مطالعات علوم کاربردی در مهندسی

دوره ۲، شماره ۳، پاییز ۱۳۹۵

صفحات ۴۴- ۵۶

Online ISSN: ٢٤٧٦-٤٥٠٧

Print ISSN: ٢٥٣٨-٢٠٥٥

www.irijournals.com

اعتماد در سیستم‌های اطلاعات مراقبتی بهداشتی مبتنی بر رایانش ابری

شهرام نصیری [۱]، بهروز وصفی ورزنده [۲]

[۱] مربی گروه کامپیوتر، بخش کامپیوتر و برق، دانشگاه صنعتی سیرجان، سیرجان، ایران

[۲] دانشجوی کارشناسی مهندسی کامپیوتر، دانشگاه صنعتی سیرجان، سیرجان، ایران

چکیده

امروزه رشد روز افزون دنیای IT[1] در سراسر جهان باعث شده است که صنعت، سازمان‌ها و مراکز درمانی از فناوری اطلاعات بعنوان نیروی محرک اصلی سازمان یاد کنند. در این مقاله به بررسی اعتماد در سیستم‌های اطلاعات مراقبتی بهداشتی یا HIS[2] مبتنی بر رایانش ابری پرداخته شده است. این پژوهش برخلاف پژوهش‌های پیشین که فقط نگاه امنیتی به چنین سیستم‌هایی داشته‌اند، اعتماد را بعنوان فاکتور تعیین کننده مد نظر قرار داده است. از جمله مواردی که در این مقاله بحث شده است؛ بررسی مدل‌های بهینه رایانش ابری، پارامترهای ارزیابی اعتماد و تاثیر گذاری اعتماد در سیستم‌های اطلاعات مراقبتی بهداشتی مبتنی بر رایانش ابری می‌باشند. مجموعه مطالعات انجام شده در این پژوهش، امکان مناسبی را برای طراحان و برنامه‌ریزان حوزه صنایع بهداشتی به وجود می‌آورد که با توجه به حساسیت اطلاعات در حوزه سیستم‌های اطلاعات مراقبتی بهداشتی بتوانند در سطح خرد و کلان تصمیمات درستی بگیرند.

واژه‌های کلیدی: سیستم اطلاعات مراقبتی بهداشتی (HIS)، اعتماد، رایانش ابری.

[1] Information Technology
[2] Healthcare Information System

۱- مقدمه

سیستم HIS به عنوان سیستم اطلاعاتی شناخته می‌شود که وظیفه مدیریت اطلاعات را بر عهده دارد و شامل بازخوانی، ذخیره، آنالیز و جستجوی انتخابی اطلاعات می‌باشد. این سیستم برای مدیریت اطلاعات اداری و بالینی در سازمان‌های مراقبتی بهداشتی طراحی شده است. نکته حائز اهمیت مدیریت این نوع سیستم‌ها، هماهنگی آن‌ها با قوانین و نیازهای بومی هر منطقه می‌باشد؛ به همین سبب ارزیابی و ارزشیابی سیستم‌های HIS برای خرید، سطح‌بندی و طراحی بایستی طبق استانداردهای بومی آن منطقه انجام پذیرد. سیستم‌های اطلاعات مراقبتی بهداشتی به دلیل تعدد موضوعاتی از قبیل گنجایش ذخیره سازی، جامعیت سیستم، هزینه بالای عملیاتی شدن و نگهداری سیستم که جزو نگرانی‌های اصلی کارگزاران این نوع سیستم‌ها می‌باشند، در سال‌های ابتدایی نتوانست به شکل موثری اجرایی شود. سازمان‌های HIS با رشد و توسعه توریستم درمانی، برای ارائه خدمات به بیمارانی که سوابقشان را در دست دارند، می‌توانند در تمامی مراکز معتبر و تحت نظر یک شبکه‌ی جامع، اطلاعات بیماران را در اختیار دیگر پزشکان قرار دهند تا مورد درمان قرار گیرند (Vasfi Varzande & Nasiri, 2015) (Degoulet, 2014).

امروزه می‌توان با بهرمندی از رایانش ابری، سرویس‌های نرم افزاری، زیر ساخت‌ها و پلت فرم‌های محاسباتی بر روی بستر اینترنت در هر مکان و زمان از سرویس‌های که مد نظر داریم استفاده کنیم. و در سال‌های اخیر، رایانش ابری توانسته با سرعت بالا به توسعه سازمان‌های بزرگ کمک کند. و مشکلات سازمان‌های بزرگ اطلاعاتی در قبال؛ افزایش ذخیره سازی و اضافه کردن قابلیت جدید بر روی سیستم کنونی را حل نماید. در حال حاضر، کاهش هزینه‌ها بهترین مزیت برای سازمان‌ها محسوب می‌شود که با فراهم آوردن بستری مناسب برای سیستم‌های مبتنی بر رایانش ابری می‌توان به این مهم دست یافت . (Masrom & Rahimli, 2014) (Bamiah et al, 2012) (Winter & Haux, 1995)

برای رسیدن به این هدف باید سه مسئله را مد نظر قرار داد. اول، موضوعات امنیتی مرتبط با فراهم کنندگان ابر (سازمان‌های فراهم کننده نرم افزار، پلت فرم و زیر ساخت مبتنی بر سرویس از طریق ابر)، دوم، موضوعات امنیتی مرتبط با مشتریان (سازمان‌ها و شرکت‌هایی که اپلیکیشن‌های میزبان یا داده‌های خود را بر روی ابر قرار می‌دهند) و سوم اعتماد مشتریان (پاسخ مناسب در هر زمان و مکان توسط سیستم را شامل می‌شود) (Yunus, 2009) (Kumar & Vajpayee, 2016) . (Boonstra & Broekhuis, 2010)

