مدیریت منابع در edge Computing با استفاده از SDN

Resource management in edge computing using SDN

فصل دوم(مبانی نظری و پیشینه مطالعاتی)

۲-۱ مقدمه

با افزایش استفاده از رایانش ابری، رشد پیچیدگی ساختارها در این مبنا روی داده است بنابراین برای بهبود عملکرد و مدیریت منابع لازم است از شیوه‌ها و مدل‌هایی استفاده شود که پروفایل کاربری مناسب در پیش‌بینی مدل ارائه می‌کند تا مناسب‌ترین منابع برای هر حجم کاری مشخص شود. مدل‌ها و ابزاری وجود دارد که ایجاد پروفایل کاربردی مناسب را حل می‌کند و می‌توان مقدار منابع مورد نیاز برای هر حجم کاری را برآورد نمود.

منافعی که مدیریت منابع در IaaS ابر دنبال می‌کند، شامل مواردی مانند مقیاس‌پذیری، کیفیت سرویس‌دهی، سودهای بهینه، کاهش سربار، افزایش توان عملیاتی، کاهش تاخیر، اختصاصی‌سازی محیط، بازدهی هزینه و ساده‌سازی واسط‌ها می باشد.

رایانش ابری راهی برای استفاده از منابع، مدیریت سرمایه و هزینه‌های پشتیبانی فناوری‌ها برای سازمان‌ها است. همچنین شبکه‌های SDN رویکردی جدید در شبکه‌های کامپیوتری است که با استفاده از آن مدیران شبکه قادر به مدیریت خدمات شبکه از طریق انتزاع سطح بالاتر می‌شوند. در این فصل از پژوهش به بررسی مبانی نظری و پیشینه مطالعاتی در زمینه مدیریت منابع در edge Computing با استفاده از SDN می‌پردازیم.

۲-۲ مبانی نظری

استفاده از منابع ابر (سخت‌افزار و نرم‌افزار) که به صورت خدمات ارائه شده‌اند، از طریق شبکه (متداول‌ترین آنها اینترنت) را رایانش ابری گویند. سیر تکاملی دستگاه‌ها و تجهیزات جانبی سیار، مجازی‌سازی سرورها و ظهور سرویس‌های ابر، منجر به بازبینی دوباره معماری رایج شبکه‌ها شده است. از جمله معماری‌های نو ظهور SDN[1] می‌باشد که ما در این پژوهش به بررسی مدیریت منابع در edge Computing با استفاده از SDN می‌پردازیم.

۱-۲-۲ تاریخچه SDN

بحث سیگنالینگ باز[2] در سال ۱۹۹۵ برای ساخت شبکه‌های ATM و تلفن همراه توسعه‌پذیر و قابل برنامه-ریزی مطرح شده است. درسال ۲۰۰۶ پروتکلی به نام NetConf برای مدیریت و اصلاح تنظیمات سیستم‌های شبکه ارائه شد. همه‌ی این تحقیقات زمینه پیدایش شبکه‌های مبتنی بر نرم‌افزار بوده است. اما ایده اصلی و نقطه شروع SDN حاصل تلاش‌های دو محقق به نام آقای نیک مکئون[3] از دانشگاه استنفورد و آقای اسکت شنکر[4] از دانشگاه برکلی در سال ۲۰۰۸ مطرح شد، پروژه آنها که Ethane نام داشت و تقریب شروع آن به ۱۵ سال پیش برمی‌گردد باهدف افزایش امنیت شبکه با استفاده از یک سری پروتکل مبتنی بر جریان داده بود.

بعدازآن گامی جدید برای پیشرفت در شبکه‌ها برداشته شد و گروه‌های تحقیقاتی زیادی بروی این شبکه‌ها شروع به فعالیت کردند. بِرَدکِیسمور تحلیلگر شرکت IDC که یک تعریف کامل از SDN بیان کرده است که می‌گوید: « فلسفه‌ی حضور شبکه‌ها این است که از نرم‌افزار پشتیبانی کنند. به عبارت دیگر شبکه‌های مبتنی بر نرم‌افزار برای این شکل گرفتند که بتوان در محیط‌های همواره در حال تغییر کسب وکار، نرم‌افزار را در cloud توسعه داد و مدیریت کرد. قرار نیست برای سرگرمی معماری نرم‌افزار را تغییر بدهیم. اگر نرم‌افزار تغییری نکرده است، دلیلی ندارد در شبکه تغییر ایجاد کنیم. وقتی حجم کار تغییر می‌کند، آنوقت است که باید نگاهی به شبکه بیندازیم و مطمئن شویم که شبکه از این نرم‌افزارها پشتیبانی می‌کند» (درویشی و همکاران، ۱۳۹٤).

[1] Software Defined Networking
[2] Open Signaling
[3] Nick Mckeown
[4] Scott Shenker

اخیراً پروژه‌های دیگری نظیر NOX ، OpenFlow، SANE،Ethane و POF نیز جداسازی سطوح کنترل و داده را مطرح کرده‌اند. جالب اینکه، این راه حل‌های اخیر نیازمند انجام تغییرات اساسی در تجهیزات پیش‌بری نیستند، که در این صورت نه تنها برای جامعه تحقیقاتی شبکه جالب می‌باشد بلکه برای صنعت شبکه نیز مفید می‌باشد. به عنوان مثال تجهیزات مبتنی بر OpenFlow می‌توانند به راحتی با تجهیزات اترنت سنتی هم زیستی داشته باشند که در نتیجه به منظور برپاسازی OpenFlow می‌توان این شبکه‌ها را در کنار شبکه‌های سنتی بر پا کرد و به مرور زمان دستگاه‌های مبتنی بر OpenFlow بیشتری را به شبکه اضافه کرد.

همچنین مفهوم سیستم عامل شبکه با معرفی سیستم عامل‌های شبکه مبتنی برOpenFlow مانند NOX، ONIX و ONOS دوباره متولد شد. سیستم عامل‌های شبکه چندین دهه است که وجود دارند. یکی از معروف‌ترین آنها IOS سیسکو می‌باشد که در اوایل دهه ۹۰ میلادی معرفی شد. دیگر سیستم عامل‌هایی که سزاوار نام بردن هستند می‌توان به JUNOS، ExtreamXOS و SR OS اشاره کرد. این سیستم عامل‌های شبکه، سخت-افزار زیرین را برای اپراتورهای شبکه تجرید کرده، کنترل زیر ساخت شبکه را آسان‌تر کرده و همچنین توسعه و گسترش پروتکل‌های جدید و برنامه‌های کاربردی مدیریتی را ساده کرده است (طالقانی، ۱۳۹٤).

۲-۲-۲ معرفی SDN

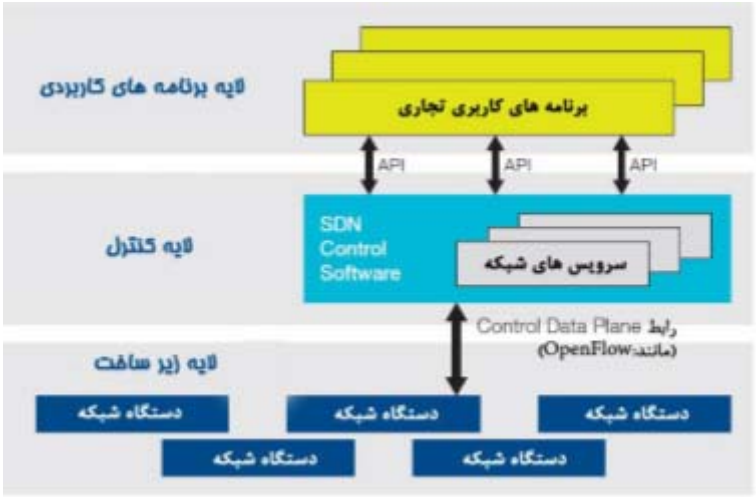
SDN یک معماری جدید شبکه است که در آن سطوح داده و کنترل از یکدیگر جدا هستند. در این شبکه‌ها با تفکیک برنامه‌های کاربردی از زیرساخت اصلی شبکه و انعطاف‌پذیری در لایه کنترلی، شبکه‌ها هوشمندتر و کنترل‌پذیرتر می‌شوند.

در چنین معماری‌ای، قابلیت کنترل از دستگاه‌های شبکه حذف می‌شود و به این ترتیب این دستگاه‌ها به اجزا ارسال (بسته) ساده تبدیل خواهند شد. منطق کنترل به یک عنصر خارجی با نام کنترلر SDN منتقل می‌شود.

دستگاه‌های زیرساخت به سادگی موتورهای ارسالی می‌شوند که در آنها بسته‌های ورودی براساس مجموعه‌ای از قوانین تولید شده توسط یک (یا تعدادی) کنترلر ارسال می‌شوند. تصمیم‌گیری کنترلر با توجه به منطق برنامه‌های از پیش تعریف شده است. در واقع به جای اینکه سیاست‌ها و پروتکل‌ها بر روی مجموعه دستگاه‌ها از هم جدا به اجرا در بیاید، از طریق یک کنترلر مرکزی واحد در کل شبکه فارغ از سخت‌افزار و شرکت سازنده آن شبکه انجام می‌گیرد (هاشمی و همکاران، ۱۳۹۵).

۳-۲-۲ معماری SDN

شکل زیر نمایی از معماریSDN را نشان می‌دهد. بخش هوشمند شبکه به طور منطقی در مرکز کنترلرهای نرم‌افزاریSDN قرار دارد که ساختار کلی شبکه را حفظ می‌کند؛ بنابراین، شبکه از دید برنامه‌های کاربردی به صورت یک سوئیچ منطقی و واحد به نظر خواهد رسید. با استفاده SDN از شرکت‌ها و اپراتورهای مخابراتی، از طریق یک کنترلر مرکزی واحد در کل شبکه می‌توانند فارغ از سخت‌افزار و شرکت سازنده آن شبکه را کنترل ومدیریت کنند. به این ترتیب، طراحی شبکه و کاربری آن، به طور چشم‌گیری، ساده‌تر خواهد شد. همچنین SDN، دستگاه‌ها و ماشین‌های به کار گرفته شده در شبکه را نیز ساده‌تر می‌کند، چرا که دیگر نیازی به شناسایی و پردازش هزاران استاندارد پروتکل نخواهید داشت و دستورات را فقط از کنترلر SDN دریافت می‌کنید (دارابی نژاد و همکاران، ۱۳۹۲).



شکل ۲-۱ معماری SDN (دارابی نژاد و همکاران، ۱۳۹۲).

۱-۳-۲-۲ لایه کاربرد

شبکه جدید از دیدگاه این لایه یک سری سوئیچ منطقی و واحد به نظر می‌رسد، از برنامه‌های کاربردی تجاری که در این لایه قرار دارند می‌توان به کاربردهای امنیتی، کاربردهای مجازی‌سازی شبکه، مانیتورینگ شبکه، کنترل دستیابی و... اشاره کرد.

