بررسی جامع شبکه مبتنی بر نرم افزار در پردازش ابری

مهرنوش سادات حسینی تشنیزی[1]، بهرنگ برکتین[2]

۱-دانشجوی کارشناسی ،دانشکده مهندسی کامپیوتر ،دانشگاه آزاد اسلامی واحد نجف آباد،نجف آباد،ایران.

۲-استادیار،دانشکده مهندسی کامپیوتر ،دانشگاه آزاد اسلامی واحد نجف آباد،نجف آباد،ایران.

خلاصه

شبکه های کامپیوتری تمامی جهان را در بر گرفته و سال ها است که تحول جدی و جدیدی در این صنعت شکل نگرفته است. شرکت ها و سازمان های مصرف کننده به عدم افزودن ویژگی های جدید به شبکه های خود گلایه داشته و دوست دارند شبکه را به صورت نرم افزاری توسعه و گسترش بدهند و نیازی به روی آوردن به سخت افزارهای گران نداشته باشند.معماری شبکه های مبتنی بر نرم افزار[1] باعث می شود سطوح داده و کنترل از یکدیگر جدا شده و شبکه هوشمندتر و کنترل پذیرتر گردد .در این روش ، زیرساخت اصلی شبکه از برنامه های کاربردی جدا و شرکت ها قادر به برنامه نویسی،خودکارسازی و کنترل بیشتر شبکه خواهند شد. علاوه بر این با پیشرفت فناوری اطلاعات ، شرکت ها و سازمان ها نیاز دارند که کارهای محاسباتی سنگین خود را بدون داشتن به نرم افزار های گران انجام دهند رایانش ابری[2] مدلی است برای فراهم کردن دسترسی آسان بر اساس تقاضای کاربر از طریق شبکه به مجموعه ای از منابع رایانشی قابل تغییر و پیکربندی که این دسترسی بتواند با کمترین نیاز به مدیریت منابع و یا نیاز به دخالت سیستم فراهم کننده سرویس به سرعت فراهم شده و یا رها گردد. در این مقاله نخست ما به بررسی ساختار SDN و مزایا و معایب آن و هم چنین نگاهی اجمالی به OpenFlow پرداخته ایم.سپس در مورد ابر و ویژگی های مربوط به آن و مزایا و معایب آن ، بعلاوه به بررسی توازن بار در رایانش ابری و در آخر به بررسی شبکه مبتنی بر نرم افزار در رایانش ابری می پردازیم.نتایج حاصل نشان می دهد که با بکارگیری SDN در ابر میتوان چالش ها و معایب موجود در ابر را برطرف کرد.

کلمات کلیدی : شبکه مبتنی بر نرم افزار ،رایانش ابری ،OpenFlow ، معماری SDN

۱.مقدمه

یک شبکه رایانه‌ای اجازه به اشتراک گذاری منابع و اطلاعات را میان دستگاه های متصل شده به هم، می‌دهد.سیر تکاملی دستگاه ها و تجهیزات جانبی سیار، مجازی سازی سرورها و ظهور سرویسهای ابر، منجر به بازبینی دوباره معماری رایج شبکه ها شده است. معماری بسیاری از شبکه های سنتی، سلسله مراتبی است که با استفاده از گره هایی از سوئیچ های اترنت در یک ساختار درختی شکل می گیرد .این معماری زمانی که بحث ارتباطات کلاینت/ سرور مطرح شود، ملموس تر خواهد بود. اما چنین معماری ایستایی، برای ارتباطات پویا و نیازهای شرکتها در زمینه مراکز داده و رسانه های سرویس دهنده، کافی نیست. SDN یک معماری نو ظهور است که کنترل شبکه در آن از انتقال ترافیک مجزا بوده و به طور مستقیم برنامه ریزی می شود.

[1] Software-Defined Network (SDN)
[2] Cloud

این مهاجرت به کنترل شبکه که قبلا محدود به سخت افزار شبکه بود ، ماشین های مجازی و زیرساخت شبکه را قادر می سازد ، انواع سرویس ها و خدمات جدیدی را تعریف و ارائه کند و با طیف جدیدی از برنامه های کاربردی برای انعطاف پذیری بیشتر شبکه و دسترسی گسترده تر به داده های رد و بدل شده ، ارتباط برقرار نماید[1].شبکه بر پایه نرم افزار در واقع جداسازی لایه سخت افزاری از لایه کنترلی است. شبکه مبتنی بر نرم افزار یک واسط باز می باشد که هر کسی توانایی کار با آن را دارد و نیاز به یادگیری و کار با تجهیزات خاص نبوده و مستقل از سوئیچ ها و مسیریاب ها می باشد[2]. از جمله مزایای SDN می توان به موارد زیر اشاره داشت:

- ارتقاء پیکربندی : در مدیریت شبکه،پیکربندی یکی از مهم ترین عملیات است.زمانی که بخواهیم تجهیزاتی را به شبکه فعلی اضافه کنیم بدلیل ناهمگونی سازندگان دستگاه های شبکه،کاری دشوار است اما در SDN بخاطر واحدسازی سطح کنترل بر روی همه دستگاه ها،قادر به پیکربندی به صورت اتوماتیک از طریق کنترل نرم افزاری را دارند.
- بهبود اجراء
- کنترل مرکزی
- صرفه جویی و بهبود تجهیزات شبکه
- امکان طراحی و توسعه برنامه های Third-party (منظور از این عبارت نرم افزارهایی هست که توسط یک شرکت سوم بر روی یک بستر منتشر میشوند)
- امکان ارائه BWoD[3] (پهنای باند بنا به درخواست)
- تامین کیفیت سرویس (QoS[4])

اما SDN بدون ایراد نیست ،که از جمله آنها می توان به موارد زیر اشاره کرد[1]:

- عدم وجود یک درایور OpenFlow منبع باز
- یک استاندارد Northbound API و یا زبان برنامه نویسی سطح بالا در توسعه برنامه های SDN
- کمبود متخصصان در این زمینه
- محدود بودن بستر آزمایشی برای تحقیقات

مدتی است مبحث رایانش ابری در جهان رواج پیدا کرده است و در چند ساله گذشته (تقریبا از سال ۲۰۰۶ به بعد)شرکت های پیشرو در صنعت IT[5] سعی در ورود به این مقوله و بکارگیری آن درفرآیندهای خدماتی خود به کاربرانشان را داشته اند. رایانش ابری مدلی است برای فراهم کردن دسترسی آسان بر اساس تقاضای کاربر از طریق شبکه به مجموعه ای از منابع رایانشی قابل تغییر و پیکربندی (مثل: شبکه ها، سرورها، فضای ذخیره سازی، برنامه های کاربردی و سرویس ها)که این دسترسی بتواند با کمترین نیاز به مدیریت منابع و یا نیاز به دخالت سیستم فراهم کننده سرویس به سرعت فراهم شده و یا آزاد (رها) گردد. عموما مصرف کننده های رایانش ابری مالک زیرساخت فیزیکی ابر نیستند،بلکه برای اجتناب از هزینه سرمایه ای آن را از عرضه کنندگان شخص ثالث اجاره میکنند . آنها منابع را در قالب سرویس مصرف میکنند و تنها بهای منابعی که به کار میبرند را میپردازند[3] .

بهره گیری از رایانش ابری مزایای فراوانی میتواند داشته باشد که برخی از آنها به این شرح اند:

- کاهش هزینه ها : در این مورد ،کاربران دیگر به خرید سخت افزارهایی با قدرت بالا و نرم افزارهای به روز آنها نیازی ندارند و تنها با یک کامپیوتر و یک مرورگر می توان پیچیده ترین فعالیت را با اتصال به اینترنت انجام دهند.
- افزایش کارایی : با استفاده از رایانش ابری دیگر نیازی به نصب برنامه های متعدد و حجیم نداشته و توان حافظه و پردازنده را صرف فعالیت های مهم تری کرده و شاهد راه اندازی سریع سیستم خود خواهیم بود.

[3] Bandwidth-on-Demand
[4] Quality-of-Service
[5] Information Technology

- مقیاس پذیری : کاربران می توانند در زمان تقاضا و به صورت دینامیک،به تدارک منابع اقدام کنند و نیازی به تدارک از قبل برای زمان های حداکثر بار نیست.بدین معنا که اگر نیازی به افزایش بیشتری باشد،امکان افزایش ظرفیت وجود دارد.
- پویایی و قابلیت حمل آسان : کاربران در رایانش ابری به یک کامپیوتر و یا شبکه خاص محدود نیستند،یعنی اگر کاربران ،سیستم خود را تغییر دهند،امکان دسترسی به فایل ها و اطلاعات و هم چنین ویرایش آنها در هر زمان و مکانی برایشان مهیا است.

اما رایانش ابری بدون ایراد هم نیست که از جمله آنها می توان به موارد زیر اشاره کرد:

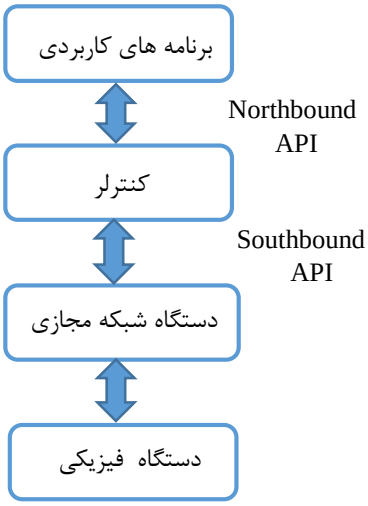
- نیاز به اتصال دائمی به اینترنت دارد: در صورتی که نتوان به اینترنت متصل شد،بدیهی است که نمی توان به اطلاعات مورد نیاز دسترسی داشت.به عبارت دیگر نبود ارتباط اینترنتی به معنای نبود اطلاعات با ارزش ما است زیرا رایانش ابری به صورت آفلاین کار نمی کند.
- داده های ذخیره شده در ابر ممکن است از امنیت کافی برخوردار نباشند.
- عدم شفافیت: در ابر عمومی سازمان هیچ‌گونه دسترسی به مراکز داده‌های خدمات‌دهنده ندارد. اطلاعات سازمان از زیرساخت خدمات‌دهنده همان قدری است که از سوی آن شرکت در اختیار سازمان قرار داده شده است.
- عدم کنترل بر پردازش ها : چون محل ذخیره داده ها و پردازش آنها برای کاربران مشخص نیست ،بنابراین کاربر نمی تواند کنترلی بر پردازش ها داشته باشد.به عبارت دیگر کلیه پردازش ها به دور از چشم کاربران و بدون اطلاع آنها از نحوه پردازش ،انجام می گیرد.

مدل های متفاوتی از رایانش ابری ارائه شده است از جمله Saas[6]، Paas[7]، Naas[8] و Iaas[9] .علی رغم همه تحقیقات و تحولات اخیر ،تکنولوژی رایانش ابری هنوز در حال تحول است.چندین شکاف و نگرانی هایی باقی مانده که در حال رسیدگی توسط انجمن ها و استاندارد می باشد.با بکارگیری SDN در رایانش ابری، برخی از چالش های موجود که در ادامه به آنها می پردازیم ،رفع خواهد شد.

۲. معماری SDN

معماری SDN در شکل زیر نشان داده شده است (شکل ۱) ، به طوریکه شامل لایه های کاربردی ،کنترلر،دستگاه های شبکه و زیرساخت می باشد که در ادامه به بررسی هر یک از لایه ها می پردازیم [5] [4] [1] .