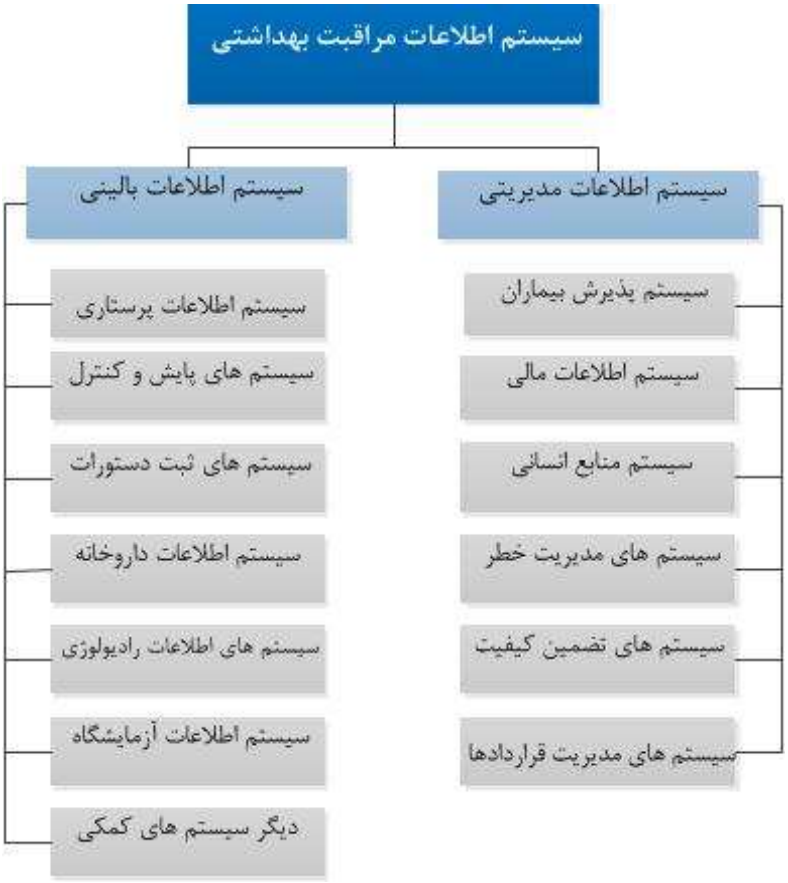
در بخش ادبیات پژوهش، مباحث تحقیق به سه بخش؛ سیستم‌های HIS، رایانش ابری و ابعاد اعتماد این نوع سیستم‌ها تقسیم شده است. در بخش مرور پژوهش‌های پیشین، ارتباط رایانش ابری با بعد اعتماد و سیستم HIS به صورت جامع و کامل مورد بررسی قرار گرفته است و موضوعاتی از قبیل؛ مدل امنیتی EHR برنامه‌های کاربردی در رایانش ابری و موضوعات مربوط به اجتماع اعتماد، رایانش ابری و HIS توجه شده است. در بخش پایانی، از پژوهش انجام شده می‌توان به عنوان یک سند راه گشا برای آگاهی از ابعاد اعتماد و مدل‌های امن در رایانش ابری مبتنی بر سیستم‌های اطلاعاتی مراقبتی بهداشتی بهره برد و پارامترهای مورد نیاز جهت طراحی چنین سیستمی را مطالعه نمود.

۲- ادبیات تحقیق

۲-۱- سیستم HIS

هدف سیستم HIS، مدیریت اطلاعاتی است که پرسنل مراقبت سلامت برای ثبت و بهبود خدمات و همچنین اثر بخشی لازم جهت تسریع خدمات با کیفیت به بیماران، نیاز دارند. از جمله مواردی که نیاز به اینگونه سیستم‌ها را توجیه می‌کند، می‌توان به کاهش هزینه‌های مراقبتی، ارتقاء کیفیت مراقبت، توسعه خدمات بهداشتی و همچنین ملاحظات استراتژیک در رابطه با کسب مزایای رقابتی اشاره کرد. بهبود بیماران در سیستم‌های HIS رابطه‌ای مستقیم با کیفیت بالای سیستم‌های اطلاعات مراقبت بهداشتی دارد. از سویی، این سیستم‌ها دارای هزینه‌های بالایی در طراحی و نصب برای سازمان‌های HIS را به همراه

دارد که این سبب می‌شود سازمان‌ها در انتخاب اینگونه سیستم‌ها دقت کنند، زیرا انتخاب یک سیستم نامناسب که خواسته‌های سازمان را بدرستی پاسخ ندهد، قطعا باعث بی‌اعتمادی بیماران و موجب خسارات جبران ناپذیری بر بیماران می‌شود. (وصفی ورزنده و نصیری، ۱۳۹۵) (ریاضی و همکاران، ۱۳۹۲) به عبارت دیگر، هدف HIS استفاده از کامپیوترها و وسایل ارتباطی برای جمع آوری، ذخیره سازی، پردازش، بازخوانی و برقراری ارتباط بین مراقبت بیمار و اطلاعات اداری در تمام فعالیت‌های مراقبتی بهداشتی و برآوردن نیازهای تمام مصرف کنندگان مجاز سیستم می‌باشد. اجزای سیستم اطلاعات مراقبت بهداشتی در نمودار شکل شماره۱ نشان داده شده است.



شکل شماره ۱. سیستم اطلاعات مراقبت بهداشتی

- **سیستم‌های اطلاعات مدیریتی:** سیستمی است که شامل موارد مربوط به فعالیت بخش‌هایی نظیر؛ آزمایشگاه، تغذیه، داروخانه، رادیولوژی، سیستم‌های اطلاعات پرستاری (جنبه مدیریتی) ثبت پذیرش- ترخیص و انتقال بیمار، خدمات جراحی، مدیریت اموال، سیستم‌های مدیریت اجرایی و سیستم‌های پشتیبان تصمیم‌گیری می‌باشد .
- **سیستم‌های اطلاعات بالینی:** اختصاصاً از داده‌ها در درمان و تشخیص بیماران استفاده می‌کنند، به عنوان مثال می‌توان به؛ پرونده پزشکی کامپیوتری، سیستم اطلاعات پرستاری (جنبه بالینی)، سیستم ثبت دستورات و گزارش‌گیری اشاره کرد. (ریاضی و همکاران، ۱۳۹۲)

۲-۲- رایانش ابری

رایانش ابری می‌تواند قابلیت افزایش ظرفیت ذخیره‌سازی را بدون در نظر گرفتن منابع موجود می‌باشد. و همچنین یک راه حل برای موضوعات مربوط به محاسبات با روش‌های سنتی می‌باشد. رایانش ابری دارای یک ساختار معماری لایه‌ای است که در هر

لایه سرویس‌هایی را ارائه می‌دهد (Masrom & Rahimli, 2014) .رایانش ابری طبق NIST[1] بدین صورت تعریف می‌گردد: "رایانش ابری، مدلی است برای فراهم کردن دسترسی آسان بر اساس تقاضای کاربر از طریق شبکه، به مجموعه‌ای از منابع محاسباتی قابل تغییر و همچنین پیکربندی شبکه‌ها، سرورها، منابع ذخیره‌سازی، برنامه‌های کاربردی و خدماتی که این دسترسی را بتوانند با کمترین نیاز برای مدیریت منابع تحویل دهند." (صادق زاده و همکاران، ۱۳۹۲) (صدر الساداتی و کارگر، ۱۳۹۲)

