بررسی می‌شود تا از این طریق بتوان در مورد فرایند انتقال داده اطمینان حاصل نمود. در نتیجه اگر داده‌های منتقل‌شده تغییر یا دزدیده شود، اطلاعات مربوط به راهبرد زمان‌بندی ذخیره‌شده در بلاک‌چین جاری و اطلاعات انتقال داده شده؛ با هم در تضاد خواهند بود و بر همین اساس به دلیل عدم برآورده‌شدن شرط جامعیت داده، عملیات مهاجرت لغو می‌شود. در واقع بکارگیری اطلاعات مربوط به بلوک این کمک را می‌کند که جامعیت داده همواره در طی فرایند تخلیه‌بار تضمین شود.



شکل ۲- نحوه ایجاد یک بلوک در راهکار

در این راهکار همانند شبکه‌های بلاک‌چین متداول، فرایند استخراج توسط دستگاه‌های IoT انجام می‌گیرد. با این تفاوت که دفترکل بجای ذخیره‌سازی در دستگاه‌ها، در گره‌های موجود در زیرساخت ابری ذخیره می‌شود. در این حالت، سرورهایی که به‌عنوان استخراج‌کننده[4] عمل می‌کنند لازم است تراکنش‌های جدید را در شبکه اعتبارسنجی کنند و برای این منظور ضروری است مقدار اثبات کار (PoW) محاسبه‌شده و به

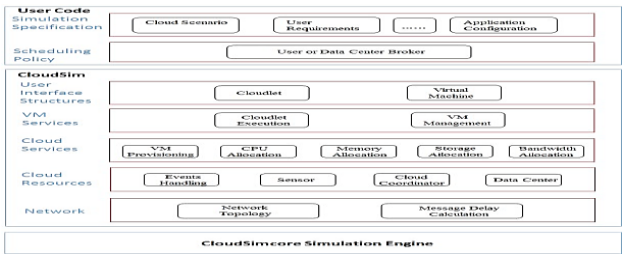
1. Miner
2. Proof of Work
3. Broadcast
4. Miner

یک اجماع با گره‌های دیگر برسند. هرگاه یک گره شبکه به‌عنوان استخراج‌کننده و برای ایجاد یک بلوک جدید؛ داده را در قالب یک تراکنش جمع‌آوری و یا ردوبدل کند، لازم است ابتدا مقدار PoW محاسبه شود. در نتیجه به منظور برقراری ارتباط بین بلوک‌ها، فرایند استخراج شامل کد هش[1] بلوکی که قبلاً استخراج شده[2] می‌باشد. بر همین اساس و به منظور محاسبه مقدار هش جدید لازم است، استخراج‌کننده به مقدار آخرین بلوک هشی که استخراج‌شده، دسترسی داشته باشد. با توجه به آنکه دفتر کل در گره‌های رایانش ابری ذخیره شده است، استخراج‌کننده می‌تواند از آنجا به این بلوک دسترسی داشته باشد. دستگاه‌ها که در واقع گره‌های شبکه هستند در صورت لزوم، می‌توانند به دفترکل دسترسی داشته باشند. به همین صورت، در هر بار استفاده از کانال ارتباطی، گره‌های رایانش ابری هر موقع آماده استخراج یک بلوک جدید باشند، قادر خواهند بود مقدار هش آخرین بلوک اضافه‌شده را در صورت درخواست، برگردانند. در این حالت تمامی گره‌های شبکه بلاک‌چین قادر خواهند بود قواعد عملیاتی خود را بصورت پایدار انجام داده و همچنن با توجه به آنکه دیگر نگرانی درباره افزایش اندازه دفترکل نیست، کارایی آنها بالاتر می‌رود. از طرف دیگر، آخرین مقدار هش بلوک تولیدشده نیز همواره در دسترس خواهد بود. بلوک جدید توسط یکی از ماینرهای شبکه استخراج خواهد شد و در فضای ابری ذخیره می‌شود. بلوک تولیدشده نیز به کمک شبکه ارتباطی با حداقل تأخیر به گره‌های ابری انتقال می‌یابد و در آنجا در کنار سایر بلوک‌هایی که قبلاً استخراج شده‌اند، ذخیره می‌گردد و در نتیجه زنجیره بصورت بهنگام نگهداری می‌شود. پس از فرایند استخراج، گره بلاک‌چینی که برای اولین بار بیشترین مقدار PoW را دریافت کرده باشد به‌عنوان استخراج‌کننده برای بلوک جدید در نظر گرفته می‌شود. استخراج‌کننده هر بلوک، از طریق کانال ارتباطی مقدار موردنظر را به گره‌های رایانش ابری جهت ذخیره‌سازی، انتقال می‌دهد. از این طریق استخراج‌کننده‌ها دفترکل بلاک‌چین را بصورت به‌روز نگه می‌دارند.

۱۰- نمونه تجربه و تحلیل روش

روش پیشنهادی توسط نسخه جدید شبیه‌ساز کلودسیم که یک ابزار شبیه‌سازی توسعه‌پذیر است و امکان مدل‌سازی و شبیه‌سازی سیستم‌های رایانش ابری و همچنین آماده‌سازی برنامه‌های کاربردی را فراهم می‌آورد، شبیه‌سازی می‌گردد. از دلایل اصلی بکارگیری این نرم‌افزار، منبع بازبودن آن و همچنین قابلیت مدل‌سازی سیستمِ آن است که رفتار مؤلفه‌های سیستم ابری از قبیل مراکز داده، ماشین‌های مجازی و سیاست‌های تأمین منابع را فراهم می‌کند.

