فصلنامه پژوهش در علوم، مهندسی و فناوری
دوره ۷، شماره ۱، بهار ۱۴۰۰
صفحات ۱۴۳-۱۵۴
ISSN: 2476-5082
www.uctjournals.com

بررسی نقش رایانش ابری بر سیستم های مراقبت سلامت در دوران کرونا

مهلا نظری سیاسر
دانش آموخته کارشناسی ارشد، گروه کامپیوتر، دانشگاه آزاد، واحد زاهدان

چکیده

پیشرفت های اخیر در زمینه ی سیستم های مراقبت سلامت از راه دور شاهد ایجاد علاقه زیادی در حوزه ی صنعت IT (مایکروسافت، گوگل، VMware و ...) بوده است، به طوریکه که سیستم های مراقبت سلامت با قابلیت گسترش آسان و در هر جا را فراهم می کند. این سیستم ها امکانی را برای اشتراک اطلاعات پزشکی، کاربردهای پزشکی و زیرساختارهای موردنیاز به صورت کاملاً خودکار و قابل دسترس در همه جا فراهم می کنند. امنیت مخابراتی و محرمانه سازی داده های فرد بیمار مواردی هستند که باعث افزایش اطمینان خاطر کاربران در حوزه ی سیستم های مراقبت از راه می شوند. این مقاله یک چارچوب مراقبت از سلامت انسانِ در حال حرکت را به صورت محاسبه ابری با استفاده از شبکه های بی سیم تعبیه شده در بدن (WBAN) ارائه می دهد.کار علمی ای که در اینجا تقدیم می شود شامل دو قسمت است: در قسمت اول، تلاش شده است که ارتباطات بین سنسوری توسط زیست سنجی های چندگانه (مانند اثرانگشت و اندازه مردمک چشم و ...) براساس طرح تولید کلیدهای رمز امنیتی در شبکه WBAN امن تر شود و در قسمت دوم، پرونده ها و داده های پزشکی الکترونیکی (EMR) به طور امن در ابر مجموعه ی بیمارستانی ذخیره شود و محرمانه بودن داده های بیماران حفظ شود. ارزیابی ها و تحلیل نشان می دهد که این مکانیزم پیشنهاد شده براساس زیست سنجی های چندگانه، اقدامات امنیتی قابل توجهی را از طریق مکانیزم تولید کلیدهای امنیتی فراهم می کند که از کارایی بسیار بالایی برخوردار است.

کلیدواژه: مراقبت سیار، شبکه ی بیسیم تعبیه شده در بدن (WBAN)، امنیت داده ها ، محاسبات ابری

مقدمه

شبکه های بیسیم تعبیه شده در بدن (WBAN) شامل گره های سنسوری کوچک و ریزی هستند که روی بدن یا درون بدن انسان به منظور اندازه گیری پارامترهای زیستی بدن تعبیه یا کاشته می شود. WBANها کارایی موفقیت آمیزی را در حوزه ی مراقبت از سلامت بدن انسان داشته اند که شامل مفاهیمی مانند سلامت الکترونیکی، نظارت و کنترل بیمار از راه دور، نظارت و کنترل سلامت سربازان در میادین جنگی می شود. با ادغام و پیوستن WBAN ها با مفاهیم محاسبات ابری، کارایی آنها، مقیاس پذیری و عملکرد کلّی این سیستم با به اشتراک گذاری منابع، باتوجه به وجود مقادیر زیاد دستگاه ها در ابر محاسباتی، افزایش می یابد. با این روش قدرت محاسبات و قابلیت ذخیره سازی اطلاعات شبکه WBAN می تواند تا حد زیادی افزایش یابد. محاسبات ابری تمایل به خلق یک نسل جدید از معماری کاربردی این سیستم را ایجاد می کند[1].

هدف این پژوهش توسعه معماری برای یک سیستم مراقبت از سلامت بیمار سیار براساس محاسبات ابری است که قابلیت هایی مانند: عمومی بودن، اطمینان و اعتماد بالا، گسترش آسان و ایمن و قابلیت استفاده در هر مکان را دارد. این پژوهش شامل دو مرحله است: در مرحله اول، امنیت ارتباطات سنسورها در شبکه WBAN امن می شود، در حالی که در مرحله ی دوم پرونده های پزشکی الکترونیکی (EMR) به طور امن در ابر مجموعه ی بیمارستانی ذخیره می شود و محرمانه بودن داده های شخصی بیماران حفظ می شود.که در این مرحله یک پرسش میدانی هم انجام شده است[2].

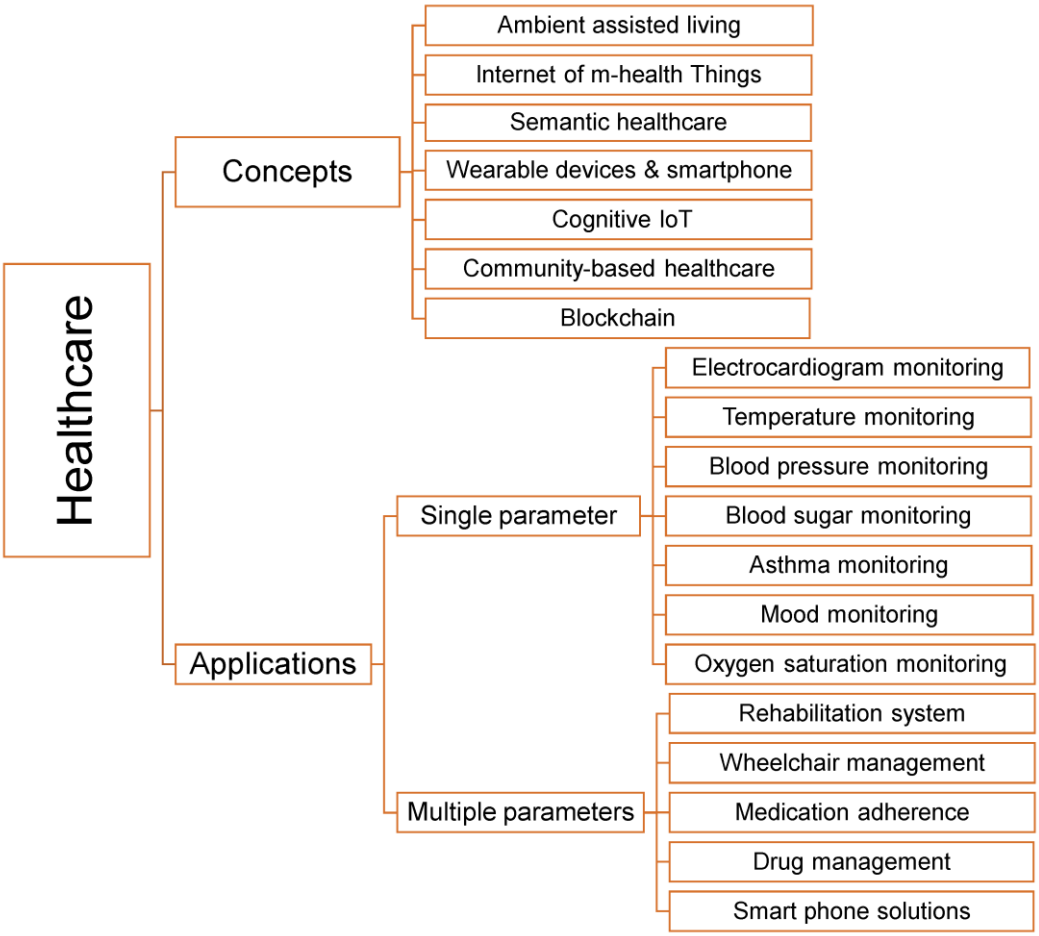
این چارچوب پیشنهادی از سنسورهایی استفاده می کند که در بدن انسان تعبیه می شود و مقادیر زیستی را اندازه می گیرد و به طور امن به سرورهای دیگری که در ابر مجموعه ی بیمارستانی قرار دارند ارسال می کند. سپس پزشکان و سایر پرسنل پزشکی که به این ابرمحاسباتی متصل هستند، معالجات بیمار را براساس این مقادیر اندازه گیری شده انجام می دهند. معماری کلی سیستم پیشنهادی ما در شکل یک نشان داده شده است که شامل سنسورهای تعبیه شده در بدن بیماران و یک گذرگاه داده برای هر بیمار است. (یعنی یک PDA یا کامپیوتر لپ تاپ). کاربران بیرونی و درونی یعنی بیماران، پزشکان و کادر پزشکی به این ابر متصل هستند و قادرند به اطلاعات و منابع به طور ویژه و مناسب دسترسی داشته باشند و هم چنین از امنیت و محرمانه بودن این منابع اطمینان داشته باشند. همه ی منابع و اطلاعاتی که ایجاد شده اند در ابر مجموعه ی بیمارستانی برای کابران ثبت شده، در دسترس می باشد. چارچوب پیشنهادی برحسب امنیت ارتباطات بین سنسوری و محرمانه بودن داده های بیماران ارزیابی شده اند. نتایج حاصل شده، خیلی دلگرم کننده هستند و اعتبار معماری پیشنهادی برای سیستم های مراقبت سیار نسل بعد را نشان می دهند[3].