رایانش ابری، از ۳ مدل سرویس، ۴ مدل توسعه یافته و ۵ ویژگی اصلی تشکیل شده است. مدل‌های سرویس آن عبارتند از؛ SaaS[2] (نرم افزار به عنوان سرویس)، PaaS[3] (پلت فرم به عنوان سرویس)، IaaS[4] (زیرساخت به عنوان سرویس)، که هر کدام بسته به نوع خود، نرم افزار، پلت فرم یا زیرساخت را به عنوان سرویس ارائه می‌دهند. مدل‌های توسعه یافته رایانش ابری شامل؛ ابر عمومی، خصوصی، ترکیبی و اجتماع ابری می‌شوند، که هر یک بسته به حوزه‌ی خود تنها به قسمی از مشتریان ارائه خدمات می‌دهند. رایانش ابری توسط مدل‌های سرویس و مدل‌های توسعه یافته خود تعریف می‌گردد، اما آگاهی از ویژگی‌های آن سبب درک بهتر ابر و محاسبات منابع آن می‌گردد. ویژگی‌های رایانش ابری شامل مواردی از جمله؛ سلف سرویس حین تقاضا، دسترسی فراگیر شبکه، ادغام منابع، انعطاف‌پذیری سریع و سرویس اندازه گیری می‌شوند (Babu & Jayashree, 2015) (Delgado, 2011) (Alam et al, 2015) (Wooten et al, 2012) (Yunus, 2009) .

۲-۳- اعتماد

آشکارسازی مفهوم اعتماد برای تشخیص آن امری آسان است، چرا که ما همه روزه آن را تجربه می‌کنیم. اما برای تعریف کردن مفهوم اعتماد یک چالش کامل به وجود می‌آید، زیرا اعتماد معانی خودش را به شکل‌های مختلفی بیان می‌کند. زمانی که هیچ تعریف پذیرفته شده‌ای برای اعتماد در رایانش ابری وجود ندارد، دسته بندی مولفه‌ها و معانی اهمیت پیدا می‌کند. واژه اعتماد در فرهنگ لغت: "سطحی از اطمینان در هر فرد یا شیء" تعریف می‌گردد. با اشاره بر این مفهوم اعتماد در ابر می توان اعتماد را به عنوان سطح اطمینان مشتریان بیان کرد و با افزایش میزان آن متعاقباً کاهش موانع فنی و روانی در استفاده از خدمات ابر را نتیجه گرفت. تعریف جامع NIST، اعتماد را چنین بیان می‌کند: "اعتماد از طریق استفاده از رایانش ابری و امنیت ابری با صرف نظر از کنترل روی قسمت‌های مهم که جنبه‌های امنیتی و حریم خصوصی دارند، انجام می‌گیرد که در نتیجه آن سازمان به انجام آن متعهد می‌شود و اعتماد بر مکانیزم‌های کنترلی سازمان را استقرار می‌یابد و فرآیندهایی را بدین جهت توسط CSP[5] ها به کار می‌گیرد." (Pearson & Benameur, 2010) (Jøsang et al, 2007) (Ko et al, 2011)

۲-۴- نقش اعتماد در HIS

مرکز ارائه‌ی مراقبت‌های بهداشتی شامل بیمار و ارائه دهنده خدمات است. ارائه موثر خدمات بهداشتی تنها نیازمند تامین مراقبت نمی‌باشد، بلکه پذیرش و استفاده از خدمات توسط بیمار نقش حیاتی در درمان موثر وی ایفا می‌کند. برای جلوگیری از مشکلات سلامت بیماران، باید رفتارهای سالم را ترویج داد. از جمله فعالیت‌های موثر بر درمان بیماران، تهیه امکانات آموزش پزشکی در سطح جامعه و ارتقای سطح فرهنگ پزشکی و درمانی می‌توان نام برد. بیماران بایستی به کادر پزشکی و سیستم اطلاعات اعتماد داشته و اطلاعات موردنیاز محرمانه خود را با کادر درمانی در میان بگذارند، این عمل در نتیجه آموزش صحیح و اطمینان خاطر آن‌ها نسبت به سیستم اطلاعات صورت می‌گیرد. (Gilson, 2003)

1 National Institute of Standards and Technology
2 Software as a Service
3 Platform as a Service
4 Infrastructure as a Service
5 Cloud Service Provide

۳- رایانش ابری و HIS

امروزه برنامه‌های آزمایشی تحویل ابر سازمان‌ها را در جهت استفاده از برنامه‌های حوزه‌ی سلامت کمک می‌کنند و اطلاعات پزشکی را در دسترس افراد مجاز قرار می‌دهد و علاوه بر این، کاهش هزینه‌های IT، سرعت خدمات و در دسترس بودن زیر ساخت‌ها سبب می‌شوند که سازمان‌های بهداشتی از رایانش ابری در سازمان خود استفاده کنند. رایانش ابری باعث انعطاف پذیری بیشتر، سهولت دسترسی به منابعی که به اشتراک گذاشته شده و زیرساخت رایج کنونی که در همه جا فراهم می‌باشد. را بعنوان راه حل مناسب در جهت مدیریت داده‌های بهداشتی دانست.

۳-۱- مدل امنیتی مرجع EHR در رایانش ابری

- **مجموعه‌ای امن و یکپارچه:** با توجه به تعریف EHR، EMR[1] و EPR[2] اولین مولفه اصلی برای مدل امنیتی مرجع، مجموعه‌ای امن و یکپارچه می‌باشد. اولین گام اجباری برای هر یک از سازمان‌های مراقبت از تحویل یا CDO[3]s این است که هر CDO ، EHR خویش را به صورت امن با دیگرCDOها یا CSPها به اشتراک گذارد. کلید اصلی این مولفه، یکپارچگی EHR می‌باشد(Yang et al, 2015).

EHR دو وظیفه مهم را بر عهده دارد؛ اول: اینکه هر EHR باید دیگر EHRها را که توسط CDOهای متنوعی ارائه می‌شوند، از نظر صحت، محرمانگی، یکپارچگی، اطمینان غیرقابل انکار و انطباق با HIPAA[4] مورد بازبینی قرار دهد. دوم: هر EHRبا داده‌های بازبینی شده دیگرEHRها، به منظور تشکیل یک EHR مرکب جدید که گواهی امنیت آن توسط ایجاد کننده صادر شده است ترکیب و یکپارچه شود .