کلودسیم به زبان جاوا نوشته شده است و می‌تواند برای شبیه‌سازی ابرهای IaaS، SaaS و PaaS مورد استفاده قرار گیرد. مقیاس‌پذیری این شبیه‌ساز بسیار بالا است و می‌تواند ابرهای بسیار بزرگی را شبیه‌سازی کند. در حال حاضر کلودسیم علاوه بر شبیه‌سازی یک ابر قادر به شبیه‌سازی محیط‌های ابری بسیار بزرگ و تشکیل شده از چندین ابر نیز می‌باشد. معماری این شبیه‌ساز در شکل ۳ نشان داده شده است.



شکل ۳- معماری لایه‌ای شبیه‌ساز کلودسیم

همانطورکه در شکل نشان داده شده است، لایه کلودسیم با تعریف واسط‌های مدیریتی برای ماشین‌های مجازی، حافظه، ذخیره‌سازی و پهنای باند، از طراحی و شبیه‌سازی محیط‌های مراکز داده مبتنی بر ابر پشتیبانی می‌کند. مسائل اساسی مانند فراهم‌آوردن میزبان برای ماشین‌های مجازی، مدیریت اجرای برنامه و نظارت پویا بر حالت سیستم در این لایه انجام می‌پذیرد. برای طراحی یک ابر IaaS موجودیت Data Center باید توسعه داده شود. این موجودیت تعدادی موجودیت Host را مدیریت می‌کند که همان ماشین‌های فیزیکی می‌باشند. هر میزبان می‌تواند یک یا بیشتر موجودیت Virtual Machine را میزبانی کند [۲۴]. ماشین‌های مجازی براساس سیاست‌های VM Provisioning بر روی ماشین‌های فیزیکی ساخته می‌شوند. هر ماشین مجازی یک Cloudlet که همان برنامه‌ی کاربر می‌باشد را اجرا می‌کند. همچنین در جدول ۲ یک مقایسه کلی بین ابزارهای مختلف شبیه‌سازی ابر را با کلودسیم می‌توان مشاهده کرد.

جدول ۲- مقایسه ابزارها مختلف شبیه‌سازی

CloudSim	Platform	Programming Language	Networking	Simulator Type	Availability
CloudAnalyst	CloudSim	Java	Limited	Event Based	Open Source
GreenCloud	NS2	C++/OTCL	Full	Packet Level	Open Source
Network CloudSim	CloudSim	Java	Full	Packet Level	Open Source
EMUSIM	AEF	Java	Limited	Event Based	Open Source
MDC SIM	CSIM	C++/Java	Limited	Event Based	Commercial

۱۱- معیارهای ارزیابی

همانطورکه قبلاً بیان شد، راهکار پیشنهادی از طریق بکارگیری بلاک‌چین قادر خواهد بود محرمانگی و جامعیت داده را در طی فرایند زمان‌بندی و تخلیه‌بار تضمین نماید. اما به جز جامعیت و محرمانگی، پارامترهای دیگری از جمله انرژی مصرفی، زمان تخلیه‌بار، میزان مصرف منابع شبکه و یا تأخیر در ارایه سرویس نیز معیارهای ضروری برای مقایسه و قضاوت در مورد کارابودن یک راهبرد تخلیه‌بار می‌باشد [۱۱]. در واقع ایجاد یک مصالحه بین این معیارها در کنار تضمین جامعیت از طریق بلاک‌چین یک چالش اصلی در این پژوهش بود و برای این منظور راهکایی که مبتنی بر بلاک‌چین و الگوریتم بهینه‌سازی ازدحام ذرات بود، ارایه

1. Hash
2. Mined

گردید. حال در این بخش نتایج حاصل از ارزیابی آن با توجه به معیارهای زیر تشریح شده است.

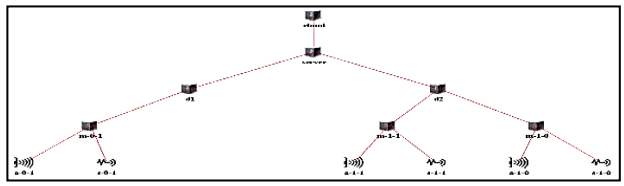
- زمان تخلیه‌بار
- انرژی
- تأخیر
- میزان مصرف شبکه

لازم به ذکر است به منظور محاسبه میزان مصرف انرژی از راهکار ارایه شده در [۱۳] استفاده شده است. براساس این راهکار میزان مصرف انرژی یک رابطه خطی با بهره‌وری پردازنده دارد و براساس رابطه ۴-۱ محاسبه می‌شود:

$$E_j = (P_{max} - P_{min}) \times U_j + P_{min} \quad (۴)$$

در رابطه فوق Pmax میزان مصرف انرژی در حالت حداکثر بهره‌وری و Pmin نیز میزان مصرف انرژی در حالت حداقل بهره‌وری می‌باشد

همچنین راهکار پیشنهادی در حالت بکارگیری رایانش ابری با راهکار FogBus که در منابع شماره [۱۲] تشریح شده است و از بلاک‌چین نیز بهره می‌برد؛ مورد مقایسه و ارزیابی قرار گرفته است. توپولوژی‌های مورد استفاده در شکل ۴ نشان داده شده است.



شکل ۴- توپولوژی مورد استفاده

لازم به ذکر است آزمایشاتی که در ادامه صورت گرفته با توجه به بکارگیری بلاک‌چین در هر دو راهکار، بدست آمده است. به عبارتی هر دو راهکار مورد ارزیابی از بلاک‌چین در طی فرایند ایمن‌سازی تخلیه‌بار بهره برده شده است و هدف اصلی از آزمایشات این بخش، بررسی میزان تأثیر تأمین امنیت به کمک بلاک‌چین بر روی معیارهای کیفیت سرویس در راهکارها و مقایسه آنها با توجه به بکارگیری بلاک‌چین و راهبردهای تخلیه‌بار متفاوت می‌باشد.

