امنیت سامانه های اینترنت اشیاء در بیمارستان

کوروش داداش تبار احمدی[۱*]، سارا همت زاده زارع[۲]
[۱]استادیار، دانشگاه صنعتی مالک اشتر، مجتمع دانشگاهی برق و کامپیوتر، Dadashtabar@mut.ac.ir
[۲]دانشجوی کارشناسی ارشد رایانش امن، دانشگاه صنعتی مالک اشتر، HemmatZadeh.Zare@Gmail.Com

چکیده : در عصر حاضر مسئله اینترنت اشیاء مرکز توجه اکثر محققین قرار گرفته است و از آن به عنوان یک بخش جدایی ناپذیر اینترنت نام برده می شود. دانش اینترنت اشیاء تا حدودی رویاهای کودکی ما را به حقیقت نزدیک کرده است و مفهوم جدیدی است که باعث حضور حسگرها در زندگی انسان شده است به طوری که تمامی اطلاعات توسط همین حسگرها جمع آوری، پردازش و منتقل می شوند.

امروزه با ظهور پرونده ی الکترونیکی بیماران در بیمارستان ها ، نیاز به تبادل اطلاعات افزایش یافته و در نتیجه محرمانگی در سیستم های اطلاعاتی باید بیشتر مورد توجه قرار گیرد. اینجاست که اهمیت اینترنت اشیاء مطرح می شود. با گسترش تکنولوژی و ظهور اینترنت، تحولی بزرگ در جهان ایجاد شد و با استقبال روز افزون مردم از آن، فعالان حوزه تکنولوژی به فکر استفاده از اینترنت در بخشهای مختلف زندگی مردم افتادند.

با استفاده از اینترنت اشیا در حوزه سلامت، بیماران می توانند خود کنترل وضعیت را در دست بگیرند و کادردرمان نیز قادر خواهند بود تا موثرترین مراقبت ها را ارائه دهند و از راه دور بسیاری از بیماری ها را شناسایی کنند و بخشی از مراحل درمان را در منزل انجام دهند و همچنین هوشمندسازی سیستم های ثبت اطلاعات منجر به افزایش دقت در امور شده که از این طریق می توان بسیاری از بیماری ها را به سرعت پیش بینی و پایش کرد. ما در این مقاله به معرفی اینترنت اشیاء و امنیت آن در سامانه های بیمارستانی پرداخته ایم.

کلید واژه‌ها: امنیت اطلاعات , امواج رادیویی(RFID) , اینترنت اشیاء(IoT) , سیستم های اطلاعاتی بیمارستانی .

۱- مقدمه

اینترنت اشیاء (IoT)[۱] در سالهای اخیر توانسته جایگاه قدرتمندی درکسب و کارهای حوزه فناوری اطلاعات پیدا کند. در ابتدا وقتی صحبت از اینترنت اشیاء به میان آمد، بیشتر محدود به تکنولوژی های حوزه شناسایی خودکار امواج رادیویی(RFID)[۲] و ارتباطات با فاصله کم(NFC)[۳] می شد، اما امروزه با پیشرفت های روز افزون تکنولوژی های کامپیوتری و ورود فناوری های ارتباطی جدید، اینترنت اشیاء شکل جدیدتری به خود گرفته است.

کلمات "اینترنت" و "اشیاء" وقتی کنار هم قرار می گیرند، معنایی را می‌رسانند که سطح درهم گسیخته‌ای از نوآوری را به جهان ICT[۴] امروزی معرفی می کنند. در حقیقت "اینترنت اشیاء" از لحاظ نحوی به معنای یک شبکه گسترده جهانی از اشیاء به هم پیوسته است که به طور انحصاری قابل نشان‌یابی است و براساس پروتکل‌های ارتباطاتی استاندارد می باشد. از این تعریف برداشت می‌شود که تعداد کثیری از اشیاء در این روند درگیر هستند. نشان‌یابی اشیاء منحصر به فرد و بیان و ذخیره‌سازی اطلاعات مبادله شده یکی از چالش برانگیزترین موضوعات می‌شوند و سومین جنبه‌ی "معنامحور اینترنت اشیاء" را ایجاد می‌کنند. [۱]

