علوم رایانش و فناوری اطلاعات
نشریه علمی انجمن کامپیوتر ایران
مجلد ۱۷، شماره ۱، ۱۳۹۸
صفحات ۲۷-۱۶
مقاله عادی

امنیت در پردازش لبه‌ای: مروری بر چالش‌ها و راه‌کارهای موجود

پریسا حسنی‌زاده[۱]، سیاوش بیات‌سرمدی[۲*]

*نویسنده مسئول، دریافت: ۹۷/۰۴/۲۰، بازنگری: ۹۷/۱۱/۲۷، پذیرش: ۹۸/۰۱/۱۴

[۱] دانش‌آموخته کارشناسی ارشد، مهندسی کامپیوتر، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف، تهران، ایران

[۲] استادیار، مهندسی کامپیوتر، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف ، تهران، ایران

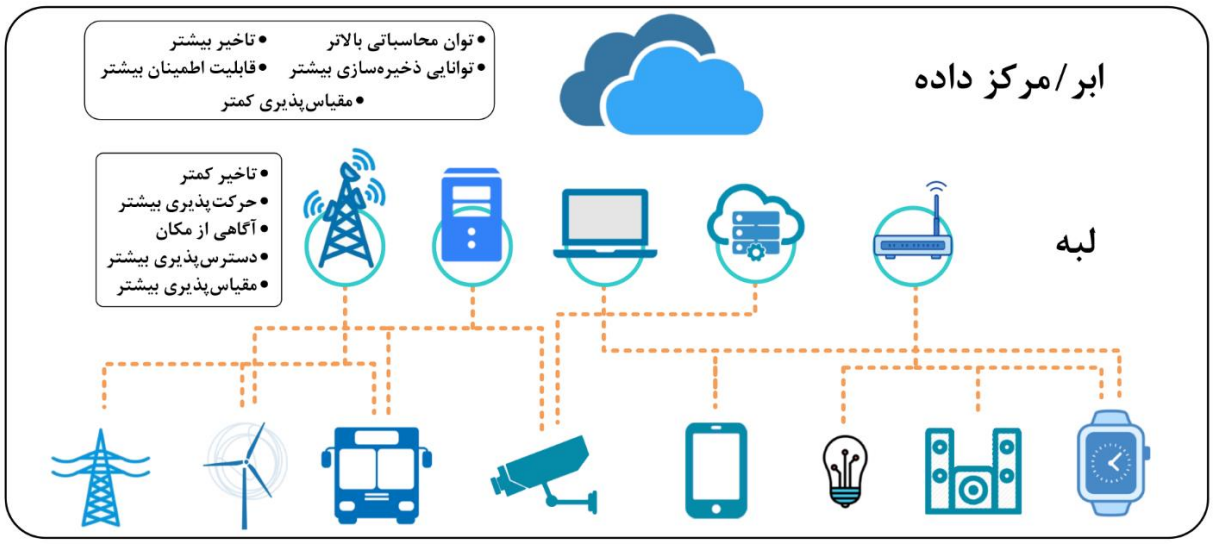
چکیده

در دنیای امروز پردازش ابری در گسترش کاربردهای اینترنت اشیا سهم قابل توجهی دارد. برخورداری از منابع نامحدود و پشتیبانی از دستگاه‌های ناهمگون ویژگی‌هایی از پردازش ابری بوده که برای اینترنت اشیا بسیار سودمند هستند. با گسترش کاربردهای اینترنت اشیا، ویژگی‌هایی چون تاخیر زمان پاسخ و پهنای باند شبکه بیش از پیش اهمیت پیدا کرده‌اند. از جمله این کاربردها می‌توان به واقعیت مجازی/افزوده و بازی‌های برخط گروهی اشاره کرد. معماری کنونی پردازش ابری به طور کامل پاسخ‌گوی این نیازها (تاخیر و پهنای باند مورد نیاز) نیست. برای رفع این محدودیت‌ها، رویکرد جدیدی به نام پردازش لبه‌ای مطرح شده است. در این رویکرد یک لایه از دستگاه‌ها با قابلیت ذخیره‌سازی، مدیریت و پردازش اطلاعات، بین مرکز داده و دستگاه‌های کاربر قرار می‌گیرد. این لایه قبل از ارسال داده به ابر مرکزی، قسمتی یا تمام فرآیند پردازش داده را انجام می‌دهد. به دلیل نزدیکی این لایه به کاربر، در صورتی که پردازش در این لایه انجام شود، به طور میانگین تاخیر انتقال و پردازش داده کاهش می‌یابد. از سویی دیگر، ترافیک شبکه گسترده نیز به دلیل ارسال داده پس از پردازش اولیه به سمت ابر مرکزی، کاهش پیدا خواهد کرد. علی‌رغم مزایا و بهبودهای پردازش لبه‌ای نسبت به پردازش ابری، این رویکرد به دلیل ماهیت توزیع‌شده و عواملی همچون پشتیبانی از کاربران متحرک با چالش‌های فراوانی روبه‌رو است. از جمله‌ی این چالش‌ها می‌توان به مجازی‌سازی، مدیریت منابع، برون‌سپاری وظایف، امنیت، حریم خصوصی و توزیع گره‌های پردازشی اشاره کرد. در این پژوهش علاوه بر معرفی پردازش لبه‌ای، معماری، ویژگی‌ها و کاربردهای این رویکرد بررسی می‌شوند. در ادامه، به چالش‌های امنیتی پردازش لبه‌ای و راه‌حل‌های موجود برای پاسخ‌گویی به این مسائل پرداخته شده‌است.

کلمات کلیدی: اینترنت اشیا، پردازش لبه‌ای، پردازش مه، تکه‌ابر، پردازش ابری متحرک، پردازش لبه‌ای متحرک، امنیت و حریم خصوصی

۱- مقدمه

در دهه‌های اخیر پردازش ابری به دلیل ویژگی‌هایی چون انعطاف‌پذیری بالا و هزینه کم جایگزین مراکز داده قدیم شده و طیف کاربران بسیاری از جمله سازمان‌ها و صاحبان کسب و کارهای بزرگ را جذب نموده است [۱]. هم‌چنین استفاده از پردازش ابری در اینترنت اشیا، سهم به‌سزایی در گسترش این فناوری داشته است. از جمله ویژگی‌های پردازش ابری می‌توان به اجازه دسترسی پویا به منابع پردازشی نامحدود، پشتیبانی از ناهمگونی[۱] (دستگاه‌ها و سیستم‌عامل‌های گوناگون) [۲]، زیرساخت مستحکم[۲] و قابل اعتماد [۲] و [۳] و مدیریت آسان‌تر زیرساخت و خدمات به دلیل متمرکز بودن [۴] اشاره کرد. غلبه بر محدود بودن منابع، دسترسی به منابع معتبر داده و هم‌کاری هم‌زمان‌ساز چند کاربر (کاربردهایی مانند نرم‌افزارهای ویدیو کنفرانس‌های برخط هم‌چون skype) از جمله ویژگی‌های پردازش ابری برای کاربران متحرک هستند که در مقاله [۵] به آن اشاره شده‌است. با گسترش اینترنت اشیا، کاربردهای جدیدی مانند واقعیت مجازی[۳] و افزوده[۴]، بازی‌های برخط گروهی و پردازش برخط ویدیو به وجود



شکل ۱ - ساختار کلی رویکرد پردازش لبه‌ای

آمده‌اند که دارای نیازمندی‌هایی مانند تاخیر پایین دریافت پاسخ از ابر و پهنای باند بالا درشبکه هستند [۶]. برای رسیدن به این ویژگی‌ها، انتقال بخشی از وظایف ابر مرکزی به لبه‌ی شبکه و نزدیک به دستگاه‌های کاربران در رویکردهای جدید مطرح شده‌است. این راه‌کار جدید، پردازش لبه‌ای[۵] نام دارد که با رویکردهای مختلف به آن پرداخته شده‌است. در واقع انگیزه اصلی برای رفتن به سمت پردازش لبه‌ای، بالا رفتن حجم و سرعت تولید داده توسط دستگاه های اینترنت اشیا است. در شکل ۱ نمایی کلی از ساختار پردازش لبه‌ای قابل مشاهده است.

در ابتدای معرفی چارچوب‌های پردازش لبه‌ای باید یادآور شد که عبارت *پردازش مه*[۶]، عبارت فراگیرتری نسبت به عبارت پردازش لبه‌ای در مقالات موجود در این زمینه است. هرچند تا به امروز استانداردی جهت به کاربردن این دو مفهوم برای چارچوبی مشخص وجود ندارد و نویسندگان مقالات با توجه به برداشت‌های خود، از این دو عبارت استفاده می‌نمایند. برای مثال در مقالات [۷] و [۸] از عبارت پردازش مه و در پژوهش [۹] از عبارت *رویکرد لبه‌ای*[۷] برای معرفی مفهوم کلی پردازش لبه‌ای استفاده شده و پردازش مه به عنوان یکی از چارچوب‌های رویکرد لبه‌ای معرفی شده‌است. مقالاتی نظیر [۱۰] وجود دارند که این دو مفهوم را معادل دانسته‌اند. از سوی دیگر، مقالاتی مانند [۱۱] تفاوت پردازش مه و پردازش لبه‌ای را بررسی نموده‌اند. هم‌چنین در مرجع [۱۲] مروری جامع پیرامون رویکردهای مختلف پردازش لبه‌ای و مقایسه‌ی آن‌ها با هم صورت گرفته است.

در این نوشتار، ما برای اشاره به این راه‌کار، از عبارت پردازش لبه‌ای استفاده می‌کنیم. منظور از لبه همان لبه‌ی شبکه است. با این تفاسیر تکه‌ابر[۸] [۱۳]، پردازش مِه [۱۴]، پردازش لبه‌ای متحرک[۹] [۱۵] و پردازش ابری متحرک[۱۰] [۱۶] چارچوب‌های رایج در پردازش لبه‌ای هستند. در ادامه به بررسی هر یک از این چارچوب‌ها می‌پردازیم.

تکه‌ابر دسته‌ای از سامانه‌های پردازشی با قابلیت اطمینان بالا و منابع پردازشی قدرتمند هستند که از طریق یک ارتباط دائمی قابل اطمینان و پرسرعت به شبکه متصل می‌شوند. ارائه‌ی خدمت به دستگاه‌های اینترنت اشیا و متحرک در شبکه‌ی محلی، هدف اصلی تکه‌ابر است. این رویکرد توسط گروه OEC[۱۱] متشکل از شرکت‌هایی چون اینتل، گوگل، تی-موبایل و دانشگاه کارنگی‌ملون توسعه داده و استانداردسازی می‌شود[۱۷]. تکه‌ابر دارای چهار ویژگی اصلی است: ۱) هر تکه‌ابر کاملاً مستقل از دیگران و توسط خود آن مدیریت می شود، ۲) دارای توان محاسباتی نسبتا بالا است، ۳) تاخیر انتها به انتهای کمی دارد و ۴) بر مبنای فناوری استاندارد پردازش ابری ساخته شده‌است.

در سال ۲۰۱۲، Bonomi و همکارانش از شرکت سیسکو برای اولین بار از عبارت *پردازش مه* در مقاله [۱۴] استفاده کردند. بنابر تعریف نویسندگان این مقاله، پردازش مه زیرساخت پردازش ابری را تا لبه‌ی شبکه گسترش می‌دهد. با این روش می‌توان کاربردها و خدمات جدیدی ارائه داد که تاکنون در پردازش ابری ممکن نبودند. تمرکز پردازش مه در این مقاله بیشتر بر روی افزایش قابلیت مقیاس پذیری زیرساخت است. پردازش مه دارای ویژگی‌هایی نظیر تاخیر کم و آگاهی از مکان[۱۲]، توزیع جغرافیایی گسترده، تحرک، تعداد بسیار گره‌های پردازشی، نقش غالب شبکه بی‌سیم و دسترسی به آن (نقش اساسی شبکه نسل۵)، امکان اجرای برنامه‌های بی‌درنگ[۱۳]، مدیریت جریان‌های فراوانی از داده‌ها و پشتیبانی از ناهمگونی است[۱۴].