ادامه تحقیق به ترتیب زیر می باشد:

بخش ۲ کارهای مربوطه انجام شده را تشریح می کند. بخش ۳ چارچوب پیشنهادی برای مراقبت سیار براساس محاسبات ابری را ارائه می دهد. بخش ۴ نتایج و تحلیل ها را نشان می دهد و بخش ۵ نیز به نتیجه گیری تحقیق می پردازد.

کارهای انجام شده مربوطه:

در شکل ۱ زمینه های پژوهشی مشخص شده است



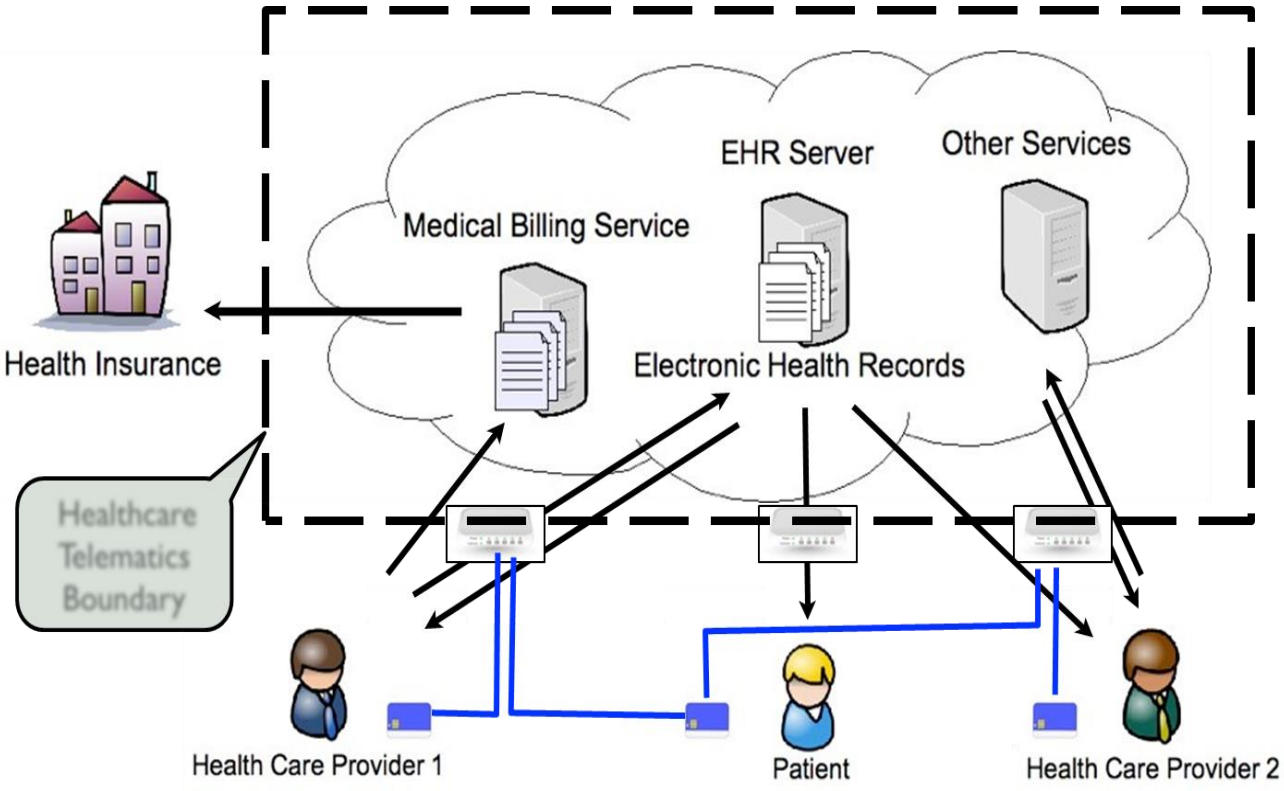
شکل ۱ زمینه های پژوهشی

این بخش براساس ماژول هایی که سیستم مراقبت امن برمبنای محاسبات ابری را تشکیل می دهند به سه قسمت تقسیم می شود که عبارتند از: سیستم نظارت و کنترل و مراقبت بیمار، معماری براساس محاسبات ابری و توافق کلید رمزی و امنیتی برپایه مقادیر زیستی. یک سیستم نظارت بیمار براساس PDA ، یک سیستم نظارت بر بیمار است که دستیار دیجیتال شخصی (PDA) و یک شبکه محلی بی سیم را به کار می گیرد (WBAN).[4] همچنین code blue برای ارتقاء توانایی نیروهای امداد و نجات پیشنهاد شد تا بیماران را در حالی که کارهای عادی خود را انجام می دهند، مورد ارزیابی قرار دهد. سیستم سلامت سیار یا Mobi Health یک طرح زیر بنایی مراقبت سلامت بیمار به صورت نقطه به نقطه برای نظارت بیمار متحرک براساس شبکه های GPRS و UMTS است. سیستم های مراقبت سیار که در بالا بحث شدند براساس محاسبات ابری طراحی نشده اند و از این جهت با مشکلاتی مانند عدم دسترسی، عدم ذخیره سازی داده ها و قابلیت های محاسباتی پایین مواجه می شدند. در مرجع [3]محققان ایده ی اتصال یک دستگاه متحرک به یک ابر محاسباتی را به منظور دریافت اطلاعات باارزش از طریق مکانیزم های پرس و جو پیشنهاد دادند، پرس و جو هایی مانند: "مقدار دمای میانگین گره ها در فاصله ی یک مایلی از موقعیت من چقدر است؟". ابر محاسباتی محرمانه و امن سیستم بیمارستان سامانهٔ VM Ware ، خدماتی را از طریق یک مدل IAAS (زیر ساخت به عنوان یک سرویس) یا SAAS (نرم افزار به عنوان یک سرویس) ارائه می کند. شرکت مایکروسافت (مرجع [3]) قصد دارد سلامت کاربر یا یک شخص را بوسیله ی نظارت و ردیابی شرایط سلامت یا فعالیت بدن از طریق شبکه سنسوری با محاسبات ابری نفوذی مدیریت کند. Dossia یک سرویس ثبت پرونده های مربوط به سلامت اشخاص است که توسط جمعی از بزرگترین کارفرمایان در ایالات متحده ارائه شده است[۵] . در مورد موضوع امنیت بر مبنای مقادیر داده ها زیستی محققان در مرجع [6]از داده های الکتروکاردیوگرام (ECG) برای تولید کلیدهای رمز با استفاده از تبدیل ویولت

گسسته (DWT) برای استخراج ویژگی، استفاده کردند. در مرجع [7]و [8]یک پروتکل مدیریت کلید رمز دو به دو پیشنهاد شده است که از داده های سرعت سنج (از یک دستگاه قابل حمل دستی) به عنوان یک مقدار داده زیستی برای تولید کلیدهای رمز استفاده می کرد. این طرح بوسیله لرزاندن فیزیکی دستگاه های ارتباطی اجرا می شود. در مراجع [9]و [10]یک پروتکل توافق کلید رمزی امن براساس مفهوم خوشه ها برای WBAN ها ارائه شده است که این شبکه را به صورت شبکه سنسوری ناهمگن در نظر می گیرد و شامل یک گره سنسور قدرتمند گران قیمت و چندین گره سنسوری ارزان می باشد. در مرجع [11]مقادیر زیستی به عنوان واسطه ای برای امنیت در شبکه های WBAN بکار می روند. سیستم های نظارت و کنترل سلامت که در بالا ذکر شد