۲-۳-۲-۲ لایه کنترل

با نام سطح کنترل هم شناخته می‌شود که شامل مجموعه‌ای از کنترلرهای نرم‌افزاری می‌باشد که یک کنترل یکپارچه و جامع را از طریق[5] APIهای باز برای نظارت بروی رفتارهای شبکه فراهم می‌کند، در این لایه دو واسط API وجود دارد که وظیفه ارتباطات کنترلر با دیگر کنترلرها و سایر لایه‌ها را برعهده دارند که این دو واسط عبارتند از:

الف) باند جنوبی: وظیفه اصلی این واسط API ، مرتبط کردن لایه کنترل با لایه پایینی آن یعنی لایه زیرساخت است همچنین پروتکل‌های ForCES و Openflow در این باند قرار دارند که این پروتکل‌ها وظیفه برنامه‌ریزی روی شبکه به صورت نرم‌افزاری را بر عهده دارند.

ب) باند شمالی: این باند وظیفه مرتبط کردن لایه کاربرد و لایه کنترل را برعهده دارد، در واقع Northbound به برنامه‌ها اجازه می‌دهد که با واحد کنترل تعامل داشته باشند، این لایه یک سیستمی است که ساختار نرم‌افزاری دارد، یک رابط برنامه‌نویسی کاربردی کوچک که استانداردسازی شده باشد و می‌تواند نقش مهمی در آینده شبکه‌های مبتنی بر نرم‌افزار بازی کند.

۳-۳-۲-۲ لایه زیرساخت

این لایه در پایین‌ترین سطح معماری SDN قرار دارد که با نام سطح داده شناخته می‌شود، سوئیچ‌های فیزیکی و مجازی در این لایه قرار دارند مطرح شدن سوئیچ‌های مجازی بر میگردد به ظهور فناوری مجازی‌سازی سرورها که توسط کنترلرها به کار گرفته می‌شوند، نقش سوئیچ‌های مجازی در ایجاد اتصال سرورهای مجازی با کارت‌های شبکه مجازی و تراکم ترافیک و ارسال آن به خارج کنترلرها در شبکه فیزیکی، بیشتر به چشم

[5]Application Programming Interface

می‌خورد. به طورکلی این لایه مسئول مدیریت و هدایت بسته‌ها در مسیری مناسب که این مسیر توسط کنترلرهای موجود در لایه کنترل تعیین می‌گردد (درویشی و همکاران، ۱۳۹٤).

۲-۲-٤ مزایای SDN

ارتقاء پیکربندی: در مدیریت شبکه، پیکربندی یکی از مهم‌ترین عملیات است.زمانی که بخواهیم تجهیزاتی را به شبکه اضافه کنیم فعلی بدلیل ناهمگونی سازندگان دستگاه‌های شبکه، کاری دشوار است اما درSDN بخاطر واحدسازی سطح کنترل بر روی همه دستگاه ها،قادر به پیکربندی به صورت اتوماتیک از طریق کنترل نرم‌افزاری را دارند.

- بهبود اجراء

- کنترل مرکزی

- صرفه جویی و بهبود تجهیزات شبکه

- امکان طراحی و توسعه برنامه های Third- party (منظور از این عبارت نرم‌افزارهایی هست که توسط یک شرکت سوم بر روی یک بستر منتشر می‌شوند)

- امکان ارائه BWoD[6](پهنای باند بنا به درخواست)

- تامین کیفیت سرویس QoS[7] (حسینی تشنیزی و همکاران، ۱۳۹٤).

۲-۲-۵ اجزای تشکیل دهنده SDN

کنترلرها (کنترل کننده‌ها): یکی از ایده‌های بزرگ SDN این است که دستگاهی به نام کنترل کننده با همه دستگاه‌های موجود در یک دامین شبکه ارتباط مستقیم داشته، از توپولوژی شبکه آگاه باشد و شبکه را از

[6] Bandwidth-on-Demand
[7] Quality-of-Service

یک نقطه مرکزی برنامه‌ریزی کند. یک کنترل کننده SDN مدل برنامه‌ریزی شده شبکه را از حالت توزیع شده به حالت متمرکز تبدیل می‌کند.

سوییچ‌های مجازی: با ظهور فناوری‌های مجازی‌سازی سرورها که توسط هایپروایزرها به کار گرفته می شوند، نقش سوئیچ مجازی در ایجاد اتصال سرورهای مجازی با کارت‌های شبکه مجازی و تراکم ترافیک و ارسال آن به خارج از هایپروایزرها در شبکه‌های فیزیکی پررنگ‌تر شده است. سوییچ‌های سخت‌افزاری و مجازی نقش مهمی در SDN ایفا می‌کند، زیرا آنها به طور مستقیم مسئول اجرای جدول‌های برنامه‌ریزی شده توسط کنترل کننده‌ها می‌باشند (موگول[8] و همکاران، ۲۰۱۲).

شبکه‌های هم‌پوشان (Overlay): شبکه‌های همپوشان شبکه‌های مجازی هستند که به طور مشترک از یک بستر شبکه فیزیکی استفاده می‌کنند، اما به طور منطقی از یکدیگر مستقل هستند. برخی کنترل کننده‌های SDN از این Overlayها برای ارتباطات خود در مرکز داده پراکنده و هاست‌های مختلف مجازی استفاده می‌کنند (تسلیوس[9] و همکاران، ۲۰۱۲).

۲-۲-۶ پروتکل OpenFlow

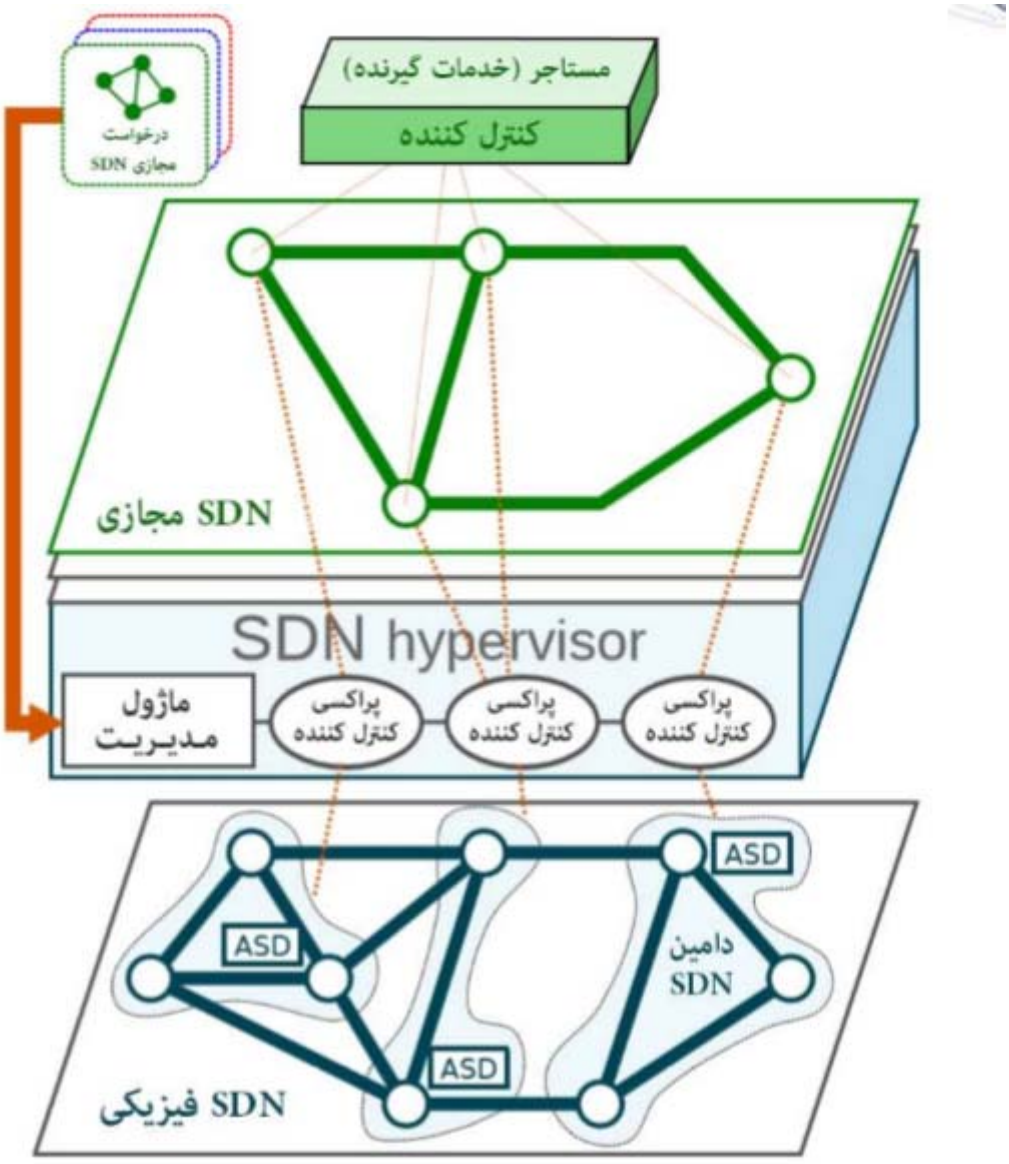
OpenFlow نخستین واسط ارتباطی استانداردی است که در معماری SDN، بین لایه‌های کنترل و ارسال تعریف می‌شود. OpenFlow امکان دسترسی مستقیم و ایجاد تغییر در برنامه ارسال تجهیزات شبکه نظیر سوئیچ‌ها و روترها را هم بصورت فیزیکی و هم بصورت مجازی فراهم می‌کند. نبود یک واسط باز در برنامه ارسال داده، باعث شده تجهیرات شبکه‌های امروزی به صورت یکپارچه، بسته و شبه پردازنده مرکزی شده است. هیچ پروتکل استاندارد دیگری در شبکه، قادر به اجرای وظایف OpenFlow نیست و پروتکلی نظیر آن لازم است تا کنترل شبکه را از سوئیچ‌های شبکه خارج و به نرم افزار کنترل کننده مرکزی منطقی هدایت کند (فنداشن[10]، ۲۰۱۲).

[8] Mogul
[9] Tselios
[10] Fundation

۷-۲-۲ صفحه‌ی کنترل

ما توجه داریم که زیر ساخت شبکه، توپولوژی vSDN را به چندین کاربر ارائه می‌دهد. تقاضای vSDN کاربر شامل مجموعه‌ای از گره‌ها و لینک با شرایط خاصی، مانند تغییر ظرفیت، پهنای باند لینک و محل می‌باشد. هنگامی که یک vSDN نصب شده باشد، کنترل می‌تواند ورودی‌های جریان را نیز نصب کنند. ما هیچ فرضیاتی راجع به نوع خدمات، به عنوان مثال، بسته انتقال و پردازش قوانین نداریم. ما فقط فرض می‌کنیم که بستر فیزیکی شامل سوئیچ OpenFlow می‌باشد، و هر کدام شامل یک جدول جریان است که می‌تواند به بخش‌های دیگر برش داده شود.