پردازش لبه‌ای متحرک، چارچوب دیگری از پردازش لبه‌ای است که در یکی از گروه‌های ETSI[۱۴] با همین نام استانداردسازی شده‌است. این رویکرد محیط خدمات پردازشی ابر را در لبه‌ی شبکه‌ی تلفن همراه و در نزدیکی مشترکین، در ناحیه زیر پوشش آنتن‌های فرستنده-گیرنده شبکه تلفن همراه[۱۵] فراهم می‌کند. هدف این رویکرد، کاهش تاخیر پاسخ، تجربه بهتر کاربر، اطمینان از عملکرد کارآمد شبکه و بهبود خدمت‌رسانی است [۱۵]. مزیت استفاده از پردازش ابری در لبه‌ی شبکه‌های متحرک مانند نسل۵، شامل تاخیر کم، پهنای باند وسیع، دسترسی به اطلاعات شبکه رادیویی و آگاهی از مکان است[۹].

چارچوب *پردازش ابری متحرک*، پردازش ابری را با محیط پردازشی خدمات تلفن همراه تجمیع کرده تا بر محدودیت‌های دستگاه‌های متحرک نظیر تلفن همراه از نظر کارایی، محیط اجرا و امنیت غلبه نماید. ویژگی‌هایی نظیر طول عمر باتری، قابلیت ذخیره‌سازی، مقیاس‌پذیری، قابلیت اطمینان و حفظ حریم خصوصی در این دستگاه‌ها محدودکننده هستند. در تعریف جدیدتری از پردازش ابری متحرک، وظایف می‌توانند علاوه بر ابر مرکزی به یک مرکز داده یا کارگزار منتقل شوند که در لبه‌ی شبکه واقع شده‌است[۹]. در جدول ۱، مقایسه‌ای اجمالی بین رویکردهای مختلف پردازش لبه‌ای با پردازش ابری ارائه شده است. بر اساس دیدگاه نویسندگان مقاله یاد شده تکه‌ابر در دسته پردازش ابری متحرک قرار می‌گیرد.

دسته‌بندی‌های مختلفی از چالش‌های امنیتی در پردازش لبه‌ای ارائه شده‌است. این دسته‌بندی‌ها دارای اشتراک‌ها و تفاوت‌هایی هستند. یکی از مهم‌ترین دست‌آوردهای این نوشتار، ارائه‌ی یک دسته‌بندی متفاوت در حوزه‌ی چالش‌های امنیتی رویکرد پردازش لبه‌ای است به نحوی که کاستی‌های سایر دسته‌بندی‌ها را پوشش دهد. هم‌چنین بررسی جامع پیرامون راه‌کارهای ارائه شده برای حل چالش

جدول ۱ – مقایسه ویژگی‌های رویکردهای مختلف در پردازش لبه‌ای [۹]

	پردازش لبه‌ای متحرک	*پردازش مه*	*پردازش ابری متحرک*	*پردازش ابری*
مالکیت	شرکت‌های مخابراتی	نهادهای خصوصی، اشخاص		نهادهای خصوصی
محل گسترش فناوری	لبه‌ی شبکه	لبه و نزدیک لبه‌ی شبکه	لبه‌ی شبکه، دستگاه‌ها	هسته شبکه
سخت‌افزار	خدمت‌گزارهای ناهمگون		خدمت‌گزارها، دستگاه‌های کاربران	خدمت‌گزارها
خدمت	مجازی‌سازی		مجازی‌سازی، غیره	مجازی‌سازی
معماری شبکه	چند لایه، توزیع‌شده، غیر متمرکز			متمرکز
تحرک‌پذیری	بله			خیر
تاخیر/ نوسان تاخیر	کم			متوسط
آگاهی محلی	بله			خیر
دسترس‌پذیری	بالا			
مقیاس‌پذیری	بالا			متوسط

امنیت و حریم خصوصی، دست‌آورد دیگر این مقاله است. در ادامه این مقاله، معماری پردازش لبه‌ای، ویژگی‌ها و کاربردهای آن در بخش دوم بررسی می‌شوند. بخش سوم به معرفی تهدیدها و چالش‌های امنیتی موجود در پردازش لبه‌ای می‌پردازد. راه‌حل‌های موجود برای حل این چالش‌ها در بخش چهارم بیان خواهد شد و در انتها نتیجه‌گیری از پژوهش حاضر ارائه می‌شود.

۲- معماری پردازش لبه‌ای و مزایای آن

پردازش لبه‌ای رویکردی جدید در پردازش ابری، با ویژگی‌هایی مانند کاهش تاخیر برنامه‌های تعاملی، کاهش ازدحام شبکه و افزایش مقیاس‌پذیری زیرساخت است. همه‌ی دستگاه‌های موجود اعم از کارگزارهای کوچک، مسیریاب‌های شبکه، مدخل‌ها[۱۶]، نقاط دسترسی[۱۷]، آنتن‌های فرستنده-گیرنده شبکه تلفن همراه و حتی تلفن‌های همراه می‌توانند یک گره پردازشی در رویکرد پردازش لبه‌ای باشند. در رویکرد پردازش لبه‌ای، حجم چشمگیری از منابع پردازشی و ذخیره‌سازی در نزدیکی دستگاه‌های کاربر و حسگرهای محیطی قرار می‌گیرند [۴]. به طور کلی پردازش لبه‌ای بیشتر از آنکه جایگزین پردازش ابری باشد، تلاشی برای گسترش و توانمندسازی آن است.

۲-۱- معماری

قبل از پیدایش مفهوم پردازش لبه‌ای در اینترنت اشیا، در اکثر کاربردهای مبتنی بر ابر مرکزی، برنامه به دو بخش کاربر و کارگزار تقسیم می‌گردید [۱۸]. به عبارت دیگر، تنها دو سطح پردازشی با قدرت متفاوت در معماری سنتی پردازش ابری وجود داشت. دستگاه‌های انتهایی واقع در سطح اول، با توجه به توان پردازشی خود قسمتی از اجرای برنامه را بر عهده می‌گرفتند و ابر مرکزی با توان ذخیره‌سازی و پردازشی بالا، در سطح دوم قرار داشت.

مشکل اصلی این معماری در بسیاری از کاربردها، توان پردازشی ناکافی دستگاه‌های سطح اول و هزینه بالای دسترسی به ابر از جهت تاخیر و پهنای باند مورد نیاز بود. با ظهور رویکرد پردازش لبه‌ای و ایجاد سطح دیگری از قدرت پردازشی در بین دستگاه‌های کاربر و ابر مرکزی، این نیازها تا حد مناسبی پاسخ داده شدند. از این رو، در بسیاری از کاربردها مانند اینترنت اشیا به استفاده از این معماری جدید روی آورده شد[۳،۱۹،۲۰].

در نگاه اول، پردازش لبه‌ای معماری سه سطحی را به ذهن متواتر می‌کند. با این حال، در بسیاری از مقالاتی که همچنان بر معماری پردازش ابری استوار هستند، از مفهوم پردازش لبه‌ای یاد می‌شود [۲۱]. بنابر فرض این مقالات، دستگاه های انتهایی تنها وظیفه تولید داده را برعهده نداشته و در صورت امکان پردازش داده‌ی تولید شده را نیز انجام می‌دهند. بنابراین می توان آنها را به عنوان گره پردازش در نظر گرفت. با توجه به افزایش توان پردازشی دستگاه‌های تلفن همراه، این دیدگاه منطقی و عملی به نظر می‌رسد. لازم به ذکر است که این معماری دو سطحی با در نظر گرفتن دستگاه‌های متحرک مانند تلفن همراه در سطح اول آن، همان پردازش ابری متحرک با دیدگاه قدیمی است. از بین این گونه مقالات می‌توان به مقاله [۲۱] اشاره کرد که در آن برای حل چالش پارک خودرو، بدون نیاز به زیرساخت‌های اضافی، راه‌کاری نرم‌افزاری ارائه داده است. در این پژوهش، تلفن همراه رانندگان از خیابان‌ها فیلم گرفته و پس از پردازش اطلاعات بدست آمده، نتیجه را به همراه افزونه‌های مکانی و زمانی، برای ابر می‌فرستد. با تجمیع داده‌های پردازش‌شده از تلفن همراه کاربران مختلف به وسیله ابر، نزدیک‌ترین جای پارک به دیگر کاربران پیشنهاد می‌شود.

پردازش در مسیر[۱۸] [۱۸] مفهومی گسترش‌یافته از پردازش لبه‌ای است که معماری آن چند سطحی است. در این مفهوم، به جای وجود تنها یک کارگزار ابری، کارگزاران متعددی برای خدمت‌رسانی آماده هستند که در فواصل جغرافیایی متفاوتی نسبت به کاربر نهایی قرار دارند. هر چه این کارگزاران به کاربران نهایی نزدیک‌تر باشند، قدرت پردازشی و تاخیر کمتری دارند. برنامه‌سازان با توجه به محتویات و ماهیت برنامه می‌توانند تصمیم بگیرند که برنامه با هم‌کاری کدام کارگزار اجرا شود. امکان اجرا کردن بخش‌های مختلف یک برنامه‌ی واحد به صورت مشارکتی بر روی کارگزاران مختلف نیز وجود دارد. با بهره‌مندی از این معماری، در کاربردهایی با هدف کاهش تاخیر، برنامه بر روی نزدیک‌ترین کارگزاری قرار می‌گیرد که قدرت پردازشی لازم را دارد. در مقابل، در کاربردهایی با هدف افزایش کارایی، دورترین کارگزاری برای اجرای برنامه انتخاب می‌شود که تاخیرش بیش از آستانه تحمل تاخیر سامانه نیست [۱۸].

۲-۲- مزایای استفاده از پردازش لبه‌ای

پردازش لبه‌ای می‌تواند ویژگی‌هایی نظیر زمان اجرا، تاخیر ارتباط و ازدحام کمتر در شبکه و از طرف دیگر قدرت پردازشی بالاتر را به قابلیت‌های پردازش ابری اضافه کند. در این بخش ویژگی‌های اصلی پردازش لبه‌ای با توجه به کاربردهای مختلف معرفی می‌شوند.

۲-۲-۱- بهبود ترافیک شبکه گسترده[۱۹]

با استفاده از پردازش لبه‌ای، در بسیاری از کاربردها می‌توان حجم داده‌ی ارسالی به ابر مرکزی را کاهش داد. در این راستا می‌توان به پژوهش [۲۲] اشاره کرد که با فرض روشن بودن وای‌فای[۲۰] تلفن همراه درصد بالایی از کاربران شبکه، راه‌کاری برای بررسی تغییرات جمعیت در مکان‌های عمومی ارائه کرده است. فرآیند جمع‌آوری اطلاعات توسط سامانه‌ای در وسایل حمل و نقل عمومی مانند اتوبوس و قطار شهری انجام می‌گیرد. این سامانه با اندازه‌گیری شدت سیگنال وای‌فای دریافتی از تلفن‌های همراه به صورت محلی تشخیص می‌دهد که صاحب

این تلفن همراه داخل وسیله‌ی حمل و نقل عمومی بوده یا در کنار آن در حال تردد است. در حالی که اگر تشخیص مکان صاحب تلفن همراه بر عهده ابر مرکزی قرار می‌گرفت، نیاز به ارسال حجم داده‌ی بزرگی به ابر- مانند وضعیت سیگنال‌های وای‌فای تمامی کاربران موجود در محدوده - به وجود می‌آمد. این انتقال داده وسیع می‌تواند دسترسی به شبکه را برای کاربران حاضر در آن مکان مختل کند. در مقاله [۲۱] راه‌کاری برای هدایت خودروها به نزدیک‌ترین جای خالی برای پارک با استفاده از پردازش لبه‌ای ارائه شده است. در این روش با تحلیل جریان ویدیوی تولیدی از دوربین تلفن همراه توسط خود، از ارسال داده از طریق شبکه‌ی گسترده به ابر مرکزی جلوگیری می‌شود. در نهایت اطلاعات استخراج‌شده از پردازش ویدیو، به همراه زمان و مکان برای ابر مرکزی فرستاده می‌شود. مقاله [۲۳] راه‌کاری برای تشخیص راننده خودرو با استفاده از پردازش لبه‌ای ارائه داده است. در این روش با تحلیل اطلاعات حسگرهای نصب شده در خودرو و با به‌کارگیری الگوریتم‌های یادگیری ماشین، می‌توان در طی چند ثانیه هویت راننده را تشخیص داد. این راه‌کار می‌تواند برای سازمان‌هایی چون پلیس و یا شرکت‌های هم‌چون بیمه قابل استفاده باشد. به دلیل تعداد فراوان خودروها و در نتیجه حجم بالای داده‌ی تولید شده توسط آنها، استفاده صرف از پردازش ابری، خدمت‌رسانی را با مشکل مواجه می‌کند. در مقابل با استفاده از پردازش لبه‌ای، می‌توان داده را به صورت محلی پردازش و از افزایش ترافیک شبکه جلوگیری کرد.

