بسمه‌تعالی

گزارش و تحلیل مقاله

A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System

تعریف مسئله و هدف اصلی مقاله

توسعه و گسترش فناوری‌های سخت‌افزاری امکان تلفیق هوش مصنوعی (AI)، اینترنت اشیا، Edge computing و تصمیم‌گیری بلادرنگ را فراهم کرده است. ادغام هوش مصنوعی و اینترنت اشیا اصطلاح جدید به نام هوش مصنوعی اشیا (AIoT) ایجاد کرده که در آن دستگاه‌های اینترنت اشیا از سیستم عصبی دیجیتال و هوش مصنوعی به عنوان مغز سیستم استفاده می‌کند.

در AIoT دستگاه‌های اینترنت اشیا محدودیت دقت و سرعت انتقال اطلاعات دارند، در حالی‌که هوش مصنوعی بر اساس یک الگو یاد می‌گیرد و خود را بهبود می‌بخشد. AIoT در امور روزانه مثل سلامت هوشمند، خانه هوشمند و خرده‌فروشی هوشمند، به کار گرفته می‌شود. در این گونه کاربردها، تجهیزات AIoT اطلاعات را به سرویس‌های ابری از طریق Edge computing برای تصمیم‌گیری، منتقل می‌کنند.

برنامه‌های بهداشتی مبتنی بر AIoT پس از ادغام با AI-enabled Edge computing و شبکه‌های اینترنت اشیا ناهمگن برای انتقال بهینه و به موقع اطلاعات پزشکی، شهرت پیدا کردند.

از آنجا که در سیستم‌های مراقبت‌های بهداشتی، تجهیزات اینترنت اشیا به طور مداوم بیماران را کنترل می‌کنند و داده‌های مورد نیاز را به طور مداوم منتقل می‌کنند، لازم است از فعالیت‌های مخرب[1] محافظت شوند.

سامانه‌های مراقبت‌های بهداشتی، با دو مشکل اصلی انتقال دائم و ایمن اطلاعات روبرو است. یکی از بهترین راه‌های ایمن‌سازی شبکه اینترنت اشیا low-power استفاده از احراز هویت سبک است. با وجود تجهیزات low-power انتقال دائم اطلاعات در حالی‌که چندین داده از بدن بیمار جمع‌آوری می‌شود، امکان‌پذیر نیست. غلبه بر این مشکلات با استفاده از روش احراز هویت سبک و پردازش داده‌ها در نزدیکی محل جمع‌آوری آن‌ها، با استفاده از Edge computing ممکن می‌شود. در AIoT هوش مصنوعی در تجهیزات تعبیه می‌شود و Edge computing برای رساندن هوشمندی به تجهیزات به کار می‌رود. یکی از روش‌های طراحی این چنین سیستمی، استفاده از کنترلر SDN در سرور Edge یا کنترلر هوشمند SDN در کمک به سرور Edge است که به موجب تعادل بار و استفاده بهینه از منابع می‌شود.

---

[1] Malicious activities

در سیستم‌های مراقب بهداشتی مبتنی بر اینترنت اشیا، تجهیزات باید قبل از ارسال اطلاعات، احراز هویت شوند. پس از احراز هویت، داده‌های حس شده باید برای پردازش سریع به Edge computing سپرده شوند. اطلاعات سپرده شده به Edge با کمک کنترلر SDN که توانایی برنامه‌ریزی کامل شبکه را دارد، به صورت هوشمندانه پردازش می‌شوند. هوشمندی SDN نیازهای Edge computing از نظر تخصیص منابع و توازن بار، برآورده می‌کند. کنترلر SDN وظیفه مدیریت داده‌ها، حساسیت به زمان، برنامه‌ریزی Edge و انتقال سریع و پایدار اطلاعات را برعهده دارد. این خصوصیات، نیازهای اصلی یک سیستم مراقبت بهداشتی هستند که به صورت جامع در یک راه‌کار ارائه نشده‌اند.

در این مقاله برای پر کردن خلا تحقیقات موجود با ترکیب این تکنولوژی‌ها، یک چارچوب ایمن برای Edge computing مبتنی بر SDN در سیستم مراقب بهداشتی مبتنی بر IoT ارائه شده است. در چارچوب پیشنهادی این مقاله یک روش احراز هویت سبک و Edge computing مبتنی بر SDN برای توازن بار بین سرورهای Edge برای غلبه بر محدودیت‌های یک سرور Edge، به کار گرفته شده است.