یک معماری هایپروایزر توزیع شده در شکل زیر ارائه شده است، که می‌تواند تعداد زیادی از پیغام‌های کنترل جدول جریان کاربران را اداره کند. هایپروایزر شامل ماژول مدیریت (MM) و پراکسی‌های کنترل چندگانه (CPX) می‌باشد که برای کنترل توزیع بار استفاده می‌شود. ما زیر لایه فیزیکی را به حوزه‌های متعدد SDN تقسیم کردیم و به هر دامین CPX اختصاص دادیم. هر CPX، دسترسی به سوئیچ‌های دامنه مربوطه را مدیریت می‌کند. در حال حاضر، ما فرض می‌کنیم که تمام حوزه‌های SDN توسط یک تامین کننده واحد SDN اداره می‌شود، با این حال، چند برش ارائه دهنده SDN ممکن است با اعمال نفوذ در معماری مجازی-سازی شبکه ایجاد شود (حسامی، ۱۳۹۳).



شکل ۲-۲ نمای کلی معماری برش خودکار(حسامی، ۱۳۹۳).

۲-۲-۸ صفحه انتقال

ما در حال حاضر به چالش‌های اصلی در طراحی سطوح انتقال توجه می‌کنیم. در یک محیط چند کاربری تعداد زیادی از جداول جریان باید بر روی حافظه بستر یک سوئیچ نگه داشته شوند. CPX جداسازی تمام جداول جریان مجازی را تضمین می‌کند و همچنین تضمین می‌کند که تمام اقدامات پردازش بسته‌ها در توالی صحیح در مورد اعمال یک گروه متصل از گره‌های مجازی به سوئیچ نقشه‌برداری (به عنوان مثال، با استفاده از یک حلقه پشت رابط) انجام شوند. مقیاس‌پذیری از پلت فرم به شدت توسط اندازه جدول جریان در

سوئیچ محدود شده است. برای غلبه بر این محدودیت، ما از به اصطلاح روش نرم افزار کمکیASD در شبکه بستر، استفاده می‌کنیم (یو[11] و همکاران، ۲۰۱۰).

هر دامنه SDN، یک ASD شامل یک سوئیچ نرم‌افزار در حال اجرا در سرور کالا، اختصاص داده شده است. در مقابل سوئیچ گسترش جریان حافظه اصلی موجود در سرور برای ذخیره‌سازی یک کپی کامل از تمام جداول جریان مورد نیاز توسط ASD مربوطه کافی است. با این حال، با وجود پیشرفت‌های اخیر در نرم‌افزار مبتنی بر معماری مسیر داده و سرورهای کالا، اختلاف بین کالا و سخت‌افزار تخصصی هنوز باقی مانده است.

برای رفع این محدودیت، ما از اموال زیپف ترافیک کل استفاده می‌کنیم به عنوان مثال این صحیح می‌باشد که بخش کوچکی از جریان، بسیاری از حجم ترافیک را تشکیل می‌دهد. ما از ASDS برای رسیدگی به حجم کم جریان ترافیک استفاده می‌کنیم، در حالی که ذخیره تعداد کمی از حجم بالا به سوئیچ‌ها اختصاص داده می‌شود. علاوه بر این CPX تضمین می‌کند که ورودی‌های جریان‌های پنهان شده از یکپارچگی معنایی برخوردار هستند. یک ترافیک موثر رویکرد بارگیری برای حمل و نقل IP را مورد بررسی قرار می‌دهد. برای این منظور، ما در حال توسعه و ذخیره هستیم. به طور خلاصه، ما تصمیم به تخلیه بر اساس و یژگی‌های انبساط ترافیک گرفته‌ایم (سرار[12] و همکاران، ۲۰۱۲).

۹-۲-۲ محاسبات ابری

پردازش ابری یک پدیده‌ی نوظهور در علم رایانه است و دلیل این نامگذاری آن است که داده‌ها و برنامه‌ها در میان ابری از سرویس دهنده‌های وب قرار گرفته‌اند. بطور ساده، پردازش ابری یعنی استفاده اشتراکی از برنامه‌ها و منابع در محیط شبکه، بدون این که مالکیت و مدیریت منابع شبکه و برنامه‌ها برای ما مهم باشد.

در سالهای اخیر، محبوبیت و رشد سریع در قدرت پردازش و فناوری ذخیره‌سازی و گسترش سریع اینترنت موجب شده است منابع محاسباتی به منابعی ارزان‌تر، قوی‌تر و در دسترس تر از قبل تبدیل شوند (آرمبروست[13] و همکاران، ۲۰۱۰).

---

[11] Yu
[12] Sarrar
[13] Armbrust

این روند فناوری به عنوان محاسبات ابری شناخته می‌شود و برای آنکه بتواند پاسخ مناسبی را به گسترش فناوری اطلاعات و ارتباطات بدهد نیازمند پیمودن راه تکاملی مناسبی است (پودال[14] و همکاران، ۲۰۱۵).

همچنین نیاز به این هست که افراد بتوانند کارهای محاسباتی سنگین خود را بدون داشتن سخت‌افزارها و نرم‌افزارهای گران، از طریق خدمات ابر انجام دهند. رایانش ابری آخرین پاسخ فناوری به این نیازها بوده است. محاسبات ابری بر روی تحویل به موقع خدمات، قابلیت اطمینان، تأمین امنیت در ارسال و دریافت داده‌ها، تحمل‌پذیری خطا در ارائه سرویس، پایداری و ایجاد زیرساخت‌های مقیاس‌پذیر برای میزبانی خدمات کاربردی مبتنی بر اینترنت متمرکزشده است. محاسبات ابری درواقع بیانگر نرم‌افزاری است که خدمات را از میان منابع محاسباتی مجازی موجود به کاربران در هر نقطه از جهان ارائه می‌دهد.

استفاده از خدمات ابر باعث می‌شود که رابطهٔ درحال توسعه‌ای در میان هر دو بخش دولتی و خصوصی برای خدمت رسانی به مردم به وجود آید. محاسبات ابری ازآن جهت برای صاحبان کسب وکار جذاب است که می‌توانند کار خود را با منابع کوچک و کمتر شروع کنند و هم‌زمان با رشد تقاضا از طرف کاربران به ظرفیت منابع خود بیفزایند و برای کاربران نیز ازآن جهت جذابیت دارد که به جای پرداخت هزینه‌های گزاف برای در اختیار گرفتن منابع محاسباتی یا نرم‌افزارهای موردنیاز کافی است هرکدام را به هراندازه که نیاز دارند به عنوان خدمت از طرف ارائه کنندگان تحویل بگیرند و بدین ترتیب صرفه جویی بسیار زیادی در زمینهٔ اقتصادی داشته باشند (ساسیکالا[15]، ۲۰۱۳).

به دلیل ماهیت خدمتگرا بودن محاسبات ابری، ارائه دهندگان خدمت نیاز دارند تا آگاهی کاملی از وضعیت سیستم محاسبات ابری خود داشته باشند و به طور مداوم بتوانند کارایی آن را ارزیابی کنند تا بتوانند پاسخ مناسب را باکیفیت مناسب به حجم خدمات مورد تقاضای کاربران ارائه دهند. در ارزیابی کارایی محیط محاسبات ابری به دلیل وجود مدل‌های کاربردی و خدماتی با چالش‌هایی مواجه می‌شویم که از آن میان می‌توان به، مختلف در اجرای سیاست‌های تخصیص منبع و الگوریتم‌های زمانبندی متفاوت بودن هزینه‌ها، عدم تولید دوباره نتایج آزمون‌ها و عدم اعتماد سرویس‌دهندگان ابر به ارزیابی مبهم و روش آزمون وخطا . همچنین برای آنکه از کیفیت خدمت ارائه شده توسط ابر اطمینان یابیم و قابلیت اطمینان این خدمات را

[14]Puthal
[15]Sasikala

افزایش دهیم نیازمند ارائه راه حل‌هایی برای شبیه‌سازی و ارزیابی کارایی رایانش ابری هستیم (حسین زاده و همکاران، ۱۳۹٤).

سیستم ابری، درساده ترین تعریف، ارائه سرویس‌های کامپیوتری بر روی اینترنت است. شکل ۲-۳ چگونگی دسترسی کاربران به خدمات و سرویس‌های درون ابر را نمایش می‌دهد. کافی است کامپیوتر شخصیتان، موبایل، تلویزیون و یا حتی یخچال و یک رابط نرم‌افزاری مثل یکی از انواع مرورگرها را برای استفاده از سرویس‌های آنلاین درون ابر در اختیار داشته باشید.

شکل ۲-۳ ارتباط کاربران با سیستم ابر(حسین زاده و همکاران، ۱۳۹٤).

رایانش ابری پدیده جدیدی است که در آن منابعی از قبیل واحد پردازش، حافظه و محل ذخیره‌سازی به صورت فیزیکی در سیستم مورد استفاده کاربران وجود ندارند و به جای آن یک ارایه دهنده سرویس وجود دارد که منابع را در اختیار داشته و مدیریت می‌کند و کاربران با دسترسی به اینترنت از خدمات استفاده می‌کنند (قلی زاده و همکاران، ۱۳۹۳).

۱۰-۲-۲ نیازهای کاربردی

نیازهای کاربردی که توسط یک سیستم تحلیل داده‌ی توزیع شده باید برآورده شود به دو دسته‌ی اصلی تقسیم می‌شود: نیازهای مدیریت منابع و نیازهای مدیریت برنامه‌های کاربردی.

نیازهای مدیریت منابع به نیازهایی اشاره دارد که به مدیریت همه‌ی منابع مربوط می‌شود (داده‌ها، ابزار، نتایج) که ممکن است یک برنامه کاربردی KDD را نیز شامل شود؛ نیازهای مدیریت برنامه‌های کاربردی به طراحی و اجرای خود برنامه‌های کاربردی مربوط می‌شود.

۱۱-۲-۲ معماری ابر

معماری مبتنی بر سرویس، معماری نرم‌افزار یا سیستمی است که امکاناتی همچون استفاده مجدد، توسعه-پذیری، سهولت و بسیاری دیگر را در اختیار کاربران قرار می‌دهد. این ویژگی‌ها برای شرکت‌هایی که به دنبال کاهش هزینه هستند و به جای فروش بر اجاره سرویس‌های نرم‌افزاری تأکید دارند، امری الزامی است. معماری سامانه‌های نرم‌افزاری رایانش ابری عموما شامل اجزایی است که با یکدیگر از طریق رابط برنامه نویسی نرم افزاری،معمولا وب سرویس ارتباط برقرار می‌کنند. طرحی شبیه به فلسفه یونیکس دارد که در آن چند برنامه مختلف که هر یک کاری را به خوبی انجام می‌دهند، از طریق واسطه‌ای جهانی با یکدیگر کار می‌کنند. لایه‌های این معماری عبارتند از:

کاربر: کاربر رایانش ابری متشکل از سخت‌افزار و نرم‌افزاری است که برای تحویل برنامه‌های کاربردی از ابر استفاده می‌کنند و یا به طور ویژه تنها برای تحویل سرویس‌های ابری طراحی شده است.

برنامه‌های کاربردی: سرویس‌های برنامه کاربردی ابری یا نرم‌افزار به عنوان سرویس (SaaS) نرم‌افزار را به صورت سرویس روی اینترنت تحویل می‌دهند و بدین وسیله نیاز به نصب نرم‌افزار روی رایانه‌های مشتریان را ازبین می‌برند ونگهداری و پشتیبانی را ساده‌تر می‌سازد.