۲-۲-۲- بهبود خدمت‌رسانی در همه نقاط

به طور معمول، ارتباطات بین نقاط دور افتاده و شبکه‌ی جهانی اینترنت از کیفیت بالایی برخوردار نیست. به همین دلیل، ارسال داده‌های بزرگ و یا داده با نرخ بالا، می‌تواند مدت زمان بسیاری به طول انجامد که این تاخیر در بسیاری از کاربردها قابل قبول نیست. مقاله [۲۴] با استفاده از مزیت پردازش لبه‌ای، راه‌کاری برای حل این چالش ارائه کرده است. در این مقاله، روشی برای برقراری ارتباط امن و مورد اعتماد بین دستگاه‌های مختلف در نقاط دور افتاده و در شبکه‌ی محلی ارائه شده است. نکته حائز اهمیت در مورد این راه‌حل، نقش کاربر هر دستگاه و تکه‌ابر در روند برقراری ارتباط شبکه‌ی گسترده است. اطلاعات لازم برای برقراری یک ارتباط امن و مورد اعتماد تنها در صورتی منتقل می‌گردد که دو کاربر در فاصله‌ی نزدیک به هم قرار داشته باشند و بدون واسطه بتوانند یکدیگر را تصدیق نمایند [۲۴].

۲-۲-۳- کاهش تاخیر ارتباط

در برخی کاربردها، برنامه‌ها نیاز به پردازش داده با تاخیر کم دارند. در نتیجه، به دلیل تاخیر فراوان انتقال داده به ابر مرکزی، امکان انجام تمام پردازش توسط ابر وجود ندارد. بازی‌های برخط گروهی، خودروهای فاقد راننده یا خودران، کاربردهای واقعیت افزوده، واقعیت مجازی و کنترل‌کننده‌های صنعتی بی‌درنگ از جمله‌ی این کاربردها هستند. دستیاران شناختی پوشیدنی[۲۱] کاربردی است که مقاله [۲۵] به ارزیابی تجربی تاثیر استفاده از پردازش لبه‌ای در عملکرد آن پرداخته است. با توجه به حجم بالای پردازش مورد نیاز این کاربرد، استفاده از رویکرد لبه، کاهش زمان پاسخ را به همراه داشته است.

۲-۲-۴- مقیاس‌پذیری

در مقایسه با زیرساخت وسیع، متمرکز و پرهزینه مراکز داده برای پردازش ابری، شبکه پردازش لبه‌ای و گره‌های آن می‌توانند سریع‌تر پیکربندی شده و در چرخه استفاده قرار بگیرند. ویژگی مقیاس‌پذیری علاوه بر قابلیت گسترش و توزیع سریع شبکه، می‌تواند راه‌حل مناسبی برای محدودیت‌هایی از جمله انتقال داده با حجم بالا باشد. برای مثال اگر ۱۲۰۰۰ کاربر به صورت هم‌زمان بخواهند جریانی از ویدیو با کیفیت ۱۰۸۰ نقطه[۲۲] را به یک مرکز داده بفرستند، نیاز به یک گذرگاه با سرعت ۱۰۰ گیگا بیت بر ثانیه دارند [۴]. این موضوع نشان می‌دهد که معماری پردازش ابری با محدودیت مقیاس‌پذیری همراه دارد. بسیاری از بسترهای جدید ارائه شده در معماری لبه بر این ویژگی تاکید دارند و آن را راه‌حل مناسبی برای بسیاری از محدودیت‌های شبکه می‌دانند [۲۰].

۲-۲-۵- خدمات مکان محور

در پردازش لبه‌ای خدمات می‌توانند بر اساس مکان کاربر، برای او شخصی‌سازی شوند. هم‌چنین با آگاهی از مکان می‌توان کیفیت خدمات ارائه شده به کاربران را بهبود بخشید [۲۶]. ویژگی‌هایی مانند توزیع جغرافیایی گره‌های لبه، تحرک کاربران، آگاهی از مکان و پشتیبانی از تعاملات با تاخیر کم، بستر پردازش لبه‌ای را در مقایسه با پردازش ابری به بستری مناسب‌تر برای ارائه‌ی خدمات مبتنی بر مکان تبدیل کرده است [۱۴]. برای مثال در خودروهای متصل[۲۳]، با وجود تعامل خودروها با یکدیگر و با وسایل کنترل ترافیک مانند چراغ راهنمایی و رانندگی و آگاهی از شرایط جوی می‌توان از وقوع تصادفات رانندگی با سربار محاسباتی کم، جلوگیری نمود.

۳- تهدیدها در پردازش لبه‌ای

پردازش لبه‌ای علی‌رغم برخورداری از ویژگی‌های مطلوبی چون تاخیر کمتر پاسخ و نیاز به پهنای باند کم‌تر (یا همان ایجاد ترافیک کمتر) در شبکه نسبت به پردازش ابری، با چالش‌هایی نیز روبه‌رو است. از جمله‌ی مهم‌ترین این چالش‌ها می‌توان به مجازی‌سازی، زیرساخت پیاده‌سازی، تخصیص منابع و برون‌سپاری وظایف، توزیع گره‌های پردازشی، تحرک کاربران، حفظ امنیت و حریم خصوصی اشاره کرد. هدف از این بخش مقاله، بررسی چالش‌های امنیتی موجود در پردازش لبه‌ای است. داشتن یک محیط پردازشی ناهمگون و در حالت کلی یک چارچوب با پشتیبانی از عناصر ناهمگون به عنوان گره‌های پردازشی، برقراری امنیت و حفظ حریم خصوصی را مشکل‌تر می‌نماید [۱۲]زیرا با پیاده‌سازی الگوریتمی واحد بر روی دستگاه‌های ناهمگون با مشخصاتی متفاوت مانند فناوری‌های متفاوت برقراری ارتباط مانند فیبرنوری، بی‌سیم و اترنت، استفاده از رابط‌های برنامه‌نویسی[۲۴] با استانداردهای متفاوت و اجرای برنامه‌های مختلف بر روی آن‌ها، تمام حالت‌های حمله را نمی‌توان پوشش داد [۲۷]. کاربران برای بهره بردن از مزیت‌های پردازش لبه‌ای باید بتوانند به آن اعتماد کنند [۹]. به همین دلیل، بدون داشتن راه‌کار مناسب برای حل چالش امنیت در پردازش لبه‌ای، تمام مزیت‌های آن با ابهام روبه‌رو خواهد شد.

از آنجا که پردازش لبه‌ای در بستر اینترنت اشیا پیشنهاد شده‌است و ریشه در پردازش ابری دارد، چالش‌های امنیتی مطرح شده در پردازش ابری به پردازش لبه‌ای نیز منتقل شده‌اند. در مقاله [۱۰] که جزو اولین مقالات در زمینه‌ی پردازش لبه‌ای و چالش‌های امنیتی آن است، مشکلات امنیت و حریم خصوصی به صورت زیر ارائه شده است:

۱- اعتماد و احراز هویت (کاربران و گره‌های لبه) ۲- امنیت شبکه ۳- ذخیره‌ی امن داده ۴- پردازش امن و خصوصی داده ۵- حریم خصوصی ۶- کنترل دسترسی ۷- تشخیص نفوذ[۲۵].

در این نوشتار یک دسته‌بندی از حملات معرفی شده در مقالات [۲۷]، [۹] و [۲۸] صورت گرفته‌است. در جدول ۲، مقایسه بین تهدیدهای بررسی شده در این مقالات ارائه شده است. مراجع [۲۸] و [۲۷] به ترتیب تهدیدها را در چارچوب پردازش ابری متحرک و چارچوب پردازش مه مورد بررسی قرار داده‌اند. اما مرجع [۹] تهدیدها را در تمام چارچوب‌های پردازش لبه‌ای مورد بررسی قرار داده است. همان‌طور که در این جدول دیده می‌شود، تهدیدهای معرفی‌شده دارای اشتراکات (مانند مشکلات مربوط به مجازی‌سازی) و تفاوت‌هایی (مانند افراز و برون‌سپاری

جدول ۲- دسته‌بندی تهدیدها در چارچوب‌های مختلف پردازش لبه‌ای

[۲۷]- رویکرد پردازش مه	[۲۸]- رویکرد پردازش ابری متحرک	[۹]- تجمیع رویکردهای پردازش لبه‌ای
مشکلات مجازی‌سازی	امنیت مجازی‌سازی	زیرساخت مجازی‌سازی
مشکلات امنیتی وب	-	
مشکلات ارتباطی داخلی و خارجی	-	زیرساخت شبکه
مشکلات امنیتی شبکه بی‌سیم	-	
مشکلات مربوط به امنیت داده	امنیت داده / حریم خصوصی داده	-
حفاظت در برابر بدافزارها	امنیت برنامه‌های کاربردی ابری متحرک	-
-	امنیت دستگاه‌های متحرک	دستگاه‌های کاربران
-	افراز و برون‌سپاری داده	-
-	حریم هویت۲۶	-
-	-	زیرساخت هسته
-	-	مراکز داده لبه

داده) هستند. در این نوشتار برای ارائه دسته‌بندی جامع از همه‌ی تهدیدها در تمام چارچوب‌های پردازش لبه‌ای، با دقیق شدن در مفهوم هر تهدید به جمع‌بندی نهایی پرداخته شده است. در ادامه هر کدام از تهدیدها به صورت خلاصه توضیح داده می‌شوند. در ادامه هر کدام از تهدیدها به صورت خلاصه توضیح داده می‌شوند.

مجازی‌سازی: با به کارگیری فناوری مجازی‌سازی می‌توان از پردازش ابری به صورت مقیاس‌پذیرتر و کاراتر بهره گرفت [۲۸] زیرا خدمت‌دهی به کاربران بیشتری در مدت زمان مشابه انجام می‌پذیرد. مجازی‌سازی در سطح سخت‌افزار و یا نرم‌افزار امکان‌پذیر است. انتخاب سطح مجازی‌سازی بستگی به منابع اجرایی هر گره پردازشی دارد. اگر گره دارای منابع اجرایی فراوانی باشد، مانند تکه‌ابر، در آن صورت از مجازی‌سازی در سطح سخت‌افزار یا ماشین مجازی استفاده می‌شود. اما برای گره‌های پردازشی کوچک مانند نقاط دسترسی، از مجازی‌سازی در سطح نرم‌افزار استفاده می‌شود. در [۲۰] مقایسه‌ی جامعی بین کارایی روش‌های مختلف مجازی برای استفاده در پردازش لبه‌ای صورت گرفته است. در هر کارگزار پردازش ابری و یا گره لبه، از مجازی‌سازی برای ارائه خدمت به کاربران گوناگون استفاده می‌شود. در این مدل به ازای هر کاربر یک ماشین مجازی (در روش نرم‌افزاری، یک ظرف[۲۷]) در نظر گرفته می‌شود که وظایف مورد درخواست آن کاربر را انجام می‌دهد. یک لایه به نام ابر دیده‌بان[۲۸] مدیریت ماشین‌های مجازی را برعهده دارد. یکی از حمله‌های موجود در مجازی‌سازی، حمله انکار خدمت[۲۹] است. در این حمله یک ماشین مجازی، منابع فراوان از میزبانی را در اختیار می‌گیرد که بر روی آن در حال اجرا است. در نتیجه سایر ماشین‌های مجازی نمی‌توانند برنامه‌های خود را اجرا کنند. سوء استفاده از منابع[۳۰] یکی دیگر از حملات این دسته است که در آن یک ماشین مجازی با استفاده از بدافزارها می‌تواند به دستگاه‌هایی دسترسی پیدا کند که به گره پردازشی لبه متصل هستند. حمله‌ی دیگر، نشت حریم خصوصی[۳۱] است. منظور از نشت حریم خصوصی شفاف نبودن استاندارد ماشین‌های مجازی در حال اجرا بر روی گره پردازشی لبه و یا کارگزار است. برای مثال نمی‌دانیم که ماشین مجازی مورد نظر از چه واسطهایی برای برنامه‌نویسی[۳۲] استفاده می‌کند و این واسطها به چه میزان آسیب‌پذیر هستند. افزایش امتیاز[۳۳] تهدید دیگری است که در آن یک ماشین مجازی خراب‌کار با بهره‌گیری از نقاط آسیب‌پذیر میزبان، به دیگر ماشین‌های مجازی حمله می‌کند. دستکاری[۳۴] ماشین مجازی حمله‌ای است که در آن میزبان تحت کنترل شخص متخاصم، به ماشین‌های مجازی در حال اجرا بر روی خود، برای مثال با اجرای بدافزار بر روی آن‌ها، حمله می‌کند. دیگر تهدیدهای این دسته در جدول ۳ نام برده شده‌اند.