هرکدام سیستم هایی با زیرساخت ثابت هستند و یا اینکه ارتباطات آنها قابلیت حضور در هرجا را ندارد و فاقد استاندارد مشخص اتصال قطعات می باشند. طرح های توافق کلید رمز برمبنای داده های زیستی که در بالا بحث گردید فقط مبتنی بر یک مقدار داده زیستی تنها می باشد و از این رو فاقد خاصیت تصادفی بودن و طول کلید رمز کافی می باشند. پژوهش ارائه شده در این مقاله یک روش مبتنی بر محاسبات ابری را ارائه می کند، به طوری که سلامت بیماران به طور ایمن با استفاده از سنسورهای کاشته شده در بدن، کنترل و نظارت می شود و در عین حال داده های حساس بیمار به طور محرمانه حفظ می شود[1].

چارچوب پیشنهادی

چهارچوب پیشنهادی این پژوهش شامل سنسورهایی است که به یک بیمار، یک سرور شخصی، یک واسط یا داده خوان پردازشگر، ایستگاه پایه از راه دور و یک ابر محاسباتی مجموعه ی بیمارستانی ضمیمه می شود، همانطور که در شکل 2 به تصویر کشیده شده است. سرورهای محاسباتی باید با استفاده از ابر محاسباتی مجموعه ی بیمارستانی گسترش یابند و چیده شوند. چارچوب سلسله مراتبی پیشنهادی، دارای دو مُد است: مُد بیمار- داخل و مُد بیمار- بیرون. در مد بیمار- درون، بیمارستان اتصالی را به ابر محاسباتی مجموعه ی بیمارستانی از طریق سرورهای محلی اش ایجاد می کند، در حالی که در مُد بیمار- بیرون، بیمار به ابر محاسباتی مجموعه ی بیمارستانی از طریق RBS وصل می شود. در مُد بیمار- داخل بیماران در بیمارستان پذیرفته می شوند و در یک اتاق یا اتاق عمومی بستری تحت نظر قرار می گیرند. سنسورهای با قابلیت اندازه گیری داده های زیستی انسانی، به بدن بیماران متصل می شوند تا داده های زیستی مانند سیگنال الکتروکاردیوگرام (ECG) و موج نگار مغزی (EEG) را حس کنند. هر بیمار یک سرور شخصی دارد(یک PDA یا یک لپ تاپ) که این سرور مسئول جمع آوری داده ها از سنسورهای روی بدن بیمار می باشند. همچنین یک واسط یا داده خوان به صورت یک ایستگاه پردازشگر برای انتقال داده ها از سرورهای شخصی به ابر محاسباتی مجموعه بیمارستانی نصب شده است[12]. هر شعبه در بیمارستان (که شامل چند اتاق می باشد) یک سرور شعبه دارد. سرورهای شعبه به سرور اصلی بیمارستان متصل می شوند. در مد بیمار- بیرون ، بیمار خارج از محوطه بیمارستان در نظر گرفته می شود و در محدوده ی سرورهای آن قرار نمی گیرد، و از این رو ، بیمار(WBAN) به یک ایستگاه پایه کنترل از راه دور (RBS) متصل می گردد وداده های بیمار را به ابر مجموعه یبیمارستانی ارسال کند. اگر بیمار در محدوده ی پوشش RBS نباشد، ارتباطات درون بدن مسیرهایی را تعیین می کنند که داده های بیمار به RBS از طریق PS های سایر بیماران (WBAN) در محدوده ی اولین بیمار ،ارسال گردد. در اولین باری که این داده ها به ابر محاسباتی هدایت شدند در سیستم EMR بیمارستان ذخیره خواهد شد. این سیستم شامل سرورهای بیمارستانی است، مانند سرور اصلی یا سرورهای کاربردی یا سرورهای پایگاه داده و... . ابر محاسباتی تشکیلات UBUNTU به همراه پایگاه داده اوکالیپتوس برای ذخیره داده ها به صورت اشیاء و سطل ها به کار خواهد رفت. داده های دریافتی از بدن بیماران با استفاده از طراحی مجدد این طرح پایگاه داده و روش رمزگذاری امن، در پایگاه داده اوکالیپتوس ذخیره می شوند ([13]).