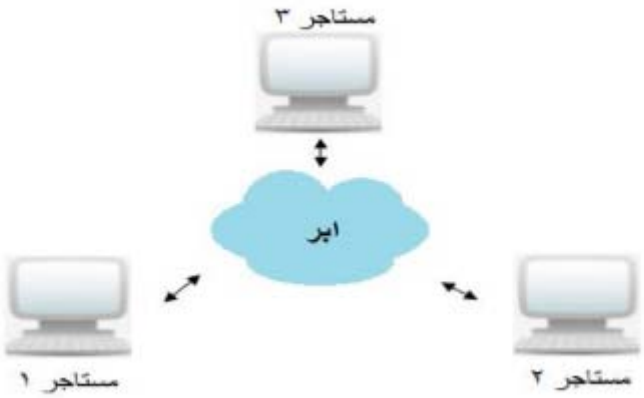
بستر: سرویس‌های بستر ابری یا (بستر به عنوان سرویس (PaaS)) بستر رایانشی ویا پشته راهکار -که اغلب روی زیرساخت ابری اجرا شده و برنامه کاربردی ابری را تغذیه می‌کنند را به صورت سرویس ارائه می‌دهد. سرویس بستر ابری استقرار – برنامه‌های کاربردی را بدون هزینه و پیچیدگی خرید و مدیریت لایه‌های نرم‌افزاری و سخت‌افزاری زیرین آسان می‌کند.

زیرساخت: زیرساخت رایانه‌ای 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 سخت‌افزار

و نرم‌افزار و فضای مرکز داده (دیتا سنتر) ویا تجهیزات شبکه، همه این زیر ساخت‌ها را به صورت یک سرویس و میزان منابع مصرف[16]شده را تهیه می‌کنند. این شیوه در واقع تکامل یافته مدل عرضه سرورهای خصوصی مجازی است.

سرور: لایه سرورها متشکل از سخت‌افزار و نرم‌افزاری است که مخصوصا برای تحویل سرویس‌های ابر طراحی شده‌اند. به عنوان مثال می‌توان از پردازنده‌های چندهسته‌ای و سیستم عامل‌های ویژه ابری نام برد (حسینی تشنیزی وهمکاران، ۱۳۹٤).

همچنین معماری رایانش ابری مبتنی بر سرویس چند مستاجری است. در این روش یک نمونه از برنامه در حال اجرا، بین گروهی از مصرف کنندگان به اشتراک می‌گذارد به طوری که یک بستر نرم‌افزاری را برای تعداد زیادی از کاربران ارائه می‌دهد. به همین دلیل از چند مستاجری به عنوان یکی از مزایای رایانش ابری یاد می‌شود. معماری رایانش ابری چند مستاجری در شکل زیر آمده است.



شکل ۲-٤ رایانش ابری چند مستاجری (کیانی و همکاران، ۱۳۹٤).

از دیدگاه معماری در پردازش ابری، ابر کامپیوتر به دو بخش ابتدایی و انتهایی تقسیم می‌شود. بخش ابتدایی شامل اطلاعات و شکل ظاهری نرم‌افزارها است که توسط کاربران مشاهده می‌شود و بخش انتهایی در

[16]Utility Computing

برگیرنده ابر (اینترنت)، چندین کامپیوتر و سرور واحدهای ذخیره می‌باشد که مسئولیت پردازش اطلاعات را برعهده دارد. مدیریت ابر و کنترل ترافیک داده‌ها و نظارت بر تبادل اطلاعات برعهده‌ی کامپیوتر می‌باشد.

کاربران رایانش ابری متشکل از سخت افزار و نرم‌افزار است که برای تحویل برنامه‌های کاربردی از ابر استفاده می‌کنند. معماری سامانه‌های نرم‌افزاری به کار گرفته شده در رایانش ابری، معمولا از طریق رابط برنامه نویسی نرم‌افزار یا وب سرویس‌ها با یکدیگر ارتباط بر قرار می‌کنند (کیانی و همکاران، ۱۳۹٤).

۱۲-۲-۲ مدل‌های استقرار در محاسبات ابری

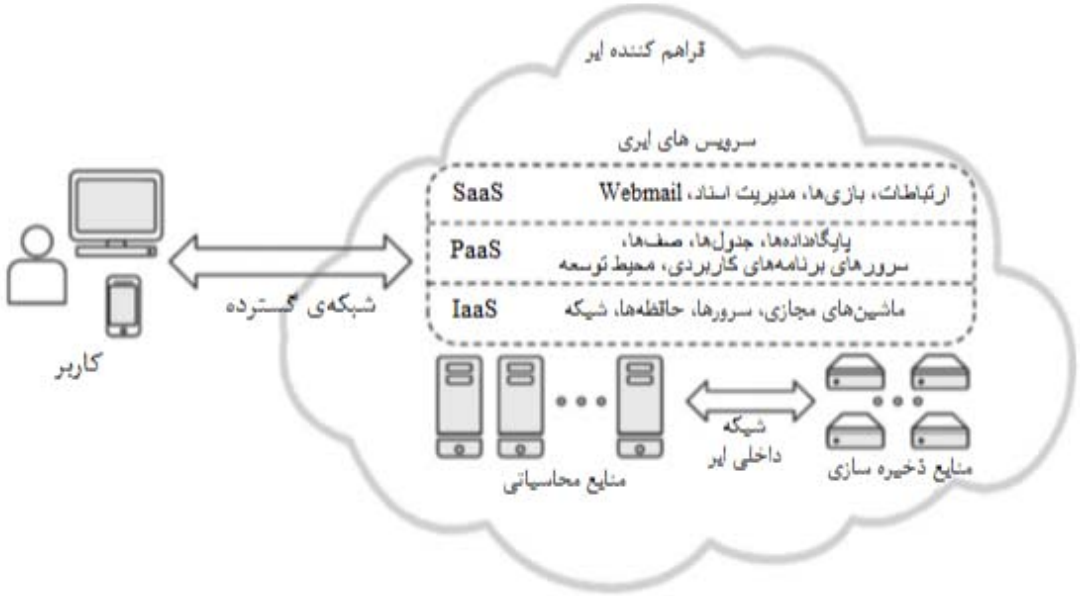
سرویس‌های محاسبات ابری مطابق سه مدل استقرار اصلی: عمومی، خصوصی و آمیخته ارائه می‌شوند.

یک فراهم کننده‌ی ابر عمومی، سرویس‌های خود را به عموم مردم از طریق اینترنت عرضه می‌کند. کاربران یک ابر عمومی، کنترل کمی بر روی تکنولوژی زیرساخت دارند و یا فاقد چنین کنترلی هستند. در این مدل، سرویس‌ها می‌توانند به صورت رایگان و یا بر طبق سیاست پرداخت به ازای مصرف ارائه شوند. فراهم-کنندگان عمومی اصلی از قبیل Google ، Amazon و Microsoft دارای مراکز داده‌ی اختصاصی بوده و مدیریت و عرضه‌ی سرویس های خود را بر روی این مراکز انجام می‌دهند.

یک فراهم کننده‌ی ابر خصوصی، عملیات و قابلیت‌هایی را به عنوان سرویس عرضه می‌کنند که بر روی شبکه‌ی اینترانت یک شرکت یا در یک مرکز داده‌ی دور دست میزبانی می‌شوند. به دلیل راه حل‌های امنیتی پیشرفته و کنترل داده‌ای که مدل ابر خصوصی ارائه می‌دهد و این راه حل‌ها در مدل ابر عمومی وجود ندارد اغلب شرکت‌های IT کوچک و متوسط مدل ابر خصوصی را ترجیح می‌دهند.

در نهایت، یک ابر آمیخته در واقع ترکیبی از دو یا چندین ابر (عمومی یا خصوصی) است که اجزاء مختلف باقی می‌مانند ولی به یکدیگر وصل شده‌اند. شرکت‌ها می‌توانند ابرهای اختصاصی خود را با استفاده از ابرهای خصوصی شرکت های همکار یا ابرهای عمومی گسترش دهند. به ویژه اینکه، با گسترش زیرساخت خصوصی با منابع ابر عمومی، سرویس دادن به بیشترین درخواست‌ها، سرویس‌دهی بهتر به درخواست کاربران و پیاده سازی استراتژی‌های با حداکثر قابلیت دسترسی را ممکن می‌سازد.

در شکل زیر معماری کلی یک ابر عمومی و اجزای اصلی آن به تصویر کشیده شده است (لی [17]و همکاران، ۲۰۱۰).



شکل ۲-۵ معماری کلی یک ابر عمومی(لی [18]و همکاران، ۲۰۱۰).

۲-۲-۱۳ امنیت و تهدیدها در رایانش ابری

موضوعات امنیتی و تهدیدهای موجود در رایانش ابری به طور ویژه بر روی سرویس عمومی، PaaS و IaaS متمرکز می‌باشد. علی رغم اینکه فراهم کنندگان سرویس ابر می‌توانند مزایایی را برای کاربران ارائه دهند، آسیب‌های امنیتی مسائل عمده‌ای را در محیط رایانش ابر ایجاد می‌کنند (پراساد[19] و همکاران، ۲۰۱۱).

کاربران تجهیزات شبکه‌ای و داده‌های اشتراکی آنلاین از کمبود بالقوه‌ی حریم خصوصی آگاهی کامل دارند (پوپا[20] و همکاران، ۲۰۱۰). از آنجایی که سرویس رایانش ابر در سطح اینترنت ایجاد می‌شود، هر گونه احتمال خطری که با اینترنت در ارتباط باشد می‌تواند بر سرویس رایانش ابر تاثیر بگذارد. منابع در سرویس رایانش

[17] Li
[18] Li
[19] Prasad
[20] Popa

ابر از طریق اینترنت در دسترس قرار می‌گیرند، به همین دلیل حتی اگر فراهم کنندگان سریس بر روی زیرساخت امنیت تمرکز کنند، هنوز داده‌ها از طریق شبکه که غیر ایمن است به کاربرها انتقال میابد. به همین علت، مشکلات امنیتی اینترنت با خطرات بیشتری بر روی رایانش ابر تاثیر می‌گذارد. تکنولوژی بکار رفته در رایانش ابری شبیه تکنولوژی بکار رفته در اینترنت است. تکنیک‌های پنهانی و پروتکل‌های ایمن‌سازی برای حفاظت از انتقال داده‌ها در رایانش ابر به اندازه کافی مناسب نمی‌باشد. لازم است که تهاجم‌های داده‌ای به رایانش ابری از طریق اینترنت توسط هکرها و مجرمان شناسایی شده و محیط رایانش ابری برای مشتریان ایمن و شخصی شود. سه فاکتور امنیتی در رابطه با تک ابرها عبارتند از: یکپارچگی داده‌ها، تهاجم داده‌ها و در دسترس بودن سرویس.

یکپارچگی داده‌ها: یکی از مهمترین مسائل مرتبط با آسیب‌های امنیتی داده‌های موجود در رایانش ابر، یکپارچگی داده‌هاست. داده‌های ذخیره شده در رایانش ابر ممکن است به هنگام انتقال و یا دریافت از فراهم کننده سرویس ذخیره‌سازی رایانش ابر دچار صدمه شوند (سوباشینی[۲۱] و همکاران، ۲۰۱۱).