[6] Software as a Service
[7] Platform as a Service
[8] Network as a Service
[9] Infrastructure as a Service



شکل ۱ – معماری SDN

لایه بالایی SDN شامل لایه کاربردی است که به ارائه خدمات مختلف از جمله دیواره آتش،تشخیص سیستم نفوذی،مسیریابی ، کیفیت سرویس ،توازن بار و غیره می پردازد.لایه دوم ، مربوط به لایه کنترلر است و از جمله وظایف این لایه میتوان به کنترل های اولویت بندی شده و نشده ،مسدود کردن سطح بسته های خاص از ترافیک و جدول مسیریابی از راه دور اشاره کرد . کنترلرهای زیادی وجود دارد که از زبان های برنامه نویسی متفاوت از جمله (پایتون ،C،C++،JAVA ،Ruby و جاوا اسکریپت)و پلت فرم هایی مانند POX، Mul ، Nox ، Jaxon ، Trema ، Beacon، Floodlight و غیره پشتیبانی میکند ،هم چنین به دلیل اینکه این لایه بین لایه بالایی و پائینی قرار داردباید یکپارچگی لازم را بین سوئیچ ها و برنامه های کاربردی فراهم کند.لایه سوم شامل دستگاه های شبکه است که در واقع یک شبیه ساز نرم افزاری برای سوئیچ های فیزیکی می باشد . کار این سوئیچ مسیریابی و زمان بندی در ترافیک است و در نهایت لایه پائینی که زیرساخت لازم را برای فناوری اطلاعات فراهم میکند . از این زیرساخت به عنوان دستگاه های شبکه ای شامل سوئیچ ها و روترها است و ممکن است یک بخش مجازی از دستگاه ها به عنوان زیرساخت فیزیکی در نظر گرفت ، استفاده کرد.رابط های برنامه کاربردی شامل Northbound و Southbound می باشد که در واقع برنامه ی کاربردی API [6] یک رابط بین اپراتور شبکه و کنترلر را فراهم می کند به طوریکه کنترل شبکه توسط برنامه نویسان سطح متوسط آشنا به C،C++ و پایتون و غیره را فراهم میکند . این رابط برنامه کاربردی فروشندگان و ارائه دهندگان خدمات شبکه را به منظور سفارشی کردن برنامه های خودشان مورد مخاطب قرار میدهند ، نکته قابل توجه این است که تا الان هیچ استانداردی برای رابط برنامه کاربردی Northbound تعریف نشده است و با اجرای هر برنامه کاربردی یک دید از جدول جریان به دستگاه های شبکه ارائه داده می شود سپس درخواست به منظور توزیع در دستگاه شبکه به کنترلر فرستاده میشود،از جمله وظایف Northbound مدیریت خودکار و اشتراک گذاری داده بین سیستم است[7] .

رابط برنامه کاربردیSouthbound ،مکانیزمی برای گره های پایانی که شامل روتر و سوئیچ های مجازی و فیزیکی است و از طریق OpenFlow و ONE PK API با کنترل می تواند تعامل داشته باشد را فراهم میکند به طوریکه ادمین شبکه به کشف توپولوژی شبکه به منظور تعریف شبکه میپردازد و یک درخواست از طریق برنامه کاربردی به برنامه کاربردی را دریافت می کند و در اینجا OpenFlow به عنوان یک برنامه کاربردی برای Southbound بیان می شود.مدیر شبکه از طریق رابط نرم افزاری که SDN فراهم میکند ،ترافیک شبکه را به طور کامل کنترل و به سازمان ها این اجازه را می دهد تا وابستگی هایشان را از سوئیچ های گران قیمت با سیستم عامل خاص را تنظیماتشان به صورت دستی است را کاهش میدهد هم چنین

متمرکز بودن SDN برای مدیران شبکه این امکان را فراهم کرده است که خدمات شبکه را به راحتی و بدون تنظیمات سخت افزاری، به صورت دستی کنترل نمایند.

در مکانیزم کنترلی هر یک از روتر ها و سوئیچ ها در کنترلر SDN از رمزنگاری SSL/TLS استفاده میکند که یک لایه ی اضافی برای امنیت در شبکه را ایجاد میکند.کنترل SDN از جدول جریان سوئیچ و روترهای راه دور استفاده نمود و کنترلر از طریق آدرس IP، آدرس MAC،آدرس TCP/UDP تصمیم گیری می کند و هم چنین به صورت آماری تراکم ترافیک را اندازه گیری میکند،که از قوانین عملیات و حالات تعریف شده برای جریان خاص استفاده میکند.

۲-۱ . مدل OpenFlow

OpenFlow یک پروتکل ارتباطی در SDN است و اولین پروتکل ارتباطی رابط استاندارد است که برای SDN طراحی شده است[6] .جداسازی لایه کنترل از لایه داده ،عبور بسته های اطلاعاتی و تشخیص آن بسته از طریق شبکه با استفاده از نرم افزار و هم چنین سفارشی کردن نیازهای کاربران از طریق لایه ی برنامه کابردی برای کاربران امکان پذیر است. با متمرکز کردن لایه ی کنترل قابلیت های جدید را معرفی میکند بدون اینکه روند شبکه را تحت تاثیر قرار دهد این تغییر در معماری شبکه به کاربران اجازه معرفی برنامه های کاربردی جدید بدون وابستگی به تنظیمات دستگاه و نیازهای فروشندگان را می دهد.استفاده از این مدل توپولوژی و تغییرات برنامه سرعت بیشتری را فراهم میکند .