۲- طرح مسئله

اینترنت اشیاء یک پارادایم جدید است که ایده اولیه آن بر اساس تعامل مستمر انواع چیزهایی که در اطراف هستند ایجاد شده است، این تعامل مستمر در به اشتراک گذاری داده ها که تقریبا در تمامی ابعاد زندگی انسان ها وجود دارد، باعث به خطر افتادن حریم خصوصی افراد گردیده، زیرا سازکارهای موثری برای شخصی سازی حریم خصوصی و حفاظت گسترده از امنیت اطلاعات، وجود ندارد. علاوه بر این دغدغه های مصرف کنندگان محتوا در خصوص کیفیت داده های محتوایی نادیده گرفته شده و چالش بین «حریم خصوصی تولیدکننده محتوا» و «کیفیت داده های محتوایی مصرف کننده محتوا» همچنان باقی است.

با توجه به گستردگی دامنه استفاده از اینترنت اشیاء و برنامه-های متعدد کاربردی آن در حوزه های گوناگون مثل برنامه های روزمره، رفتارها ، مسائل بهداشت و یا مسائل عاطفی، ضرورت و پیچیدگی توجه به موضوعات مرتبط با حریم خصوصی و امنیت اطلاعات در این فضا بیش از پیش مورد توجه همگان قرار گرفته است. مسلما با رشد گستره تحت پوشش اینترنت اشیاء و افزایش ارتباطات و تبادلات داده ای مشکلات امنیتی افزایش پیدا می کند.

[1] . Internet of Things (IoT)
[2] . Radio Frequency Automatic Identification (RFID)
[3] . Near Field Communication (NFC)
[4] . Information and Communications Technology (ICT)

امنیت اطلاعات و شبکه باید با خصوصیاتی از جمله شناسایی، قابلیت اعتماد، تلفیق و غیرقابل انکار بودن برآورده شود. علم IoT باید به حوزه‌های مهمی از اقتصاد ملی مانند سرویس درمانی، مراقبت پزشکی، سلامت هوشمند، حمل و نقل هوشمند و ... اعمال شود تا امنیت آن مهم دانسته شود، بنابراین رمزنگاری (اطلاعات مهمی که به ناچار باید در محیط های نا امن مبادله و یا ذخیره شوند.) نقش مهمی در زمینه امنیت سیستم های اطلاعاتی و سامانه های اینترنت اشیاء ایفا میکند. [۲]

۳- شرح موضوع

۳-۱- اهداف اصلی پژوهش

- آشنایی با اینترنت اشیاء و کاربرد های آن در بیمارستان ها.
- آشنایی با امنیت سامانه ها و گجت های اینترنت اشیاء در حوزه سلامت و خدمات بهداشتی درمانی به بیماران.
- چالش های به کارگیری اینترنت اشیاء در بیمارستان ها.

۳-۲- سوالات پژوهش

- اینترنت اشیاء چیست؟
- امنیت اینترنت اشیاء و سامانه های آن در خدمات درمانی بیماران چگونه حفظ می‌شود؟
- چالش های امنیتی اینترنت اشیاء و چالش های به کارگیری آن در بیمارستان‌ها کدامند؟
- بایدها و نبایدهای حفظ حریم گجت‌های اینترنت اشیاء در زمینه محرمانگی و حفاظت از اطلاعات بیمار و بیمارستان؟
- روش های پیاده سازی اینترنت اشیاء کدامند؟

۳-۳- مبانی نظری پژوهش

امنیت اطلاعات از این جهت که از سیستم های اطلاعاتی در برابر تهدیدات داخلی و خارجی محافظت می کند، موضوع مهمی است. در واقع، سرنوشت یک سازمان به سطوح فن آوری اطلاعات و حفاظت اطلاعات آن سازمان وابسته می باشد. حفاظت از تجهیزات پزشکی، کامپیوتری، داده ها، اطلاعات و خدمات کامپیوتری در برابر دسترسی های ناخواسته و غیرمجاز، حوادث غیرمترقبه و تخریب های فیزیکی، برای هر سازمان امری حیاتی است. امنیت اطلاعات بخشی از اصول سه گانه محرمانگی، یکپارچگی و قابلیت دسترسی(مثلث CIA)[5] می باشد. محرمانگی تضمین می کند که فقط افراد مجاز حق استفاده از اطلاعات را دارند. یکپارچگی تضمین می کند که اطلاعات به روش غیرمجاز در معرض تغییر و تخریب قرار نمی گیرد. قابلیت دسترسی نیز تضمین می کند که افراد مجاز در مواقع نیاز می توانند به اطلاعات دسترسی داشته باشند.