بررسی مفاهیم پایه

اینترنت اشیا

اینترنت اشیا در حال پیشرفت است و میلیاردها تجهیز متصل به اینترنت آن را شکل می‌دهد. اینترنت اشیا الگوی جدیدی در ارتباطات است که اتصال دستگاه‌های موجود با هوشمندی بیشتر را فراهم می‌کند. این دستگاه‌ها، داده‌های حس شده را پردازش می‌کنند و از طریق اینترنت با دستگاه‌های دیگر ارتباط برقرار می‌کنند. ابتدا بر پایه روش‌های مثل ZigBee عمل می‌کردند. امروزه بر پایه 4G عمل می‌کنند و در حال گسترش برای استفاده از تکنولوژی 5G هستند.

امنیت در اینترنت اشیا

محدودیت منابع، تجهیزات اینترنت اشیا را در معرض تهدیدات مختلف قرار می‌دهد. تهدیداتی که active یا passive هستند و از بیرون یا داخل شبکه اعمال می‌شوند. حملاتی مانند reply، sniffing و eavesdropping کیفیت شبکه را کاهش می‌دهند. در این میان حملات Sybil و DoS خطرناک‌ترین نوع حملات هستند که شبکه را مختل و منابع هدر می‌دهند. در مطالعات پیشین، معماری Cloud-Fog مبتنی بر اینترنت اشیا، برای مدیریت بهینه منابع پیشنهاد شده است.

شبکه‌های نرم‌افزار محور SDN

محور اصلی شبکه‌های SDN تفکیک Data plane و Control plane است. SDN به ساده شدن مدیریت شبکه‌های آینده، اینترنت اشیا، محاسبات ابری و سیستم‌های مجازی-فیزیکی کمک می‌کند. البته خود SDN با مشکل Single point of failure (SPF) روبرو است که می‌تواند کل شبکه را به چالش روبرو کند.

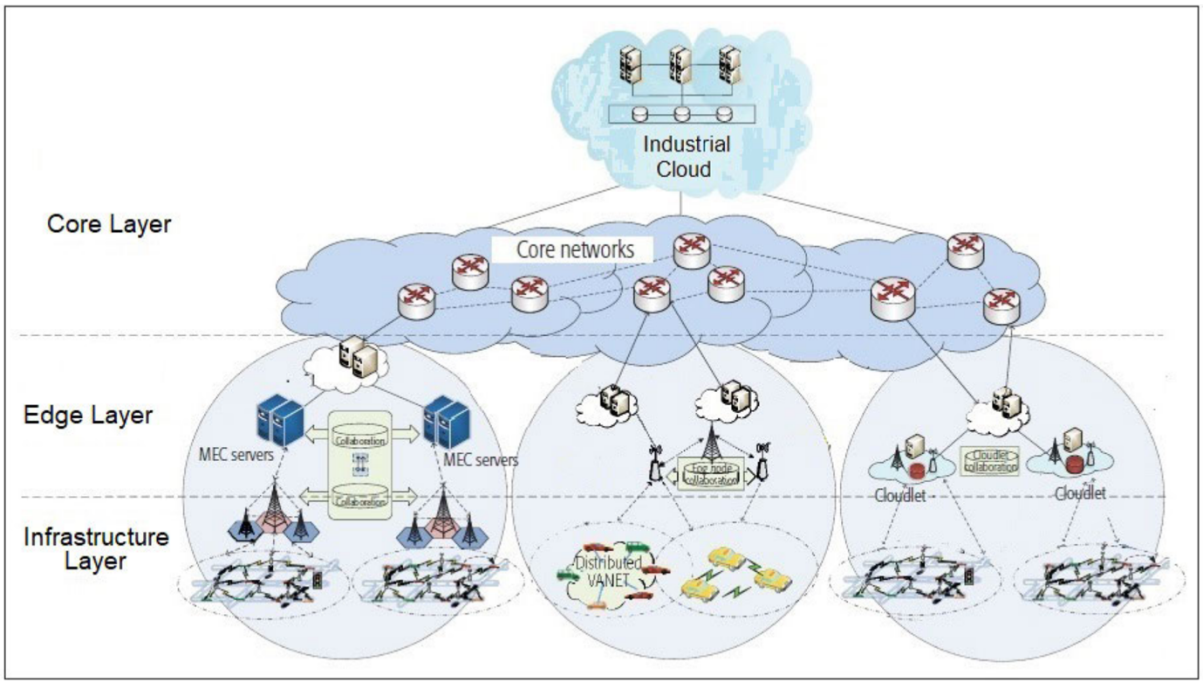
Edge computing

پارادایم Edge computing، یک پارادایم اقتصادی و بهینه برای گسترش محاسبات ابری است. این روش با نزدیک کردن منابع محاسباتی به لبه شبکه IoT، خدمات داده با تاخیر کم را ارائه می‌کند. در یکی از تحقیقات پیشین، با مفهوم خوشه‌بندی، توانایی پردازش کل سیستم افزایش داده شده است. هم‌چنین در تحقیقی دیگر، با استفاده از Edge computing، ارتباط ایمن مغز-به-مغز که گیرنده، ادراک فرستند را دریافت می‌کند، ایجاد شده است.