۱۲- پاسخ به سؤالات تحقیق

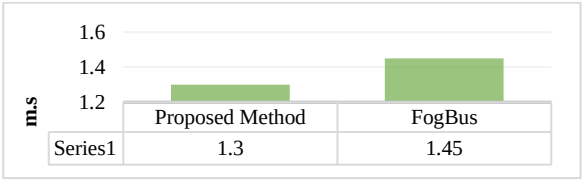
در ابتدای این پژوهش مهم‌ترین سؤالاتی که جهت بکارگیری راهکار مبتنی بر بلاک‌چین در محیط ابری مورد نظر بود، ارایه گردید. حال در این بخش و پس از شبیه‌سازی و تحلیل نتایج به بررسی پاسخ این سؤالات می‌پردازیم.

سؤال ۱- به چه صورت می‌توان بلاک‌چین را جهت بهبود امنیت در محیط رایانش ابری بکار برد؟

اولین سؤال این پژوهش مربوط به نحوه بکارگیری بلاک‌چین جهت بهبود امنیت در محیط رایانش ابری بود. همانطور که در فصل سوم مورد بررسی قرار گرفت در این راهکار از بلاک‌چین به منظور بهبود امنیت و جامعیت در فرایند تخلیه‌بار در محیط زیرساخت‌های رایانشی از جمله رایانش ابر و رایانش مه استفاده می‌شود. در واقع با توجه به آنکه در طی فرایند انتقال و تخلیه‌بار، ضعف و مشکلات مختلفی مربوط به امنیت و جامعیت داده در اثر نشت و یا نقص عملیات انتقال ممکن است رخ دهد. به عبارتی، هنگامی‌که یک وظیفه پردازشی از طریق بکارگیری الگوریتم زمان‌بند به یک ماشین مجازی در ابر جهت پردازش، تخلیه‌بار می‌شود این ماشین مجازی قادر نخواهد بود که کاربرهای عادی موبایل را از حمله‌کننده‌ها تشخیص دهد. در نتیجه می‌تواند حریم خصوصی نقض و امنیت داده انتقال‌یافته تضمین نشود. بر همین اساس در این پژوهش از بلاک‌چین برای رفع این مشکل استفاده می‌شود. به اینصورت‌که پس از تعیین راهبرد تخلیه‌بار، اطلاعات مربوط به مهاجرت، بجای یک کنترلر مرکزی توسط سایر مراکز پردازشی ارزیابی می‌گردد. اطلاعات هر سرور می‌تواند در قالب یک بلوک، کپسوله‌شده و از بلاک‌چین به منظور رمزنگاری اطلاعات تخلیه‌بار از جمله مقدار هش بلوک قبلی، اطلاعات کاربر، اطلاعات وظیفه و سایر موارد استفاده گردد. سایر ماشین‌ها به جز ماشینی که سرویس موردنظر را برای دستگاه موبایل ارایه داده است جهت اعتبارسنجی رکورد مربوط به عملیات تخلیه‌بار باهم رقابت خواهند کرد. پس از آنکه اطلاعات مربوط به سرویس توسط تمام ماشین‌ها مورد بررسی قرار گرفت، می‌توان مطمئن شد که امنیت و جامعیت در طی فرایند تخلیه‌بار بطور کامل اعمال شده است و در نتیجه عملیات تخلیه‌بار شروع می‌شود. در ادامه این پژوهش نحوه انجام عملیات زمان‌بندی مورد بررسی قرار می‌گیرد و سپس نحوه تأمین امنیت و جامعیت آن به کمک بلاک‌چین بررسی می‌شود.

سؤال ۲- بکارگیری بلاک‌چین جهت تأمین امنیت در زیرساخت رایانش ابری چه تأثیری بر روی پارامترهای کیفیت سرویس دارد؟

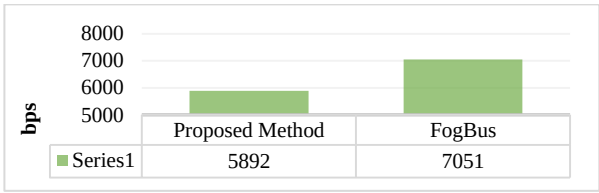
با توجه به آنکه بکارگیری بلاک‌چین نیاز به منابع پردازشی و ذخیره‌سازی بالایی دارد در نتیجه ضروری است که سودمندی آن با توجه به میزبان سربارای که بر روی منابع پردازشی بوجود می‌آورد مورد بررسی قرار گیرد. بر همین اساس در بخش ارزیابی مجموعه آزمایشاتی در زمینه میزان تأثیر بلاک‌چین بر روی منابع پردازشی انجام گرفت. ابتدا در شکل ۵ راهکارها از نظر تأخیر در سرویس مورد بررسی قرار گرفته‌اند.