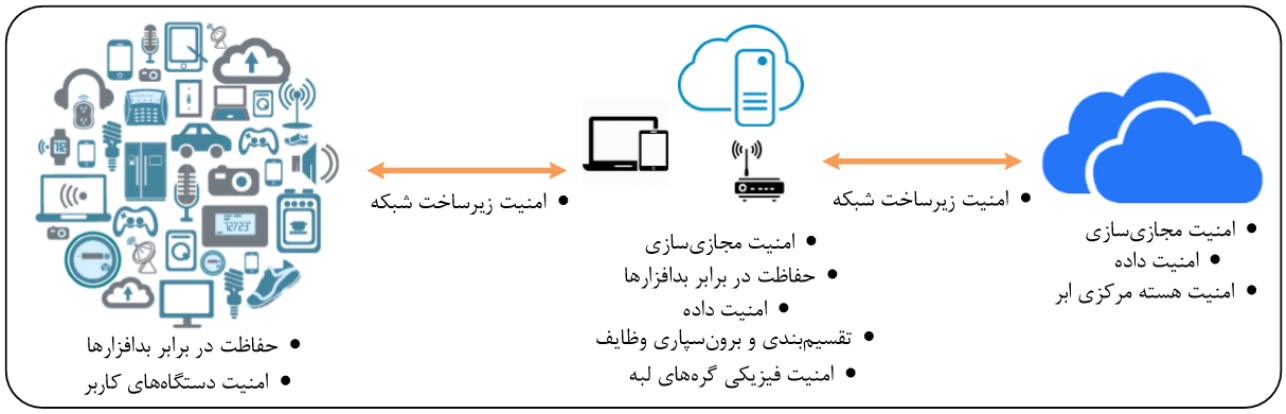
زیرساخت شبکه: زیرساخت شبکه شامل ارتباطات بین دستگاه‌های کاربران و گره‌های پردازشی لبه، ارتباطات بین گره‌های لبه و مراکز داده و هسته‌ی شبکه (از جمله مسیریاب‌ها و سوئیچ‌ها) است. همه‌ی ارتباطات در برابر حمله انکار خدمت و ارتباطات از نوع بی‌سیم در برابر حمله پارازیت[۳۵] آسیب‌پذیر هستند. این دو حمله می‌توانند مسیرهای ارتباطی را به کل مسدود نمایند تا کاربران مجاز نتوانند از طریق این مسیرها با گره‌های پردازشی ارتباط برقرار نمایند. یک حمله‌ی شایع دیگر حمله‌ی مرد میانی[۳۶] است که فرد متخاصم می‌تواند کنترل یک بخش از شبکه را در دست گرفته و به استراق سمع و تزریق داده در شبکه بپردازد. قرار دادن دروازه تقلبی[۳۷] در محیط پردازش لبه‌ای به عنوان گره لبه یکی دیگر از حملات قابل اجرا در این دسته به شمار می‌آید. سایر تهدیدهای موجود در این دسته در جدول ۳ نام برده شده‌اند.

امنیت داده: در سامانه‌های اطلاعاتی، امنیت اطلاعات و حریم خصوصی همیشه در اولویت قرار دارد [۳۰] زیرا هر کاربری از افشا شدن داده محرمانه‌ی خود بیم دارد و درصورت عدم اطمینان از حفظ حریم داده خود از سامانه یاد شده استفاده نخواهد کرد. مشکلات امنیت داده که در پردازش ابری به دلیل برون‌سپاری داده مطرح هستند در پردازش لبه‌ای نیز مطرح می‌شوند زیرا در این رویکرد پردازشی نیز در بعضی از مواقع، داده برون‌سپاری می‌شود. علاوه بر بررسی سامانه پردازش لبه‌ای از جهت دارا بودن روش‌هایی برای حفظ یکپارچگی داده و پشتیبان‌گیری از آن، باید مطمئن باشیم که از داده‌ها بدون داشتن مجوزهای لازم استفاده نخواهد شد [۱۰]. تغییر و از دست رفتن داده، دسترسی غیرمجاز به داده‌ی برون سپاری‌شده، دسترسی غیرمجاز به داده در محیط‌های دارای چند کاربر مانند بستر اجرای ماشین‌های مجازی و در دسترس نبودن داده‌ی برون‌سپاری‌شده از جمله تهدیدهای موجود در زمینه‌ی امنیت داده هستند. برای حل این چالش‌ها راه‌کارهایی مانند رمزگذاری، بخش‌بندی و ذخیره داده در نزدیکی کاربر مطرح می‌شود که در بخش ۴ به آن‌ها پرداخته خواهد شد. تهدیدهای مرتبط با امنیت داده در جدول ۳ آورده شده‌است.

بدافزارها: پیچیده‌تر شدن سطوح حمله‌ی بدافزارها و به روز نبود روش‌های تشخیص آن‌ها، سامانه‌ها را در برابر حملاتی از این دست آسیب‌پذیرتر از قبل کرده است [۲۷]. بدافزارها می‌توانند در هر لایه از پردازش لبه‌ای، وجود داشته باشند. در سمت کاربر، بدافزار می‌تواند با ارسال درخواست‌های فراوان به یک گره لبه، اقدام به حمله‌ی انکار خدمت کند. در یک گره لبه، بدافزارها می‌تواند یکپارچگی[۳۸] و محرمانگی داده‌های کاربران را تحت شعاع قرار دهد. وجود بدافزار در سمت کارگزار می‌تواند صحت داده‌های ذخیره شده‌ی کاربران را تهدید کند و یا قابلیت دسترس‌پذیری را کاهش دهد. در حالت کلی حمله‌هایی که از طریق بدافزارها

جدول ۳- خلاصه‌ای از تهدیدها و مشکلات امنیتی موجود در پردازش لبه‌ای

دسته‌بندی حمله	تهدیدهای احتمالی	راه‌حل‌های احتمالی
مجازی‌سازی	حملات ابر دیده‌بان حملات بر پایه ماشین مجازی حملات کانال جانبی افزایش امتیاز سوء استفاده از خدمت ارائه شده ناکافی بودن سیاست‌های اعمال شده برای منابع حمله انکار خدمت استفاده ناکارآمد از منابع نشت حریم خصوصی دسترسی غیر مجاز حمله ماشین مجازی به ماشین مجازی دیگر ارتباطات غیرامن از یک ماشین به ماشین مجازی دیگر	اصالت‌سنجی چند عاملی[۳۹] سامانه تشخیص نفوذ منزوی‌سازی داده رمزگذاری بر پایه صفت/هویت کنترل دسترسی بر پایه امتیاز جداسازی فرآیندهای در حال اجرا
زیرساخت شبکه	حمله انکار خدمت دروازه تقلبی حمله پارازیتی حین برون‌سپاری داده تزریق SQL ربودن حساب کاربری حمله مرد میانی ناکافی بودن سیاست‌ها و قوانین کنترل دسترسی ضعیف سرویس‌های و واسط‌های برنامه‌نویسی غیرامن نقاط ضعف برنامه‌های کاربردی تک نقطه‌ی خرابی[۴۰]	به‌روز رسانی منظم نرم‌افزارها بررسی‌های دوره‌ای محافظت توسط ضد ویروس‌ها سامانه جلوگیری از نفوذ ارتباطات رمزگذاری‌شده اصالت‌سنجی چند عاملی منزوی کردن گره‌های سازش‌گر محدود کردن تعداد ارتباط‌ها مدیریت امن کلیدها مسیریابی امن شبکه خصوصی پروتکل‌های بی‌سیم امن رصد ترافیک شبکه
امنیت داده	تکرار و به اشتراک گذاری داده دستکاری و پاک کردن داده دسترسی غیرمجاز به داده برون‌سپاری‌شده مشکلات مربوط به مالکیت داده عنصر داخلی مخرب[۴۱] مشکلات مربوط به چند کاربره بودن حمله انکار خدمت از دست رفتن دادن نقص اطلاعات	اجرای سیاست‌ها سامانه کنترل دسترسی امنیت درون معماری طراحی‌شده رمزگذاری مدیریت امن کلیدها مبهم‌سازی نقاب‌گذاری داده دسته‌بندی داده
حفاظت در برابر بدافزارها	بدافزار: ویروس، تروجان، کرم نرم‌افزارهای جاسوسی	برنامه‌های ضد بدافزار سامانه تشخیص نفوذ پشتیبان‌گیری دقیق از داده‌ها برطرف کردن نقاط آسیب‌پذیر قرار دادن نقاط بازیابی
دستگاه‌های کاربران	تزریق اطلاعات دستکاری خدمت مورد انتظار حمله خالی کردن توان باتری دستگاه	اصالت‌سنجی گره لبه حفاظت فیزیکی برنامه‌های ضد بدافزار
حفظ هویت	خدمات مکان‌محور/ نشت اطلاعات مکانی نشت حریم خصوصی	پنهان‌سازی آدرس و مستعارسازی
زیرساخت هسته (ابر)	افشای حریم خصوصی دستکاری خدمت مورد انتظار زیرساخت تقلبی[۴۲]	محیط اجرایی مورد اعتماد برنامه‌های ضد بدافزار محاسبات امن پیمانه بستر مورد اعتماد برای اصالت‌سنجی
گره‌های لبه	آسیب فیزیکی نشت حریم خصوصی افزایش امتیاز دستکاری خدمت مورد انتظار گره پردازشی تقلبی	حفاظت فیزیکی محیط اجرایی مورد اعتماد محاسبات امن پیمانه بستر مورد اعتماد برای اصالت‌سنجی برنامه‌های ضد بدافزار



شکل ۲- تهدیدهای موجود در هر لایه از معماری پردازش لبه‌ای

صورت می‌گیرند، می‌توانند محرمانگی، یکپارچگی و اصالت داده و ارتباطات را تحت تاثیر قرار دهند [۲۷].

دستگاه‌های کاربران: احتمال حملات فیزیکی به دستگاه‌های کاربران به دلیل نداشتن حفاظت‌های فیزیکی خاص وجود دارد به همین دلیل امکان حملاتی چون تزریق اطلاعات به این دستگاه‌ها بالا است. هم‌چنین بدافزارهایی که قابلیت نصب بر روی این دستگاه‌ها را دارا هستند، می‌توانند داده‌های اشتباه به گره‌های میانی فرستاده و یا باعث اختلال در ارتباط گره کاربر با گره میانی شوند. در نتیجه، یک گره پردازشی لبه باید بتواند دستگاه‌های کاربران را اصالت‌سنجی کند تا طمینان حاصل کند که دستگاه دچار سازش نشده‌است و داده‌ی ارسالی آن معتبر است.

زیرساخت ابر : منظور از زیرساخت ابر در پردازش لبه‌ای همان لایه ابر مرکزی در پردازش ابری است. زیرساخت ابر شامل مراکز داده (خدمت‌گزارها و پایگاه‌های داده) و ارتباطات بین مراکز داده و گره‌های لبه است. نشت اطلاعات از مراکز داده، حمله انکار خدمت و زیرساخت نامناسب از جمله تهدیدهایی هستند که در پردازش ابری وجود دارند. در مرجع [۱] مدل‌های حمله در پردازش ابری بررسی شده‌اند. در پژوهش [۳۱] تهدیدهای امنیتی در پردازش ابری به صورت واسط کاربری ناامن، تخصیص بدون محدودیت منابع، آسیب‌پذیری‌های مربوط به داده، آسیب‌پذیری‌های ماشین‌های مجازی، آسیب‌پذیری‌های مرتبط با تصاویر ماشین‌های مجازی، آسیب‌پذیری‌های ابر دیده‌بان و آسیب‌پذیری‌های شبکه‌ی مجازی آمده‌است. در بعضی از مدل‌های تهدید، کارگزارهای ابر به صورت نیمه صادق[۴۳] در نظر گرفته می‌شوند [۳۲]، [۳۳] و [۳۰].