OpenFlow یک واسط برای ارتباط سوئیچ ها و کنترلرهای SDN می باشد.در ابتدا، OpenFlow کنترلر مرکزی را تعریف می کند و بعد می گوید چگونه این کنترلر می تواند به صورت امن به دستگاه های شبکه متصل و آن را کنترل کند . سپس OpenFlow مشخص می کند که چگونه باید بسته های دریافتی را دستکاری و پردازش و دوباره ارسال کرد .قبل از OpenFlow، هیچ استانداردی برای دستکاری و ارسال رو به جلو جدول مسیریابی شبکه وجود نداشت؛ بنابراین، SDN بدون OpenFlowناچار بود به صورت انحصاری اجرا شود یا با کاستی ها و عیب هایی در عملکرد روبرو باشد.از جمله مزایای این مدل ،عملیات شبکه را آسان میکند و شبکه را قادر می سازد تا منابع فیزیکی و مجازی را به اشتراک بگذارد که اینکار باعث بهبود مقیاس و عملکرد شبکه می شود . کنترل از راه دور برای سوئیچ و داده را فراهم میکند[8].

۲-۱-۱ . سوئیچ های مجازی در SDN

با ظهور فناوری های مجازی سازی سرورها که توسط هایپروایزرها به کار گرفته می شوند،نقش سوئیچ مجازی در ایجاد اتصال سرورهای مجازی با کارت های شبکه مجازی و تراکم ترافیک ارسال آن به خارج از هایپروایزرها در شبکه های فیزیکی،پررنگ تر شده است.سوئیچ های سخت افزاری و مجازی نقش مهمی در SDN ایفا می کنند،زیرا آنها به طور مستقیم مسئول ارسال جدولهای برنامه ریزی شده توسط کنترلر هستند[10] [9] .

۳.رایانش ابری

رایانش ابری را میتوان ، نوعی از سیستم موازی و توزیعی است که از تعدادی کامپیوتر متصل به هم و مجازی تشکیل شده است که به عنوان یک واحد نشان داده می شوند و هدف از این سیستم ،ارائه سرویس به متقاضیان است.باید توجه داشت که رایانش ابری زمانی بیشترین تاثیر و مزیت را برای یک سازمان به ارمغان خواهد داشت که در شرایط زیر مورد استفاده قرار گیرد[11]:

۱- هنگامی که فرآیندها،برنامه ها و داده ها به میزان زیادی مستقل باشند و نقاط یکپارچگی به خوبی تعریف شده باشند.

۲- هنگامی که سطح پایین تری از امنیت مورد نظر باشد زیرا سیستم های رایانش ابری در حال حاضر امنیت را در حد کافی فراهم می کنند ولی برای اطلاعات محرمانه فعلا مناسب نیستند.

۳- هنگامی که هزینه ، مساله باشد و مزایای آشکاری در استفاده از رایانش ابری وجود داشته باشد.

۳-۱.معماری ابر

معماری مبتنی بر سرویس، معماری نرم افزار یا سیستمی است که امکاناتی همچون استفاده مجدد، توسعه پذیری، سهولت و بسیاری دیگر را در اختیار کاربران قرار می دهد . این ویژگی ها برای شرکت هایی که به دنبال کاهش هزینه هستند و به جای فروش بر اجاره سرویس های نرم افزاری تأکید دارند، امری الزامی است.

معماری سامانه های نرم افزاری رایانش ابری عموما شامل اجزایی است که با یکدیگر از طریق رابط برنامه نویسی نرم افزاری،معمولا وب سرویس ارتباط برقرار می کنند.طرحی شبیه به فلسفه یونیکس دارد که در آن چند برنامه مختلف که هر یک کاری را به خوبی انجام میدهند،از طریق واسطه ای جهانی با یکدیگر کار میکنند.

لایه های این معماری عبارتند از:

کاربر : کاربر رایانش ابری متشکل از سخت افزار و نرم افزاری است که برای تحویل برنامه های کاربردی از ابر استفاده میکنند و یا به طور ویژه تنها برای تحویل سرویس های ابری طراحی شده است.

برنامه های کاربردی : سرویس های برنامه کاربردی ابری یا نرم افزار به عنوان سرویس (SaaS) نرم افزار را به صورت سرویس روی اینترنت تحویل میدهند و بدین وسیله نیاز به نصب نرم افزار روی رایانه های مشتریان را ازبین میبرند ونگهداری و پشتیبانی را ساده تر میسازد.

بستر : سرویسهای بستر ابری یا(بستر به عنوان سرویس (PaaS)) بستر رایانشی ویا پشته راهکار - که اغلب روی زیرساخت ابری اجرا شده و برنامه کاربردی ابری را تغذیه می کنند – را به صورت سرویس ارائه می دهد. سرویس بستر ابری استقرار برنامه های کاربردی را بدون هزینه و پیچیدگی خرید و مدیریت لایه های نرم افزاری و سخت افزاری زیرین آسان میکند.

زیرساخت : زیرساخت رایانه ای را که عموما یک بستر مجازی است را به صورت سرویس ارائه (IaaS) زیرساخت به عنوان سرویس « سرویسهای زیرساخت ابری » میدهند . کاربران به جای خرید سخت افزار و نرم افزار و فضای مرکز داده(دیتا سنتر)ویا تجهیزات شبکه، همه این زیر ساختها را به صورت یک سرویس و میزان منابع مصرف (Utility Computing) شده را تهیه می کنند.است.این شیوه در واقع تکامل یافته مدل عرضه سرورهای خصوصی مجازی است.

سرور :لایه سرورها متشکل از سخت افزار و نرم افزاری است که مخصوصا برای تحویل سرویسهای ابر طراحی شده اند. به عنوان مثال میتوان از پردازندههای چندهسته ای و سیستم عامل های ویژه ابری نام برد [12] .