راه‌حل پیشنهادی مقاله برای مسئله

مدل راه‌حل پیشنهادی

سه لایه در مدل پیشنهادی این مقاله در نظر گرفته شده است (تصویر- ۱).



تصویر- ۱

- لایه Infrastructure: این لایه شامل تجهیزات اینترنت اشیا و سنسورهای low-power مثل تجهیزاتی که بدن بیمار متصل شده و یا در بیمارستان نصب هستند، می‌باشد. این تجهیزات باید با اطلاعات معتبر و در ارتباط با دیگر تجهیزات به صورت کارآمد استفاده شوند.
- لایه Edge computing: این لایه از سرورهای مختلف Edge شکل گرفته است. این لایه عملکردهای مختلفی مانند تبادل اطلاعات، ذخیره‌سازی، پردازش و انتقال عملیات بین سرورها را دارد. این لایه خود حملاتی نظیر man-in-the-middle، reply، محرمانگی و یکپارچگی داده را دارد که تاخیر و سربار زیادی را به شبکه تحمیل می‌کند.

- لایه Core computing: این لایه دو بخش شبکه‌های Core و سرویس‌های ابری را دارد. شبکه‌های Core وظیفه میزبانی از برنامه‌های مختلف IoT و سرویس‌دهی و مدیریت end-to-end معماری IoT را برعهده دارد. این لایه مکانیزم‌های جلوگیری از حملات به جز حمله DoS را دارد. مقابله با تهدیدات این لایه از طریق احراز هویت، اعطای دسترسی و رمزنگاری صورت می‌پذیرد.

روش پیشنهادی مقاله، SDN-BASED EDGE IN IoT-ENALBED HEALTHCARE

سه فاز اصلی برای روش پیشنهادی این مقاله وجود دارد که در ادامه به شرح آن می‌پردازیم.

رویکرد احراز هویت سبک

لایه زیرساخت یا همان لایه مراقبت بهداشتی مبتنی بر IoT، هیچ مکانیسم درونی امنیتی درونی ندارد. در چارچوب پیشنهادی یک روش احراز هویت سبک ارائه داده شده است.

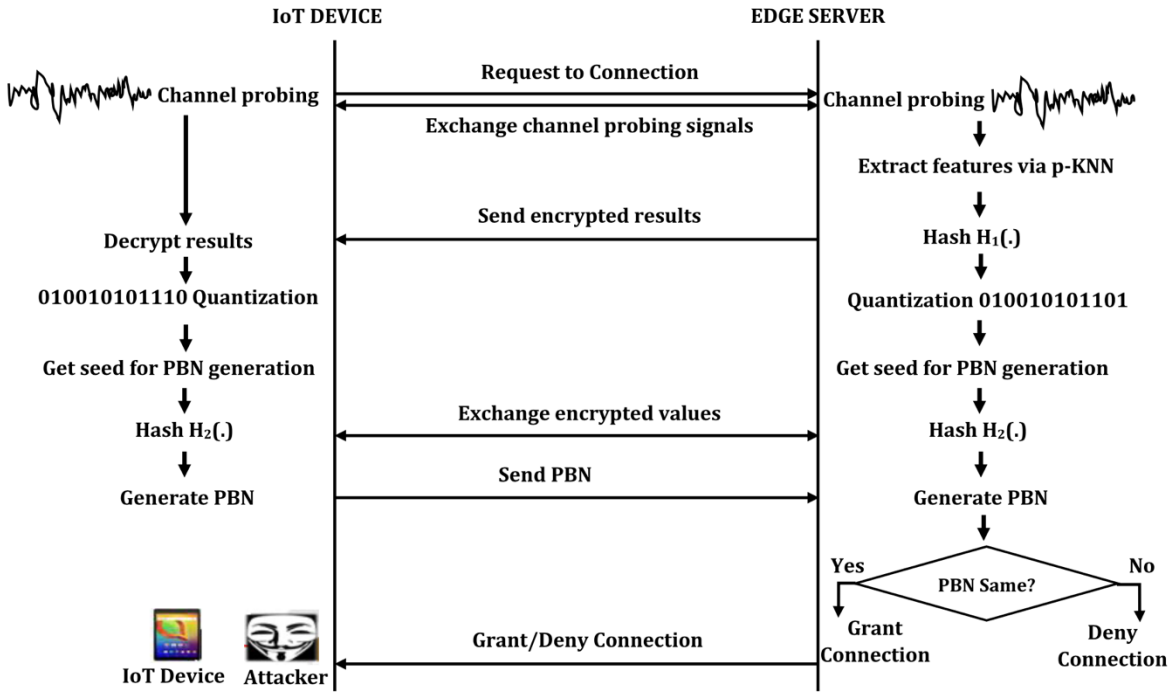
در این چارچوب با استفاده از probabilistic k-nearest neighbor (p-KNN) مشخصات کانال ارتباطی استخراج شده و دو تابع Hash (H1 و H2) برای رمزگذاری مشخصات انتخابی و نتایج پیمانه شده، به کار می‌رود. در این روش تجهیزات IoT بر اساس باند فرکانس کاری، فرکانس‌های دسترسی و فرجه‌های زمانی[1]، شناسایی می‌شوند. روند کامل این روش در تصویر- ۲ شرح داده شده است.