تهدیدات امنیتی سیستم های اطلاعات مراقبت سلامت در سال های اخیر به صورت چشمگیری افزایش یافته است. امنیت سیستم های اطلاعات سلامت آسیب پذیر می باشد. این در حالی است که حفظ محرمانگی و رازداری اطلاعات، یکی از نگرانی های عمده بیماران محسوب می شود.

۳-۳-۱- اینترنت اشیاء

اینترنت اشیاء (IoT) در واقع آینده اینترنت را نشان می‌دهد که تمام ابزارها و وسایل با هم در ارتباط هستند و می‌توانند درکی از محیط اطراف خود داشته و با دیگر وسایل و ابزار ارتباط برقرار نمایند. برای برقراری این ارتباط نیاز به قراردادهای ارتباطی وجود دارد تا دستگاه ها بتواند از طریق آن با اینترنت و دیگر دستگاه ها ارتباط داشته باشند. برقراری این ارتباط با استفاده از قراردادهای ارتباطی اینترنتی موجود می تواند در زمینه ی سنجش از راه دور هزینه بر باشد ، زیرا قرارداد های اینترنت دارای برنامه هایی است که نیاز به منابع (پردازش، حافظه، انرژی و ...) زیادی داشته و به دلیل اینکه دستگاه های سنجش از راه دور دارای منابع محدودی به خصوص از لحاظ انرژی هستند نمی توانند کارایی لازم را داشته باشند. تاپیش از این تصور عموم این بود که تنها این انسانها هستند که قرار است با ابزار هایی که در اختیار دارند توسط شبکه اینترنت به هم متصل شوند و شخصا از قابلیت های آن بهره ببرند. اما بیش از یک دهه است که مفاهیم جدیدی شکل گرفته است. [۳]

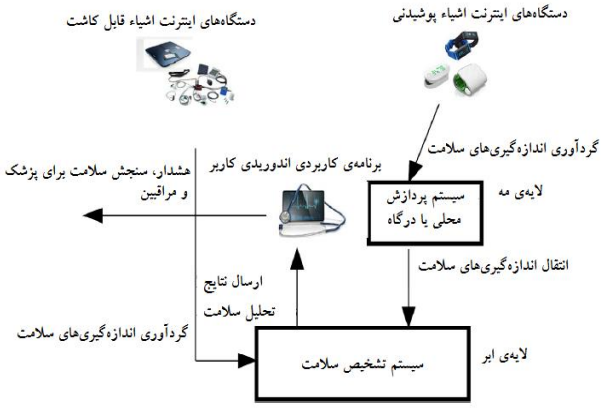
اینترنت اشیا شبکه ای است که هر شیء را به اینترنت وصل میکند و از ادغام و ترکیب چندین فناوری ازجمله شناسایی خودکار امواج رادیویی(RFID)[6]، ارتباطات میدان نزدیک(NFC)[7]، حسگر[8]، سیستم موقعیت یاب جهان(GPS)[9] و اسکنرهای لیزری[10] تشکیل شده است که باعث برقراری تبادل اطلاعات و ارتباطات می شود و هدف اصلی آن شناسایی هوشمند، ردیابی محل، نظارت و مدیریت است. [۴]

[5] . Confidentiality & Integrity & Availability (CIA)
[6] . Radio Frequency Automatic Identification
[7] . Near Field Communication
[8] . Sencor
[9] . Global Positioning System
[10] . Laser Scanners

اتحادیه بین المللی ارتباط از راه دور(ITU)[11] بیان نموده است که IoT در هر زمان و مکانی، برای هر کس و با هر شیء ارتباط برقرار میکند. IoT در صنایع مختلف کاربرد دارد از جمله میتوان به بخش خانه ها و شهرهای هوشمند، انرژی و بهره وری، حمل و نقل، بخش تولید و تدارکات، دام و حیوانات، کشاورزی و صنعت بیمه اشاره نمود. این فناوری نیز در بخش مراقبت سلامت به ویژه سلامت الکترونیک(eHealth) به عنوان یکی از ضروری ترین و پرکاربرد ترین موضوعات در سال های اخیر مطرح شده است. [۵]