شکل 2 معماری سیستم مراقبت از سلامت بیمار متحرک بر اساس ابر محاسباتی

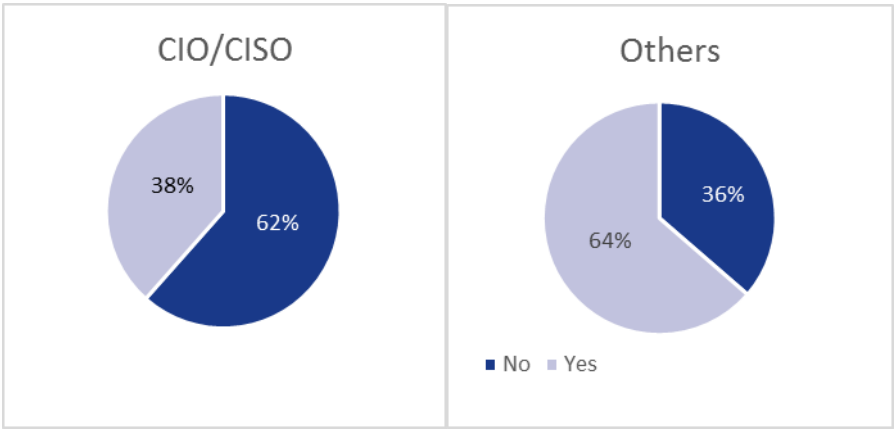
بررسی وضعیت فعلی رایانش ابری و بررسی راهکار ها

برای اینکه وضعیت موجود را بررسی کنم به صورت مساحبه میدانی از گروه فناوری بیمارستان ، بیماران ، کادر درمان و کادر غیر درمان سوالات مطابق زیر پرسده شده است

ابتدا برای اینکه متوجه بشویم در بیمارستان ها و مراکز خدمات درمانی چقدر از رایانش ابری استفاده میشود سوالاتی طرح کرده خروجی ها را در قالب نمودار و جدول ارائه میکنیم.

اولین سوال: چه میزان برای پشتیبانی از سیستم / خدمات الکترونیک سلامت رایانش ابری را پیاده سازی شده است در مرکز شما؟

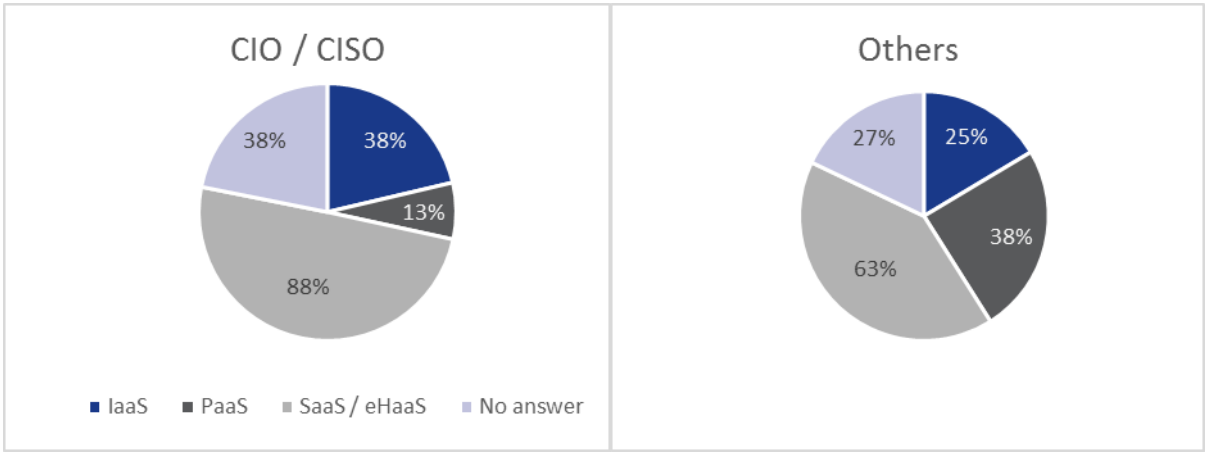
برای دو گروه مطرح شده است گروه اول مدیران فناوری اطلاعات و امنیت و گروه دوم بقیه پاسخ دهنده گان بوده اند که نتایج در شکل 3 مشخص شده است. و همانطور که مشخص است حدود ۶۲ درصد مراکز هنوز از رایانش ابری استفاده نمیکند.



شکل3 میزان استفاده از رایانش ابری

سوال دوم: از کدام مدل سرویس ابری بیشتر استفاده شده است.

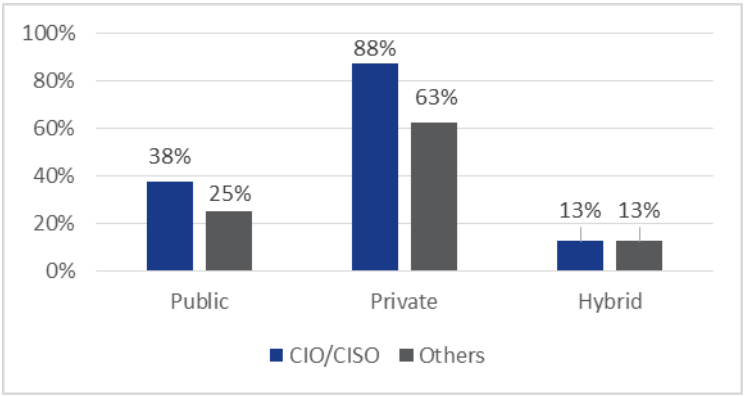
نتایج در شکل 4 مشخص شده است و ۸۸ درصد saas انتخاب کردن و ۳۸ درصد paas و ۳۸ درصد هم iaasو ۱۳ درصد هم پاسخی به سوال نداده اند.