۳-۲.اجزاء ابر

به طور ساده و از منظر نموداری،اجزای رایانش ابری از سه عنصر ساخته می شود:

۱- مشتریان :مشتریان در معماری محاسبات ابری دقیقا همان چیزی هستند که در شبکه های محلی نقش دارند. به عبارت دیگر می توانند کامپیوتر شخصی، لپ تاپ، PDA و حتی کامپیوترهای بزرگ باشند.

۲- مرکز داده : مرکز داده مجموعه ای از سرورها است که برنامه ای که ما آن را به اشتراک گذاشته ایم در آن قرار می گیرد.

۳- سرورهای توزیع شده :الزامی نیست که تمامی سرورها در یک مکان مشخص باشند . در اغلب موارد سرورها از لحاظ مکانی پراکنده می باشند اما این سرورها برای کاربران با استفاده از تکنیک اشتراک ابر، همانند زمزمهٔ چند نفر کنار یکدیگر عمل می کند . این عنصر، به ارائه دهندگان خدمات ابری، انعطاف و امنیت بیشتری را ارائه می دهد [12].

۳-۳.امنیت در ابر

امنیت محاسبات ابری (گاهی اوقات به امنیت ابری تعبیر می شود) که زیر مجموعه ای از امنیت کامپیوتری، امنیت شبکه و در حالت کلی تر امنیت اطلاعات به حساب می آید. این مفهوم شامل مجموعه ای از سیاست ها، تکنولوژی ها و کنترل ها جهت محافظت از داده ها، برنامه ها و زیرساخت های امنیتی در محاسبات ابری است.مسائل و نگرانی های امنیتی در ارتباط با محاسبات ابری وجود دارد اما تمام این نگرانی ها به ۲ دسته کلی تقسیم می شوند: اول، مسائل امنیتی مربوط به فراهم

کنندگان محاسبات ابری و دوم، مسائل امنیتی مربوط به مشتریان.در اغلب موارد، فراهم کننده باید از ایمن بودن زیرساختش مطمئن باشد و از داده های مشتریانش و برنامه های کاربردی محافظت کند در حالیکه، مشتری باید از عملکرد فراهم کننده خدمات محاسبات ابری در راستای ایجاد معیارهای امنیتی مناسب برای محافظت از داده هایش مطمئن شود.معماری امنیت ابری فقط در صورتی کاراست که پیاده سازی های دفاعی صحیح وجود داشته باشد. یک معماری امنیت ابری کارا باید مسائل امنیتی در سطح مدیریتی را شناسایی کند. مدیریت امنیت مسائل کنترل های امنیتی را نشان می دهد[13]. این کنترل ها برای محافظت از هر نوع ضعفی در سیستم و کاهش اثر یک حمله قرار داده شده اند. اگرچه که بسیاری از انواع کنترل، پشت معماری امنیتی محاسبات ابری وجود دارد، آنها می توانند در دسته های زیر قرار گیرند[13] :

- **کنترل های بازدارنده**

این کنترل ها به منظور جلوگیری از هر نوع حمله عمدی در یک سیستم محاسبات ابری تنظیم شده است. این کنترل ها، باعث کاهش آسیب پذیری واقعی یک سیستم نمی‌شوند.

- **کنترل های پیش گیرنده**

این کنترل ها به کمک مدیریت آسیب پذیری ها سبب افزایش قدرت سیستم می شوند. کنترل پیش گیرنده، از آسیب پذیری های سیستم محافظت خواهد کرد، اگر یک حمله اتفاق بیفتد، بعد از آن این نوع از کنترل ها سعی در پوشش حمله و کاهش خرابی امنیت سیستم می کند.

- **کنترل های تصحیح کننده**

این کنترل سعی در کاهش اثر حمله دارد. برخلاف کنترل پیش گیرنده، کنترل تصحیح کننده در حین وقوع حمله، عکس العمل نشان می دهد.

- **کنترل شناسایی کننده**

این نوع از کنترل سعی در شناسایی حمله حین وقوع آن دارد. در زمان رخداد حمله، کنترل شناسایی کننده، سیگنالی برای کنترل های پیش گیرنده یا تصحیح کننده برای مشخص کردن مشکل ارسال می کند.

نگرانی های امنیتی در محاسبات ابری را می توان به ابعاد مختلفی تقسیم بندی کرد،این ابعاد به ۳ دسته کلی تقسیم شده اند: مسائل امنیتی و خصوصی سازی، مسائل پذیرش و مسائل حقوقی و قراردادی.

- **مسائل امنیتی و خصوصی سازی**

مدیریت هویت هر سازمانی به منظور کنترل دسترسی به اطلاعات و منابع محاسباتی نیاز به سیستم مدیریت هویت خودش دارد[14]. فراهم کنندگان محاسبات ابری یا سیستم مدیریت هویت مشتریان به زیرساخت هایشان را با کمک تکنولوژی SSOیکپارچه می کنند [14] و یا یک راه حل اختصاصی در مدیریت هویت ارائه می دهند [15] .امنیت پرسنلی و فیزیکی ارائه دهنده ها مطمئن هستند که ماشین های فیزیکی به اندازه کافی امن هستند و دسترسی به این ماشین ها و داده های مربوط به مشتریان تنها محدودیت نیست و تمام دسترسی ها مستند می شوند .دسترس پذیری ارائه دهنده ها مطمئن هستند که آهنا دسترسی مرتب و قابل پیش بینی به داده ها و برنامه هایشان دارند. امنیت برنامه ها ارائه دهنده ها مطمئن هستند که برنامه ها به عنوان یک سرویس روی محاسبات ابری که امنیت آنها با پیاده سازی رویه های تست و پذیرش برای به خارج فرستادن یا کد برنامه های پکیج شده در دسترس هستند. همچنین این مکانیزم، نیاز به معیارهایی برای امنیت برنامه ها در محیط کارفرما دارند [14].