۲-۳-۳- اینترنت اشیاء در پزشکی

علم IoT می‌تواند در زمینه های مختلف پزشکی از جمله دستگاه‌های مراقبت از راه دور و هشدار دهنده موارد اورژانسی ، برنامه های تناسب اندام ، بیماری های مزمن و مراقبت از سالمندان مورد استفاده قرار گیرد و کارکرد های مهمی را در حوزه سلامت اعم از مدیریت مؤثر در کل موسسه مراقبت بهداشتی و درمانی ، هماهنگی و برقراری ارتباط بین پزشک و بیمار به ارمغان گذارد ، به طوری که داده های حاصل از علائم حیاتی به صورت خودکار از طریق پوشیدن لباس های هوشمند در وضعیت های مختلف (مثل قدم زدن، خوردن، خوابیدن و ورزش کردن) ثبت و گردآوری می-شود و در صورت هرگونه تغییر در ارتباط با سبک زندگی و وضعیت سلامت به افراد هشدار می دهد.



شکل ۱: اینترنت اشیاء در حوزه سلامت

البته درکنار کاربردهایIoT در نظام مراقبت سلامت و به منظور محقق شدن وعده های آن یکسری چالشها و موانع امنیتی مطرح است. برخی ازاین مشکلات و چالشهای امنیتی ناشی از ویژگی ها و قابلیت های اینترنت اشیاء اعم از ناهمگونی، سیاربودن(تحرک) ، مقیاس پذیری، آدرس دهی و شناسایی و محدودیت منابع است.

از آنجا که صنعت مراقبت سلامت با جان یک انسان سر وکار دارد و نقش امنیت IoT در حوزه پزشکی نسبت به سایر صنایع اهمیت بیشتری پیدا می کند، این موضوع به ویژه در هنگام جمع آوری داده های بلا درنگ و تحلیل داده ها در برنامه های کاربردی محسوس تر است و مفاهیم امنیتی مورد توجه قرار میگیرد. زیرا تجهیزات و برنامه های کاربردی دربرگیرنده اطلاعات خصوصی و حیاتی بیمار مثل داده های مراقبت سلامت فردی هستند.

۳-۳-۳- امنیت در اینترنت اشیاء بیمارستانی

اینترنت اشیاء بخش جدایی ناپذیری از آینده اینترنت است، پروتوکل های ارتباطی جدید هم به عنوان بنیاد این شبکه ایفای نقش می کنند . وظیفه ی این پروتوکل ها این است که تعامل و یکپارچگی کامل اشیاء مجازی و فیزیکی جهان را تضمین کنند. کامپیوترها، گوشی ها، تلویزیون ها، حسگرها، خودروها،یخچال ها و حتی بسته های غذا و دارو در این شبکه متشکل از اشیا قرار میگیرند، لیکن خطراتی در خصوص اینترنت اشیاء وجود دارد و به همین دلیل نمی توان امنیت آن را صد در صد دانست.

در اینترنت اشیاء، دستگاه ها اطلاعاتی را فرستاده و دستوراتی را دریافت می کنند ، از این رو نفوذ هکر و سوءاستفاده آن، چندان هم دور از انتظار نیست. با افزایش دستگاه های متصل به اینترنت اشیاء، خطر نفوذ هکرها نیز افزایش می یابد، شاید برخی دستگاه‌ها از امنیت کافی برخوردار نباشند. مسئله حریم خصوصی در اینترنت اشیاء بسیار پیچیده تر از ارتباطات اینترنت است، زیرا اساس ارتباطات در اینجا به صورت دو سویه و چند سویه بوده ، لذا حریم خصوصی در اینترنت‌اشیاء بایدبیان کند مدیریت داده‌های محتوایی جمع آوری شده برای بخش مصرف کننده محتوا نیز باشد.