شکل ۵- میزان تأخیر در راهکارهای مورد ارزیابی (میلی‌ثانیه)

در این ارزیابی تأخیر براساس زمان اجرای برنامه‌ها و همچنین تأخیر در انتشار شبکه مشخص شده است. همانطور که در شکل ۵ ملاحظه می‌شود، تأخیر راهکار پیشنهادی به نسبت هر به روش FogBus کمتر می‌باشد. بطوریکه این میزان تأخیر به میزان ۱۵ میلی‌ثانیه کاهش یافته است. دلیل اصلی این میزان از بهینگی در بکارگیری زمان‌بند مبتنی بر

PSO و بررسی‌کننده منبع می‌باشد زیرا از طریق بکارگیری آنها این امکان فراهم شده است که وظایف پردازشی به شکل مؤثری بین زیرساخت رایانش ابری پخش شود زیرا زمان‌بندی مبتنی بر PSO این امکان را فراهم می‌کند یک نوع همکاری و اشتراک‌گذاری اطلاعات بین ذره‌ها بوجود آید بطوریکه با توجه به آنکه در PSO از مفهوم جمعیت ذرات استفاده شده است در نتیجه هر عضو از این جمعیت، موقعیت خود را با توجه به بهترین وضعیت موجود تغییر می‌دهد در نتیجه می‌توان مزیت‌های تکاملی بهره برد و براساس وضعیت بهترین ذرات، راهبرد انتخاب را تعیین نمود. بر همین اساس این تخلیه‌بار بهینه که به کمک بلاک‌چین نیز ایمن شده است، میزان تأخیر را به شکل چشم‌گیری کاهش داده است. همچنین در شکل ۶ میزان استفاده راهکارها از منابع شبکه مورد بررسی قرار گرفت. با توجه به نیاز بالای بلاک‌چین به منابع زیاد شبکه، هدف از این ارزیابی بررسی میزان تأثیری است که پردازش بلاک‌چین بر روی شبکه دارد.



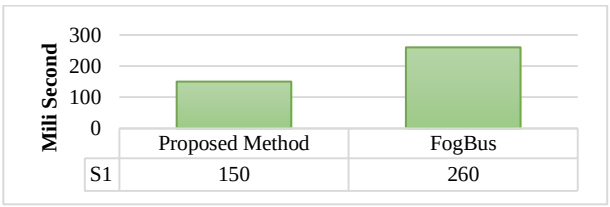
شکل ۶- میزان استفاده راهکارها از منابع شبکه (BPS)

همانطورکه ملاحظه می‌شود در این حالت نیز روش پیشنهادی به نسبت راهکار FogBus منابع کمتری از شبکه را مصرف کرده است. در واقع بهره‌گیری از الگوریتم PSO، توانسته در این میزان از کاهش مصرف منابع مؤثر باشد. زیرا به کمک الگوریتم PSO و بررسی وضعیت منابع در دسترس، این امکان فراهم می‌شود که بتوان برای اجرای وظایف، بهترین سرورهای در دسترس انتخاب شود که نتیجه آن کاهش تأخیر و مصرف منابع می‌باشد. همچنین بکارگیری الگوریتم PSO به دلیل وجود مزایایی همچون مفهوم ساده، پیاده‌سازی آسان و همگرایی سریع به نسبت راهبرد تخلیه‌بار FogBus راحت‌تر اجرا می‌شود که در نتیجه هزینه کمتری برای زیرساخت شبکه خواهد داشت.

سؤال ۳- چگونه می‌توان از زمان‌بند در جهت تخصیص منبع برای بلاک‌چین استفاده نمود؟

آخرین سؤال در زمینه نحوه بکارگیری زمان‌بند در کنار بلاک‌چین می‌باشد بطوریکه بتوان تخصیص منبع را به شکلی بهینه انجام داد. برای این منظور از یک زمان‌بند مبتنی بر الگوریتم بهینه‌سازی ازدحام ذرات استفاده شده است که در کنار آن از زنجیره بلاک‌چین به منظور تأمین محرمانگی و جامعیت راهبردهای زمان‌بندی و تخلیه‌بار بهره برده شده است. بر همین اساس به منظور انتخاب یک سرور پردازشی جهت اجرای وظایف، از یک مانیتور منبع استفاده خواهد شد که به کمک آن وضعیت منابع سرورها مورد بررسی قرار می‌گیرد و براساس آن تصمیمات مربوط به درخواست تخلیه‌بار از یک دستگاه به سرور موردنظر تعیین و انجام می‌گیرد. این راهبرد انتخاب براساس میزان منابع در دسترس و همچنین عدم بوجودآمدن سربار در یک سرور در صورت پذیرشِ میزبانی، می‌باشد. بر همین اساس بصورت دوره‌ای و قبل از انجام عملیات زمان‌بندی وضعیت گره‌های پردازشی مورد بررسی قرار می‌گیرد و گره‌ای انتخاب می‌شود که بالاترین میزان منبع در دسترس را داشته باشد. در نتیجه از طریق بکارگیری چنین راهبرد همواره یک نوع توازن‌بار بین گره‌های پردازشی برقرار می‌باشد و از ایجاد ازدحام نیز جلوگیری می‌شود که نتیجه آن بهبود بهره‌گیری از منابع و در نتیجه کاهش تأثیر بکارگیری بلاک‌چین بر روی این منابع پردازشی می‌باشد زیرا درصورتیکه چنین زمان‌بندی انجام نشود و یک گره دارای منبع کافی برای اجرای وظایف نباشد، دچار ازدحام می‌شود که نتیجه این ازدحام افزایش زمان اجرا و مصرف انرژی می‌شود.

همانطور که در شکل ۷ ملاحظه می‌شود، از طریق بکارگیری زمان‌بند توانسته‌ایم زمان تخلیه‌بار راهکار پیشنهادی به نسبت FogBus را کاهش دهیم که این بیانگر بهینه‌تربودن آن در زمان تخلیه‌بار است. در واقع با توجه به آنکه در روش پیشنهادی از زمانبند مبتنی بر بهینه‌سازی ازدحام ذرات جهت انجام عملیات تخلیه‌بار استفاده شده است، در نتیجه از طریق زمان‌بندی کارایی که به کمک بخش مانیتورینگ انجام شده، توانسته است در فرایند تخلیه‌بار تأثیرگذار باشد. در واقع از آنجا که در الگوریتم بهینه‌سازی ازدحام ذرات اعضای جمعیت باهم در ارتباط هستند و از طریق این تبادل اطلاعات به حل مسأله می‌رسند در نتیجه از سرعت همگرایی بالایی برخوردار است و می‌تواند زمان‌های اجرا و تخلیه‌بار را کاهش دهد. در کنار آن اطلاعات مناسبی که از طریق بخش مانیتورینگ فراهم می‌شود الگوریتم را قادر می‌سازد که بهترین نتایج را بدست آورد. همانطور ملاحظه می‌شود در ۱۵۰ میلی‌ثانیه این عملیات انجام شده است که به نسبت FogBus، ۱۲۴ میلی‌ثانیه کاهش داشته است.