- **مسائل پذیرش**

تعداد زیادی از مقررات مربوط به ذخیره سازی و استفاده از داده ها از قبیل: استاندارد امنیت داده ها در صنعت کارت های پرداخت(PCI DSS) ، بیمه سلامت قابل حمل و حسابرسی . بسیاری از این مقررات، نیاز به گزارش ها حسابرسی های منظم دارند. ارائه دهندگان محاسبات ابری باید قادر باشند مشتریانشان را مجبور کنند تا این قوانین را رعایت کنند [16].

- **مسائل حقوقی و قراردادی**

گذشته از امنیت و رعایت مسائل برشمرده شده در بالا، ارائه دهندگان محاسبات ابری و مشتریان آنها درباره مسئولیت هایی مذاکره خواهند کرد از قبیل مشخصه های معنوی و زمان پایان خدمات (زمانیکه داده و برنامه های کاربردی در نهایت به مشتری بازگردانده می شود) [17].

۴-۳.توازن بار در ابر

فناوری توازن بار[10] یک راه حل کلیدی در جهت افزایش کارایی و سرعت در امور شبکه است. به طور کلی توازن بار یعنی توزیع پردازش و فعالیتهای ارتباطی به طور مساوی بر روی سروهای اصلی شبکه‌های کامپیوتری به صورتی که بر روی هیچ سرور واحدی بار پردازشی بیش از حد مجاز یا ناهماهنگ با سایر سرورها اعمال نگردد بدین صورت از اعمال فشار پردازش بر روی یک سرور جلوگیری می‌شود.

توازن بار برای سرورهایی اهمیت دارد که در مورد آنها پیش بینی تعداد درخواستهای ارسالی به سرور دشوار می‌باشد. سایتهایی با بازدیدهای بالا و سایتهای دانشگاهی که نیازمند ثبت نام تعداد زیادی کاربر به صورت هم زمان می‌باشند از این جمله به شمار می‌آیند .اکثر وب سایتهای پر بازدید و معتبر به طور معمول از دو یا چند سرویس دهنده وب (Web Server) به صورت موازی جهت انجام عملیات توازن بار استفاده می‌نمایند، بدین صورت که اگر میزان استفاده از منابع یک سرور بیش از حد استاندارد تعیین شده باشد، به طوری که ادامه این فعالیت باعث Down شدن و از دسترس خارج گردیدن سرور شود، درخواستها به سرور دیگری که دارای ظرفیت تحمل بار بیشتری است ارجاع می‌شود .

۱-۴-۳.عملکرد توازن بار

به طور کلی توازن بار بین یک کلاینت و میزبان قرار می‌گیرد .هنگامیکه یک میزبان با اختلال مواجه شده و یا Fail شود، سرویس توازن بار این مشکل را شناسایی کرده و سریعا درخواستهای کلاینت های مربوط به آن میزبان خارج از دسترس را به سمت میزبان های سالم راهنمایی و یا در واقع Route می‌کند .باید در نظر داشت که این پروسه به صورت اتوماتیک انجام می‌شود، بدین طریق که تمامی ارتباطات مربوط به میزبان مختل، قطع شده و در ادامه کار آن کلاینت ها به میزبان سالم ارتباط داده می‌شوند. این پروسه بدون اینکه کاربر متوجه این اختلال گردد، رخ می‌دهد. بنابراین در مجموع در دسترس بودن سرویس نسبت به حالتی که یک سرور تنها به درخواستها پاسخ می‌دهد، به حداکثر رسیده و نهایتا قطعی سرورها به حداقل می‌رسد .تمامی پروسه شناسایی هاست مختل شده تا مسیر دهی مجدد و ایجاد ارتباط با میزبان سالم در کمتر از ۱۰ ثانیه رخ می‌دهد، از این رو کاربر به هیچ عنوان با قطعی سرویس ناشی از Down بودن یک سرور مواجه نخواهد شد .

۲-۴-۳.الگوریتم های توازن بار

الگوریتم های توازن بار ، براساس معیارهای مختلفی تعیین می‌شوند که در آنها ارجهیت هر کدام از سرورها در پاسخگویی به درخواستهای کلاینت مشخص خواهد شد. هدف این الگوریتمها توزیع هوشمندانه پردازش و یا بیشینه کردن در دسترس بودن تمامی سرورها می‌باشد.

انواع الگوریتم های توازن بار عبارتند از:

- Round-robin :

این الگوریتم مستقل از تعداد ارتباط های فعال و مدت زمان پاسخ دهی آنها پردازش را بین سرورها به صورت مساوی تقسیم می‌کند. این الگوریتم زمانی مناسب است که توان پردازش سرورها یکسان باشد، زیرا در غیر

[10] Load balancing

اینصورت بعضی سرورها ممکن است بیشتر از ظرفیت خود ارسال درخواست داشته باشند، در حالیکه سرورهای قوی‌تر فقط بخشی از منابع و امکانات خود را استفاده نمایند.

- Weighted round robin :

این الگوریتم توان پردازشی هر سرور را در نظر می‌گیرد، بدین صورت که مدیر شبکه، به صورت دستی به هر سرور یک وزن عملیاتی را اختصاص می‌دهد، سپس یک تواتر زمانبندی شده به صورت خودکار و بر طبق وزن هر سرور ایجاد می‌گردد و پس از آن درخواستها به سوی هر سرور بر طبق زمانبندی آن ارسال خواهد شد.

- Least-Connection :

زمانی که الگوریتم "حداقل- اتصال" به Load Balancer اعمال می‌شود، درخواستهای جدید به سرور موجود با کمترین اتصال فعال در میان سرورها ارسال می‌گردد.