- **انبارش امن و مدیریت دسترسی:** EHR انبارش امن و مدیریت دسترسی EHR از دو موجودیت اصلی (سرور انبارش امن و موتور کنترل دسترسی) تشکیل شده است. در گذشته داده‌های مرکب هر EHR ابتدا کد گذاری می‌شد و سپس تنها با اجازه دسترسی ذخیره می‌گردید .

موتور کنترل دسترسی مجموعه‌ای از سیاست‌های مبتنی بر نقش، سیاست‌های کنترل دسترسی مبتنی بر صفات، سیاست‌های انطباق با HIPAA را شامل می‌شود، و همچنین وظیفه اجرای این سیاست‌ها را برای جلوگیری از دسترسی غیرمجاز به داده‌ها را نیز بر عهده دارد. تنها پزشکان با رعایت مکانیزم‌های تایید هویت و رمزنگاری اجازه دارند به داده‌های EHR دسترسی داشته باشند(Yang et al, 2015).

- **مدل استفاده امن در EHR:** این قسمت، دسترسی محتوی قابل بررسی را که به صورت امن برای مصرف کنندگان داده‌های EHR شامل بیماران و پزشکان سازمان بهداشتی می‌باشد را فراهم می‌آورد. بدین ترتیب، بلوک‌های کاربردی اساسی در این مولفه، امضاء و تایید می‌شوند.

۳-۲- مزایای رایانش ابری در HIS

از جمله مزایای رایانش ابری بر بیماران این است که سیستم اطلاعات می‌تواند بیماران را قادر سازد تا داده‌های سلامت در حوزه‌های متفاوت بهداشت و درمان را تولید و به اشتراک گذارند. به عنوان نمونه، داده‌های تولید شده در خانه و پیش از بستری شدن در بیمارستان، مواقع اضطراری در بیمارستان را در دسترس به پزشکان قرار می‌دهد. تولید داده‌ها در خانه با استفاده از بهداشت و درمان و دستگاه اکوسیستم می‌تواند هزینه‌های مراقبتی رسمی را کاهش دهد. توانایی به اشتراک گذاری آن، بیماران را قادر به "حمل" پرونده‌ی سلامت الکترونیکی می‌کند و به جای استفاده از فرآیندهای وقت گیر و دشواری مانند

1 Electronic Medical Record
2 Electronic Personal Record
3 Care Delivery Organization
4 Health Insurance Portability and Accountability Act

دوره ۲، شماره ۳، پاییز ۱۳۹۵، صفحات ۴۴- ۵۶

حمل نسخه فیزیکی آزمایشات به مشاوران، پزشکان، داروخانه‌ها و غیره می‌توان آن را به عنوان پرونده بیمار به صورت جهانی قابل دسترس ساخت (جدول شماره ۱) (Abayomi-Alli et al, 2014). (Ekonomou et al, 2011) (Ahuja et al, 2012) (Archenaa & Anita, 2015) (Adueni et al, 2016)

جدول شماره ۱. مزایای رایانش ابری بر بیماران و HIS

بیماران	HIS
گردش بالینی کارآمد	نظارت بر اورژانس همراه
بهبود کیفیت درمان	کنترل ترافیک داده در زمان اوج تقاضا
سرعت در ارسال نتایج آزمایشگاهی	کاهش هزینه‌های IT
بهبود همکاری بیمار و پزشکان	قابلیت اشتراک گذاری داده‌های پزشکی

۳-۳- معرفی منابع متن باز، برنامه‌های کاربردی و پلت فرم‌های برتر در رایانش ابری

این قسمت، با مروری بر معرفی منابع متن باز، برنامه‌های کاربردی و پلت فرم‌های برتر در رایانش ابری به محققان، مدیران و طراحان HIS جهت آشنایی و شناسایی بهتر در حوزه‌ی سلامت کمک کند. در ادامه به بزرگترین و مشهورترین منابع متن باز در سراسر جهان پرداخته شده و در جدول شماره۲ نشان داده شده است.

جدول شماره ۲. منابع متن‌باز در رایانش ابری

منابع متن باز	توضیحات
Eucalyptus	زیرساخت متن باز برای ابر خوشه‌ای که مشابه عملکرد ECD2[1] آمازون می‌باشد.
Red Hat’s Cloud	لینوکس متن باز با تمرکز بر توسعه رایانش ابری می‌باشد.
Cloudera	فریمورک متن باز Hadoop که به سبب انعطاف پذیری در حال گسترش روزافزون است.
Puppet	برای مدیریت ماشین‌های مجازی و سرورها بدون داشتن تنظیمات پیچیده است.
Zoho	مجموعه‌ی متن باز برای کاربران می‌باشد.
OpenNebula	ابزارهای بسیاری با رابط کاربری آسان در ابر فراهم می‌کند.
Reservoir	طرح پژوهش اصلی اروپا در زیرساخت‌های مجازی و رایانش ابری است.

منابع متن باز که تحت پوشش بسیاری از سازمان‌های بهداشتی قرار گرفته‌اند، توانسته‌اند با ایجاد محیطی امن برای پرونده سلامت بیماران و دسترسی آسان به مدارک موردنیاز و انعطاف پذیری بالا، نسبت به دیگر منابع جایگاهی ویژه در میان صنایع وابسته بیابند. همچنین رابط کاربری آسان در ابر و امکان مدیریت ماشین‌های مجازی و سرورها بدون صرف هزینه‌های کلان فراهم آورده شده است. علاوه بر آن، صرفه جویی در زمان از مزیت‌های استفاده از منابع متن باز در سیستم‌های مدیریت سلامت بیماران به شمار می‌آید. شرکت‌های بزرگی مانند آمازون نیز برای بهره برداری از این بخش، ابزار ECD2 را ارائه کرده‌اند. این خود نشان دهنده‌ی توسعه روز افزون منابع متن باز در رایانش ابری و افزایش سرمایه گذاری در بخش سلامت می‌باشد. جدول شماره ۲ بیانگر این موضوع می باشد. (Alam et al, 2015)