حریم خصوصی: در پردازش ابری، برای استفاده از خدمات مبتنی بر مکان، باید موقعیت مکانی کاربر برای کارگزار ابر ارسال شود. ارسال این اطلاعات به ابر موجب نقض حریم خصوصی کاربر می‌شود. در نقطه مقابل استفاده از خدمات مبتنی بر مکان درپردازش لبه‌ای نیاز به فرستادن اطلاعات مکانی ندارد، زیرا گره لبه و گره کاربر در یک محدوده مکانی قرار دارند، در نتیجه ارسال خدمات مبتنی بر مکان بسیار ساده‌تر می‌شود و به نوعی حریم خصوصی کاربر حفظ شده است[۳۰]. اما از طرفی در صورت استفاده کاربران از گره‌های پردازشی لبه، می‌توان به الگوی مسیر طی شده توسط کاربر دست‌یافت. حفظ هویت کاربران و اطلاعات مکانی آن‌ها در پردازش لبه‌ای یک چالش مهم است. بنابراین نیاز به سازوکاری برای پنهان‌سازی این دست از اطلاعات امری ضروری است. مسئله حفظ هویت پیش از این هم در پردازش ابری مطرح بوده است[۳۰].

زیرساخت لبه: همان‌طور که در شکل ۱ قابل مشاهده است، طیف گسترده‌ای از دستگاه‌ها در پردازش لبه‌ای به عنوان گره پردازشی می‌توانند مورد استفاده قرار بگیرند. با توجه به نوع هر گره و میزان منابعی که در اختیار دارد، حملات مختلفی بر روی آن قابل اعمال است. یک حمله‌کننده برای حمله از ورودی‌های ارتباط با گره‌های پردازشی استفاده می‌کند. این مدخل‌ها شامل APIها و برنامه‌های کاربردی هستند که بر روی شبکه اجرا می‌شوند. هم‌چنین حملات فیزیکی به این گره‌ها را باید در نظر گرفت. از جمله حملات فیزیکی می‌توان به حملات کانال جانبی[۴۴] اشاره نمود. در این نوع حمله بدون آسیب رساندن به دستگاه و صرفا با اندازه‌گیری متغیرهای مختلف مدار چون جریان و یا توان، به استخراج اطلاعات از دستگاه پرداخته می‌شود. حملات تحلیل توان یکی از پرکاربردترین این حملات هستند [۳۴]. ایجاد سازوکارهایی برای جبران کاهش امنیت محیط پیرامون تکه‌ابرها و کارگزاران فعال در لبه نسبت به مراکز داده‌ی ابری، یکی دیگر از چالش‌های مهم مطالعاتی در حوزه پردازش لبه‌ای است. گسترش محیط مقاوم در برابر دستکاری[۴۵]، نظارت از راه دور[۴۶] و استفاده از پیمانه بستر مورد اعتماد[۴۷] از جمله راه‌کارهای موجود در این زمینه هستند[۴]. در هر صورت مرکز داده برای اعتماد به داده‌ی دریافتی از گره لبه، باید بتواند آن را اصالت‌سنجی نماید. یکی از روش‌های متداول برای اصالت‌سنجی گره لبه توسط ابر مرکزی، ترکیبی از پروتکل‌های ارزیابی از راه دور و استفاده از پیمانه بستر مورد اعتماد است [۳۵]. شکل۲ یک جمع‌بندی کلی از تهدیدهای لایه‌های مختلف در پردازش لبه‌ای را ارائه می‌کند.

۴- چالش‌ها و راه‌حل‌ها

معیار مشترک بسیاری از چالش‌ها در رویکرد پردازش لبه‌ای، طبیعت غیر متمرکز و توزیع شده این رویکرد نسبت به رویکرد پردازش ابری است[۹]. علاوه بر این برخلاف پردازش ابری، در پردازش لبه‌ای گواهی‌نامه‌های استاندارد امنیتی هنوز وجود ندارد[۲۷]. حتی تعریف واحد و یکسانی برای این موضوع ارائه نشده است به طوری که بسیاری از چارچوب‌های ارائه شده در بستر پردازش ابری و پردازش متحرک در حال حاضر نمونه‌هایی از رویکرد پردازش لبه‌ای نیز می‌توانند باشند [۱۲]. با توجه به نبود تعریف برای استانداردهای امنیتی در پردازش لبه‌ای و در نظر گرفتن محدودیت‌های دستگاه‌های واقع در لبه از لحاظ منابع اجرایی، ذخیره‌سازی و انرژی، پیاده‌سازی روش‌های مقابله با تهدیدهای امنیتی در این رویکرد مشکل است. از طرفی، نمی‌توان روش‌های پیچیده امنیتی را در مدل پردازش لبه‌ای استفاده کرد چرا که این روش‌ها نیازمند منابع اجرایی فراوانی هستند. توجه به این موضوع ضروری است که راه‌حل‌های ارائه شده برای پردازش لبه‌ای باید حالت کلی داشته باشند. چرا که راه‌حل‌های اقتضایی[۴۸] و خاص مورد، به دلیل تفاوت‌های پیاده‌سازی‌های مختلف از رویکرد پردازش لبه‌ای، ممکن است قابلیت توسعه به یکدیگر را دارا نباشند. به عبارت دیگر باید بتوان راه‌حل‌ها را در تمام چارچوب‌های پردازش لبه‌ای استفاده نمود. این راه‌حل‌ها تا حد امکان نباید به صورت وصله[۴۹] باشند، در نتیجه بهترین راه‌کار این است که از ابتدای طراحی یک چارچوب برای

پردازش لبه‌ای، روش‌های جلوگیری از حملات گوناگون را در طراحی ارائه شده پیاده‌سازی نمود. راه‌حل‌های کلی قابل اعمال برای برطرف کردن تهدیدها در ادامه معرفی می‌شوند.

اصالت‌سنجی و احراز هویت: مقاله [۸] اصالت‌سنجی بین چارچوب پردازش لبه‌ای و کاربران نهایی را به عنوان مهم‌ترین چالش امنیتی در پردازش لبه‌ای قلمداد کرده است. هر عنصر در هر لایه از پردازش لبه‌ای می‌تواند عناصر موجود در لایه‌ای را اصالت‌سنجی کند که با آن در حال تعامل است برای مثال ابر مرکزی، گره پردازشی لبه‌ای که با آن در ارتباط است را اصالت‌سنجی می‌نماید. علاوه بر این گره‌های پردازشی موجود در لایه‌ی میانی، در صورت تعامل با یکدیگر باید بتوانند یکدیگر را تصدیق نمایند. یکی از چالش‌هایی که گره‌های پردازشی لبه با آن روبه‌رو هستند، احراز هویت کاربران توسط گره‌های پردازشی لبه، حتی در زمان در دسترس نبودن ابر مرکزی است. در واقع پردازش لبه‌ای به یک سامانه اصالت‌سنجی توزیع شده نیاز دارد تا در زمان در دسترس نبودن یکی از عناصر، سامانه هم‌چنان به کار خود ادامه دهد. در مقاله [۸] یک پروتکل برای اصالت‌سنجی در محیط پردازش لبه‌ای ارائه شده‌است.

استفاده از پیمانه بستر مورد اعتماد یکی دیگر از روش‌های اصالت‌سنجی است [۴]. مقادیری تعیین کننده در بسیاری از سامانه‌ها حفظ یکپارچگی سامانه، بررسی صحت سامانه و اصالت آن را بر عهده دارند. پیمانه بستر مورد اعتماد با استفاده از این مقادیر، خدمات یادشده (به طور خاص اصالت‌سنجی) را فراهم می‌آورد [۳۶]. در پژوهش [۳۵] یک پروتکل سخت‌افزاری بر پایه پیمانه بستر مورد اعتماد برای ارزیابی از راه دور حسگرهای شبکه‌ی حسگر بی‌سیم ارائه شده است.

در مقاله [۲۴] برای احراز هویت و شناسایی در محیط‌های غیرمتصل یا با اتصال محدود و یا گسسته به شبکه، راه‌کاری بر پایه تولید و تبادل امن کلید ارائه شده‌است. در چنین محیط‌هایی، سامانه‌های هوشمند همراه با قابلیت‌های پردازشی و ذخیره‌ای محدود به‌کار برده می‌شوند. در مرجع [۳۷] تعدادی گره پردازشی لبه با یکدیگر در ارتباط هستند و منابعی را در اختیار کاربران قرار می‌دهند. کاربر می‌تواند شبکه و منابع آن را طبق خواسته خودش پیکربندی و مدیریت کند. مواردی که در این مقاله پیاده‌سازی شده‌اند، عبارت هستند از:

۱- تصدیق اعتبار کاربرانی که دسترسی مجاز دارند.

۲- کنترل دسترسی کاربران به منابعی که اجازه استفاده از آن‌ها را دارند.

۳- جدا سازی ترافیک کاربران مختلف به صورت نرم‌افزاری.

سامانه کنترل دسترسی: کنترل دسترسی کاربر، رمزگذاری داده‌ها و استفاده از پروتکل امن لایه حمل و نقل[۵۰] برای ایمنی دسترسی به داده و حفظ حریم خصوصی در نظر گرفته می‌شود [۲۷]. برای مدیریت منابع و کنترل دسترسی‌های مجاز به منابع و خدمات، نیاز است تا به نحوی تمام دسترسی‌های مجاز هر کاربر به خدمات و منابع موجود در کل زیرساخت و سامانه پردازش لبه‌ای تعیین و نگهداری شوند. پیاده‌سازی این سامانه برای حفظ محرمانگی داده‌های کاربران و جلوگیری از استفاده نابه‌جا از منابع زیرساخت امری ضروری است. یکی از راه‌کارهای موجود برای حل این چالش، استفاده از رمزگذاری بر پایه ویژگی[۵۱] برای پیاده‌سازی سیاست‌های کنترل دسترسی است [۳۸]. استفاده از روش‌های صوری[۵۲] راه‌حلی است که در پژوهش [۳۹] برای حل مسئله کنترل دسترسی در محیط پردازشی لبه‌ای متحرک ارائه شده‌است. در مرجع [۴۰] نویسندگان، سامانه‌ای مبتنی بر قوانین، برای مدیریت منابع در پردازش مه ارائه داده‌اند. این سامانه با گسترش چارچوب پایه‌ای پردازش مه، قابلیت هم‌کاری به طور ایمن بین منابع مختلف درخواستی کاربران را فراهم می‌کند. سامانه‌ی ارائه شده، دارای ۵ قسمت اصلی به شرح مقابل است: ۱- موتور تصمیم‌گیری سیاست[۵۳]، برای تصمیم‌گیری بر اساس سیاست‌های از پیش تعیین شده، ۲- مدیر برنامه[۵۴]، برای مدیریت چند کاربر در پردازش مه، ۳- تصمیم‌گیر سیاست[۵۵]، برای اصالت‌سنجی بر اساس ویژگی‌ها و صفات، ۴- ظرف نگه‌داری قوانین[۵۶] و ۵- اجرا کننده‌ی سیاست برای شناسایی هر گونه اختلاف و تفاوت در پیاده‌سازی سیاست‌ها. از نقاط ضعف این سیستم می‌توان به عدم کارایی در کاربردهای حساس به زمان و آسیب‌پذیری در مقابل حمله انکار خدمت به دلیل فرآیند پیچیده اصالت‌سنجی اشاره کرد.

امنیت شبکه: اگر امنیت زیرساخت شبکه تامین نشود، تمام خدمات ارائه شده توسط پردازش لبه‌ای توسط مهاجمان داخلی و خارجی، تحت تاثیر قرار می‌گیرد [۹]. امنیت شبکه شامل امنیت پیوندهای ارتباطی بین گره‌ها از یک لایه به لایه دیگر، پیوندهای ارتباطی در یک لایه و امنیت هسته‌ی شبکه (زیرساخت شبکه عمومی و شبکه تلفن همراه) است. پروتکل‌های ارتباطی و فناوری‌های شبکه مورد استفاده در پردازش لبه‌ای، همان فناوری‌ها و پروتکل‌های استفاده شده در پردازش ابری بوده و در نتیجه دارای استانداردهای امنیتی لازم هستند. با اجرای برنامه‌هایی همچون CloudWatcher [۴۱] می‌توان ترافیک شبکه را رصد نمود تا رفتارهای غیرعادی مشخص و از انتشار بسته‌های مخرب در شبکه جلوگیری نمود. هم‌چنین به دلیل ماهیت محلی گره‌های پردازشی لبه، استفاده از شبکه‌های مجازی خصوصی[۵۷]، می‌تواند از حملات خارجی جلوگیری نماید [۲۷]. جدا سازی ترافیک شبکه‌ی کاربرانی که از ماشین‌های مجازی در حال اجرا بر روی یک سخت‌افزار خدمت می‌گیرند نیز در این بخش مورد بررسی قرار می‌گیرد. استفاده از شبکه‌های نرم‌افزار پذیر[۵۸] و مجازی‌سازی عملکرد شبکه[۵۹] [۴۲] می‌تواند در رویکردهای مختلف پردازش لبه‌ای مفید واقع شود. این فناوری‌ها با استفاده از مجازی‌سازی عملکرد مسیریاب‌ها و پیاده‌سازی شبکه‌های قابل بازپیکربندی، مدیریت شبکه را آسان‌تر می‌نمایند. هم‌چنین به وسیله‌ی این فناوری‌ها می‌توان به موارد زیر دست یافت:

۱- دستگاه‌های ناامن شبکه را از دیگر دستگاه‌ها منزوی نمود.