- Load-based :

در الگوریتمLoad-based ، درخواستها بر اساس اینکه کدامیک از سرورها دارای حداقل بار پردازشی می‌باشند، ارسال می‌شوند[18].

۴.شبکه های مبتنی بر نرم افزار در رایانش ابری

در مدل IaaS ،که عموما یک بستر مجازی است،دارای چندین شکاف و نگرانی است از جمله این که آیا در حال حاضر استفاده از تکنولوژی های موجود برای اجزاءIaaS در شبکه مجازی وجود دارد؟آیا فضای مناسبی برای شبکه های نرم افزار محور (SDN) برای رسیدگی به چالش های شبکه مجازی را دارد؟SDN یک پلت فرم مورد توجه ،شبکه های مجازی است و از زمانی که منطق کنترل مشتریان بر روی یک کنترلر و نه در یک سوئیچ فیزیکی قرار گرفته است.SDN به عنوان یک مکانیسم جدید و نو برای حل این مشکلات ارائه شده است.در ابتدا چالش های موجود بررسی شده و سپس راهکار آن ارائه شده است.

معماری موجود در شبکه ابر به طور متداول از یک الگوی"one size fit all" در ابزارهای متنوع ، استفاده و پیروی میکند.توپولوژی شبکه ،پروتکل های ارسال و سیاست های امنیتی، همگی به دنبال مجموعه ای از تجهیزات برای استفاده بهینه و مدیریت مناسب پیاده سازی شده است.مشتریان ابر باید همگی قادر به دسترسی پهنای باند مورد نیاز برای برنامه ها ،حصول اطمینان از این عملکرد بر روی بخش اجرا باشد.بسیاری از لایه های کاربردی نیاز به یک پهنای باند مطمئن بین سروری برای معاملات درون یک قاب زمانی پذیرفته شده و از پیش تعریف شده SLAS را دارند.اجرای جداسازی ترافیک و کنترل دسترسی کاربران نهایی در میان چندین سیاست ارسالی باعث می شود که این سیاست ها به طور مستقیم بر روی هر پیکربندی، روتر و سوئیچی تاثیرگذار باشد.تغییر قوانین،پروتکل های متفاوت،پروتکل درختی پوشا در لایه ۲(STP) ، همراه با پروتکل های خاص فروشندگان،SDN را برای بهره برداری و اتصالات بین شبکه ای در مقیاسی از شبکه ابر به چالش می انگیزد.

برنامه ها باید خارج از بخش سخت افزاری بویژه برای آدرس دادن به IP و برای مکانیزم های وابسته به شبکه اجرا شوند هم چنین ممکن است برنامه ها احتیاج به دوباره نویسی و پیکربندی قبل از استقرار در ابر برای آدرس دهی به چندین شبکه مرتبط داشته باشند.تجهیزات شبکه ای وhypervisor ها به صورت استاتیک به شبکه پیکربندی شده متصل هستند که به طور غیر مستقیم و ضمنی یک مکان بدون محدودیت و وابستگی را ایجاد می کند.توپولوژی شبکه ای مراکز داده معمولا تنظیماتی را برای تجهیزات ترافیکی از قبل تعریف کرده است که به طور متداول از ۳ لایه شامل:Top Of Rack(TOR) لایه اتصال سرورهای درون rack ،لایه تجمعی و لایه هسته ای که اتصالات را از طریق اینترنت مهیا می کند ، تشکیل شده است.

این معماری چند لایه ای پیچیدگی قابل توجهی را در مرزهای تعریف شده دامنه لایه ۲تحمل می کند ،سیاست ها و شبکه ارسال لایه ۳ و لایه های خاص شبکه چند فروشنده،ارتباط بین مراکز داده ای یکی دیگر از چالش هاست.گاهی اوقات برای یک شرکت موقعیتی به وجود می آید که باید قادر به کار با چند ارائه دهنده ابر با توجه به محل دسترسی ،انتقالات ،ادغام

شرکت با ارائه دهندگان ابر های مختلف و غیره داشته باشند.شرکت ابر باید یک ارائه واضحی از حجم کاری ارکستراسیون [11] بین ابر ها دهد.

پروتکل های فعلی شبکه و هم چنین معماری هایی همانند STP وMCLAG مقیاس پذیری ،زمان تاخیر،توان عملیاتی و انتقال در شبکه ابر می توان محدودیت ساز باشند.در حالیکه لایه ۳ شبکه یک روش اثبات شده برای رسیدگی به تجهیزات مورد نیاز برای مرکز داده ای مجازی ابر ارائه داده و چندین شرکت استاندارد وجود دارد که ویژگی های لایه ۲ را ارتقاء و بهبود دهد از جمله استفاده از ارتباطات داخلی شفاف تعداد زیادی از لینک ها(TRILL) ،کوتاه ترین مسیر(SPB) و یا سیستم مبتنی بر SDN و OpenFlow .انگیزه اصلی این روش ها وجود توپولوژی مرکز داده ای و تجهیزات ارسال بسته از میان کوتاه ترین مسیر بین سرورها برای کاهش زمان تاخیر به نسبت مسیرهای اصلی و یا مکانیزم اولویت بندی که معمولا در STP استفاده می شود.

SDN یک معماری شبکه ای در حال ظهور است که عملیات کنترل شبکه از عملیات ارسال جدا شده و به طور مستقیم قابل برنامه ریزی است.این جابه جایی و تغییر در کنترل که قبلا در تجهیزات مجزا مجتمع شده بود ،به دستگاه های Computing در دسترس (مرکز منطق) این امکان را می دهد که زیر ساخت هایی برای برنامه ها و سرویس های شبکه انتزاعی داشته باشند.مزایای کلی برای شرکت های اتخاذ شبکه SDN به عنوان یک زیر ساخت ارتباطی برای اتصال Hybrid cloud و یا Private cloud وجود دارد که از جمله آنها :ارائه یک منطق متمرکز شده در سطح کنترلSDN ،یک دید جامع از منابع ابر و دسترسی های شبکه ای قابل دسترس .این رویداد موجب نظارت کافی بر مرکز داده، بر روی لینک های پهنای باند و سطح های سرویس شده است.