شبه کد این روش احراز هویت، به صورت زیر است:

Initialization: sum = 0.
input: communication channels

procedure
  for each $Edge_{server}$ **do**
    Perform channel probing using [28]
    Extract features using p-KNN, and remove outliers
    Encrypt features with hash $H_1(.)$
    Send encrypted data to $Device_i$
    Perform quantization using [31] ▷ $Device_i$ also performs quantization
    Exchange encrypted (using $H_2(.)$) quantization results
    $Edge_{server}$ and $Device_i$ acquires the seed for generating the PBN ▷ Both parties generate PBN
    $Device_i$ sends PBN to the $Edge_{server}$ for authentication
    $Edge_{server}$ check if PBN are identical
    if true **do**
      Grant access to this legitimate $Device_i$
    else
      Abort connection and save ID as intruder
    end if
  end for
end procedure

[1] Time-slots



تصویر- ۲

مشارکتی مبتنی بر SDN Edge computing

لایه Edge computing از سرورهای مختلف Edge مبتنی بر SDN شکل گرفته است که مسئولیت پردازش هوشمند داده‌ها، ذخیره‌سازی و تعامل با دیگر سرورها را دارد. کنترلر SDN بر اساس بار این سرورها و قوانین از پیش تعیین شده، شیوه تعامل بین سرورهای Edge را مشخص می‌کند. بر اساس الگوریتم زیر این روند انجام می‌شود:

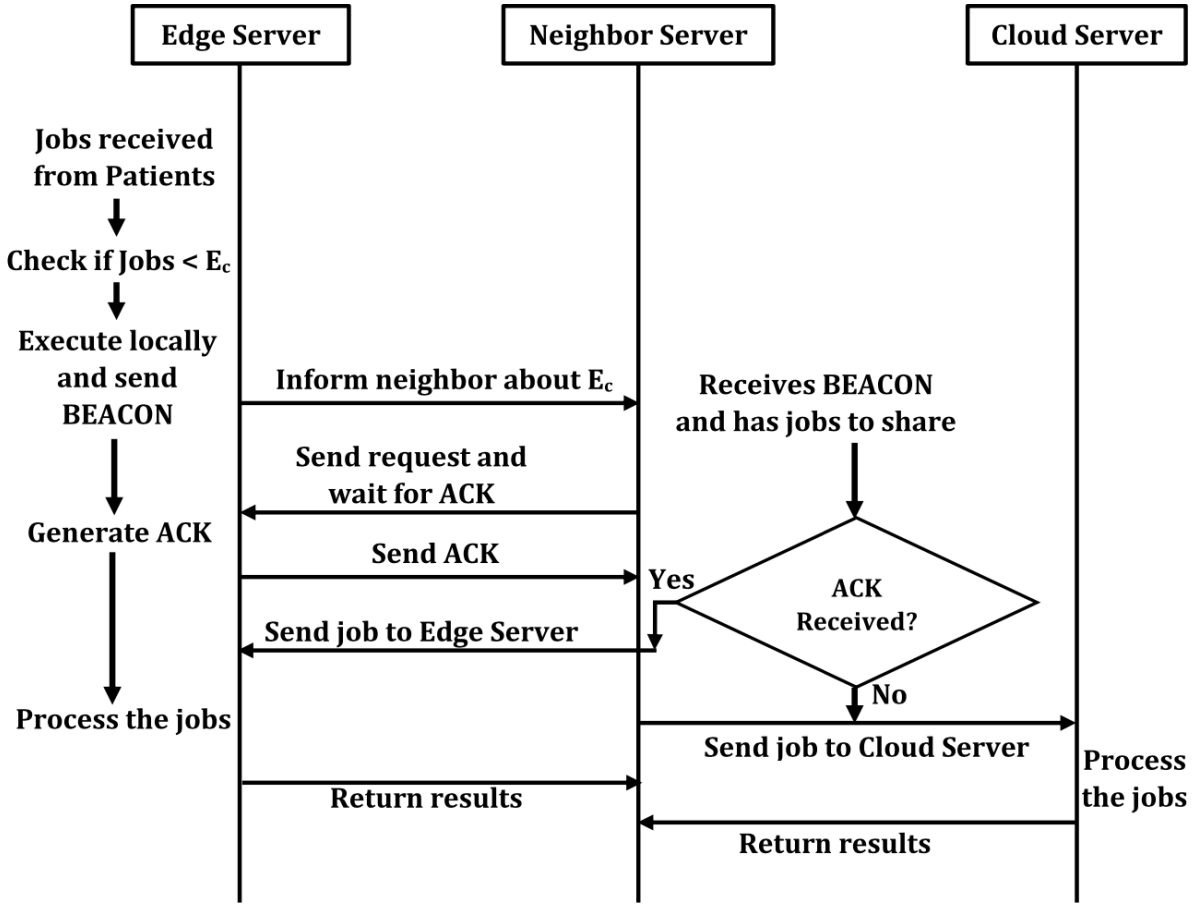
Initialization: sum = 0.
input: j ▷ A job j, submitted by a node in IoT-enabled network.

1: **procedure**
2: **for** each E_i **do** ▷ E_i is Edge server
3: sum the size of all submitted jobs j
4: $sum_i = sum_i + size_j$
5: **if** $sum_i < E_c$ **do** ▷ E_c is Edge server capacity
6: Process the job locally
7: E_i also sends a BEACON to its neighbors E_{i-1} and/or E_{i+1} as a potential candidate space and time for sharing processing ▷ BEACON shows available
8: **else**
9: E_i submits j to Neighboring server
10: **end if**
11: **end for**
12: **end procedure**

انتقال وظایف بین سرورهای Edge

روند انتقال وظایف در تصویر- ۳ به نمایش درآمده است. هنگامی که یک سرور Edge کاری را از تجهیزات بیمار دریافت می‌کند، تعداد کارها را بر اساس ظرفیت خود را بررسی می‌کند. اگر ظرفیت خالی داشت کار را به صورت محلی انجام داده و یک Beacon به سرورهای همسایه ارسال می‌کند. این سیگنال Beacon اطلاعات تعداد کارهایی که فرستنده می‌تواند انجام دهد را شامل می‌شود. هنگامی که سرور همسایه کار برای اجرا دارد

و این Beacon را دریافت می‌کند، یک درخواست برای انجام کار ارسال کرده و منتظر ACK می‌شود. اگر ACK در زمان مورد انتظار دریافت شود، کار به سرور همکار ارسال شده و در غیر این‌صورت به سرور ابری جهت پردازش ارسال می‌شود.



تصویر- ۳

الگوریتم این روش به صورت زیر است:

input: List of Potential Candidates from Algorithm 2.

1: **procedure**
2: **while** BEACON received AND has a job to share? **do**
3: Neighbor node sends j to E_i and waits for ACK
4: **if** ACK received on-time **do**
5: E_i submits j to E_i
6: **else**
7: j is submitted to Cloud server
8: **end if**
9: **end while**
10: **end procedure**

ارزیابی روش پیشنهادی

راه‌اندازی آزمایشی

شرایط شبیه‌سازی روش پیشنهادی این مقاله در جدول تصویر- ۴ آمده است.

Parameters	Values
Number of Patients	1000
Number of Edge Servers	[5 -50]
Channel data rate	1 [Mbps]
Antenna type	Omni direction
Radio Propagation	Two-ray ground
Transmission range	250 [m]
Simulation time	1000 [s]

تصویر- ۴

معیارهای ارزیابی عملکرد

معیارهای ۵ گانه ارزیابی عملکرد روش پیشنهادی به این صورت هستند:

۱) Average Response Time: میانگین زمانی که سرور Edge اطلاعات پردازش شده را به بیمار برمی‌گرداند.