تهاجم به داده‌ها: طبق نظر گارفینکل[۲۲]یکی دیگر از خطرات امنیتی که ممکن است برای یک فراهم کننده سرویس رایانش ابر مثل آمازن پیش بیاید، هک شدن رمز عبور یا تجاوز به داده‌ها است. اگر شخصی به رمز عبور حساب کاربری آمازن دسترسی پیدا کند، می‌تواند به تمامی منابع حساب کاربری دسترسی پیدا کند. بنابراین رمز عبور به سرقت رفته، به هکرها این امکان را می‌دهد که تمامی اطلاعات بر روی دستگاه مجازی را پاک کرده، تغییر داده و یا خدمات آن را غیر فعال کنند (آلزاین[۲۳] و همکاران، ۲۰۱۲).

دسترس بودن سرویس: یکی دیگر از دغدغه‌های اصلی در رایانش ابر، در دسترس بودن آنها است. شرکت-هایی که به دنبال محافظت از سرویس در قبال این خرابی‌ها می‌باشند می‌بایست از آن نسخه‌های پشتیبان تهیه کرده و یا از چند کننده سرویس بگیرند (سوباشینی و همکاران، ۲۰۱۱). موضوعات مهم امنیتی بر اساس ویژگی رایانش ابری در ذیل تشریح شده است.

مدیریت داده مشتری توسط فراهم کننده سرویس ابر: داده‌های مشتری توسط فراهم کننده سرویس ابر مدیریت می‌شود. در کل چگونگی مدیریت داده‌ها، وابسته به فراهم کننده سرویس می‌باشد. لذا، یکی از مشکلات مشتری عدم شناخت چگونگی کاربرد و مدیریت داده‌های خود می‌باشد. پس از اینکه تمام داده مشتری ذخیره

[21]Subashini
[22] Garfiinkel
[23]AlZain

و مدیریت شد، روشی جهت اطلاع مشتری از نسخه‌های فراهم کننده سرویس ابری وجود ندارد، بعلاوه انتقال و تغییر داده‌ها بدون اطلاع و اجازه‌ی مشتری نیز امکان پذیر است.

چند مالکیتی (منابع به اشتراک گذاشته شده): چند مالکیتی یک فناوری به اشتراک گذاری منابعی همانند CPU، حافظه، شبکه و ... به وسیله‌ی چندین مشتری می‌باشد. برخلاف مدل‌های رایانش پیشین که منابع به یک مشتری اختصاص داده می‌شد، رایانش ابری مبتنی بر یک مدل شغلی می‌باشد که منابع به وسیله چندین مشتری در سطح شبکه، میزبان و اپلیکیشن به اشتراک گذاشته می‌شود.

مجازی‌سازی: مجازی‌سازی یک فناوری به منظور یکپارچه‌سازی و واقعی‌سازی منطقی منابع فیزیکی در یک سرور فیزیکی توسط چندین سرور مجازی می‌باشد. به عبارت دیگر مجازی‌سازی اجازه می‌دهد تا یک مجموعه سخت‌افزار بیش از یک ماشین مجازی را میزبانی کند. این فناوری در بیشتر شرکت‌های بزرگ استفاده می‌شود و در تجارت‌های کوچک نیز روبه گسترش است.

تمرکز داده‌ها و خدمات: خدمات و داده‌های مشتری در منابع فیزیکی مشابهی مدیریت می‌شود. بدلیل اینکه در مجازی‌سازی و چند مالکیتی همانند سرویس‌های کاربردی اینترنت موجود، بیشترین داده و خدمات متمرکز شده، لذا آسیب وارده از یک منبع فیزیکی یا سرویس فراهم کننده ابر می‌تواند به طور تصاعدی افزایش یابد. در واقع هنگامی که خدمات و داده‌های کلیدی بسیاری از مشتریان متمرکز می‌شود، آنها به آسانی می‌توانند مورد هدف هک یا حمله‌ی DDOS قرار گیرند. یک هک و یا حمله‌یDDOS می‌تواند منجر به اختلال در سرویس تمام مشتریان و لذا آسیب در مقیاس بالا شود. اگر چنانچه داده‌ها ذخیره شده در سرور ابر سری و محرمانه باشد، به وسیله هک تمام داده‌های مشتریان می‌تواند نشت شود (مطهری و همکاران، ۱۳۹۳).

درحال حاضر یکی از مفیدترین راهکارهای حفظ امنیت در رایانش ابری، "مجازی‌سازی" است. مجازی سازی می‌تواند به عنوان یکی از مولفه های امنیتی مورد استفاده قرار گیرد، به عنوان مثال ماشین‌های مجازی که در اینترنت قرار دارند، در معرض بسیاری از فعل و انفعالاتی قرار دارند که فناوری مجازی سازی می‌تواند به فیلتر کردن آنه بپردازد.

به طور خلاصه می‌توان گفت هدف از محاسبات مجازی، بهبود استفاده از منابع به وسیله یک پلتفرم واحد، برای کاربران است، به بیان دیگر، مجازی سازی نظارت بر ماشین مجازی و همچنین امکان مدیریت سرویس دهنده‌ها و خوشه‌های پیچیده را آسانتر می‌کند. در فناوری مجازی‌سازی، از سیستم عامل، میان‌افزار (یا نرم‌افزار واسط) و برنامه کاربردی یک کپی عینی گرفته می‌شود و به صورت پیش ساخته در یک رایانه فیزیکی یا بخشی از یک سرویس دهنده قرار داده می‌شود، این کپی برداری به کاربران امکان می‌دهد تا بتوانند بیش

از یک بار از یک مجوز استفاده کنند و امکانات و منابع رایانش ابری در اختیار بگیرند. شکل زیر، لایه های ابر و سیستم حفاظت ابر را نمایش می‌دهد. در این شکل کاربر سرویس ابر می‌تواند از خدماتی چون نرم‌افزار به عنوان یک سرویس، پلتفرم به عنوان یک سرویس، زیرساخت به عنوان یک سرویس و همچنین از فضای ذخیره‌سازی، به عنوان یک سرویس استفاده نماید. تامین امنیت در ارائه سرویس‌های ابر به کاربر و همچنین در لایه های مجازی‌سازی، سخت افزار و سیستم عامل، بحثی ضروری می‌باشد (حق پرست خانکهدانی و همکاران، ۱۳۹٦).

شکل ۲-٦ لایه های ابر و سیستم حفاظت ابر(حق پرست خانکهدانی و همکاران، ۱۳۹٦).

۱٤-۲-۲ مدیریت منابع

امروزه انواع مختلفی از ابرها مورد استفاده قرار می‌گیرد. صرف نظر از نوع ابر، مدیریت منابع در ابر از اهمیت زیادی برخوردار است. بررسی‌های اخیر نشان می‌دهد که امنیت و کارایی دو اولویت اصلی برای مصرف کنندگان خدمات ابری هستند.

که کارایی بشدت تحت تاثیر شیوه مدیریت منابع قرار دارد و یکی از بزرگترین چالش‌ها در این حوزه، مدیریت منابع است. یک استراتژی کارآمد برای، مدیریت منابع باید باعث بهره وری بیشتر از سخت‌افزارهای توزیع شده، زیرساخت و همچنین دستیابی به کارایی بالاتر سیستم گردد موفقیت خدمات ابری به شدت به مدیریت موثر منابع مجازی، وابسته است. تخصیص منابع، فرآیند اختصاص منابع موجود به برنامه‌های در حال اجرا روی ابر است، اگر منابع به درستی تخصیص نیابد سرویس‌ها امکان اجرا نمی‌یابند و یا اجرایشان با مشکلاتی همراه می‌گردد. در رایانش ابری، تامین منابع نقش بسیار مهمی در کارایی فرآیندها و رضایت مشتریان دارد. به مجموعه فعالیت‌هایی که ارائه دهنده ابر برای به کارگیری و تخصیص منابع به برنامه‌ها انجام می‌دهد، به نحوی که نیاز برنامه‌ها تامین گردد، استراتژی تخصیص منابع گفته می‌شود (پاتل[۲۴] و همکاران، ۲۰۱۵).

۱۵-۲-۲ مشکلات مدیریت منابع

همان طور که گفته شد مدیریت منابع چالش‌هایی در محیط ابر به وجود آورده است. برخی از مشکلات همراه با چالش‌های آنها در ادامه بیان می‌شود.

فراهم‌سازی منابع: یکی از موضوعات مورد مطالعه در محاسبات ابری فراهم‌سازی منابع می‌باشد. فراهم سازی منابع یعنی فراهم‌سازی QOS[۲۵] بهتر و ایده آل‌تر در ساختارIaaS توسط تهیه کنندگان سرویس و منابع، برای کاربران و برنامه‌های کاربردی. این کار با استفاده از مکانیزم‌هایی مانند مکانیزم توازن بار و مکانیزم دسترسی سطح بالا انجام می‌شود. چالش‌هایی که در فراهم‌سازی منابع وجود دارد عبارتست از: چگونگی اختصاص برنامه‌ها به میزبان‌ها به گونه‌ای که SLA[۲۶] (مانند زمان پاسخ و توان عملیاتی) حفظ شود. چگونه مدل پیش‌بینی منابع را بهبود بخشیم به گونه‌ای که در نوسانات بارکاری، ابر قابلیت ارائه خدمات با کارایی و دسترس‌پذیری بالا داشته باشد. چگونگی طراحی سیستم‌هایی که از برنامه‌های کاربردی خوشه‌ای و چندسطحی پشتیبانی کنند. ارائه و گسترش مدل‌های پیش‌بینی برای تعیین و پیش‌بینی گلوگاه و همچنین برای غلبه بر مشکل زمان تاخیر راه اندازی ماشین مجازی.

[24] Patel
[25] Quality Of Service
[26] Service Level Agreement

تخصیص منابع: در این زمینه، موضوع تخصیص منابع برای اجرای محاسبات با حداقل زمان و هزینه می‌باشد. در تخصیص منابع در جستجوی منابعی هستیم که جهت اجرای Task، به آن اختصاص بدهیم. IaaS، منابع را مبتنی بر سیاست‌های تخصیص، به تقاضاها اختصاص می‌دهد.

چالش‌های مورد بحث در حیطه تخصیص منابع: چگونگی طراحی شمای تخصیص منابع که در محیط خوشه‌ای و مراکز داده قابل استفاده باشد. چگونه مکانیزمی را ایجاد کنیم که قادر به کنترل موازنه بین هزینه پیکربندی و حداکثر بهره وری ابر باشد. چه تکنیک‌هایی را می‌توان برای بازدهی انرژی به کار برد، مصرف انرژی را کاهش داد و آن را بهینه ساخت؟ طراحی استراتژی‌های مبتنی برSLA و حداقل کردن تخلف SLA با داشتن حداکثر مزیت و سود چگونه باید باشد (منوی[۲۷] و همکاران، ۲۰۱٤).