شکل ۴ نوع سرویس

سوال سوم: نوع ابر استفاده شده کدام است:

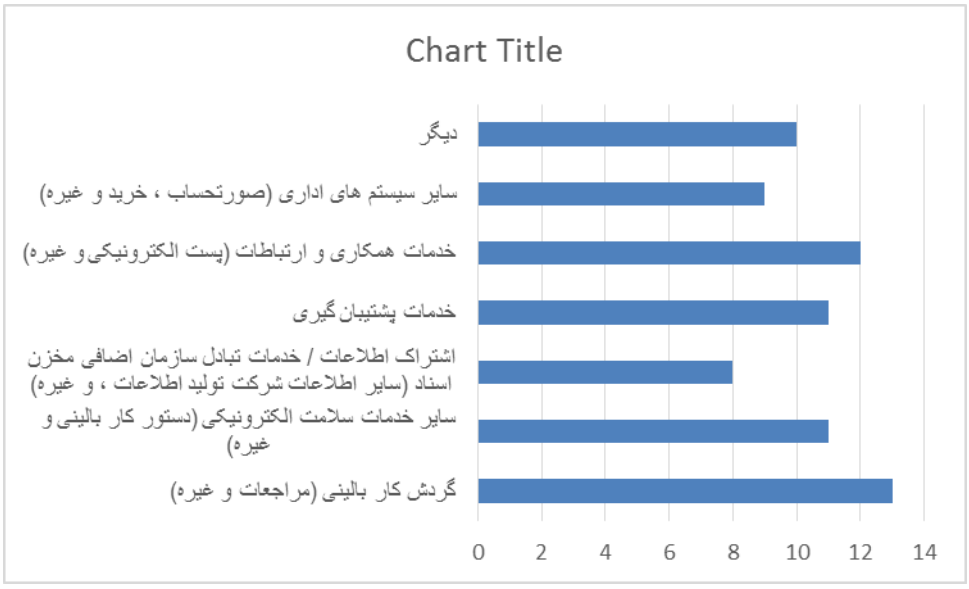
همانطور که از شکل ۵مشخص است حدود ۸۳ درصد پاسخ دهندگان ابر خصوصی و ۳۸ درصد ابر عمومی و ۱۳ درصد ابر ترکیبی را انتخاب کردن



شکل ۵ مدل نوع ابر

سوال چهارم: از رایانش ابری در کدام حوزه بیشتر استفاده میکنید.

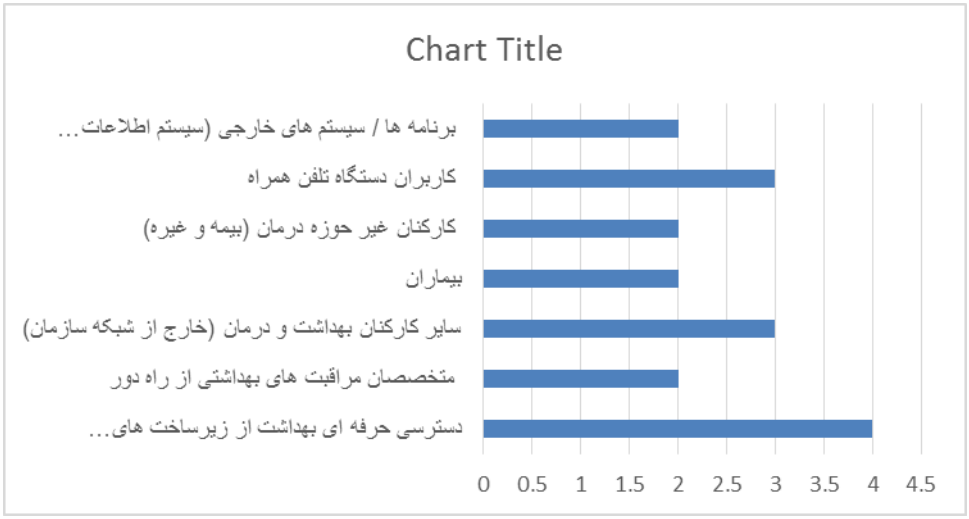
و همانطور که در شکل ۶ مشخص است بیشتر پاسخ در خصوص گردش کار بالینی که در رتبه اول است و بعد ان خدمات همکاری و ارتباطات و در رتبه سوم خدمات پشتیبانگیری مشخص شده است. که جزییات بیشتر در شکل۶ مشخص است.



شکل۶حوزه های استفاده کننده از ابر

سوال پنجم : چه نوع کاربران خارجی می توانند به خدمات Cloudدسترسی پیدا کنند؟

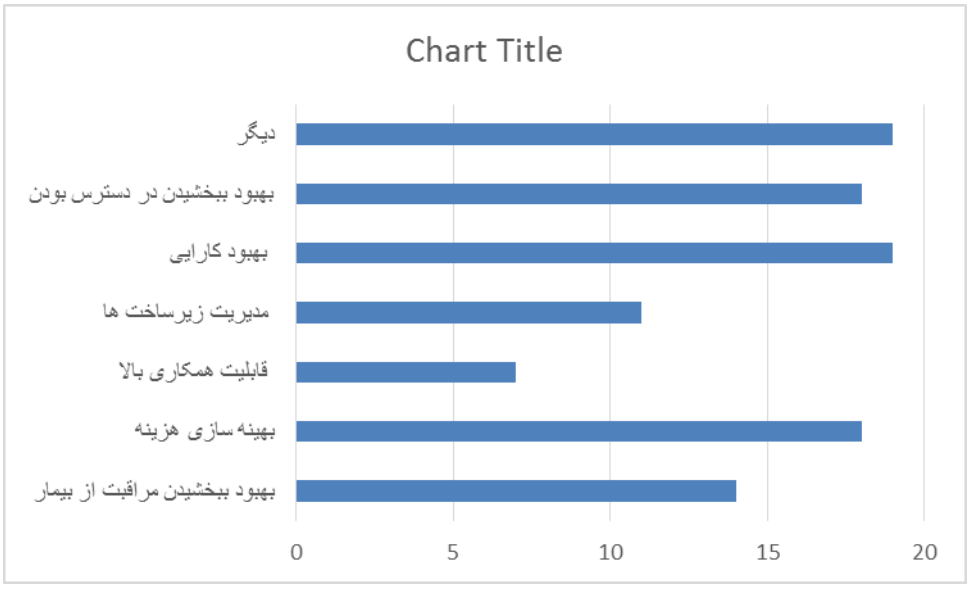
نتایج این سوال در شکل۷ مشخص است و همانطور که ملموس است در رتبه اول دسترسی حرفه ای بهداشت از زیرساخت ها شبکه عمومی و در رتبه دوم کارکنان بهداشت و درمان خارج از شبکه سازمان و رتبه سوم کاربران تلفن همراه است که جزییات بیشتر در شکل مشخص است.