۲) Packet Delivery Ratio: تعداد بسته‌های ارسالی به تعداد بسته‌های دریافتی

$$pdr = \frac{\sum_{i=1}^{n} S_i}{\sum_{i=1}^{n} R_i} \times 100$$

۳) Average Delay:

تاخیر (δ) کل زمانی است که نیاز است تا بسته در مقصد به صورت موفق دریافت شود. که τ زمان انتقال بسته و μ زمان دریافت موفق در مقصد است.

$$\delta = \tau - \mu$$

میانگین تاخیر

$$E(\delta) = \frac{\sum_{i=1}^{n} \delta_i}{n}$$

۴) Throughput (η): نرخ داده در شبکه به صورت نرمال بر حسب bps یا pps است که جمع تمام نرخ گره‌های شبکه Throughput است.

$$\eta = \frac{\sum_{i=1}^{n} R_i}{\sum_{i=1}^{n} S_i}$$

۵) Control Overhead (υ): نرخ کل پیام‌های کنترلی ایجاد شده توسط هر گره در شبکه به کل بسته‌های صحیح دریافتی است که در آن Ci تعداد بسته‌های کنترلی است

$$v = \frac{\sum_{i=1}^{n} C_i}{\sum_{i=1}^{n} R_i}$$

نتایج ارزیابی

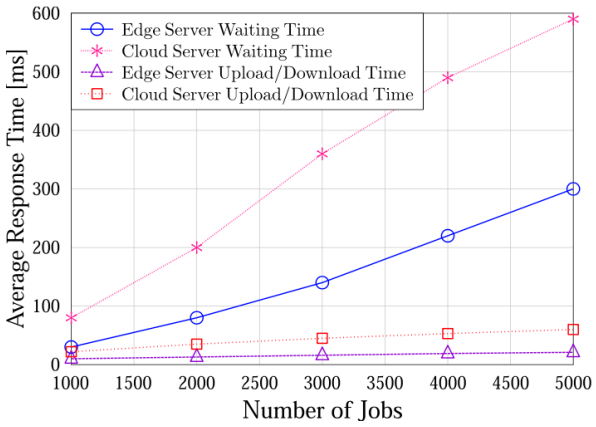
۱) AVERAGE RESPONSE TIME (ART): در تصاویر تصویر- ۵، تصویر- ۶ و تصویر- ۷ ارزیابی ART به نمایش درآمده است.

۲) PACKET DELIVERY RATIO (PDR): در تصویر- ۸ بر اساس سه سناریو PDR محاسبه شده است.

۳) AVERAGE DELAY: میانگین تاخیر بر اساس سه سناریو در تصویر- ۹ و تصویر- ۱۰ به نمایش در آمده است.

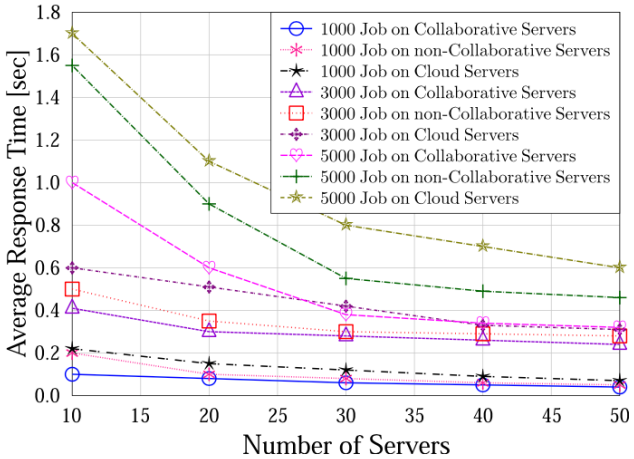
۴) THROUGHPUT: در تصویر- ۱۱ بر اساس به سه سناریو به نمایش در آمده است.

۵) CONTROL OVERHEAD: هم‌چنین میزان سربار کنترل در تصویر- ۱۲ بر اساس به سه سناریو به نمایش در آمده است.