۲- ترافیک شبکه را به سمت دستگاه‌های امن هدایت کرد.

۳- پیکربندی شبکه را در صورت ورود (خروج) گره‌های پردازش لبه‌ای به (از) زیرساخت، به صورت بی‌درنگ تغییر داد [۹].

پیاده سازی کانال امن برای انتقال داده، روشی است که در مقالات [۱۹] و [۲۰] از آن برای انتقال امن داده بین گره لبه و ابر مرکزی استفاده شده است.

تشخیص نفوذ: برای اطمینان از صحت عملکرد چارچوب پردازش لبه‌ای، نیاز به یک روش یا سامانه جهت تشخیص نفوذ هست. در پردازش لبه‌ای، گره‌های لبه معمولاً گزینه‌های مناسبی برای حمله به شمار می‌روند، زیرا در مقایسه با کارگزارها از حفاظت فیزیکی کمتری برخوردار هستند و اطلاعات گره‌های نهایی در آن‌ها تجمیع شده است. در نتیجه حمله فیزیکی به آن‌ها نسبت به ابر مرکزی ساده‌تر است و نسبت به حمله به یک گره‌ی کاربر، اطلاعات بیشتری را می‌توان از گره‌ی لبه استخراج کرد. تشخیص حمله به یک گره از آنجا اهمیت بیشتری پیدا می‌کند که هر گره لبه می‌تواند با گره‌های دیگر لبه و یا ابر مرکزی در ارتباط باشد و در صورت نفوذ به یک گره پردازشی لبه، امکان بروز تهدید یا سازش در کل زیرساخت وجود دارد. برای تشخیص حمله در بستر پردازش لبه‌ای، سامانه تشخیص نفوذ باید بتواند در یک زیرساخت توزیع‌شده، ناهمگون و غیرمتمرکز – ویژگی‌های زیرساخت پردازش لبه‌ای- پاسخ‌گو باشد. هم‌چنین اطلاعات تشخیص نفوذ در هر بخش برای جلوگیری از پیشرفت برنامه‌ی نفوذی، باید بلافاصله در اختیار بخش‌های دیگر چارچوب قرار بگیرد. در مقاله [۴۳] یک سامانه تشخیص نفوذ در پردازش لبه‌ای متحرک به نام HoneyBot ارائه شده که یک روش دفاعی در برابر حملات ارتباطی بین دستگاه‌ها است. روش دیگری در پژوهش [۴۴] ارائه شده‌است که در آن، بار تصمیم‌گیری تشخیص نفوذ به هر گره در شبکه نسل ۵، توسط چارچوب مشخصی، به ابر مرکزی انتقال می‌یابد، در واقع وظیفه تشخیص نفوذ بر عهده ابر است. هر چند این چارچوب برای خدمات متمرکز در پردازش ابری ارائه شده‌است، اما با تعمیم چشم‌انداز روش ارائه شده، برای رویکردهای

پردازش لبه‌ای نیز قابل استفاده است. در مرجع [۴۵] یک شبکه متشکل از تکه‌ابرها پیشنهاد شده‌است که می‌تواند نفوذ در ابر مرکزی، ارتباطات بین دستگاه‌های موبایل و تکه‌ابرها را تشخیص دهد.

حریم خصوصی: در کنار مهاجمان خرابکار، دسته‌ی دیگری از مهاجمان با نام صادق اما کنجکاو[۶۰] وجود دارند که خارج از سطح دسترسی و اجازه خود کاری انجام نمی‌دهند اما با دسترسی‌های فعلی خود به دنبال کشف اطلاعات کاربران هستند. در پردازش ابری معمولاً کارگزاران در این دسته قرار می‌گیرند[۳۳]، [۳۲]. حفظ حریم خصوصی دارای سه بخش حریم خصوصی داده، حریم خصوصی هویت و حریم خصوصی مکان[۶۱] است. برای حل چالش حریم خصوصی داده راه‌حل‌هایی مانند رمزنگاری همریخت[۶۲] و یا داده‌ی قابل حسابرسی[۶۳] ارائه شده‌اند که دارای سربار محاسباتی بالایی هستند ولی از حفظ محرمانگی داده پشتیبانی می‌کنند. ارسال داده از دستگاه‌های کاربر به گره‌های لبه با استفاده از رمزگذاری کلید عمومی و پروتکل Diffie-Hellman نیز از راه‌کارهای موجود در این بخش هستند. در مقاله [۷] نویسندگان، بهره‌وری استفاده از روش‌های حفاظت از داده در سامانه‌ها را با استفاده از مدل کردن پردازش لبه‌ای بررسی کرده‌اند. پژوهش [۳۰] به مشکلات موجود در روند طراحی سامانه‌هایی با قابلیت حفظ حریم خصوصی و امنیت داده پرداخته است. هم‌چنین این پژوهش راه‌حل‌های ارائه شده در پردازش ابری برای حل این چالش را در پردازش لبه‌ای ناکارآمد دانسته است. یکی از دلایل ارائه شده اشاره به این نکته دارد که داده‌ها در مدل پردازش ابری به طور مستقیم از کاربر به ابر مرکزی می‌رسند اما در مدل پردازش لبه‌ای، داده‌ها پس از پردازش در لبه به ابر منتقل می‌شوند. در نتیجه در صورتی که ابر مرکزی بخواهد از روش‌هایی چون اصالت‌سنجی هم‌ریخت و یا داده بازرسی شده استفاده نماید، به دلیل آن‌که به طور مستقیم به داده‌ی خام دسترسی ندارد و نمی‌تواند فرآیند برگشت داده‌ی رمزشده به داده‌ی خام را انجام دهد. به طور مشابه در روش رمزگذاری داده بر پایه‌ی برچسب نیز روال به همین گونه است. زیرا سیاست دسترسی به متن پس از انجام پردازش توسط گره‌های لبه، به همان منوال قبل باقی نمی‌ماند.

در حریم خصوصی هویت، باید به دنبال یک راه‌حل میانه بین گم‌نامی[۶۴] و مسئولیت‌پذیری هر کاربر بود تا در صورت مشاهده رفتارهای خلاف قوانین توسط یک کاربر بتوان آن را شناسایی نمود. در حریم خصوصی مکان، لازم است علاوه بر استفاده از خدمات پردازش لبه‌ای، اطلاعات مکانی هر کاربر حفظ شود. در حالت کلی با توجه به مشخص بودن این موضوع که یک کاربر از کدام گره‌های لبه در حال گرفتن خدمت است، مکان و مسیر طی شده توسط آن قابل شناسایی است. در پژوهش [۲۸] مرور جامعی بر راه‌حل‌های ارائه شده به منظور حل چالش حریم خصوصی در پردازش ابری متحرک صورت گرفته است.

استفاده از کانال امن برای انتقال داده از گره‌های لبه به مراکز داده، راه‌کار پیاده‌سازی شده در مقالات [۱۹] و [۲۰] برای حفظ امنیت داده در شبکه است.

دیدگاه‌های متفاوتی به مسئله امنیت و حفظ حریم خصوصی در پردازش لبه‌ای وجود دارد. در مقاله [۲۰] از عدم الزام مرکز داده به اعتماد بر گره‌های پردازشی لبه صحبت شده‌است (در این حالت ابر مورد اعتماد فرض شده‌است). در نتیجه یک راه‌کار سخت‌افزاری -استفاده از پیمانه بستر مورد اعتماد- برای اصالت‌سنجی گره‌ها و اجرای امن برنامه‌ها بر روی بستر غیرقابل اعتماد نرم‌افزاری ارائه شده‌است. از طرفی دیگر، در مقاله [۲] نویسندگان با در نظر گرفتن نقاط دسترسی به عنوان گره‌های پردازشی لبه و تقویت قابلیت ذخیره‌سازی آن‌ها، داده کاربر را فقط در مواقعی خاص به مرکز داده می‌فرستند. در سایر موارد داده در همان نقطه دسترسی – واقع در محل استفاده کاربر- به صورت محلی ذخیره می‌شود. بنابر ادعای مقاله با ذخیره داده به صورت محلی، حریم خصوصی داده کاربر حفظ شده‌است (ابر متخاصم در نظر گرفته شده است). با در نظر گرفتن ابر مرکزی به عنوان عنصر متخاصم و یا قابل اعتماد رویکردها برای حل مسئله حفظ حریم خصوصی تغییر می‌کنند.

مجازی‌سازی: پردازش لبه‌ای برای بهبود عملکرد خود و با توجه به محدودیت منابعی که در اختیار دارد، از مجازی‌سازی گره‌های لبه استفاده می‌کند، همان‌طور که در بخش قبل اشاره شد، با توجه به منابع اجرایی گره‌ی لبه، مجازی‌سازی می‌تواند در سطح سخت‌افزار و یا نرم‌افزار باشد. امنیت ماشین‌های مجازی در حال اجرا بر روی کارگزارها، از جمله مباحث بسیار مهم است که در پژوهش‌های موجود در این حوزه تمرکز ویژه‌ای به آن شده‌است[۳۱]. چالش‌هایی نظیر جداسازی ترافیک شبکه‌ی هر ماشین مجازی، امنیت ابر دیده‌بان، جلوگیری از دسترسی به یک ماشین مجازی توسط ماشین مجازی دیگر و غیره در پردازش لبه‌ای نیز مطرح هستند. به دلیل عدم نیاز به مدیریت متمرکز و هم‌چنین وابستگی نه چندان بالای مجازی‌سازی به سخت‌افزار (با فرض برآورده شدن حداقل نیازها) راه‌حل‌های ارائه شده در پردازش ابری در پردازش لبه‌ای نیز قابل استفاده هستند [۹]. یکی از راه‌حل‌های ارائه شده برای حفظ امنیت هر ماشین مجازی، استفاده از پیمانه بستر مورد اعتماد مجازی[۶۵] است [۴۶]. در پژوهش [۴۷] یک چارچوب امنیتی برای زیرساخت پردازش ابری ارائه شده است. این چارچوب قابلیت برپایی یک ماشین مجازی مورد اعتماد با استفاده از اجرای یک پروتکل را دارد. با استفاده از این پروتکل و ذخیره داده به صورت حفاظت شده، می‌توان یکپارچگی داده‌ی کاربر را تضمین کرد. مقاله [۴۸] یک روش سخت‌افزاری برای محافظت از ماشین‌های مجازی در برابر یک ابر دیده‌بان خرابکار معرفی نموده‌است.

حفاظت در برابر بدافزارها: یکی از راه‌کارها برای حفظ امنیت سامانه‌های پردازش لبه‌ای، حفاظت در برابر بدافزارهای قدیمی و نو ظهور است. برنامه‌های امنیتی کاربردی برای حفاظت در برابر بدافزارها در پردازش ابری به دو دسته قابل تقسیم هستند؛ برنامه‌هایی که بر روی ابر مرکزی اجرا و برنامه‌هایی که بر روی دستگاه‌های کاربران نصب می‌شوند. استفاده از روش‌های یادگیری ماشین[۶۶] برای شناسایی بدافزارهای ناشناخته راه‌کار ارائه شده در مقالات [۴۹] و [۵۰] است. هم‌چنین نرم‌افزار BareCloud [۵۱] بر روی چارچوب پردازش لبه‌ای برای تشخیص انواع بدافزارها قابل استفاده است. در مرجع [۵۲] یک پژوهش مروری پیرامون ارزیابی، تشخیص و شناسایی بدافزارها برای دستگاه‌های تلفن همراه صورت گرفته است. مقاله [۴۵] یک روش برای تشخیص بدافزارهای دستگاه‌های متحرک، با استفاده از توابع امنیتی در بستر تکه‌ابرها ارائه داده است.