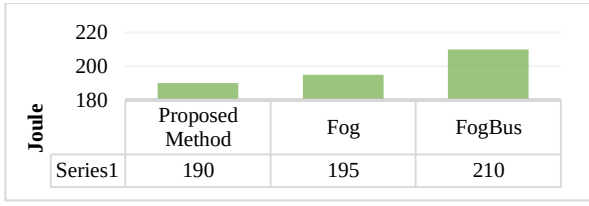


شکل ۷- مقایسه زمان تخلیه‌بار در راهکارهای مورد ارزیابی (برحسب میلی‌ثانیه)

سؤال ۴- به چه صورت می‌توان فرایند تخلیه‌بار از دستگاه‌های موبایل به محیط ابری را بهبود و به کمک بلاک‌چین تأمین امنیت نمود؟

بستر رایانش ابری، یک بستر سرویس‌دهنده کاملاً خودکار است که به کاربر اجازه‌ی خرید، ایجاد از راه دور، مقیاس‌پذیری پویا و مدیریت سیستم را می‌دهد. ارائه‌دهندگان خدمات ابری از تکنیک‌های مجازی‌سازی در ترکیب با سایر قابلیت‌های خدماتی، جهت ارائه انواع سرویس‌های مختلف استفاده می‌کنند. از سوی دیگر، به خاطر تنوع ناهمگنی منابع و ماهیت بسیار متغیر و غیرقابل پیش‌بینی محیط ابری، لازم است جایابی و مدیریت منبع به‌عنوان یکی از مسائل چالش برانگیز به منظور افزایش کارایی

رایانش ابری مورد بررسی قرار گیرد. یک اپلیکیشن متشکل از چندین سرویس مختلف است که در گره‌های مجازی‌سازی شده ابری گسترش‌یافته و با یکدیگر در جهت کارکرد مناسب، تعامل می‌کنند. مشکل جایگذاری سرویس در چشم‌انداز رایانش مه، طرح بهینه جایگذاری بین سرویس‌های مختلف و گره‌های ابری با هدف بیشینه‌نمودن بهره‌برداری از منابع ابری می‌باشد که در عین حال تحقق ملزومات کیفیت سرویس خدمات را تعیین می‌کند. از آنجا که در مسایل جایابی، راه‌حل‌های ممکن مسأله با افزایش تعداد سرویس‌ها و درخواست‌ها به سرعت بالا رفته و بررسی تمامی حالت‌های ممکن برای رسیدن به بهترین جایابی امکان‌پذیر نبوده و این مسایل از دسته NP-Hard می‌باشند در نتیجه از روش‌های قطعی نمی‌توان در حل این دسته از مسایل به دلیل زمان‌بربودن، استفاده نمود و باید روش‌های فراابتکاری برای حل مناسب این مسائل توسعه داده شود. روش‌های فراابتکاری به علت سادگی، انعطاف‌پذیری، نیاز نداشتن به مشتق‌گیری و فرار از بهینه محلی، برای این دسته از مسائل می‌تواند سودمند باشد. بر همین اساس در این پژوهش یک راهکار مبتنی بر الگوریتم بهینه‌سازی ازدحام ذرات به منظور جایابی برنامه‌های کاربردی بر روی منابع رایانش ابری ارائه می‌شود تا از طریق بکارگیری آن بتوان زمان اجرا و همچنین میزان انرژی مصرفی را کاهش داد. بر همین اساس و همانطور که در شکل ۸ ملاحظه می‌شود، راهکار پیشنهادی به نسبت راهکارهای دیگر انرژی کمتری مصرف کرده است. در واقع با توجه به آنکه روش پیشنهادی سرورهای کمتری را درگیر کرده است و همچنین توازن را بصورت بهینه از طریق بکارگیری زمان‌بند برقرار کرده است، در نتیجه انرژی مصرفی نهایی نیز در راهکار پایین‌تر آمده است. در واقع بررسی‌کننده منبع این امکان را می‌دهد که عملیات زمان‌بندی با توجه به وضعیت منابع انجام گیرد و در نتیجه از ایجاد ازدحام در طی فرایند تخلیه‌بار جلوگیری به عمل آید. کاهش ازدحام و در نتیجه ایجاد توازن بهینه، زمینه‌ساز این میزان از کاهش میزان مصرف انرژی بوده است.



شکل ۸- مقایسه انرژی مصرفی در راهکارهای مورد ارزیابی (ژول)

همانطورکه در شکل ۸ نشان داده شده است، راهکار پیشنهادی به شکل مؤثری بهتر از راهکار FogBus در میزان انرژی مصرفی عمل کرده است. بطوریکه به میزان ۲۰ ژول انرژی کمتری مصرف کرده است. این میزان از بهینگی جهت بکارگیری بلاک‌چین در رایانش ابری، می‌تواند از جنبه اقتصادی نیز بسیار مفید باشد. زیرا علاوه بر عملکرد مناسب در کاهش کاهش زمان تخلیه‌بار، میزان انرژی مصرفی نیز به شکل قابل توجهی کاهش پیدا کرده است. این میزان از کارایی به دلیل بکارگیری الگوریتم بهینه‌سازی ازدحام ذرات در کنار بلاک‌چین می‌باشد زیرا به نسبت بخش مدیریت منبع راهکار FogBus ساده‌تر می‌باشد و همچنین با توجه به آنکه الگوریتم PSO یکی از قوی‌ترین راهکارهای بهینه‌سازی مبتنی بر هوش جمعی می‌باشد در نتیجه سرعت همگرایی آن بالا است و همین امر باعث می‌شود در زمان کمتری بتوان عنلیات تعیین راهبرد تخلیه‌بار را اجرا کرد و در نتیجه پارامترهای کیفیت سرویس بهینه‌تر خواهند بود.