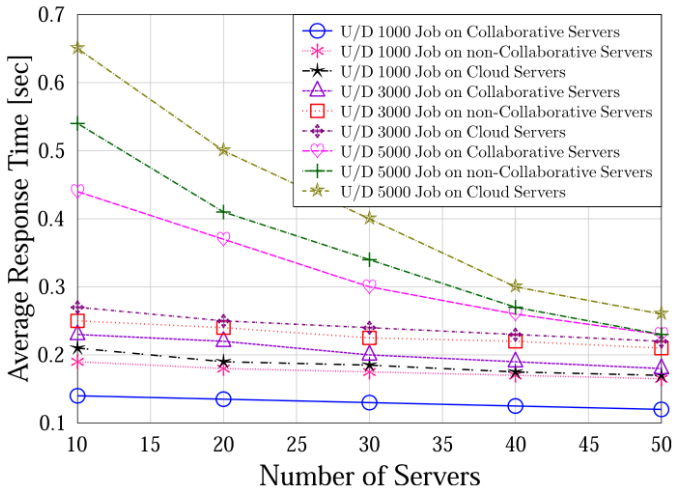
Waiting and upload/download time of edge and cloud server.

تصویر- ۵



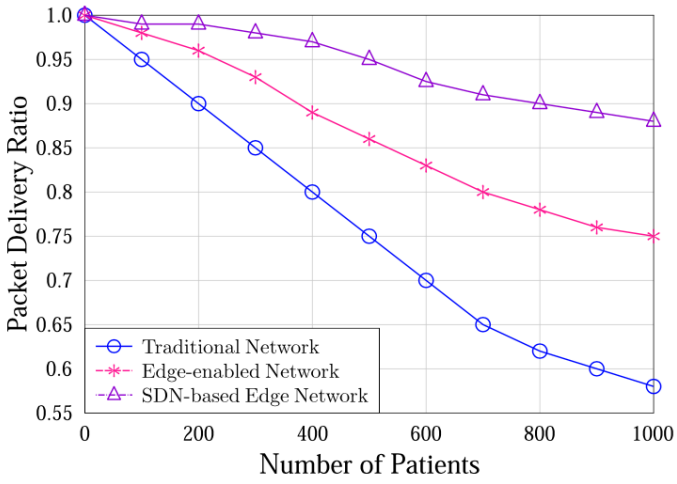
System loads for various number of servers.

تصویر- ۶



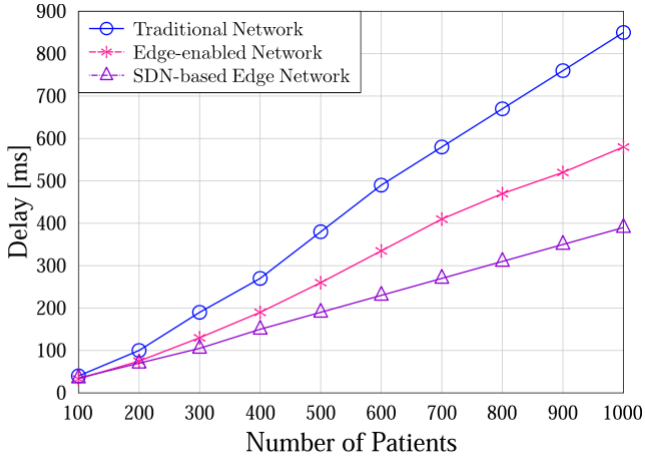
Packet loss against number of nodes.

تصویر- ۷



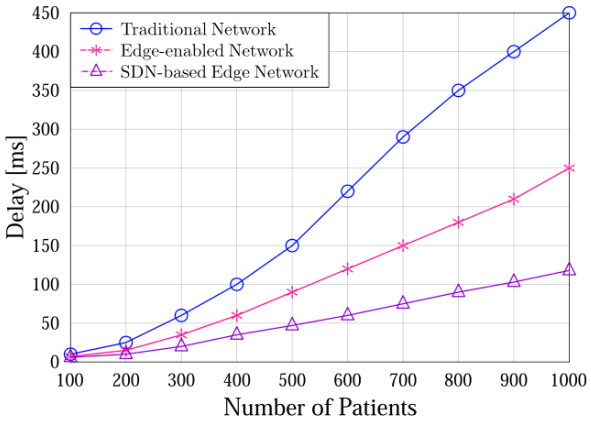
Packet deliver ratio against the number of patients.