شکل ۷ کاربران ابری

سوال ششم : مزایای اصلی خدمات الکترونیکی سلامت با استفاده از Cloud کدام است؟

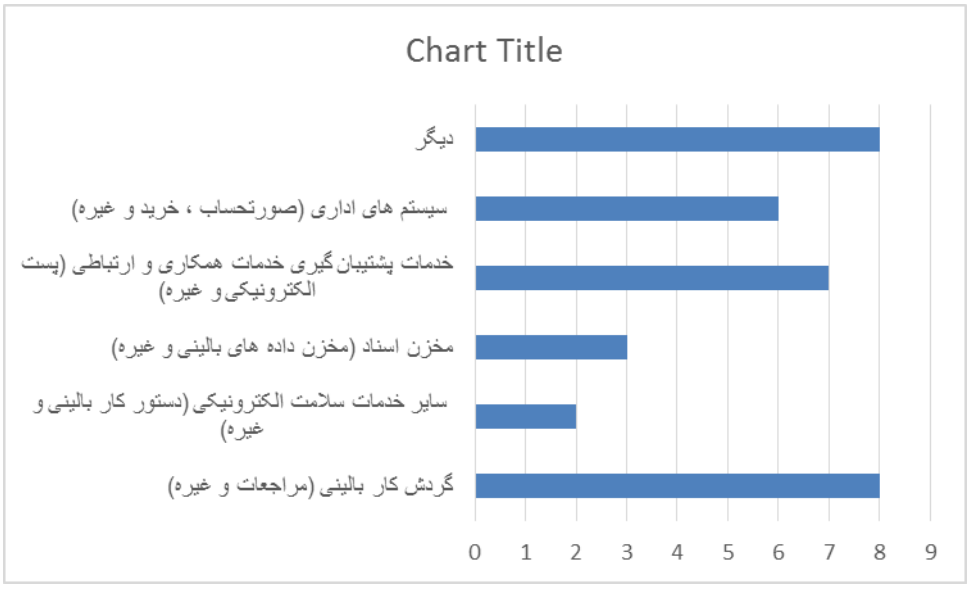
و همانطور که در شکل ۸ مشخص شده است حداکثر گزینه سایر انتخاب کردن که یعنی گزینه مربوطه جز گزینه های سوال نبوده و مابقی هم به بهبود کارایی و بهینه سازی هزینه ها اشاره کردن و جزییات بیشتر در شکل ۸ مشخص است.



شکل ۸ مزایای اصلی خدمات الکترونیکی سلامت

سوال هفتم : با استفاده از استقرارهای ابری از کدام سرویس ها هنوز پشتیبانی نمی کنید اما قصد دارید یا می خواهید در آینده این کار را انجام دهید؟

نتایج این سوال هم در شکل ۹کاملا مشخص است و بیشتر پاسخ جز گرش کار بالینی بوده است.



شکل ۹ استقرار ابری

در ادامه با توجه به سوالات و پاسخ ها به طراحی و ببرسی رایانش ابری در سلامت جامعه پرداخته شده است.

طراحی مبتنی بر سیگنال های زیستی چند گانه :

طرح داده های زیستی چندگانه، دو داده زیست سنجی که شامل دو مقدار زیستی مانند سیگنال های ECG و EEG هستند را با هم ترکیب یا ادغام می کند. انگیزه نهفته در استفاده از چند مقدار پارامترهای زیستی، افزایش طول کلید رمز وحصول یک کلید رمز امن تر و با قابلیت تصادفی بودن بیشتر است. جزئیات این طرح به صورت زیر است:

انتخاب ویژگی:

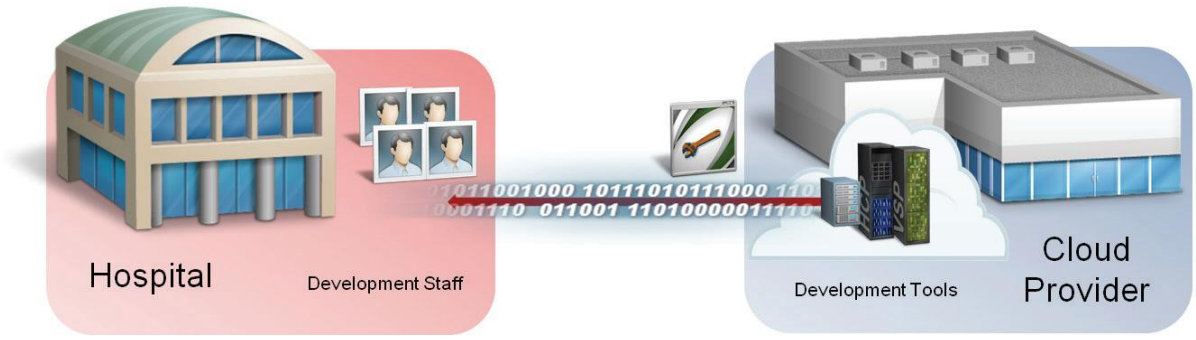
این ویژگی ها از سیگنالهای ECG و EEG با بکارگیری تبدیل موجک گسسته استخراج و برای ارتباطات بین سنسورها کوآنتیزه می شوند. ورودی این سیستم دو سیگنال EEG و ECG است، در حالی که یک کلید رمز ترکیبی طویل و با میزان تصادفی بودن بیشتر تولید می شود.

برای ارتباط بین SN ها و PS ها سنسورها سیگنال های EEG و ECG را با نرخ نمونه برداری ۱۲۵ هرتز در یک دوره زمانی ۵ ثانیه نمونه برداری می کنند. این فرآیند به صورت موازی انجام میشود تا کلید رمز طولانی تر و تصادفی تر تولید شود. ویژگی های انتخاب شده از سیگنال های EEG و ECG سپس به صورت بردار ویژگی (EEGFV و ECGFV) در دو بردار جمع آوری می شوند. در مرحله کوآنتیزه کردن بردار ویژگی تولید شده از سیگنال های EEG و ECG به ۲۰ بلوک تقسیم می شوند که هر بلوک شامل ۱۶ ضریب برای سیگنال های EEG و ECG می باشند و سپس به صورت یک جریان باینری، کوآنتیزه می شوند. این بلوک ها با بکارگیری الگوریتم درهم سازی کلیدرمز تغییر می کنند (HMAC-MD5) .

تولید کننده رمز:

در قسمت پایانی مرحله دریافت داده ها، هر دو سنسورها بلوکهای داده ی EEG و ECG را جمع آوری می کنند و الگوریتم KeyGen را اعمال می کنند. الگوریتم KeyGen دو کلید رمز با طول های ۱۶۰ بیت تولید می کند. سپس کلید های رمز تولیدشده به طور افقی به یکدیگر متصل می شوند تا یک کلید رمز طویل تر که ۳۲۰ بیت دارد ایجاد شود. فرآیند تولید و تبدیل کلید رمز در شکل ۱۰ نشان داده شده است.

هر گره سنسوری بلوک های دریافت شده را مقایسه می کند تا بلوک های مشترک استخراج شوند. این عمل استخراج با ایجاد یک ماتریس انجام می شود، به طوری که هر عنصر این ماتریس بیانگر فاصله همینگ بین i امین بلوک سنسور ۱ و j امین بلوک سنسور ۲ می باشد. این کلیدهای رمز تولید شده توسط سنسورها برای تایید کد تصدیق پیام (MAC) دریافت شده مورد استفاده قرار می گیرند. به محض تایید موفق MAC ، گره های سنسوری این کلیدها را برای ارتباطات بعدی به کار می برند.