از جمله مزایای این روش می توان به موارد زیر اشاره داشت که :

- OpenFlow را قادر می سازد که نودهای سازنده و اصلی را به شرکت و مراکز ارائه دهنده ابر متصل کند.
- OpenFlow را قادر می سازد که ترافیک بین گره های اصلی را سوئیچ کند.
- OpenFlow و یا SDN مبتنی بر کنترلر قادر به پیکربندی جدول های ارسال جریان درون گره های اصلی ابر و فراهم آوردن یک برنامه مجازی شبکه wan .
- عملیات یک hybrid Cloud و ارکستراسیون نرم افزار برای مدیریت شرکت و رخدادهای مرکز داده ای و مدیریت منابع محاسباتی، ذخیره سازی و مدیریت شبکه ای مرکز داده است.

این روش باعث دسترسی اتوماتیک به پهنای باند برای ad-hoc ،انتقال به موقع حجم کاری مرکز داده و پردازش خواهد شد[20] [19].

۵.نتیجه گیری

SDNیک محصول یا مفهوم سخت افزاری / نرم افزاری نیست بلکه یک معماری و رویکرد جدید برای انعطاف پذیری و کنترل پذیری بیشتر شبکه ها و ظرفیت سازی برای استفاده از انواع برنامه های کاربردی، سرویسها و خدمات نرم افزاری روی شبکه های کنونی است .از وظایف و نقش پررنگ سخت افزار و تجهیزات شبکه می کاهد و به وظیفه و نقش لایه های نرم افزاری شبکه می افزاید و مدیریت و کنترل شبکه را ساده تر می کند .اینکه SDN چطور می تواند شبکه شما را بهبود بخشد به مقدار زیادی بستگی به مشکلاتی که شما در صدد رفع آن هستید دارد .با به کارگیری راه حل های مناسب SDN ، می توانید فرآیندهای عملیاتی خود را آسان کنید، خطاهای انسانی را کاهش دهید یا ترافیک را به روش های غیر متعارف تعریف شده توسط معیارهای اختصاصی سازمان خود، هدایت و منتقل کنید .به طور خلاصه، شما کارایی و انعطاف پذیری را بدست خواهید آورد.با بکارگیری SDN در ابر میتوان چالش ها و معایب موجود در ابر را برطرف کرد. OpenFlow یک پروتکل ارتباطی در SDN است و اولین

[11] orchestration

پروتکل ارتباطی رابط استاندارد است که برای SDN طراحی شده است و بواسطه همین پروتکل نیز برخی از مشکلات در ابر رفع گردیده است.

مراجع

[1] White paper, Software-Defined Networking: The New Norm for Networks, Open Networking Foundation, April 13, 2012. Retrieved August 22, 2013.
[2] "Software-defined networking: The new norm for networks," Palo Alto,CA, USA, White Paper, Apr. 2012. [Online]. Available: https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdnnewnorm.pdf
[3] Wenfeng xia,Yonggang wen, IEEE ,Chuan Heng Foh ,Dusit Niyato ," A Survey on Software-Defined Networking ".
[4]H. Yin *et al.*, SDNi: A Message Exchange Protocol for Software Defined Networks (SDNS) across Multiple Domains, Jun. 2012, Internet draft. [Online]. Available: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf
[5]H. Xie et al., "Software-defined networking efforts debuted at IETF 84," IETF J., Oct. 2012. [Online]. Available: http://www.internetsociety.org/ fr/node/45708
[6]Gurabani ,Vijay K ," Abstracting network state in software defined network for rendezvous" ,2012
[7]Brent Salisbury."The Northbound API –A big problem" ,www.networkstatic.net,2012
[8] McKeown,Nick." OpenFlow:enabling innovation in campus Network".
[9] G. Lu, R. Miao, Y. Xiong, and C. Guo. Using cpu as a traffic co-processing unit in commodity switches. In Proceedings of the first workshop on Hot topics in software defined networks, HotSDN '12, pages 31-36, New York, NY, USA, 2012. ACM.
[10]J. C. Mogul and P. Congdon. Hey, you darned counters!: get off my asic! In Proceedings of the first workshop on Hot topics in software defined networks, HotSDN '12, pages 25-30, New York, NY, USA, 2012. ACM.
[11]Hakim Amin,Mohammad Shahriyar ,1391,"CloudComputing" .
[12]Alireza Haghigh,"Architecture of cloud & management in CloudComputing" .
R. Enns. NETCONF Configuration Protocol. RFC 4741 (Proposed Standard), Dec. 2006. Obsoleted by RFC 6241.
[13] Krutz,Ronald,and Russell Dean vines."Cloud Computing Security Architecture".Cloud Security :A comprehensive Guide to secure cloud computing.
[14] Haghighat.M,Zanouz,Abdel-Mottaleb,M.[2015],"Trust worthy cloud based and cross-enterprise biometric identification"
[15] "Identity management in cloud" ,information week , 2013
[16] DLA piper,"managing legal risks arising from Cloud Computing " .
[17] Adams, Richard(2013) "emergence of Cloud storage & the need for a new digital forensic process model" .
[18] Asadian Arezo,www.parsData.com/articles/what is load balancing.
[19] Siamak Azodolmolky,Ramin Yahyapour,Philip wieder," SDN based cloud computing networking." June 2013
[20] N.McKeown,T.Anderson,H.Balakrishnan,G.parulkar,L.peterson."OpenFlow:enabling innovation in campus network"