افزایش قابلیت اطمینان: داشتن یک پشتیبان از مراکز داده در هنگام وقوع تخریب توسط حوادث طبیعی و یا تهدید امنیت داده توسط حمله سایبری، امری ضروری است. با توجه به سربار بسیار بالای این روش، نیازی به پشتیبان‌گیری[۶۷] از تمام داده‌ها نیست هم‌چنین پشتیبان‌گیری از داده‌ها پس از انجام پردازش بر روی آن‌ها انجام می‌شود. در [۵۳] مروری جامع پیرامون روش‌های پشتیبان‌گیری از داده و بازیابی آن در پردازش ابری انجام شده‌است. در [۵۴] برای پشتیبان‌گیری برخط از ماشین‌های مجازی چارچوبی ارائه شده‌است. گره‌های لبه نیز درصورت ذخیره داده‌های کاربر توسط خودشان، باید پشتیبانی از داده‌های ضروری تهیه نمایند. برای این منظور یکی از راه‌کارهایی که توسط این گره‌ها می‌تواند انجام گیرد، ارسال داده‌ها به ابر مرکزی برای ذخیره‌سازی به صورت رمز شده است.

محیط اجرایی مورد اعتماد: اطمینان از صحت اجرای برنامه‌های کاربردی بر روی گره‌های لبه اهمیت فراوانی دارد. امنیت محیطی گره‌های پردازشی لبه از ابر مرکزی کم‌تر است. در نتیجه احتمال دستکاری فیزیکی و حملات کانال جانبی بر روی این گره‌ها بالا است. علاوه بر این، سیستم‌های عامل در حال اجرا بر روی گره‌ها نیز می‌توانند دچار سازش شوند. برای اطمینان از عدم تغییر برنامه‌های اجرایی بر روی گره‌های لبه، دو راه‌کار سخت‌افزاری قابل استفاده، پیمانه بستر مورد اعتماد و محیط اجرایی امن[۶۸] هستند. برای پیاده‌سازی محیط اجرایی امن، از

فناوری‌هایی مانند TrustZone شرکت آرم [۵۵] و SGX شرکت اینتل می‌توان استفاده کرد [۵۶]. در فناوری TrustZone، یک محیط امن دارای سه مولفه اصلی است که عبارت از پشتیبانی سخت‌افزار از منزوی‌سازی[۴۹]، راه‌اندازی امن و سیستم‌عامل مورد اعتماد هستند. با استفاده از این فناوری یک محیط عادی و یک محیط امن بر روی یک پردازنده ایجاد می‌شوند که با یکدیگر در تعامل هستند. برنامه‌های حساس در قسمت سیستم عامل امن اجرا می‌شوند. در مقابل فناوری SGX اختیار اجرای امن را به برنامه‌نویس‌ها می‌دهد. در این فناوری قطعاتی از کد که باید به صورت امن اجرا شوند توسط برنامه‌نویس‌ها مشخص و بر روی قسمت‌های مخصوصی از پردازنده با نام enclave اجرا می‌شوند. در [۲۰] یک سامانه برای اجرای امن با استفاده از فناوری SGX پردازنده‌های اینتل پیاده سازی شده‌است. حفظ یکپارچگی برنامه اجرایی بر روی لبه، اجرای امن آن و محرمانگی داده از جمله ویژگی‌های سامانه‌ی ارائه شده در این مقاله هستند. در مقالات [۵۷] و [۵۸] نویسندگان با استفاده از پردازنده‌های آرم و فناوری TrustZone یک محیط امن برای اجرای برنامه‌های مهم ارائه داده‌اند.

۵- نتیجه‌گیری

پردازش لبه‌ای (پردازش مه، پردازش لبه‌ای متحرک، پردازش ابری متحرک و تکه ابر) به عنوان رویکردی جدید در گسترش کاربردهای اینترنت اشیا، کاستی‌های پردازش ابری در کاربردهای نو پدید، مانند تاخیر پردازش را برطرف نموده است. از آنجا که پردازش لبه‌ای تعمیم و بهبود یافته‌ی رویکرد پردازش ابری است، بعضی از چالش‌های آن مانند حفظ امنیت داده و حریم خصوصی کاربران را به ارث برده است. هم‌چنین این رویکرد علاوه بر چالش‌های موجود در پردازش ابری، به دلیل مسائلی مانند زیرساخت توزیع‌شده، ناهمگون و غیرمتمرکز با چالش‌های جدیدی نیز همراه است. از جمله این چالش‌ها می‌توان به مجازی‌سازی، تخصیص منابع و برون‌سپاری وظایف، پشتیبانی از ناهمگونی گره‌ها، توزیع گره‌های پردازشی، تحرک کاربران و غیره اشاره نمود. در چارچوب‌های ارائه شده برای پردازش لبه‌ای، مسئله امنیت و حریم خصوصی نسبت به دیگر چالش‌ها کمتر مورد توجه قرار گرفته است. مزیت‌های استفاده از پردازش لبه‌ای بدون در نظر گرفتن مسئله امنیت تقریباً قابلیت استفاده‌ی عملی را ندارد. در نتیجه با توجه به روند افزایشی استفاده از چارچوب‌های پردازش لبه‌ای، ارائه و پیاده‌سازی راه‌کارهای حل چالش امنیت بیش از پیش حائز اهمیت شده‌اند.

در این مقاله در بخش اول، ابتدا مفهوم پردازش لبه‌ای و رویکردهای آن معرفی شدند. در ادامه، معماری و کاربردهای آن در بخش دوم مورد بررسی قرار گرفتند. در بخش سوم به معرفی تهدیدهای موجود در پردازش لبه‌ای پرداخته شد. در انتها با تجمیع راه‌کارهای ارائه‌شده برای حل چالش‌ها و تهدیدهای امنیتی از جدیدترین مقالات ارائه شده در این موضوع، یک دسته‌بندی از راه‌کارها تبیین شد. بر اساس دسته‌بندی تهدیدها، چالش‌های امنیتی موجود در بخش‌های مختلف ساختار رایانش لبه‌ای شامل مجازی‌سازی، زیرساخت شبکه، امنیت داده، حفاظت در برابر بدافزارها، دستگاه‌های کاربران، حفظ هویت، امنیت زیرساخت هسته (ابر) و امنیت گره‌های پردازشی لبه هستند.

با توجه به گستردگی مسئله امنیت در پردازش لبه‌ای و چالش‌های بسیار آن، راه‌کارهای ارائه شده تا به امروز به طور کامل پاسخ‌گوی نیازهای امنیتی رویکردهای موجود نیستند. هر کدام از این راه‌کارها با دارا بودن مورد یا مواردی از متغیرهای امنیت(محرمانگی، یکپارچگی و اصالت‌سنجی) ارائه شده‌اند. به دلیل نوپا بودن این رویکرد، چارچوب‌های ارائه شده در پردازش لبه‌ای، درحال حاضر متغیرهایی چون کارایی، قابلیت اطمینان و قابلیت پیاده‌سازی را به عنوان اهداف اصلی طراحی در نظر گرفته‌اند. اما با توجه به گسترش استفاده از چارچوب‌های پردازش لبه‌ای و اهمیت بیش از پیش مسئله امنیت، نیاز است تا چارچوب‌های پردازش لبه‌ای با این رویکرد بازطراحی شوند. چارچوب‌های ارائه شده باید در گام نخست بتوانند ویژگی‌های پایه‌ای امنیت را تامین کنند و در ادامه از کارایی و قابلیت اطمینان بالایی نیز برخوردار باشند.

مراجع

[1] N. Alhebaishi, L. Wang, S. Jajodia, and A. Singhal, "Threat Modeling for Cloud Data Center Infrastructures," *In International Symposium on Foundations and Practice of Security*. Springer, Cham, pp. 302-319, 2016.

[2] P. Liu, D. Willis, and S. Banerjee, "ParaDrop: Enabling Lightweight Multi-tenancy at the Network's Extreme Edge," *in IEEE/ACM Symposium on Edge Computing,* washingtion DC, pp. 1-13 , 2016.

[3] S. Nastic, H.L. Truong, and S. Dustdar, "A Middleware Infrastructure for Utility-based Provisioning of IoT Cloud Systems," *in IEEE/ACM Symposium on Edge Computing*, washington DC, pp. 28-40, 2016.

[4] M. Satyanarayanan, "The Emergence of Edge Computing," *Computer*, vol. 50, no. 1, pp. 30 - 39, 2017.

[5] M. Satyanarayanan, G. Lewis , E. Morris, S. Simanta, J. Boleng, and K. Ha, "The role of cloudlets in hostile environments," *IEEE Pervasive Computing*, vol. 12, no. 4, pp. 40-49, 2013.

[۶] پریسا حسنی‌زاده، خالد دغلاوی، محمد حسین فرزام، علی رسایی، سیاوش بیات سرمدی، "نگاهی بر پردازش لبه: مزایا، چالش‌ها و امنیت،" در مجموعه مقـالات بیست و سومین کنفرانس ملی سالانه انجمن کامپیوتر ایران ,تهران, ۱۳۹۶ .

[7] T.D. Dang and D. Hoang, "A data protection model for fog computing," *in Second International Conference on Fog and Mobile Edge Computing (FMEC)*, pp. 32-38 , 2017.

[8] I. Stojmenovic, SH. Wen, X. Huang and H. Luan, "An overview of Fog computing and its security issues," *Concurrency and Computation: Practice and Experience*, vol. 28, no. 10, pp. 2991-3005, 2016.

[9] R. Roman, J. Lopez, and M. Mambo., "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680-698, 2018.

[10] S. YiEmail, Zh. Qin, and Q. Li, "Security and Privacy Issues of Fog Computing: A Survey," *in International Conference on Wireless Algorithms, Systems, and Applications*, pp. 685-695, 2015.

[11] P. Hu, S. Dhelim, H. Ning, and T. Qiu., "Survey on fog computing: architecture, key technologies, applications and open issues," *Journal of Network and Computer Applications*, vol. 98 , pp. 27-42, 2017.

[12] A. Yousefpour, C. Fung, T. Nguyen, K. Kadiyala, F. Jalali, A. Niakanlahiji, J. Kong, and J.P. Jue., "All one needs to know about fog computing and related edge computing paradigms: A complete survey," *Journal of Systems Architecture*, Elsevier, 2019.

[13] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The Case for VM-Based Cloudlets in Mobile Computing," *IEEE Pervasive Computing* , vol. 8, no. 4, pp. 1-10 , 2009.

[14] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," *in MCC '12 Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, pp. 13-16, 2012.

[15] Y. Ch. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile Edge Computing a key technology towards 5G," *ETSI (European Telecommunications Standards Institute)*, pp. 1-16 , 2015.

[16] H.T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," *Wireless communications and mobile computing*, vol. 13, no. 18, pp. 1587-1611, 2013.

[17] Open Edge Computing Initiative, [Online]. Available: http://openedgecomputing.org.

[18] SH. Mortazavi, M. Salehe, CS. Gomes, and C. Phillips, "CloudPath: A Multi-Tier Cloud Computing Framework," *in IEEE/ACM Symposium on Edge Computing*, p. 20 , 2017.

[19] C. Streiffer, A. Srivastava, V. Orlikowski, N. Raval, A. Machanavajjhala, L. P. Cox, Y. Velasco, and V. Martin, "ePrivateEye: To the Edge and Beyond!," *in IEEE/ACM Symposium on Edge*

Conference on Artificial Intelligence Applications and Innovations (AIAI 2016), pp. 653-665, 2016.

[40] C. Dsouza, G. J. Ahn, and M. Taguinod, "Policy-driven Security Management for Fog Computing: Preliminary Framework and a Case Study," *in Proceedings of the IEEE 15th International Conference on Information Reuse and Integration (IRI)*, pp. 16-23, 2014.

[41] S. Shin, and G. Gu, "CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?)," *in 20th IEEE International Conference on Network Protocols (ICNP)*, pp. 1-6 , 2012.

[42] N. Bizanis and F. Kuipers, "SDN and Virtualization Solutions for the Internet of Things: A Survey," *IEEE Access*, vol. 4, pp. 5591 - 5606, 2016.

[43] A. Mtibaa, K. Harras, and H. Alnuweiri, "Friend or Foe? Detecting and Isolating Malicious Nodes in Mobile Edge Computing Platforms," *in IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom'15)* , pp. 42-49 , 2015.

[44] K. Gai, M. Qiu, L. Tao and Y. Zhu, "Intrusion detection techniques for mobile cloud computing in heterogeneous 5G," *Security and Communication Networks*, vol. 9, no. 16, pp. 3049-3058, 2016.