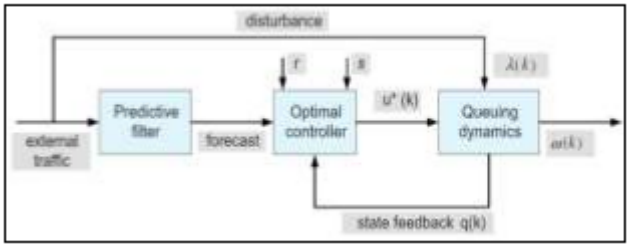
۱٦-۲-۲ مکانیزم‌های اصلی برای پیاده سازی روش‌های مدیریت منابع

در منابع کلاسیک سیستم خود تطبیق چنین تعریف شده است: "یک سیستم خود تطبیق رفتار خود را ارزیابی نموده و هنگامی که این رفتارها در جهت اهداف تعیین شده برای نرم‌افزار نباشند و یا کارایی بالاتری ممکن باشد، این رفتارها را تغییر می‌دهد." مفهوم رایانش خودمختار اولین بار توسط آقای پاول هورن مدیر ارشد تحقیقات شرکت IBM در یک سخنرانی برای یک آکادمی مهندسین بین المللی در دانشگاه هاروارد معرفی شد. در ادامه مکانیزم‌های اصلی برای پیاده‌سازی روش‌های مدیریت منابع را بیان می‌کنیم.

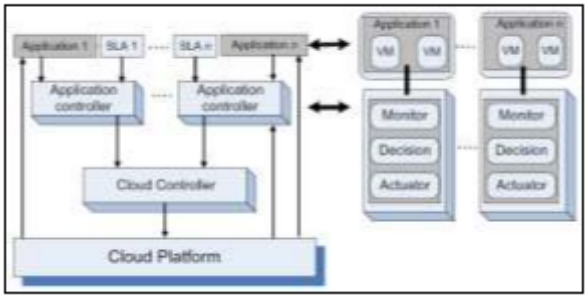
تئوری کنترل یکی از مکانیزم‌ها می‌باشد. تئوری کنترل از بازخورد جهت تضمین استحکام سیستم و پیش‌بینی رفتارهای ناپایدار استفاده می‌کند، اما فقط می‌تواند برای پیش‌بینی محلی انجام شود تا برای رفتارهای عمومی. تئوری کنترل برای طراحی مدیریت منابع خودکار برای دسته‌ای از برنامه‌های کاربردی، شامل مدیریت انرژی، زمانبندی Task تطبیق QOS در سرور وب و توازن بار، استفاده می‌شود. متد کنترل بازخورد کلاسیک در تمام حالات جهت تنظیم و کنترل پارامترهای عملیاتی کلیدی سیستم (براساس مقدار ورودی سیستم) به کار می‌رود. در این متد کنترل بازخورد یک زمان خطی، مدل سیستم ثابت و حلقه کنترل کننده بسته را شامل می‌شود. تکنیکی که سیستم خود مدیریت مبتنی بر مفاهیم تئوری کنترل دارند، امکان داشتن اهداف چندگانه QOS را دارد و می‌تواند در سروروب، سرور پایگاه داده، سیستم‌های موبایل و سرورهای برنامه‌های کاربردی توزیع شده یا منفرد بکار رود ساختار کنترلر در تصویر ۲-۷ مشخص است. کنترلر از یک بازخورد برای

[27] Manvi

ملاحظه و بررسی شرایط فعلی استفاده می‌کند، تا از این طریق درمورد آینده تخمین‌هایی بزند. تصویر ۲-۸ معماری کنترل دو سطحی را نشان می‌دهد. مدیریت منابع پویا مبتنی بر کنترلر دو سطحی، یکی برای فراهم کننده سرویس و دیگری برای برنامه های کاربردی، در تصویر مشخص است (مارینسو[۲۸]،۲۰۱۷).



شکل ۲-۷ ساختار کنترلر(مارینسو،۲۰۱۷).



شکل ۲-۸ معماری کنترل دو سطحی(مارینسو،۲۰۱۷).

۲-۳ پیشینه مطالعاتی

مطالعات داخلی

مرخانی نژاد غلامی در سال ۱۳۹۶ به بررسی انتقال چند رسانه‌ای در شبکه‌های مجازی‌سازی شده و شبکه‌های تعریف شده با نرم‌افزار پرداخت. رویکرد جدید شبکه‌های تعریف شده با نرم‌افزار، در واقع نوعی نگاه لایه لایه به انتقال داده در شبکه است که طراحی سلسله مراتبی براساس جداسازی اطلاعات کنترلی از سایر ترافیک جاری در شبکه امکان تصمیم گیری در مورد هدایت شبکه را ایجاد نموده است و مولفه‌های تصمیم

[28] Marinescu

گیرنده آن در بسیاری از موارد به عملکرد بهینه سخت افزار شبکه کمک می‌نماید. طبعا چنین دیدگاهی در خصوص بهبود پارامترهای انتقال محتوای چند رسانه ای چه بصورت پخش زنده و غیر از آن که دارای حجم بسیاری از ترافیک است کمک می‌نماید. ایشان در این پژوهش به مرور محتوا و پیشنهادات مقالات مرجع در خصوص بکارگیری SDN و NFV برای حمل ترافیک چند رسانه‌ای در شبکه پرداخته‌اند. همچنین قصد ایشان در این پژوهش مرور مطالب و نهایت جمع‌بندی روش‌ها بوده است که مقدمه‌ای برای بکارگیری و توسعه راهکارهای تعریف شبکه با نرم‌افزار و توابع مجازی‌سازی شبکه بدست آمده می‌باشد.

محمدزاده دوگاهه و همکاران در سال ۱۳۹۵ به بررسی ارایه روشی مبتنی برترکیب محاسبات ابری و SDN به جهت دفاع در برابر حملات DDOS پرداختند. محاسبات ابری تبدیل به روند فعلی مدل سرویس IT شرکت‌ها شده است که پردازش مقیاس پذیر و کارآمد از لحاظ هزینه را با خود به همراه دارد. در عین حال، شبکه‌های تعریف شده به روی نرم‌افزار (SDN) به دلیل انعطاف در سرویس مدیریت شبکه و کاهش هزینه عملیاتی، محبوبیت قابل توجهی را در میان شبکه‌های شرکتی بدست آورده است. ظهور شبکه‌های تعریف شده به روی نرم‌افزار (SDN)خط مشی جدیدی را جهت دفاع در برابر حملات DDoS فراهم آورده است. در این پژهش، ایشان در ابتدا حملات DDoS را از دیدگاه معماری شبکه مدل‌سازی می‌کنند. سپس، یک مکانیزم شبکه امنیتی تعریف شده به روی نرم‌افزار (SDSNM) را جهت حذف یا محدود کردن شرایط ضروری خلاصه شده از این مدل، پیشنهاد می‌دهند. مکانیزم SDSNM به طور عمده در شبکه‌هایSDN مرزی و همچنین شبکه‌هایی که زیر ساختار شبکه اصلی IP را به ارث برده‌اند، پیاده‌سازی می‌شود. برای پیگیری هدف بوسیله معماری جدید، یک سیستم تشخیص حمله مبتنی بر مدل گرافیکی را پیشنهاد داده‌اند. در صورت استفاده از سیاست‌گذاری‌های کنترل دستیابی سختگیرانه در SDSNM بهبود یافته(ISDSNM) ، حملات DDoS نمی‌توانند به اجرا درآیند. در عوض، زمانی که از سیاست‌های کنترل دستیابی ضعیف استفاده شود، مکان و موقعیت مهاجم و میزبان‌ها در بات نت به طور دقیق و به سرعت شناسایی و مشخص می‌شود.

شاه‌سنایی و همکاران در سال ۱۳۹۵ به بررسی شبکه‌های نرم‌افزار محور SDN با پروتکل OpenFlowپرداختند. شبکه تعریف شده نرم‌افزاری (SDN) به عنوان یک تغییر بزرگ جهت سهولت و بهبود مدیریت شبکه ایجاد شده است با توجه به باز بودن و استانداردSDN در این پژوهش محققان توابع شبکه، ابتکار جدید و پروتکل‌هایی را جهت ساده‌سازی و انعطاف‌پذیری شبکه طراحی کرده‌اند پروتکل طراحی شده OpenFlow مفهوم SDN را برای کنترل کننده‌ها و سوییچ‌ها فراهم می‌کند. همچنین در این پژوهش

شبکه‌های نرم افزار محور SDN می‌توانند هوشمندی و امنیت شبکه را افزایش دهد. بخش کنترل داده از سخت افزار (سوییچ‌ها و مسیریاب‌ها) به لایه‌ی نرم‌افزار مجازی شبکه انتقال داده شده است که باعث کنترل دقیق شبکه می‌گردد، همچنین ایشان در این فکرند که در آینده نزدیک این شبکه جایگزین لایه‌ی TCP/IP گردد. هربست از شبکه SDN طبق دستور مدیر شبکه جابه‌جا می‌گردد. مهمترین نتایج حاصل از این پژوهش، استفاده از مجازی‌سازی و کاهش هزینه شبکه در شبکه نرم‌افزار محور خواهد بود.

فروزنده سامانی و همکاران در سال ۱۳۹۵ به بررسی کارایی کنترلر Open Flow به منظورافزایش کیفیت سرویس در شبکه‌های مبتنی بر نرم‌افزار(SDN) پرداختند. شبکه‌های SDN یکی از روش‌های پیاده‌سازی شبکه براساس سخت‌افزارهای کمتر و روش‌های نرم‌افزاری مورد توجه قرار گرفته است. در شبکه‌های SDN قسمت کنترل از قسمت ارسال یا انتقال داده مجزا شده و به صورت برنامه‌ریزی طراحی و سازی می‌گردند. یکی از مسائل اصلی در این نوع شبکه‌ها کنترلر و عملکرد کنترلرها برای کنترل سخت‌افزار می‌باشد. کنترلر نه تنها می‌تواند به عنوان یک سیستم کنترلر برای سخت افزار عمل کند بلکه می‌تواند مدیریت یکپارچه و بهینه شبکه و نقش یک سیستم عامل را ایفا نماید. در واقع عملکرد اصلی این نوع شبکه‌ها را مدیریت می‌نماید. در این پژوهش مفاهیم مربوط به شبکه SDN و عملکردهای کنترلر مورد بحث و بررسی قرار گرفته است. همچنین هدف این پژوهش بیان چالش‌ها و تحقیقات مربوط به کنترلرها می‌باشد.

اسمعیل پور و همکاران در سال ۱۳۹۵ به بررسی تخصیص منابع در محاسبات ابری برای بهره‌وری انرژی با استفاده از توسعه الگوریتم ژنتیک والگوریتم سیاه چاله پرداخته است. در این تحقیق به ارایه یک الگوریتم موثر برای تخصیص منابع در محاسبات ابری، در جهت کاهش مصرف انرژی پرداخته شده است، روش پیشنهادی مبتنی بر ترکیب الگوریتم ژنتیک و الگوریتم سیاه چاله بوده که همواره بر سرعت تخصیص و کیفیت تخصیص در جهت کاهش زمان و انرژی تاکید دارد. برای تست و کارایی الگوریتم چند مجموعه داده تست تهیه شده استو الگوریتم پیشنهادی با الگوریتم ژنتیک و الگوریتم بهینه سازی ذرات، بر اساس معیارهای زمان اتمام پردازش، انرژی مصرفی، پایداری، زمان اجرا، مورد ارزیابی قرار گرفته‌اند، نتایج شبیه‌سازی نشان داده است روش پیشنهادی همواره نسبت به الگوریتم مورد مقایسه دارای کارایی بهتری از نظر معیارهای مقایسه بوده است و توانسته انرژی مصرفی منابع را بهبود دهد.