هرچند این فرایند تخلیه‌بار توانسته است مصرف انرژی و زمان اجرا را کاهش دهد اما در طی عملیات تخلیه‌بار مشکلات امنیتی مختلفی وجود دارد که می‌تواند محرمانگی و جامعیت داده را دچار مشکل کند. در واقع هنگامی‌که یک وظیفه پردازشی از طریق بکارگیری الگوریتم زمان‌بند به یک ماشین مجازی در ابر جهت پردازش، تخلیه‌بار می‌شود این ماشین مجازی قادر نخواهد بود که کاربرهای عادی موبایل را از حمله‌کننده‌ها تشخیص دهد. در نتیجه می‌تواند حریم خصوصی نقض و امنیت داده انتقال‌یافته تضمین نشود. بر همین اساس در این پژوهش از بلاک‌چین برای رفع این مشکل استفاده شده است. در نتیجه پس از تعیین راهبرد تخلیه‌بار، اطلاعات مربوط به مهاجرت، بجای یک کنترلر مرکزی توسط سایر مراکز پردازشی ارزیابی می‌گردد. اطلاعات هر سرور می‌تواند در قالب یک بلوک، کپسوله‌شده و از بلاک‌چین به منظور رمزنگاری اطلاعات تخلیه‌بار از جمله مقدار هش بلوک قبلی، اطلاعات کاربر، اطلاعات وظیفه و سایر موارد استفاده گردد. سایر ماشین‌ها به جز ماشینی که سرویس مورد نظر را برای دستگاه موبایل ارایه داده است جهت اعتبارسنجی رکورد مربوط به عملیات تخلیه‌بار باهم رقابت خواهند کرد. پس از آنکه اطلاعات مربوط به سرویس توسط تمام ماشین‌ها مورد بررسی قرار گرفت، می‌توان مطمئن شد که امنیت و جامعیت در طی فرایند تخلیه‌بار بطور کامل اعمال شده است و در نتیجه عملیات تخلیه‌بار شروع می‌شود. در واقع به‌دلیل بکارگیری فناوری رمزنگاری در بلاک‌چین و همچنین بدون یک کنترل متمرکز یا یک ذخیره داده متمرکز، بلاک‌چین می‌تواند از حمله‌هایی مختلفی در طی فرایند تخلیه‌بار جلوگیری به‌عمل آورد. بایگانی بلاک‌چین بر روی مجموعه‌ای از کامپیوترهای متصل بهم است که اطلاعات یکسانی دارند. اگر بروزرسانی بلوک‌های یک بخش دچار مشکل شود، سیستم آن را رد می‌کند. همچنین حفاظت چند امضا یا الزام بیش از یک کلید برای اجازه دادن به فرایندهای تراکنش می‌تواند امنیت و حریم خصوصی را بهبود بخشد. حتی اگر هکری به زیرساخت مورد نظر نفوذ کرده و سعی در تخریب آن نماید، چندین نسخه اضافی و تکراری از همان دفتر در سراسر جهان ذخیره شده است. که اگر یکی از آنها شکسته شود، بسیاری دیگر به‌عنوان پشتیبان وجود دارند. به عبارت دیگر داده‌ها در بلاک‌چین درکامپیوترهای توزیع‌شده که به هم متصل هستند، قرار دارد و برای موفقیت‌آمیزبودن تلاش‌های شنود، بیش از ۵۰ درصد از سیستم‌ها در شبکه باید مورد شنود قرار گیرند. این همان دلیل بکارگیری آن در این پژوهش به‌عنوان تأمین‌کننده امنیت در فرایند تخلیه‌بار می‌باشد و از طریق آن می‌توان فرایند

تخلیه‌بار که دارای سودمندی‌های بسیار زیادی است را با امنیت قابل قبولی انجام داد و در نتیجه سعی در توسعه و افزایش کارایی آن نموده‌ایم.

۱۳- نتیجه‌گیری

امنیت می‌تواند به‌عنوان یکی از موارد مورد توجه در مسائل مربوط به رایانش ابری مورد بررسی قرار گیرد. برای محیط ابری، مدل امنیتی مشخصی وجود ندارد، ولی می‌دانیم که زیرساخت‌های رایانشی به سیستم‌های توزیع‌شده ارتباط بسیار زیادی دارد، بنابراین مدل‌های جدید براساس مطالعات قبلی که مربوط به سیستم‌های توزیع‌شده بودند، استوار هستند. بر همین اساس در این پژوهش یک راهکار مبتنی بر زنجیره بلاک‌چین در کنار زمان‌بند مبتنی بر ازدحام ذرات ارایه شده است. در این روش از زنجیره بلاک‌چین به منظور تأیید جامعیت راهبرد تخلیه‌بار در رایانش ابری استفاده می‌شود. در واقع از طریق این راهکار ترکیبی علاوه بر افزایش امنیت می‌توان کارایی را نیز در زیرساخت رایانش ابری بالا برد.