[45] Y. Shi, S. Abhilash, and K. Hwang, "Cloudlet mesh for securing mobile clouds from intrusions and network attacks," *in 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, pp. 109-118, 2015.

[46] R. Perez., R. Sailer, and L. van Doorn, "vTPM: virtualizing the trusted platform module," *in Proc. 15th Conf. on USENIX Security Symposium*, pp. 305-320, 2006.

[47] N. Paladi, C. Gehrmann, and A. Michalas, "Providing user security guarantees in public infrastructure clouds," *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 405-419, 2017.

[48] S. Jin, J. Ahn, J. Seol, S. Cha, J. Huh, and S. Maeng, "H-svm: Hardware-assisted secure virtual machines under a vulnerable hypervisor," *IEEE Transactions on Computers*, vol. 64, no. 10, pp. 2833-2846, 2015.

[49] M. Zolotukhin, and T. Hamalainen, "Detection of zero-day malware based on the analysis of opcode sequences," *in IEEE 11th Consumer Communications and Networking Conference (CCNC)*, pp. 386-391, 2014.

[50] P.M. Comar, L. Liu, S. Saha, P.N. Tan, and A. Nucci, "Combining supervised and unsupervised learning for zero-day malware detection," *in Proceedings of IEEE INFOCOM*, pp. 2022-2030, 2013.

[51] D. Kirat, G. Vigna, and C. Kruegel, "BareCloud: Bare-metal Analysis-based Evasive Malware Detection," *in USENIX Security Symposium*, pp. 287-301, 2014.

[52] G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, and A. Ribagorda, "Evolution, detection and analysis of malware for smart devices," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 961-987, 2014.

[53] S. Suguna and A. Suhasini, "Overview of data backup and disaster recovery in cloud," *in International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 1-7, 2014.

[54] L. Zeng, S. Xu, and Y. Wang, "VMBackup: an efficient framework for online virtual machine image backup and recovery," *Concurrency and Computation: Practice and Experience*, vol. 28, no. 9, pp. 2630-2643, 2016.

[55] "Security on Arm TrustZone," Arm, 2018. [Online]. Available: https://www.arm.com/products/security-on-arm/trustzone. [Accessed 2018].

[56] I. Anati, S. Gueron, S. Johnson, and V. Scarlata, "Innovative technology for CPU based attestation and sealing," *in Proceedings of the 2nd international workshop on hardware and architectural support for security and privacy*, pp. 1-6 , 2013.

[57] J. Jang, C. Choi, J. Lee, , N. Kwak, S. Lee, Y. Choi. and B. Kang, "PrivateZone: Providing a Private Execution Environment using ARM TrustZone," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 5, pp. 797-810, 2016.

Computing, p. 18 , 2017.

[20] K. Bhardwaj, M. Shih, P. Agarwal, A. Gavrilovska, T. Kim, and K. Schwan, "Fast, scalable and secure onloading of edge functions using AirBox," *in IEEE/ACM Symposium on Edge Computing*, pp. 14-27 , 2016.

[21] G Grassi, K Jamieson, P Bahl, and G Pau, "ParkMaster: An in–vehicle, edge–based video analytics service for detecting open parking spaces in urban environments," *in IEEE/ACM Symposium on Edge Computing*, p. 16, 2017.

[22] B. Qi, L. Kang, and S. Banerjee, "A Vehicle-based Edge Computing Platform for Transit and Human Mobility Analytics," *in IEEE/ACM Symposium on Edge Computing*, p. 1 , 2017.

[23] G. Kar, S. Jain, M. Gruteser, J. Chen, F. Bai, and R Govindan, "PreDriveID: Pre-Trip Driver Identification from In-Vehicle Data," *in IEEE/ACM Symposium on Edge Computing*, p. 2 , 2017.

[24] S. Echeverría, D. Klinedinst, K. Williams, and G. A. Lewis, "Establishing Trusted Identities in Disconnected Edge Environments," *in IEEE/ACM Symposium on Edge Computing*, pp. 51-63, 2016.

[25] Z. Chen, W. Hu, J. Wang, S. Zhao, B. Amos, G. Wu, K. Ha, K. Elgazzar, P. Pillai, R. Klatzky, and D. Siewiorek, "An Empirical Study of Latency in an Emerging Class of Edge Computing Applications for Wearable Cognitive Assistance," *in IEEE/ACM Symposium on Edge Computing,* p. 14 , 2017.

[26] P. Hua, S. Dhelima, H. Ninga, and T. Qiud, "Survey on fog computing: architecture, key technologies, applications and open issues," *Journal of Network and Computer Applications*, vol. 98, pp. 27-42, 2017.

[27] S. Khan, S. Parkinson, and Y. Qin, "Fog computing security: a review of current applications and security solutions," *Journal of Cloud Computing*, vol. 6, no. 1, p. 19, 2017.

[28] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *Journal of Network and Computer Applications*, vol. 84, pp. 38-54, 2017.

[29] Z. Kozhirbayev and R.O. Sinnott, "A performance comparison of container-based technologies for the cloud," *Future Generation Computer Systems*, vol. 68, pp. 175-182, 2017.

[30] Y. Guan, J. Shao, G. Wei, and M. Xie, "Data Security and Privacy in Fog Computing," *IEEE Network*, vol. 99, pp. 1-6, 2018.

[31] M. Almorsy, J. Grundy, and I. Müller, "An analysis of the cloud computing security problem," *arXiv preprint*, 2016.

[32] P. Li, J. Li , Z. Huang, CZ. Gao, WB. Chen , and K. Chen, "Privacy-preserving outsourced classification in cloud computing," *Cluster Computing*, vol. 21 , no. 1, pp. 277-286, 2017.

[33] J. Li, X. Tan, X. Chen, DS. Wong, and F. Xhafa, "OPoR: enabling proof of retrievability in cloud computing with resource-constrained devices," *EEE Transactions on cloud computing* , vol. 3, no. 2, pp. 195-205, 2015.

[34] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks: Revealing the secrets of smart cards*, Springer Science & Business Media, 2008.

[35] D. Fu and X. Peng, "TPM-based remote attestation for Wireless Sensor Networks," *Tsinghua Science and Technology*, vol. 21, no. 3, pp. 312-321, 2016.

[36] T. C. Group, "Trusted Platform Module TPM Summary," 2008. [Online]. Available: https://trustedcomputinggroup.org/trusted-platform-module-tpm-summary/. [Accessed 2017].

[37] A. Gosain, M. Berman, M. Brinn, T. Mitchell, C. Li, Y. Wang, H. Jin, J. Hua, and H. Zhang, "Enabling Campus Edge Computing using GENI Racks and Mobile Resources," *in IEEE/ACM Symposium on Edge Computing,* pp. 41-50, 2016.

[38] X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, "Robust Multi-Factor Authentication for Fragile Communications," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 6, pp. 568–581, 2014.

[39] V. Vassilakis, I. P. Chochliouros, A. S. Spiliopoulou, E. Sfakianakis, M. Belesioti, N. Bompetsis, M. Wilson, C. Turyagyenda, and A. Dardamanis, "Security Analysis of Mobile Edge Computing in Virtualized Small Cell Networks," *in Ch. 12th IFIP International*

[58] L. Guan, P. Liu, X. Xing, X. Ge, S. Zhang, M. Yu, and T. Jaeger, "TrustShadow: Secure execution of unmodified applications with ARM trustzone," *in Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, pp. 488-501 , 2017.

پریسا حسنی‌زاده مدرک کارشناسی و کارشناسی ارشد خود را در به ترتیب در سال های ۹۴ و ۹۷ از دانشکده فنی دانشگاه تهران و دانشگاه شریف در رشته مهندسی کامپیوتر دریافت نموده است. علاقه مندی های پژوهشی وی عبارتند از: امنیت و اعتماد سامانه های سخت‌افزار، طراحی سامانه‌ها برای پردازش لبه‌ای، طراحی توام سخت‌افزار و نرم‌افزار و تئوری رمزنگاری.
آدرس پست الکترونیکی ایشان عبارت است از:
hasanizadeh@ce.sharif.edu

سیاوش بیات‌سرمدی مدرک کارشناسی و کارشناسی ارشد خود را به ترتیب از دانشکده فنی دانشگاه تهران و دانشگاه شریف دریافت نموده است. او مدرک دکترای خود را در سال ۸۶ از دانشگاه واترلوی کانادا دریافت کرده‌است. وی از سال ۸۶ تا ۹۲ در شرکت AMD در کانادا مشغول به کار بوده و از سال ۹۲ استادیار دانشکده کامپیوتر دانشگاه شریف است. زمینه‌های پژوهشی مورد علاقه ایشان شامل مهندسی رمزنگاری، امنیت و اعتماد سخت‌افزار، امنیت سامانه‌های فیزیکی-سایبری، معماری‌های امن، کارا و قابل اطمینان است.
آدرس پست الکترونیکی ایشان عبارت است از:
sbayat@sharif.edu

[1] Heterogeneity
[2] Robust
[3] Virtual reality
[4] Augmented reality
[5] Edge computing
[6] Fog computing
[7] Edge paradigm
[8] Cloudlet
[9] Mobile edge computing (MEC)
[10] Mobile cloud computing (MCC)
[11] Open edge computing (OEC)
[12] Location awareness
[13] Real-time
[14] European telecommunications standard institute (ETSI)
[15] Base transceiver station (BTS)
[16] Gateway
[17] Access point
[18] Path computing
[19] Wide-area network (WAN)
[20] Wi-Fi
[21] Wearable cognitive assistant
[22] 1080p (Full HD)
[23] Connected vehicle
[24] Application programming interface (API)
[25] Intrusion detection
[26] Identity privacy
[27] Container
[28] Hypervisor
[29] Denial of service
[30] Misuse of resources
[31] Privacy leakage
[32] API
[33] Privilege escalation
[34] Manipulation
[35] Jamming
[36] Man-in-the-middle
[37] Rouge gateway
[38] Integrity
[39] Multi-factor authentication
[40] Single-point of failure
[41] Malicious insider
[42] Rouge infrastructure
[43] Semi-honest
[44] Side-channel attack
[45] Tampering
[46] Remote attestation
[47] Trusted platform module (TPM)
[48] Ad-hoc
[49] Patch
[50] Transport Layer Security(TLS)
[51] Attribute-based encryption
[52] Formal methods
[53] Policy driven engine
[54] Application administrator
[55] Policy resolver
[56] Policy repository
[57] Virtual private networks (VPN)
[58] Software defined network (SDN)
[59] Network function virtualization (NFV)
[60] Honest but curious
[61] Location privacy
[62] Homomorphic encryption
[63] Auditable data
[64] Anonymity
[65] virtual trusted platform module (vTPM)
[66] Machine learning
[67] Backup
[68] Trusted execution environment (TEE)
[69] Isolation

The CSI Journal on Computing Science and Information Technology

The CSI Journal on
Computing Science and
Information Technology
Vol. 17, No.1, 2019

Security of edge computing: a survey of challenges and solutions

Parisa Hasanizadeh, Siavash Bayat-Sarmadi

Department of Computer Engineering, Sharif University of Technology, Tehran, Iran

Abstract

In today's technology, cloud computing has a significant role in expanding applications of the Internet of Things (IoT). Support of unlimited resources and heterogeneous devices are interesting features of cloud computing in IoT. By expanding IoT applications to virtual reality, augmented reality and online group gaming, requirements such as latency of response time and network bandwidth have become increasingly important. The current architecture of cloud computing does not fully meet these requirements. To overcome such limitations, a new approach, namely edge computing, has been introduced recently. In edge computing, a layer of devices with storage, networking and processing capabilities is deployed between the cloud layer and user devices. This layer performs part or all of the needed data processing before sending it to the cloud. Due to the proximity of edge nodes to the user, processing in edge layer will reduce transferring and processing latencies. On the other hand, network traffic will also decrease due to pre-process of data before transferring to the cloud. Despite the advantages and improvements of edge computing compared to cloud computing, this approach faces many challenges due to its distributed nature and factors such as support for mobile users. Some of the aforementioned challenges are virtualization, resource management, outsourcing, security, privacy, and distribution of processing nodes. In this study, the edge computing architecture, features, and applications are introduced. Moreover, security challenges and available solutions in edge computing have been analyzed.

Keywords: Internet of Things, edge computing, fog computing, cloudlet, mobile edge computing, mobile cloud computing, security and privacy.