رمضانپور کلابنی و همکاران در سال ۱۳۹٤ به بررسی تخصیص بهینه منابع در محاسبات ابری با استفاده از اتوماتای یادگیر سلولی پرداخته است. در این تحقیق الگوریتمی با استفاده از اتوماتی یادگیر سلولی ارائه شده است که اتوماتی یادگیر مستقر در یک سلول آن، قادر خواهد بود که محیط‌های غیر قطعی و پیچیده که چندین

تصمیم گیرنده (همسایگان) در آن وجود دارد، فعالیت نموده و با تشخیص عمل عادلانه در محیط، به آن هم گرا گردد. این الگوریتم برای مسئله تخصیص منبع بروش مزایده ای/مناقصه دیگر محیط محاسبات ابری بررسی شده است.

سلطانی نژآد و همکاران در سال ۱۳۹۳ به بررسی معماری کنترل کننده شبکه‌های تعریف شده با نرم‌افزار (SDN) پرداختند. در دنیای امروز شاهد ایجاد علاقه شدیدی به شبکه‌های تعریف شده با نرم‌افزار (SDN) هستیم تا این که درباره تکنولوژی‌های مختلفی که SDN را اجرا می‌کند مانند پروتکل OpenFlow بحث های فراوانی صورت گرفته است اما برای کنترل کننده‌های SDN کمتر پرداخته شده است و زمانی که کاربران قصد مقایسه بین این رده جدید از روش‌های طراحی را دارند دچار سردرگمی می‌شوند و مطمئن نیستند که کدام یک از روش‌ها بهترین انتخاب پیش روی آنها است. هدف ایشان از این پژوهش بررسی شرایطی است که باید در هنگام انتخاب کنترل کننده SDN در نظر گرفته شود.

سالاروند در سال ۱۳۹۲ به بررسی شبکه‌های نرم‌افزار محور(SDN) پرداخت. در این پژوهش به نسل جدیدی از شبکه‌ها با تعاریف نرم‌افزاری (SDN) پرداخته می‌شود که با استفاده از لایه‌های مجازی، سویچ‌های مجازی،کنترلر مرکزی،استانداردهای ارتباطی وAPI های سطح بالا سعی می‌کنند برخی از کارهای کنترلی و مدیریتی سوییچ‌ها و روترهای شبکه را در لایه‌های بالاتر به صورت نرم‌افزاری انجام دهند. هدف ایشان از این پژوهش این است که SDNوابستگی به سخت‌افزار را کاهش داده و قابلیت‌های نرم‌افزاری و هوشمندی شبکه را افزایش می‌دهد. سال‌ها است که صنعت شبکه رنگ و بوی تحول تازه‌ای را ندیده و بعد از پروتکل TCP/IPو انتقال و کنترل اطلاعات توسط سوییچ‌ها و روترهای سخت‌افزاری، استاندارد جدیدی معرفی نشده است. سه دهه است که شرکت‌های سازنده سخت‌افزار حاکمان بلامنازع این صنعت هستند و هرساله مدل‌های جدید محصولات خود را با ویژگی‌های تکراری «سرعت بیشتر» یا «امنیت بیشتر» روزانه بازار می‌کنند و شرکت‌های کوچک و بزرگ هم ناگزیر به خرید و استفاده این جعبه‌های دربسته مرموز هستند.

مطالعات خارجی

عبدالقادر[۲۹] و همکاران در سال ۲۰۱۸ به بررسی SecSDN ابرشکست دادن آسیب‌پذیری‌ها از طریق شبکه‌های نرم‌افزار امن پرداخته شده است. هدف این مطالعه طراحی یک محیط ابر SDN با امنیت یکپارچه است که

[29] Abdulqadder

می‌تواند مقاومت در برابر سه نوع حمله مختلف داشته باشد: بارگذاری جدول جریان، اشباع کنترل کننده و حملات بیزانس. یک امضای دیجیتالی جدید با هش کردن امن هرج و مرج برای تأیید هویت کاربر استفاده می‌شود و به دنبال آن یک پروتکل مسیریابی چند طبقه‌ای بهینه‌سازی ذرات بهبود یافته PSO برای بهبود کیفیت خدمات مورد استفاده قرار می‌گیرد. کنترل کننده‌ها به وسیله یکپارچه‌سازی یک الگوریتم ژنتیک پیشرفته با یک الگوریتم جستجوی تغییر یافته فکوس به سوئیچ‌ها اختصاص داده می‌شوند. شناسایی جریان مخرب شامل تجزیه و تحلیل تپه ساخته شده از ویژگی‌های استخراج شده از بسته است. ایشانSecSDN ابر پیشنهاد شده در شبیه‌ساز OMNeT ++را اجرا کردند و عملکرد آن را از لحاظ از دست دادن بسته، تاخیر دادن تولید، زمان تاخیر و پهنای باند ارزیابی کردند.

گارگیس[۳۰] و همکاران در سال ۲۰۱۷ به بررسی پشتیبانی از ابر رایانه محاسبات با استفاده از شبکه‌های تعریف شده توسط نرم‌افزار پرداخته شده است. در این تحقیق، ایشان یک حل مسئله محاسبات ابری بصری را ارائه می‌دهند با تعریف یک مجموعه معماری، محاسبات و مصرف C ۳ که با پشتیبانی محاسبات مه در لبه شبکه با استفاده از شبکه تعریف شده توسط نرم‌افزار SDN می‌باشد. همچنین استفاده از SDN برای تقاضای محاسبه تخلیه با استفاده از تراکم اجتناب از فرمان ترافیک برای افزایش کیفیت کاربر از راه دور از تجربه در یک برنامه منطقه‌ای در مقیاس را نشان می‌دهند. بهینه‌سازی محاسبات مه در لبه شبکه با استفاده از پردازش ابری هسته برای مدیریت تجزیه و تحلیل‌های تصویری باعث کاهش تاخیر، تراکم و افزایش کارایی می‌شود.

لیانگ[۳۱] و همکاران در سال ۲۰۱۷ به بررسی یک مجتمع معماری برای شبکه‌های دسترسی رادیویی و رادیویی مجازی با رایانه محاسبات پرداخته شده است. در این پژوهش، ایشان یک معماری یکپارچه برای شبکه‌های دسترسی به رادیو تعبیه شده و مجازی با محاسبات مه را ارائه می‌دهند. ایشان یک نرم‌افزار را به عنوان یک سرویس OpenPipe پیشنهاد می‌کنند، که مجازی سازی در سطح شبکه را امکان پذیر می‌سازد. برای ادغام SDN ها و مجازی‌سازی شبکه با محاسبات مه، یک مدل کنترل ترکیبی با دو سطح کنترل سلسله مراتبی اتخاذ می‌کنند که در آن کنترل کننده SDN سطح بالایی را تشکیل می‌دهد و کنترل‌کننده‌های محلی سطح پایین را تشکیل می‌دهند. موارد استفاده معمول از معماری شبکه پیشنهاد شده از طریق مشاهدات آزمایشگاهی معتبر است.

[30] Gargees
[31] Liang

گای[۳۲] و همکاران در سال ۲۰۱۷ به بررسی مدیریت منابع در سیستم‌های جامع فیزیکی پایدار با استفاده از محاسبات ابری ناهمگن پرداختند. رشد قابل توجهی از محاسبات توزیع شده با استفاده از محاسبات ناهمگن باعث گسترش گسترده‌ای در سیستم‌های فیزیکی سایبر شده است. ترکیب CPS با محاسبات ابری ناهمگن روشی جایگزین برای افزایش پایداری سیستم است. با این حال، اجرای مدیریت منابع در سیستم‌های ابر هنوز با چند چالش مواجه است، از جمله محدودیت‌های ظرفیت وب سرور و وظایف کار در ابر ناهمگن است. تقاضای خدمات ناپایدار اغلب موجب تاخیر در خدمات می‌شود که رقابت پذیری شرکت‌ها را مختل می‌کند. ایشان در این پژوهش به مسئله تخصیص وظیفه در ابرهای ناهمگون پرداخته‌اند، که به عنوان یک مشکل NP-hard ثابت شده است. رویکرد پیشنهادی مدل کارآیی بهینه‌سازی هوشمند مبتنی بر ابر (SCOW) است که از ظرفیت‌های پیش‌بینی کننده ابر استفاده می‌کند و عوامل پایدار را برای اختصاص وظایف به ابرهای ناهمگن مورد توجه قرار می‌دهند. برای رسیدن به هدف بهینه‌سازی، ایشان چند الگوریتم پیشنهاد می‌کنند که شامل الگوریتم کمینه‌سازی حجم کار (WRM)، الگوریتم تخصیص هوشمند (STA) و الگوریتم ترسیم نقشه برداری (TMA) می‌باشد. ارزیابی تجربی ایشان عملکرد طرح پیشنهادی را بررسی کرده است.

نگوین[۳۳]و همکاران در سال ۲۰۱٦ به بررسی معماری شبکه همراه - LTE مبتنی بر ارتباط جمعی پرداختند. شبکه‌سازی تعریف‌شده نرم‌افزار(SDN) ویژگی‌های جداسازی صفحه کنترل و صفحه اطلاعات، یک شبکه قابل‌برنامه‌ریزی و مجازی‌سازی است، که اشتراک زیرساخت شبکه و" نرم افزار " عملکردهای شبکه را ممکن می‌سازد. اخیرا، بسیاری از تحقیقات انجام‌شده تلاش کرده‌اند که شبکه تلفن همراه سنتی را با استفاده از دو مورد از این مفاهیم طراحی مجدد کنند تا با چالش‌هایی که اپراتورهای تلفن همراه با آن مواجه هستند، مانند رشد سریع ترافیک همراه و خدمات جدید. در این تحقیق، ابتدا مروری برSDN ، مجازی‌سازی شبکه، و مجازی سازی عملکرد شبکه ارایه شده است و سپس ساختار شبکه تلفن همراه فعلی و همچنین چالش‌ها و مسائل آن را توصیف شده است. با تحلیل و دسته‌بندی طیف وسیعی از آخرین کاره‌ای تحقیقاتی بر SDN و مجازی‌سازی در شبکه‌های تلفن همراهLTE ، ایشان یک معماری عمومی برای SDN و مجازی‌سازی در شبکه‌های تلفن همراه ارایه می‌دهند و سپس یک طبقه‌بندی سلسله مراتبی را براساس سطوح مختلف شبکه حامل پیشنهاد می‌کنند. ایشان همچنین تحلیل عمیق در مورد تغییرات مربوط به عملیات پروتکل و معماری

[32] Gai
[33] Nguyen

در زمان اتخاذ SDN و مجازی سازی در شبکه‌های تلفن همراه را ارایه می‌دهند. به علاوه، ایشان موارد استفاده خاص و برنامه‌های کاربردی که از SDVMN سود می‌برند را فهرست کرده‌اند.