1 Elastic Compute Cloud 2

دوره ۲، شماره ۳، پاییز ۱۳۹۵، صفحات ۴۴- ۵۶

جدول شماره ۳. انواع برنامه‌های کاربردی و پلت فرم‌های رایانش ابری

برنامه‌های کاربردی	دسترسی به پرونده سلامت شخصی بیماران تا ارائه مراقبت به موقع است. سرویس به اشتراک گذاری داده‌های خصوصی وکشف سوابق مختلف بهداشتی خود مدیریتی سلامت بیماران سیستم مدیریتی اطلاعات مبتنی بر ابر	Emergency Medical System Health Cloud eXchange HealthATM kiosks @Health Cloud
پلت فرمها	پلت فرمی با پشتیبانی Hadoop است. ذخیره سازی زمینه ای برای خوشه ای از Hadoop را قادر می سازد. رابط کاربری را برای توزیع وظایف فرعی مهیا می کند. به زیرساخت متمرکز اجازه می دهد تا خدمات مختلفی ارائه دهد.	Hive The Hadoop Distributed File System (HDFS) MapReduce Zookeeper

کسب آگاهی از منابع متن باز، برنامه‌های کاربردی و انواع پلت¬فرم‌ها از آن جهت مورد توجه قرار گرفته‌اند که سازمان‌های مرتبط با حوزه سلامت و بهداشت فردی و اجتماعی با بهره¬گیری از آن‌ها می‌توانند؛ از افزایش بیهوده‌ی هزینه‌های اسناد پزشکی، مدیریت سیستم و مراقبت بیماران جلوگیری کنند. موضوع توریسم درمانی نیز یکی از دلایل با اهمیت بودن ابزارها به شمار می‌آید، زیرا با توسعه‌ی صنعت درمان، اشتراک گذاری پرونده‌ی سلامت بیماران در محیطی امن جزء دغدغه‌های اصلی سازمان‌ها می‌باشد. برنامه‌ها و پلت فرم‌های مذکور، جزء برترین ابزارهای حوزه‌ی سلامت به حساب می‌آیند. از جمله مزیت استفاده از آن‌ها، می‌توان به مدیریت یکپارچه پرونده سلامت پزشکی، خود مراقبتی بیماران، ذخیره سازی آسان و همچنین ارتباط با زیرساخت‌های مختلف اشاره کرد. مدیران سازمان‌های حوزه‌ی سلامت و بهداشت با درنظر گرفتن اهداف سازمان و به تناسب نیازهای بومی خویش برای مدیریت بهینه می‌توانند از ابزارهای موجود استفاده کنند. مجموعه این برنامه‌ها و پلت فرم‌ها در جدول شماره۳ بیان شده‌اند. (Raghupathi & Raghupathi, 2014) (Wooten et al, 2012) (Prajapati et al, 2015)

۴- اعتماد و رایانش ابری

طبقه بندی گرایش‌های موجود در این زمینه از اهمیت اعتماد در دو شاخه سخن می‌گوید. این قسمت با بیان موضوعات در شاخه‌ی فناوری‌های پذیرفته شده و گرایش‌های پژوهشی به بیان پیشینه این نوع تحقیقات پرداخته است. بخش اعظمی از پژوهش‌های پیشین به فناوری‌های اعتماد در سطح رایانش ابری تاکید کرده‌اند. همچنین گرایش‌های پژوهشی که در ادامه بیان شده است جزء موضوعات چالش برانگیز این حوزه می‌باشند.

۴-۱- فناوری پذیرفته شده

- **تفاهم نامه سطح خدمات یا SLA**[1]: قراردادی است حقوقی فی ما بین ارائه دهنده و استفاده کننده از خدمات که جهت تضمین پارامترهای کیفی سرویس منعقد می‌گردد. کیفیت خدمات به سطح معینی از کیفیت اطلاق می‌شود، که هر یک از شرکت‌ها برای رسیدن به آن تلاش می‌کنند؛ به این ترتیب برای هر یک از خدمات باید مشخصات خاصی تهیه شود و SLA تعیین کننده سطح کیفت خدمات، مسئولیت‌ها و ضمانت‌های اجرای آن‌ها است. در عمل، یک راه برای ایجاد اعتماد برای CSPتحقق SLAها است.

1 Service-level agreement

- **حسابرسی:** CSPها استانداردهای حسابرسی مختلفی را به کار می‌گیرند. استانداردهایSAS[1]70II ، FISMA[2]، ISO[3]27001 برای اطمینان کاربران در مورد خدمات و پلت فرم‌ها ارائه شده‌اند. به عنوان نمونه، گوگل از گواهینامه‌های SAS70IIو FISMA برای اطمینان کاربران در مورد اقدامات امنیتی و حفظ حریم خصوصی آن‌ها برای برنامه‌های کاربردی خویش بهره می‌گیرد.
- **رتبه و اندازه گیری:** CSPها بر اساس پرسشنامه‌ای که باید توسط مصرف کنندگان فعلی هر CSP پر شوند رتبه‌بندی می‌شوند. امروزه، با توسعهCSPها، بازارهایی برای حمایت از مصرف کنندگان جهت شناساییCSPهای مورد اعتماد برپا می‌شود .
- **پرسشنامه خود ارزیابی:** این پرسشنامه ابزاری برای ارزیابی قابلیت‌ها و شایستگی CSPها از نظر بررسی ویژگی‌های مختلف (انطباق و امنیت اطلاعات و حکومت) را فراهم می‌کند.

۴-۲- گرایش¬های پژوهشی

- مدل‌های اعتماد و اعتبار یا TR[4]: این مدل‌ها برای تصمیم گیری در انواع محیط‌های خدماتی مفید واقع شده‌اند، که از جمله آن می‌توان به؛ تجارت الکترونیک، شبکه‌های نقطه به نقطه و بررسی محصول اشاره کرد. روش تصمیم گیری مبتنی بر TRدر محیط‌های مختلف معمولا نیاز به ساخت حسابی با صفات چندگانه (عملکرد، امنیت، حمایت مشتری) و صفات متنی (مدل‌های مختلف تحویل سرویس برای محیط رایانش توری و انتخاب سرویس وب) ندارد. این مدل‌ها و مباحث مربوط به کیفیت خدمات هریک در هر مدل مبتنی بر رایانش ابری از موضوعات روز می باشند(Habib et al, 2011) .
- **محاسبات اعتماد:** جدا از گرایش مدل‌های TR، پژوهش‌های قابل توجهی در زمینه محاسبات مطمئن برای تضمین زیرساخت قابل اعتماد ابر انجام گرفته است. زیرساخت مجازی خصوصی یا PVI[5] یک معماری امنیتی برای رایانش ابری است و از مدل اعتماد برای به اشتراک گذاشتن مسئولیت امنیتی بین CSP و کاربران استفاده می‌کند.