با نوجه به آنکه منابع پردازشی دستگاه‌های موبایل بسیار محدود می‌باشند، وظایفی که در دستگاه‌های موبایل دارای پیچیدگی پردازشی هستند به گره‌های موجود در ابر تخلیه‌بار می‌شوند به اینصورت می‌توان به منابع پردازشی بالا دسترسی پیدا کرد. در رایانش ابری مراکز داده با ظرفیت پردازشی بالا وجود دارند که به آسانی توسط دستگاه‌های موبایل قابل دسترس است. اما در طی فرایند انتقال، ضعف و مشکلات مختلفی مربوط به امنیت و جامعیت داده در اثر نشت و یا نقص عملیات انتقال ممکن است رخ دهد. در واقع هنگامی‌که یک وظیفه پردازشی از طریق بکارگیری الگوریتم زمان‌بند به یک ماشین مجازی در ابر جهت پردازش، تخلیه‌بار می‌شود این ماشین مجازی قادر نخواهد بود که کاربرهای عادی موبایل را از حمله‌کننده‌ها تشخیص دهد. در نتیجه می‌تواند حریم خصوصی نقض و امنیت داده انتقال‌یافته تضمین نشود. بر همین اساس در این پژوهش از بلاک‌چین برای رفع این مشکل استفاده شده است. در نتیجه پس از تعیین راهبرد تخلیه‌بار توسط واحد زمان‌بند، اطلاعات مربوطه، بجای یک کنترلر مرکزی توسط سایر مراکز پردازشی ارزیابی می‌گردد. اطلاعات هر سرور می‌تواند در قالب یک بلوک، کپسوله‌شده و از بلاک‌چین به منظور رمزنگاری اطلاعات تخلیه‌بار از جمله مقدار هش بلوک قبلی، اطلاعات کاربر، اطلاعات وظیفه و سایر موارد استفاده گردد. سایر ماشین‌ها به جز ماشینی که سرویس مورد نظر را برای دستگاه موبایل ارایه داده است جهت اعتبارسنجی رکورد مربوط به عملیات تخلیه‌بار باهم رقابت خواهند کرد. پس از آنکه اطلاعات مربوط به سرویس توسط تمام ماشین‌ها مورد بررسی قرار گرفت، می‌توان مطمئن شد که امنیت و جامعیت در طی فرایند تخلیه‌بار بطور کامل اعمال شده است و در نتیجه عملیات تخلیه‌بار شروع می‌شود.

در انتها جهت ارزیابی، راهکار پیشنهادی در محیط شبیه‌ساز کلودسیم پیاده‌سازی و شبیه‌سازی گردید. به منظور پیاده‌سازی ویژگی معماری iFogSim، قابلیت‌های شبیه‌سازی یک رویداد پایه در CloudSim به‌کار گرفته شد. شی‌ها در کلودسیم مانند مراکز داده‌ها، با عملیات ارسال پیام (ارسال رویدادها) با یکدیگر ارتباط برقرار می‌کنند. از این جهت، لایه هسته کلودسیم مسئول مدیریت رویدادها بین اجزای محاسباتی است. در طی فرایند شبیه‌سازی معیارهای مختلفی از جمله انرژی مصرفی، میزان تأخیر و زمان موردنیاز برای تخلیه‌بار مورد بررسی قرار گرفت. همچنین ارزیابی‌ها با توجه به راهکار مبتنی بر FogBus صورت گرفته است. در ادامه نتایج حاصل از ارزیابی بیانگر آن بود که راهکار پیشنهادی از طریق بکارگیری زمان‌بند مبتنی بر بهینه‌سازی ازدحام ذرات در کنار بخش‌های دیگری از جمله مانیتورینگ منبع توانسته است بهترین زمان‌بندی‌ها را جهت تخلیه‌بار انتخاب نماید بطوریکه کمترین تأثیر منفی را بر روی پارامترهای مورد ارزیابی داشته باشد، همچنین با توجه به اینکه از بلاک‌چین به منظور ایمن‌سازی فرایند تخلیه‌بار استفاده شده است، این نتیجه حاصل شده است که فرایند بکارگیری بلاک‌چین نیز به نسبت راهکار مورد ارزیابی، تأثیر کمتری بر روی منابع شبکه داشته است و به نسبت منبع کمتری مصرف شده است.

۱۴- پیشنهادها

در راستای توسعه راهکار ارایه‌شده، می‌توان پیشنهادات زیر را ارایه داد:

- استفاده از رایانش مه یا رایانش لبه بجای رایانش ابری. زیرا با توجه به آنکه در رایانش لبه فاصله کاربر با گره‌های پردازشی کمتر می‌شود در نتیجه میزان تأخیر در فرایند تخلیه‌بار حداقل خواهد شد.
- بکارگیری یک عامل متوازن‌کننده در کنار راهکار پیشنهادی تا پس از زمان‌بندی نیز در صورت بوجودآمدن ازدحام (به دلایل نرم‌افزاری یا سخت‌افزاری)، بتوان توازن را مجدداً برقرار نمود. زیرا در محیط ابری به دلیل مقیاس بالای آن، در هر لحظه این امکان وجود دارد که پس از عملیات زمان‌بندی یک گره به دلایلی مانند نقص سخت‌افزای یا نرم‌افزای نتواند وظایف مربوطه را اجرا کند و در نتیجه دچار ازدحام شود، چنین گره‌هایی می‌توانند به‌عنوان یک گلوگاه عمل کرده و در نتیجه زمان اجرا را بالا می‌برند. بر همین اساس درصورتیکه از یک عامل متوازن‌کننده استفاده شود، می‌توان از طریق تکنیک‌هایی مانندِ مهاجرت ماشین مجازی، وظایف آن را به یک گره دیگر که دارای منابع کافی است، انتقال داد تا در نتیجه گلوگاه ایجاد شده از بین برود.