آگراوال[۳۴] و همکاران در سال ۲۰۱۶ به بررسی حفاظت از دستگاه های[۳۵] IOT با استفاده از SDN و محاسبات لبه پرداختند. در دیدگاه فناوری در حال حاضر شاهد افزایش چشم‌گیری در ارتباط دستگاه‌های ناهمگون و کنترل آنها از راه دور هستیم. یکی از آخرین فن‌آوری‌هایی که این مفهوم را قادر می‌سازد "IoT" است. از آنجا که دستگاه‌هایی که در حال اتصال هستند، می‌توانند به طور مستقیم زندگی انسان را کنترل کنند، امنیت این دستگاه ها اهمیت می‌یابد. به ویژه هنگامی که IoT "شبکه‌های ناهمگون" را به "شبکه‌های فوق العاده ناهمگن" دستگاه‌های هوشمند تبدیل می‌کند، امنیت آن بسیار پیچیده می‌شود. SDN یک پارادایم شبکه هوشمند است که می‌تواند به سرعت و به طور خودکار دستگاه‌های شبکه را مجددا تنظیم کند، ترافیک مجدد و درخواست احراز هویت و قوانین دسترسی می‌تواند راهی برای امنیت بیشتر و مکانیسم‌های کنترل دسترسی را باز کند. در این پژوهش تلاش شده است تا یک روش ارائه امنیت به IoT با استفاده از SDN (شبکه تعریف شده نرم‌افزار) و محاسبات لبه ایجاد شود.

[34] Aggarwal
[35] internet of things

خلاصه فصل دوم

در این پژوهش مدیریت منابع درedge Computing با استفاده از SDN مورد بررسی قرار گرفته است. بنابراین در این فصل از پژوهش به بیان مبانی نظری که شامل بررسی SDN و محاسبات ابری و مدیریت منابع می‌باشد و همچنین پیشینه مطالعاتی پرداخته‌ایم.

منابع

۱.اسمعیل پور، فاطمه. بزرگی راد، یاسر. ۱۳۹۵. تخصیص منابع در محاسبات ابری برای بهره وری انرژی با استفاده از توسعه الگوریتم ژنتیک والگوریتم سیاه چاله . چهارمین کنفرانس بین المللی مهندسی برق و کامپیوتر

۲. حسامی، یونس. ۱۳۹۳. موارد مقیاس پذیری در معماری SDN. کنفرانس ملی علوم مهندسی، ایده های نو (۸)

۳. حسین زاده، محمد، بجانی، صادق.۱۳۹٤ . بررسی معیارهای ارزیابی کارایی محیط های محاسبات ابری. علوم رایانشی . ۳۳.

٤. حسینی تشنیزی، مهرنوش سادات، برکتین، بهرنگ. ۱۳۹٤. بررسی جامع شبکه مبتنی بر نرم افزار در پردازش ابری.سومین کنفرانس بین المللی پژوهشهای کاربردی در مهندسی کامپیوتر و فن آوری اطلاعات

۵. حق پرست خانکهدانی، حمیده، منافی، سید امیر رضا، خورشید سوار، علی، ۱۳۹٦، بررسی امنیت رایانش ابری در شبکه های نرم افزار محور، چهاردهمین اجلاس سراسری فناوری رسانه

٦. دارابی نژاد، بابک، میرعابدینی، سید جواد. ۱۳۹۲. بررسی شبکه تعریف شده با نرم افزار. همایش ملی مهندسی کامپیوتر و توسعه پایدار با محوریت شبکه های کامپیوتری، مدل سازی و امنیت سیستمها

۷. درویشی، محمد، صالح اصفهانی، محمود، ۱۳۹٤، بررسی شبکه‌های مبتنی بر نرم‌افزار، دانشگاه جامع امام حسین (ع)

۸.رمضانپور کلابنی، مرضیه. حاج سید جوادی، سید حمید. مکی آبادی، بهادر. ۱۳۹٤. تخصیص بهینه منابع در محاسبات ابری با استفاده از اتوماتای یادگیر سلولی. نخستین کنفرانس بین المللی فناوری اطلاعات

۹. سلطانی نژآد، فاطمه، علائی، محمد. ۱۳۹۳. معماری کنترل کننده شبکه‌های تعریف شده با نرم‌افزار (SDN).دومین همایش ملی پژوهش های کاربردی در علوم کامپیوتر و فناوری اطلاعات

۱۰. شاه سنایی، رضا، سلطان آقایی کوپایی، محمدرضا. ۱۳۹۵. بررسی شبکه های نرم افزار محور SDN با پروتکل .OpenFlow اولین همایش ملی فناوری اطلاعات، ارتباطات و محاسبات نرم

۱۱. طالقانی، مجید، ۱۳۹٤، معرفی شبکه‌های نرم‌افزار محور (SDN)، ارشد شبکه

۱۲. فرشته مطهری، سعید روحانی، احد زارع رواسان. ۱۳۹۳. معرفی رایانش ابری: امنیت و تهدیدات. اولین همایش ملی پژوهش های مهندسی رایانه

۱۳. فروزنده سامانی، آرزو، خیام باشی، محمدرضا. ۱۳۹۵. بررسی کارایی کنترلر Open Flow به منظورافزایش کیفیت سرویس در شبکه های مبتنی بر نرم افزار .(SDN) کنفرانس بین المللی مهندسی کامپیوتر و فناوری اطلاعات

۱٤. قلی زاده، پریا، توحیدی، محسن، میرعلایی موردی، مریم. ۱۳۹۳. راهبردهای هوشمندانه جهت مدیریت ریسک در رایانش ابری. کنفرانس بین المللی توسعه و تعالی کسب و کار

۱۵. کیانی، شهلا ، عظیمی، نوشین. ۱۳۹٤. رایانش ابری و معماری لایه های آن. سومین همایش ملی کامپیوتر

۱٦. محمدزاده دوگاهه، مریم، اکباتانی فرد، غلامحسین. ۱۳۹۵. ارایه روشی مبتنی برترکیب محاسبات ابری و SDN به جهت دفاع در برابر حملات . DDOS کنفرانس بین المللی مهندسی و علوم کامپیوتر

۱۷. مرخانی نژاد غلامی، مسعود. ۱۳۹٦. انتقال چند رسانه ای در شبکه های مجازی سازی شده و شبکه های تعریف شده با نرم افزار . چهارمین کنفرانس بین المللی تحقیقات دانش بنیان در مهندسی کامپیوتر و فناوری اطلاعات

۱۸. هاشمی، مسعودرضا، اسمعیلی مرندی، فریبا. ۱۳۹۵. مدیریت کیفیت سرویس در شبکه های مبتنی بر نرم افزار.دولتی – وزارت علوم، تحقیقات، و فناوری – دانشگاه صنعتی اصفهان – دانشکده کامپیوتر و فناوری اطلاعات

19. Abdulqadder, I. H., Zou, D., Aziz, I. T., Yuan, B., & Li, W. (2018). SecSDN-Cloud: Defeating Vulnerable Attacks through Secure Software-Defined Networks. IEEE Access.
20. Aggarwal, C., & Srivastava, K. (2016, October). Securing IOT devices using SDN and edge computing. In Next Generation Computing Technologies (NGCT), 2016 2nd International Conference on (pp. 877-882). IEEE.
21. AlZain, M. A., Pardede, E., Soh, B., & Thom, J. A. (2012, January). Cloud computing security: from single to multi-clouds. In System Science (HICSS), 2012 45th Hawaii International Conference on (pp. 5490-5499). IEEE.
22. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

23. Fundation, O. N. (2012). Software-defined networking: The new norm for networks. ONF White Paper, 2, 2-6.
24. Gai, K., Qiu, M., Zhao, H., & Sun, X. (2017). Resource management in sustainable cyber-physical systems using heterogeneous cloud computing. IEEE Transactions on Sustainable Computing.
25. Gargees, R., Morago, B., Pelapur, R., Chemodanov, D., Calyam, P., Oraibi, Z., ... & Palaniappan, K. (2017). Incident-supporting visual cloud computing utilizing software-defined networking. IEEE Transactions on Circuits and Systems for Video Technology, 27(1), 182-197.
26. Li, A., Yang, X., Kandula, S., & Zhang, M. (2010, November). CloudCmp: comparing public cloud providers. In Proceedings of the 10th ACM SIGCOMM conference on Internet measurement (pp. 1-14). ACM.
27. Liang, K., Zhao, L., Chu, X., & Chen, H. H. (2017). An integrated architecture for software defined and virtualized radio access networks with fog computing. IEEE Network, 31(1), 80-87.
28. Manvi, S. S., & Shyam, G. K. (2014). Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey. Journal of Network and Computer Applications, 41, 424-440.
29. Marinescu, D. C. (2017). Cloud computing: theory and practice. Morgan Kaufmann.
30. Mogul, J. C., & Congdon, P. (2012, August). Hey, you darned counters!: get off my ASIC!. In Proceedings of the first workshop on Hot topics in software defined networks (pp. 25-30). ACM.
31. Nguyen, V. G., Do, T. X., & Kim, Y. (2016). SDN and virtualization-based LTE mobile network architectures: A comprehensive survey. Wireless Personal Communications, 86(3), 1401-1438.
32. Patel, R., Patel, H., & Patel, S. (2015). EFFICIENT RESOURCE ALLOCATION IN CLOUD COMPUTING. International Journal for Technological Research in Engineering, 2(7).
33. Popa, R. A., Lorch, J. R., Molnar, D., Wang, H. J., & Zhuang, L. (2011, June). Enabling Security in Cloud Storage SLAs with CloudProof. In USENIX Annual Technical Conference (Vol. 242, p. 31).
34. Prasad, P., Ojha, B., Shahi, R. R., Lal, R., Vaish, A., & Goel, U. (2011, March). 3 dimensional security in cloud computing. In Computer Research and Development (ICCRD), 2011 3rd International Conference on (Vol. 3, pp. 198-201). IEEE.
35. Puthal, D., Sahoo, B. P. S., Mishra, S., & Swain, S. (2015, January). Cloud computing features, issues, and challenges: a big picture. In Computational Intelligence and Networks (CINE), 2015 International Conference on (pp. 116-123). IEEE.
36. Sarrar, N., Uhlig, S., Feldmann, A., Sherwood, R., & Huang, X. (2012). Leveraging Zipf's law for traffic offloading. ACM SIGCOMM Computer Communication Review, 42(1), 16-22.

37. Sasikala, P. (2013). Research challenges and potential green technological applications in cloud computing. International Journal of Cloud Computing, 2(1), 1-19.
38. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.
39. Tselios, C., Papageorgiou, C., Birkos, K., Politis, I., & Dagiuklas, T. (2012). Real-time communications in autonomic networks: system implementation and performance evaluation. Journal of Computer Networks and Communications, 2012.
40. Yu, M., Rexford, J., Freedman, M. J., & Wang, J. (2010). Scalable flow-based networking with DIFANE. ACM SIGCOMM Computer Communication Review, 40(4), 351-362.