واژه امنیت در IoT گستره بزرگی از مفاهیم و الزامات امنیتی همچون محرمانگی، تصدیق یا احراز هویت، تمامیت، اعطای مجوز و قابلیت دسترسی را در برمیگیرد که این الزامات با استفاده از مکانیسم های مختلف امنیتی فراهم می شود . وضعیت امنیت IoT با توجه به ماهیت آن در نظام سلامت نسبت به سیستم های فعلی شرایط را به مراتب پیچیده و حساس تر می کند زیرا با گسترش اینترنت اشیاء در سلامت الکترونیک تهدیدات امنیتی در حال پیشرفت است و دستگاه های هوشمند دائم مورد حمله قرار میگیرند به گونه ای که ممکن است یک مهاجم با دستکاری فیزیکی در تجهیزات پزشکی و استخراج کدهای رمزنگاری برنامه را تغییر داده و/یا دستگاه ها را تخریب نماید. [۶]

[11] . International Telecommunication Union

از طرف دیگر، براساس گزارش گارتنر[12] بیش از ۵۰ درصد اتصالات اینترنت بینIoT است تا سال ۲۰۲۰پیش بینی شده که ۲۶ بیلیون وسیله به اینترنت وصل خواهد شد. حال باتوجه به این حجم وسیع دستگاه های متصل به هم و انتقال و تبادل اطلاعات بین آنها نگرانی هایی امنیتی و ناتوانی افراد در کنترل حریم خصوصی شکل می گیرد. درکنار استفاده گسترده از IoT در مراکز مختلف به منظور به حداقل رساندن چالشهای امنیتی و نگرانی های به وجود آمده در زمینه حریم خصوصی افراد، نفوذهکرها به شبکه های بیمارستان و اختلال در تجهیزات پزشکی نیاز به تلاش و اقدامات قانون گذاران و سیاست گذاران و مداخله طراحان سیستم جهت شناسایی راهکارها و مکانیسم های مقابله ای در برابر تهدیدات و حملات دارد. بنابراین، قبل از طراحی معماری امنیت در IoT لازم است تا چارچوبی ارائه شود که تمام زوایا و عوامل مرتبط با امنیت به همراه مکانیسم های آن شناسایی شود. لذا، شناسایی تمام عوامل مرتبط با امنیت در IoT می تواند از بروز تهدیدات و حملات پیشگیری نماید که باعث تأمین امنیت در رمزگذاری داده ها در دستگاه ها و مسیر انتقال شبکه، داده های جمع آوری شده توسط حسگرها، داده های ذخیره شده در پایگاه های داده و امنیت در خدمات اطلاع رسانی شود. موضوع IoT در صنعت مراقبت سلامت هنوز به بلوغ نرسیده و در مرحله ابتدایی قرار دارد. با توجه به نقشIoT در ارتقای مدیریت اطلاعات، تمامی اشیا در دستگاه های مراقبت بهداشتی (افراد و تجهیزات) می توانند به طور مداوم ردیابی و پایش شوند. بنابراین، IoT باید قابلیت امکان دستیابی افراد مجاز را به تمامی اطلاعات پزشکی یک بیمار در محلهای مختلف (بیمارستانها و مطب پزشکان) فراهم نماید. ضمن اینکه حفاظت از IoT در صنعت سلامت به دلیل محرمانگی و حساس بودن اطلاعات بیمار و دسترسی به موقع اطلاعات برای متخصصان مراقبت سلامت به مراتب دشوار تر است. [۷]

مکانیسم های امنیت IoT در ۱۱طبقه اصلی سازماندهی شده اند که اکثر مطالعات به مکانیسم های رمزنگاری[13]، توزیع و مدیریت کلید[14]، مدیریت هویت دیجیتال[15]، مدیریت نگهداشت چرخه حیات سیستم[16] و مسیریابی امن[17] در هر دو صنعت سلامت و غیر سلامت توجه کرده اند. یافته های مطالعه حاضر نشان داد که پنج مورد از مکانیسم های امنیتی باوجود اهمیتی که دارند در صنعت سلامت پرداخته نشده است، این مکانیسمها در ارتباط با صرفه جویی توان مصرفی[18]، طراحی امن و حفاظت فیزیکی از سخت افزار سیستم[19]، سیستم تشخیص نفوذ و پیشگیری (IDPS)[20]، مدیریت اعتماد[21]و تشخیص و تحمل خطا[22] بودند.