۴-۳- مولفه‌های اعتماد در رایانش ابری

برای درک کاهش موثر موانع، نیاز به درک مولفه‌های موثر در اعتماد ابر است. مولفه‌های اعتماد در رایانش ابری در ۴ مورد بیان می گردد: (Kanagasabapathy & Paul, 2016) (Sun et al, 2011) (Ko et al, 2011)

- **امنیت:** امنیت در حوزه زیر ساخت و شریان‌های اطلاعاتی بسیار حیاتی است. فرصت جدید ایجاد شده برای حرفه‌های متنوع در مواردی از قبیل؛ فضای اتوماسیون اداری، تبادل و همکاری، تجارت الکترونیکی، تولید هدفمند منجر به تولید، ذخیره‌سازی و بهره برداری از اطلاعات حساس فراهم شده است. علاوه بر آن، وابستگی به شبکه‌های پر سرعت و پردازشگرهای قدرتمند روزبه روز افزایش می یابد و سیستم‌ها را در معرض خطرات طبیعی مانند؛ آتش و طوفان تا بزهکاری و تروریسم سایبری قرار می‌دهد، بنابراین نیاز به مدیریت و نظارت دقیق دارد .
- **حریم خصوصی:** قلمرویی از زندگی هر شخص است که آن شخص، عرفاً یا با اعلان قبلی در چارچوب قانون، انتظار دارد تا دیگران بدون رضایت وی به حریم آن وارد نشوند یا بر آن نظارت نکنند و یا به اطلاعات راجع به وی دسترسی نداشته باشند یا در آن قلمرو، وی را مورد تعرض قرار ندهند. جسم، البسه و اشیاء همراه افراد، اماکن خصوصی و منازل، محل‌های کار، اطلاعات شخصی و ارتباطات خصوصی با دیگران، حریم خصوصی محسوب می‌شوند .

1 Statement on Auditing Standard
2 The Federal Information Security Management Act
3 International Organization for Standardization
4 Trust & Reputation
5 Private Virtual Infrastructure

- **مسئولیت:** از آنجایی که راهکارهای جلوگیری از نشت داده کاربران و حفظ محرمانگی و حریم خصوصی آن‌ها برای ارائه دهندگان خدمات ابری یک هدف مطلوب به حساب می‌آید، مسئولیت‌های آنان نیز در قبال کاربران افزایش پیدا می‌کند؛ بدیهی است تا زمانی که بزرگ داده‌ها به پردازش در ابر نیاز دارند، هیچ ساز و کار مؤثر و مناسبی وجود نخواهد داشت تا بتواند عمل پردازش را بدون اجازه‌ی ارائه دهندگان خدمات ابری انجام دهد و مسئولیت این امر تنها بر عهده ارائه دهنده خدمات می‌باشد .
- **بازرسی:** تأیید درستی و صحت مجموعه‌ای از واقعیت‌های بیان شده (مانند حساب‌های مالی) است.

مولفه‌های اعتماد می توانند در دو گروه کنترل‌های پیشگیرانه و کنترل‌های شناسایی تقسیم شوند. ابتدا هر یک را تعریف نموده و پس از آن برای تشخیص بهتر در شکل شماره۲ طبقه بندی شده‌اند(Ko et al, 2011).

- **کنترل‌های پیشگیرانه:** برای کاهش وقوع مشکلات یا خطرات محتمل و جلوگیری از تکرار مجدد آن‌ها مورد استفاده قرار می‌گیرد. به عنوان نمونه یک لسیت کنترل دسترسی می‌تواند به افراد مجاز دسترسی دهد تا در صورت بروز مشکل در یک فایل، پایگاه داده، شبکه یا دیوارهای آتش، آن را بخواند و یا در صورت لزوم اصلاح کند.
- **کنترل‌های شناسایی:** این کنترل‌ها برای شناسایی وقوع خطرات امنیتی و حریم خصوصی که برخلاف سیاست‌های اتخاذ شده پیش می‌روند و تولید می‌شوند، استفاده می‌شوند. برای نمونه می‌توان از سیستم تشخیص نفوذ بر روی‌هاست یا شبکه یا گزارش‌ها و ابزارهای تحلیل نام برد.

شکل شماره۲. مولفه‌های اعتماد در رایانش ابری

۵- اجتماع اعتماد و رایانش ابری در HIS

تاکنون به مرور بخش‌های مهمی در حوزه HIS، رایانش ابری و اعتماد پرداخته شده و رابطه‌ی هریک با دیگری مورد مطالعه قرار گرفته است، اما اکنون با در نظر گرفتن هر سه مولفه‌ی اعتماد، رایانش ابری و HIS سعی شده مدل‌های اعتماد مبتنی بر رایانش ابری در HIS مورد بحث قرار گیرد. در ادامه به بیان پارامترهای ارزیابی اعتماد در HIS و مکانیزم‌های افزایش اعتماد در سازمان‌های بهداشتی پرداخته شده است.

۵-۱- ویژگی‌هایی مدل‌های TR (اعتماد و اعتبار)

مدل‌های اعتماد اساسا تجربی، رفتاری و تعاملی هستند. به عنوان نمونه شبکه‌های نقطه به نقطه، رایانش توری و سرویس‌های وب را می توان نام برد. جنبه‌ها و پارامترهای وابسته بطور متعادل برای بررسی در زمان انتخاب CSP بسیار اهمیت دارد. پارامترها و کیفیت خدمات مدل‌های TR شامل موارد زیر می‌شوند: (Habib et al, 2012)

- **SLA:** موجودیت‌هایی که سرویس‌هایی را فراهم می‌کنند، نیاز به پیروی از استانداردسازی SLA دارند. به عنوان مثال انجمن‌های مورد کاربرد رایانش ابری که پیش از این ارائه شده‌اند .
- **انطباق:** CSPها از استانداردهای حسابرسی برای اطمینان از تجربه‌ی فنی استفاده می‌کنند. علاوه بر این، کنترل‌های سازمانی که وابسته به سرویس‌های پیشنهادی می‌باشند، موثر هستند. بازرسان این کنترل‌ها و گواهینامه‌های مرتبط را براساس گزارشات ارزیابی می‌کنند.

قابلیت‌های همکاری، حمل، جغرافیایی و مکان: اطلاعات مربوط به پارامترهای مذکور به طور مستقیم از طرفCSP ها بدست می‌آید.