شکل ۱۰ : فرآیند تولید کلید رمز بر اساس چند سیگنال زیستی

EMR مبتنی بر ابر محاسباتی :

به منظور فراهم کردن مراقبت از سلامت با کیفیت بالا، این نکته مهم است که پرسنل پزشکی و پزشکان مربوطه باید با EMR ها در هر جایی دسترسی داشته باشند. دسترسی در همه جا می تواند با ذخیره کردن EMR روی ابر محاسباتی فراهم شود. مرحله اول چارچوب پیشنهادی ما برروی امنیت ارتباطات WBAN متمرکز است. دومین موردی که باید بر روی آن متمرکز باشیم محرمانه بودن ذخیره داده های پزشکی بیماران به صورت محاسبات ابری است. امنیت داده های پزشکی بیماران در حالی که در حال حمل و جابجایی هستند و محرمانه بودن این داده ها وقتی که در یک محل ثابت هستند، باید با همدیگر لحاظ شوند. اگر داده های پزشکی مخابره شده به صورت امن ذخیره نشوند ممکن است جان انسان به مخاطره افتد.برای اطمینان از محرمانه بودن داده های پزشکی بیماران، ما از یک مکانیزم انطباق حفاظت از محرمانه بودن داده های کاربران ابر محاسباتی بر اساس بازسازی دینامیکی فراداده استفاده کرده ایم.(مراجعه شود به مرجع [13])

۳-۲-۱) انواع داده های پزشکی بیماران:

انواع داده های پزشکی بیماران که شناسایی شده اند وسیستم مراقبت از بیمار سیار می تواند به طور عمومی از آن ها استفاده کند به قرار ذیل است:

۱-اطلاعات شخصی بیماران:

a: عدد شناسایی منحصر به فرد هر بیمار

b: نام بیمار

c: آدرس بیمار

۲- تاریخچه پزشکی بیمار

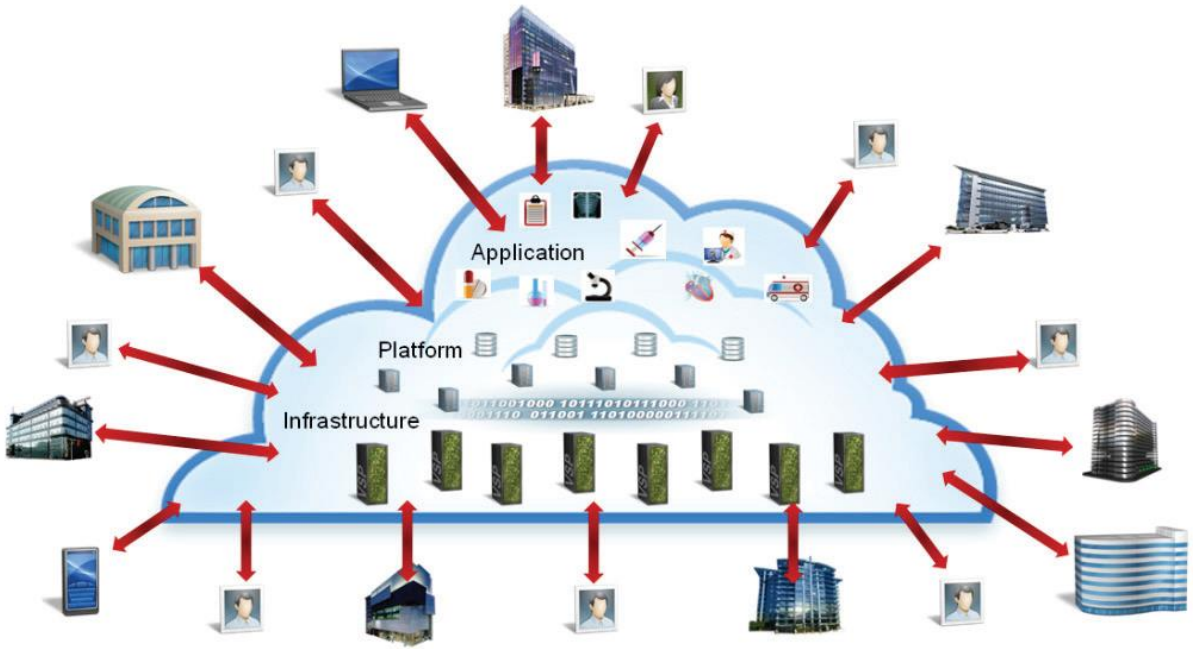
a : شناسه منحصر به فرد شرایط پزشکی

b : نام شرایط پزشکی

c: تاریخ تشخیص بیماری

d: معالجات پیشنهاد شده

۳- حفظ محرمانه بودن داده های پزشکی بیماران که در سرور پایگاه داده ذخیره شده است. در اینجا، ما هرکدام از اقلام داده که به صورت یکی از انواع فوق الذکر شناسایی شد را به صورت سه کلاس پارامتری سازی حساسیت الف) خصوصی و منحصر بفرد (درجه ۱ و۲)، ب) تاحدی خصوصی (درجه ۱ و ۲) و غیر خصوصی تقسیم می کند (شکل ۱۱)



شکل ۱۱: پارامتری سازی حساسیت داده های بیماران به صورت داده های خصوصی منحصر بفرد و تا حدی خصوصی

در این خصوص از مرجع [14]که مدل داده NHS لغت نامه خاص آن استفاده شده است. با استفاده از SQL Server 2008 R2 یک پایگاه داده عمومی را ایجاد کرده ایم که شامل اقلام داده اشاره شده در بالا است. با استفاده از مراحلی که در مرجع [15]طراحی شده است، طبقه بندی داده ها را روی این پایگاه داده نمونه که از مکانیزم چند دسته کردن جدول عمودی/افقی تبعیت می کند، انجام داده ایم.

چالش‌ها

آزمایشات و نتایج

اغلب تکنیک ها و پروتکل های امنیتی قدرت رمزنگاری شان را بر حسب تعداد بیت ها (کلیدها)یی که یک مهاجم نیاز دارد تا کلید امنیتی را حدس بزند و سیستم را با شکست مواجه کند بیان می کنند.

مثلا اگر مهاجم با کلید رمزی که بخشی از آن قابل پیش بینی است عملیات را شروع کند، این موضوع ضعف سیستم امنیتی را فارغ از نوع الگوریتم یا پروتکل مورد استفاده، نشان می دهد.

اگر کلید رمز ۱۲۸ بیتی شامل ۱۶ بیت قابل پیش بینی باشد، با بکارگیری الگوریتم AES 128 حفاظت ۱۲۸ بیت مطمئن نخواهد بود و فقط ۱۱۲ بیت آن حفظ خواهد شد. ایجاد امنیت این سیستم تا سطح زیادی به خطر می افتد. برای اطمینان از امنیت این سیستم، کلید رمز استفاده شده باید به خوبی تصادفی باشد. در پیاده سازی صورت گرفته در این پژوهش، کلید رمز تولید شده توسط Dieharder [مرجع ۱۶] بررسی شده است که واحد تست روی یک ماشین UBUNTU است. یکی از مشهورترین واحدهای تست کردن تصادفی بودن کلیدهای رمز DIEHARD است که شامل ۱۲ تست می باشد. DIEHARD به صورت مجموعه منبع باز (GPL) از تست ها توسعه یافته است که تحت عنوان Dieharder شناخته می شود و شامل DIEHARD ، تست های NIST و موارد جدید آن می شود.