۱۵- مراجع

۱- قمری، مسعود و فروغی، سعید و خواجه، هادی، مدل پیشنهادی جهت امنیت اینترنت‌اشیاء و رایانش ابری با استفاده از الگوریتم AES و RSA، پنجمین همایش بین‌المللی علوم و تکنولوژی با رویکرد توسعه‌پایدار، شیراز، ۱۳۹۸.https://civilica.com/doc/967361

۲- فیروزبخت، محسن و کاظمی، زیبا،ارائه یک الگوریتم کارا جهت احراز هویت کاربران در رایانش ابری، اولین کنفرانس بین‌المللی چشم‌اندازهای نو در مهندسی برق و کامپیوتر، تهران، https://civilica.com/doc/555536، ۱۳۹۵.
۳- حاج‌صمدی ورنوسفادرانی، حمیدرضا و تاجفر، امیرهوشنگ، استفاده از فناوری بلاک‌چین برای بالابردن امنیت در داده‌های ابری،دوازدهمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات، بابل، https://civilica.com/doc/1224702، ۱۴۰۰.
۴- جوزدانی، مریم و مظفری، سعید، پذیرش بلاک‌چین به‌عنوان یک ضرورت در تجارت الکترونیک، https://civilica.com/doc/990998، ۱۳۹۸.
۵- نیک فطرت، صدف و شیری، محمدابراهیم، امنیت داده‌های ذخیره‌شده در ابر با استفاده از بهبود الگوریتم رمزنگاری متقارن، نهمین سمپوزیوم بین‌المللی پیشرفت‌های علوم و تکنولوژی، مشهد، https://civilica.com/doc/841546، ۱۳۹۷.
6- Sunyaev, A. Cloud computing. In Internet computing (pp. 195-236). Springer, Cham, 2020.
7- De Donno, M., Tange, K., & Dragoni, N. Foundations and evolution of modern computing paradigms: Cloud, iot, edge, and fog. Ieee Access, 7, 150936-150948, 2019.
8- Pavithra, S., Ramya, S., & Prathibha, S. A survey on cloud security issues and blockchain. In 2019 3rd International Conference on Computing and Communications Technologies (ICCCT) (pp. 136-140). IEEE, 2019.
9- Singh, H. P., Singh, R., & Singh, V. Cloud Computing Security Issues, Challenges and Solutions (No. 2533). EasyChair, 2020.
10- Basu, S., Bardhan, A., Gupta, K., Saha, P., Pal, M., Bose, M., & Sarkar, P. Cloud computing security challenges & solutions-A survey. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 347-356). IEEE, 2018.
11- Roman, R., Lopez, J., & Mambo, M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, 78, 680-698, 2018.
12- Lin, I. C., & Liao, T. C. A Survey of Blockchain Security Issues and Challenges. IJ Network Security, 19(5), 653-659, 2017.
13- Guo, S., Hu, X., Guo, S., Qiu, X., & Qi, F. Blockchain meets edge computing: A distributed and trusted authentication system. IEEE Transactions on Industrial Informatics, 2019.
14- Wang, J., Wu, L., Choo, K. K. R., & He, D. Blockchain based anonymous authentication with key management for smart grid edge computing infrastructure. IEEE Transactions on Industrial Informatics, 2019.
15- Casado-Vara, R., de la Prieta, F., Prieto, J., & Corchado, J. M. Blockchain framework for IoT data quality via edge computing. In Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems (pp. 19-24). ACM, 2018.
16- Xu, X., Zhang, X., GAO, H., Xue, Y., Qi, L., & Dou, W. Become: blockchain-enabled computation offloading for IOT in mobile edge computing. IEEE Transactions on Industrial Informatics, 2019.
17- Kang, J., Yu, R., Huang, X., Wu, M., Maharjan, S., Xie, S., & Zhang, Y. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things Journal, 2018.
18- Damianou, A., Angelopoulos, C. M., & Katos, V. An Architecture for Blockchain over Edge-enabled IoT for Smart Circular Cities. In 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS) (pp. 465-472). IEEE, 2019.
19- Alamoudi, B. O., Alqahtani, R. H., Aldossary, L. A., Alotaibi, S. S., Nagy, N. M., Alsowaigh, R. E., & Aldossary, T. S. Enhancing Blockchain Security in Cloud Computing with IoT Environment. 2022,
20- Krishnaraj, N., Bellam, K., Sivakumar, B., Daniel, A. The Future of Cloud Computing: Blockchain-Based Decentralized Cloud/Fog Solutions – Challenges, Opportunities, and Standards. In: Baalamurugan, K., Kumar, S.R., Kumar, A., Kumar, V., Padmanaban, S. (eds) Blockchain Security in Cloud Computing. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-70501-5_10 , 2022
21- Aldmour, R., Yousef, S., Baker, T., & Benkhelifa, E. An approach for offloading in mobile cloud computing to optimize power consumption and processing time. Sustainable Computing: Informatics and Systems, 31, 100562, 2021.
22- GAO, Y., Guan, H., Qi, Z., Hou, Y., & Liu, L. A multi-objective ant colony system algorithm for virtual machine placement in cloud computing. Journal of computer and system sciences, 79(8), 1230-1242, 2018.
23- Tiwari, H., & Madhumala, R. B. A Review of Particle Swarm Optimization in Cloud Computing. Smart IoT for Research and Industry, 93-108, 2021.
24- Xu, X., Chen, Y., Yuan, Y., Huang, T., Zhang, X., & Qi, L. Blockchain-based cloudlet management for multimedia workflow in mobile cloud computing. Multimedia Tools and Applications, 1-26, 2019.