- **حمایت از مصرف کننده:** CSP معمولاً در قالب فرم‌های SLA قرار می‌گیرند و مصرف کنندگان در هر زمان می‌تواند این اطمینان را ازCSP ها دریافت کنند.
- **امنیت:** CSPها اغلب زمانی که منابعشان در اختیار مصرف کنندگان قرارگرفته خواهان اعمال کنترل‌های امنیتی معین هستند. همچنین جهت اطمینان سرویس‌های میزبانیCSP ها، در پلت فرم‌های مجازی مورد اعتماد با استفاده از فناوری‌های محاسبات اعتماد راه اندازی می‌شوند.
- **بازخورد کاربر:** بازخورد توصیه و بررسی آن از مصرف کنندگان برای انتخاب خدمات در بازارهای الکترونیکی بسیار با ارزش است. این پارامتر بهCSP ها برای ارزیابی عملکرد ایشان کمک می‌کند تا خدمات بهتر را ارائه کنند.
- **عملکرد:** در محیط‌های رایانش ابری اطلاعات مرتبط با پارامترهای عملکرد با استفاده از سرویس فناوری‌های نظارتی به دست می‌آید. مدل‌های اعتماد معمولاً دارای زمینه‌ای ویژه هستند و مهم این است که برای محیط‌های ابری از بررسی مدل‌ها TR استفاده شود.

۵-۲- مکانیزم‌هایی برای افزایش سطح اعتماد

مکانیزم‌های اجتماعی و فنی هر دو برای افزایش اعتماد رایانش ابری ضروری هستند. مکانیزم‌های اجتماعی شامل آموزش کادر پزشکی و افزایش آگاهی بیماران نسبت به در اختیار گذاشتن اطلاعات صحیح همراه با رعایت نکات امنیتی لازم در اعتماد ماندگار موثر می‌باشند. همچنین این مکانیزم‌ها نمونه‌هایی از مکانیزم‌های اساسی هستند که در طول زمان تغییر می‌کنند، اما به صورت نسبتاً پایدار می‌باشند. مکانیزم‌های فنی شامل استفاده از مدل‌های اعتماد ابری، پروتکل‌های امنیتی و کسب گواهینامه‌های معتبر فرآیند می‌شوند.(Pearson & Benameur, 2010)

۵-۳- پارامترهای ارزیابی اعتماد

CSPها تکنیک‌های متفاوتی برای مدیریت اعتماد در جمع آوری بازخوردها به کار می‌گیرند، که یکی از درخواست‌هایشان ارزیابی اعتماد سیستم محسوب می‌شود. در ادامه، به مهمترین معیارها جهت ارزیابی اعتماد توسط سیستم مدیریت اعتماد بیان شده‌اند. (Noor et al, 2016)

- **چشم انداز:** سیستم‌های مدیریت اعتماد می توانند چشم اندازCSP ها، سرویس درخواست کننده چشم انداز و یا هر دو را پشتیبانی کنند. سیستم‌هایی که قابلیت پشتیبانی هر دو چشم انداز را دارند، جامع‌تر می‌باشند .
- **تکنیک:** سیستم‌های مدیریت تکنیک می توانند یک روش مانند سیاست را به کار گیرند یا از روش‌های چندگانه مانند سیاست و اعتبار استفاده کنند. یک سیستم از چندین روش استفاده می‌کند تا در ارزیابی به نتایج دقیق‌تری دست یابد .

- **سازگاری:** ارزیابی اعتماد می‌تواند معیارهای سفارشی مانند وزن بازخورد اعتماد براساس هزینه معامله یا معیارهای عمومی برای تعیین موجودیت مورد اعتماد را دنبال کند. توانایی بروزرسانی بازخورد اعتماد و ارزیابی نتایج در پاسخ به تغییرات سفارشی، اشاره بر این دارد که سیستم مدیریت اعتماد دارای سازگاری می باشد.

۶- بحث و نتیجه‌گیری

پژوهش پیش رو توانسته با مطالعه‌ی مباحث حال حاضر حوزه‌ی سلامت از جمله استفاده از رایانش ابری و اعتماد سیستم به بررسی ویژگی‌ها، برنامه‌های کاربردی و پلت فرم‌ها به سوی پیاده سازی اعتماد در رایانش ابری بپردازد. علاوه بر این، با درنظر گرفتن تمامی موضوعات و نگرانی‌های رایانش ابری و اهمیت آن در سیستم‌های HIS با پیشنهاد استفاده از مدل‌های اعتماد مبتنی بر رایانش ابری بحث نوینی را در حوزه‌ی سلامت بیان نماید. همچنین، با برنامه‌ریزی صحیح در طراحی سیستم‌های HIS می‌توان به پیشرفت درمان بیماران کمک شایانی کرد؛ به همین خاطر با تاکید بر مزایای رایانش ابری در این حوزه سعی بر این دارد تا دیدگاه کنونی مدیران سازمان‌های بهداشتی درمانی را به این سمت جلب نماید. در این میان، ذکر این نکته لازم است که با در نظر گرفتن تمامی امکانات رایانش ابری، همچنان نگرانی‌های امنیتی مانع از موافقت مدیران در اجرای چنین سیستم‌هایی می‌شود؛ به همین سبب، در این پژوهش علاوه بر رایانش ابری، بعد اعتماد در HIS مطرح شده تا در کنار نگرانی‌های امنیتی، استفاده از مدل‌های TR با ویژگی‌ها و امکانات پیشرفته‌ی آن موجب رفع نگرانی مسئولین بهداشتی عدم اعتماد به سیستم‌های مراقبتی بهداشتی تحت رایانش ابری می‌شود. همچنین موضوعات مهمی از قبیل؛ مولفه‌های اعتماد در رایانش ابری، مکانیزم‌های افزایش اعتماد و پارامترهای ارزیابی آن مورد مطالعه قرارگرفته تا بتواند در کنار استفاده از مزایای رایانش ابری در HIS، این آگاهی به مدیران سیستم داده شود که بتوانند با ابزارها و پارامترهای مذکور، افزایش سطح کیفیت خدمات به بیماران را اندازه گیری کنند. پژوهش انجام شده نیز می‌تواند به عنوان یک چارچوب برای پژوهشگران حوزه سلامت و مدیران سازمان‌های بهداشتی در نظر گرفته شود تا به کمک آن برای ارتقاء سطح کیفیت خدمات به بیماران از آن بهرمند شوند.

منابع

۱. ریاضی، حسین؛ عابدیان، سمیه؛ بیطرف، احسان. (۱۳۹۲). ارزیابی عملکردی سیستم‌های اطلاعات بیمارستانی. چاپ اول، انتشارات، سرورکیان تهران.