۴-۱- تصادفی بودن

برای بررسی میزان تصادفی بودن، یک مجموعه از مقادیر P برای هر تست آماری تولید شده است، یک مقدار P اندازه احتمال بدست آوردن یک آمارگان تست بزرگتر از مقدار مشاهده شده است. البته در صورتی که توالی داده ها تصادفی باشد. به طور مشابه، مقادیر کوچک نشان می دهند که یک رشته توالی داده ها با احتمال کمتری تصادفی است. قاعده تصمیم در این مورد بیان می کند که برای یک مقدار معنادار ثابت α یک دنباله در مواجه با یک تست آماری، اگر مقدار P آن کوچکتر از α باشد خطا خواهد داد. یک دنباله در صورتی که مقدار P بزرگتر یا مساوی α باشد تست را با موفقیت می گذراند و در غیر این صورت شکست می خورد [مرجع ۱۷]. فرض کنید که یک تست اگر یک مقدار P کمتر یا مساوی با 0.0001 یا بزرگتر مساوی 0.9999 را نتیجه دهد. در این صورت یک فاصله اطمینان برای مقادیر P بین 0.0001 و 0.9999 به دست می آید. در این پژوهش، کلیدهای رمز برای ۲۵ شخص متفاوت تولید شده است. داده های EEG و ECG پایگاه داده بانک پزشکی دانشگاه MIT گرفته شده اند. واحد تست Dieharder روی کلیدهای رمز تولید شده از داده های رمز EEG و ECG ۲۵ شخص به کار رفته است. جدول یک میانگین مقادیر P این ۲۵ کلید رمز و ارزیابی نسبی آن ها را نشان می دهد. از جدول یک مشهود است که هیچکدام از مقادیر P شرایطی که در مرجع [18]تعیین شده است را نقض نکرده اند.

نتیجه گیری و کارهای آینده:

این مقاله یک چارچوب امن را برای سیستم مراقبت سیار ارائه کرد که بر امنیت ارتباطات بین سنسوری مانند امنیت و محرمانه بودن داده های بیماران متمرکز شده است. سیستم پیشنهادی از داده های شبکه های زیست سنجی چندگانه برای تولید یک کلید مشترک برای ارتباطات بین سنسوری استفاده می کند. چارچوب پیشنهادی برحسب امنیت ارتباطات بین سنسوری ارزیابی شد و نتایج نشان می دهد که سیستم پیشنهادی یک راه حل مناسب برای نسل بعدی سیستم های مراقبت از بیمار سیار می باشد. چارچوب پیشنهادی به دلیل این که یک چارچوب کامل براساس محاسبات ابری و راه حل امنیتی برای سیستم های مراقبت از بیمار سیار و حاضر در همه جا است، به عنوان یک طرح منحصر به فرد شناخته می شود.

منابع

[1]CISCO, "Internet of Things at a Glance," Available: https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf, Accessed on: 23 February 2019.

[2] W. contributors. (14 October 2019 17:04 UTC). *Health care*. Available: https://en.wikipedia.org/w/index.php?title=Health_care&oldid=919514905
[3] M. L. Dang, J. M. Piran, D. Han, K. Min, and H. Moon, "A Survey on Internet of Things and Cloud Computing for Healthcare," *Electronics*, vol. 8, no. 7, 2019.
[4] Statista, "Size of the Internet of Things market worldwide in 2014 and 2020, by industry," Available: https://www.statista.com/statistics/512673/worldwide-internet-of-things-market/, Accessed on: 24 February 2019.
[5] H. Truong and S. Dustdar, "Principles for Engineering IoT Cloud Systems," *IEEE Cloud Computing*, vol. 2, no. 2, pp. 68-76, 2015.
[6] E. I. Konstantinidis, P. E. Antoniou, G. Bamparopoulos, and P. D. Bamidis, "A lightweight framework for transparent cross platform communication of controller data in ambient assisted living environments," *Information Sciences*, vol. 300, pp. 124-139, 2015/04/10/ 2015.
[7] R. Zgheib, A. D. Nicola, M. L. Villani, E. Conchon, and R. J. I. t. I. C. o. E. T. I. f. C. E. Bastide, "A Flexible Architecture for Cognitive Sensing of Activities in Ambient Assisted Living," pp. 284-289, 2017.
[8] F. Corno, L. D. Russis, and A. Roffarello, "A Healthcare Support System for Assisted Living Facilities: An IoT Solution," in *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, 2016, pp. 344-352.
[9] M. Tariq, H. Majeed, M. Beg, F. Khan, and A. Derhab, "Accurate detection of sitting posture activities in a secure IoT based assisted living environment," *Future Generation Computer Systems*, 02/01 2018.
[10] A. Rghioui, S. Sendra, J. L. Mauri, A. J. N. P. Oumnad, and Algorithms, "Internet of Things for Measuring Human Activities in Ambient Assisted Living and e-Health," vol. 8, pp. 15-28, 2016.
[11] L. Mainetti, L. Manco, L. Patrono, A. Secco, I. Sergi, and R. Vergallo, "An ambient assisted living system for elderly assistance applications," in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2016, pp. 1-6.
[12] A. Rashed *et al.*, *Integrated IoT medical platform for remote healthcare and assisted living*. 2017, pp. 160-163.
[13] E. Konstantinidis, G. Bamparopoulos, A. Mpillis, and P. Bamidis, "Internet of Things for an Age-Friendly Healthcare," *Studies in health technology and informatics*, vol. 210, pp. 587-91, 05/20 2015.
[14] G. Marques and R. Pitarma, "An Indoor Monitoring System for Ambient Assisted Living Based on Internet of Things Architecture," in *International journal of environmental research and public health*, 2016.
[15] S. Jabbar, F. Ullah, S. Khalid, M. Khan, and K. Han, "Semantic Interoperability in Heterogeneous IoT Infrastructure for Healthcare %J Wireless Communications and Mobile Computing," vol. 2017, p. 10, 2017, Art. no. 9731806.
[16] A. Jara, A. M. Alberti, G. Tripathi, and D. Singh, "Semantic edge computing and IoT architecture for military health services in battlefield," p. 6 p., 2017 2017.
[17] A. Kelati, I. B. Dhaou, and H. Tenhunen, "Biosignal Monitoring Platform Using Wearable IoT," presented at the Proceedings of the 22st Conference of Open Innovations Association FRUCT, Jyvaskyla, Finland, 2018.
[18] R. Zgheib, E. Conchon, and R. Bastide, "Engineering IoT Healthcare Applications: Towards a Semantic Data Driven Sustainable Architecture," in *eHealth 360°*, 2016.