تصویر- ۸



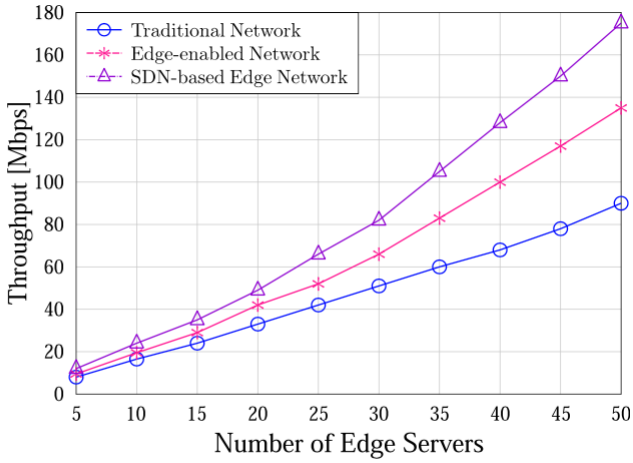
Average delay against number of patients.

تصویر- ۹



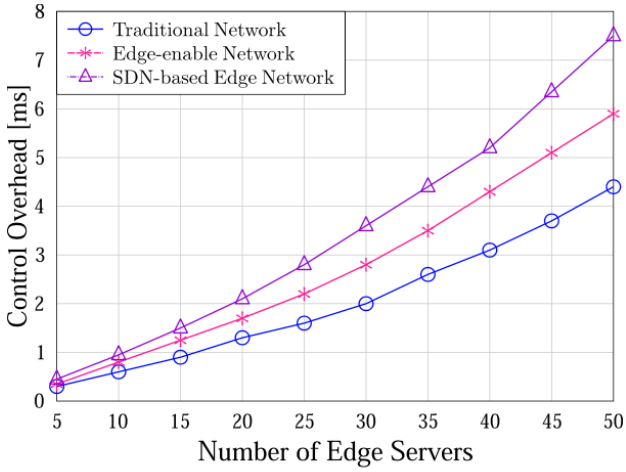
Average delay of critical data against number of patients.

تصویر- ۱۰



Throughput against number of edge servers.

تصویر- ۱۱



Control overhead against number of edge servers.

تصویر- ۱۲

نقاط قوت و ضعف مقاله

نقاط قوت این مقاله:

- افزایش کارایی و عملکرد شبکه در کنار سربار ناچیز کنترلری اعمال شده
- درنظر گرفتن توان کم تجهیزات اینترنت اشیا و روش ابتکاری احراز هویت سبک

نقاط ضعف این مقاله:

- معماری پیشنهادی به دلیل اتکا بر یک کنترلر SDN می‌تواند در برابر مخاطرات یا تهدیدات، به دلیل مشکل SPF، دچار شکست شود.

جمع‌بندی و پیشنهادات برای کارهای آتی

در این مقاله، یک چارچوب امن برای Edge computing مبتنی بر SDN در سیستم‌های مراقبت‌های بهداشتی مجهز به اینترنت اشیا ارائه شده است. احراز هویت دستگاه‌های اینترنت اشیا با استفاده از یک طرح احراز هویت سبک انجام می‌شود. پس از احراز هویت، داده‌های بیماران برای پردازش به سرور Edge ارسال می‌شود. سرورهای Edge برای تعادل بار همکاری می‌کنند و دارای یک کنترل کننده SDN پیکربندی شده برای تصمیم گیری هوشمند هستند. Edge computing مبتنی بر SDN دارای همکاری بهتر Edge و استفاده بهینه از منابع از طریق پیکربندی بهینه شبکه است. این منجر به عملکرد بهتر شبکه در شاخص‌هایی مانند زمان پاسخگویی متوسط، نسبت تحویل بسته، تاخیر، توان عملیاتی و سربار کنترل شبکه می‌شود. نتایج شبیه‌سازی برای سه سناریوی مختلف شبکه، کارایی طرح پیشنهادی مقاله را تایید می‌کند.

در این راه‌کار مواردی در نظر گرفته نشده است و یا نیاز به تکمیل دارند که به صورت کار آتی می‌توان در نظر گرفت:

- افزایش امنیت چارچوب پیشنهادی با محافظت از حریم خصوصی بیماران و داده های آن‌ها
- ذخیره الگوهای داده و استفاده از یک الگوریتم یادگیری ماشین برای پیش بینی فعالیت های مخرب در شبکه
- افزودن روش‌های لاگ‌برداری در راستای افزایش امنیت شبکه
- افزودن Redundancy به کنترلر SDN برای حل مشکل SPF در SDN

مشخصات دقیق مقاله

Li, Junxia, Jinjin Cai, Fazlullah Khan, Ateeq Ur Rehman, Venki Balasubramaniam, Jiangfeng Sun, and P. Venu, "A Secured Framework for SDN-Based Edge Computing in IoT-Enabled Healthcare System", IEEE Access, vol.8, pp.135479-135490, 2020