۲. صادق زاده، پیام؛ بهره پور، داود؛ صادق زاده، پیمان، (۱۳۹۲). تحلیل و بررسی چالش‌های امنیتی موجود در محاسبات ابری. همایش ملی مهندسی کامپیوتر و توسعه پایدار با محوریت شبکه‌های کامپیوتری، مدل سازی و امنیت سیستم‌ها، مشهد، موسسه آموزش عالی خاوران، http://www.civilica.com/Paper-CESD01-CESD01_154.html.

۳. صدرالساداتی، سید محسن؛ کارگر، محمدجواد. (۱۳۹۲). چالش‌های امنیتی در رایانش ابری و ارائه راهکاری جهت بهبود امنیت آن در راستای توسعه خدمات عمومی دولت الکترونیک. همایش ملی مهندسی کامپیوتر و توسعه پایدار با محوریت شبکه‌های کامپیوتری، مدل سازی و امنیت سیستم‌ها، مشهد، موسسه آموزش عالی خاوران.

۴. وصفی ورزنده، بهروز؛ نصیری، شهرام. (۱۳۹۵). مروری بر بعد امنیت رایانش ابری در سیستم‌های اطلاعات مراقبت بهداشتی. دومین کنفرانس بین المللی مدیریت و فناوری اطلاعات و ارتباطات، تهران، شرکت خدمات برتر.

5. Abayomi-Alli, A. A., Ikuomola, A. J., Robert, I. S., & Abayomi-Alli, O. O. (2014). An Enterprise Cloud-Based Electronic Health Records System.Journal of Computer Science, 2(2), 21-36.
6. Adueni, I. A. B., Hayfron-Acquah, J. B., & Panford, J. K. (2016). Developing a common cloud platform to manage Ghana’s healthcare system. Case study: Ghana

Health Service (GHS). Journal of Communications Technology, Electronics and Computer Science, 4, 6-10.

7. Ahuja, S. P., Mani, S., & Zambrano, J. (2012). A survey of the state of cloud computing in healthcare. Network and Communication Technologies, 1(2), 12.
8. Alam, M. I., Pandey, M., & Rautaray, S. S. (2015). A comprehensive survey on cloud Computing. International Journal of Information Technology and Computer Science (IJITCS), 7(2), 68.
9. Archenaa, J., & Anita, E. M. (2015). A survey of big data analytics in healthcare and government. Procedia Computer Science, 50, 408-413.
10. Babu, R., & Jayashree, K. (2015). A Survey on the Role of IoT and Cloud in Health Care. International Journal of Scientific Engineering and Technology Research, 4(12), 2217-2219.
11. Bamiah, M., Brohi, S., & Chuprat, S. (2012, December). A study on significance of adopting cloud computing paradigm in healthcare sector. InCloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on (pp. 65-68). IEEE.
12. Boonstra, A., & Broekhuis, M. (2010). Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions. BMC health services research, 10(1), 1.
13. Degoulet, P. (2014). Hospital information systems. In Medical Informatics, e-Health (pp. 289-313). Springer Paris.
14. Delgado, M. (2011, July). The evolution of health care it: Are current us privacy policies ready for the clouds?. In 2011 IEEE World Congress on Services (pp. 371-378). IEEE.
15. Ekonomou, E., Fan, L., Buchanan, W., & Thuemmler, C. (2011, November). An integrated cloud-based healthcare infrastructure. In Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on (pp. 532-536). IEEE.
16. Gilson, L. (2003). Trust & the development of health care as a social institution. Social science and medicine, 56(7), 1453-1468.
17. Habib, S. M., Hauke, S., Ries, S., & Mühlhäuser, M. (2012). Trust as a facilitator in cloud computing: a survey. Journal of Cloud Computing: Advances, Systems and Applications, 1(1), 1.
18. Habib, S. M., Ries, S., & Muhlhauser, M. (2011, November). Towards a trust management system for cloud computing. In 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (pp. 933-939). IEEE.
19. Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. Decision support systems, 43(2), 618-644.
20. Kanagasabapathy, J., & Paul, C. S. (2016). Secure and Trusted Information Brokering In Cloud Computing.

21. Ko, R. K., Jagadpramana, P., Mowbray, M., Pearson, S., Kirchberg, M., Liang, Q., & Lee, B. S. (2011, July). TrustCloud: A framework for accountability and trust in cloud computing. In 2011 IEEE World Congress on Services (pp. 584-588). IEEE.
22. Kumar, S. N., & Vajpayee, A. (2016). A Survey on Secure Cloud: Security and Privacy in Cloud Computing. American Journal of Systems and Software, 4(1), 14-26.
23. Masrom, M., & Rahimli, A. (2014). A Review of Cloud Computing Technology Solution for Healthcare System. Research Journal of Applied Sciences, Engineering and Technology, 8(20), 2150-2153.
24. Noor, T. H., Sheng, Q. Z., Maamar, Z., & Zeadally, S. (2016). Managing Trust in the Cloud: State of the Art and Research Challenges. Computer, 49(2), 34-45.
25. Pearson, S., & Benameur, A. (2010, November). Privacy, security and trust issues arising from cloud computing. In Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on (pp. 693-702). IEEE.
26. Prajapati, B., Buchanan, W. J., Smales, A., Macfarlane, R., & Spyra, G. (2015). Review of e-Health Frameworks.
27. Raghupathi, W., & Raghupathi, V. (2014). Big data analytics in healthcare: promise and potential. Health Information Science and Systems, 2(1), 1.
28. Sun, D., Chang, G., Sun, L., & Wang, X. (2011). Surveying and analyzing security, privacy and trust issues in cloud computing environments.Procedia Engineering, 15, 2852-2856.
29. Vasfi Varzande, Behrouz & Shahram Nasiri, (2015), An Overview on Information Security Threats In Healthcare Systems,Conference on Management & ICT(Information & Communication Technology), http://www.civilica.com/Paper-ICTMNGT01-ICTMNGT01_021.html.
30. Winter, A., & Haux, R. (1995). A three-level graph-based model for the management of hospital information systems. Methods of Information in Medicine, 34, 378-378.
31. Wooten, R., Klink, R., Sinek, F., Bai, Y., & Sharma, M. (2012, May). Design and implementation of a secure healthcare social cloud system. InProceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012) (pp. 805-810). IEEE Computer Society.
32. Yang, J. J., Li, J., Mulder, J., Wang, Y., Chen, S., Wu, H., & Pan, H. (2015). Emerging information technologies for enhanced healthcare.Computers in Industry, 69, 3-11.
33. Yunus, M. (2009). Swamp Computing" aka Cloud computing. Web Security Journal, 12-28.