درصنعت مراقبت سلامت به مکانیسم های تشخیص و تحمل خطا توجه نشده است در حالی که یک طرح امنیتی باید تضمین نماید که خدمات اینترنت اشیاء حتی در صورت وجود خرابی دستگاه ها ، بلایای طبیعی در مقابل حملات و تهدیدات بتوانند کار کنند و از فعالیت باز نمانندبسیاری از تهدیدات امنیتی مرتبط با لایه ادراکی و طراحی بخش سخت افزار سیستم IoT است. [۸]

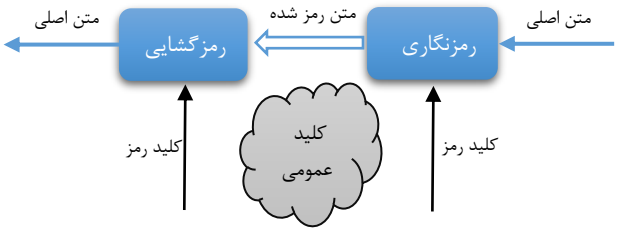
زندگی هوشمند	سلامت هوشمند	صنعت هوشمند	انرژی هوشمند	ساختمان هوشمند	حمل و نقل هوشمند	شهر هوشمند
قابلیت های امنیتی :	**لایه کاربرد :** کاربردهای اینترنت اشیاء					قابلیت های مدیریتی :
قابلیت های عمومی امنیتی	**لایه پشتیبان کاربرد و خدمات :** پشتیبانی عمومی ، پشتیبانی ویژه					قابلیت های عمومی مدیریتی
قابلیت های ویژه امنیتی	**لایه شبکه :** قابلیت های شبکه سازی، قابلیت های انتقال					قابلیت های ویژه مدیریتی
	لایه وسیله ها : درگاه ها، وسیله ها					

جدول ۱: مدل لایه ای معماری اینترنت اشیاء

بنابراین، دستگاه ها باید از لحاظ فیزیکی امن بوده و اجزای مدارهای فرکانس رادیویی نباید قابل تغییر و دستکاری باشند. از آنجا که داده ها از طریق حسگرها و دستگاه های مختلف IoT جمع آوری می شوند، حفاظت و امنیت فیزیکی آنها در همان ابتدا مهم است. بنابراین، امنیت فیزیکی دستگاه در قالب پوشش یا عایقی برای طراحی آنتن، گره های حسگر، ساختار سخت افزار و مدار مورد نیاز است تا از هرگونه دستکاری سخت افزار و جعل هویت جلوگیری شود. برای نمونه، استفاده از مکانیسم خود تخریبی می تواند مانع از جعل و دستکاری گره های حسگر شود بدین صورت که به محض باز شدن گره حسگر توسط مهاجم تمام اطلاعات مهم و حساس از بین می رود. [۹]

[12] . Gartner
[13] . Cryptography
[14] . Key distribution and management
[15] . Digital identity management
[16] . System life-cycle maintenance management
[17] . Secure routing
[18] . Power saving
[19] . Secure design and physical protection
[20] . Intrusion Detection and Prevention System
[21] . Trust management
[22] . Fault detection and tolerance

با توجه به اینکه اکثر کاربران پیرامون مسائل امنیتی در فضای مجازی و محافظت از اعتبارنامه ها آگاهی کافی و دانش لازم را ندارند، این عوامل زمینه را برای بسیاری از حملات مانند جستجوی فراگیر[۲۳]، حمله دیکشنر[۲۴]، مهندسی اجتماعی [۲۵]و فیشینگ[۲۶] فراهم می کند که کاربران ناخواسته کدهای مخرب را با کلیک روی لینکهای آلوده در ایمیل ها دانلود کرده و مهاجم رمز عبور کاربر را حدس می زند. از اینرو، آموزش و آگاهی کاربران در خصوص آسیب ها و تهدیدات امنیت IoT به ویژه مدیریت رمزعبور و نحوه استفاده صحیح از خدمات این فناوری حائز اهمیت است. بیشتر مطالعات مکانیسم های مرتبط با مدیریت هویت دیجیتال و رمزنگاری، مدیریت کلید را برای حفاظت از دستگاه‌های IoT مهم شناخته اند زیرا مکانیسم های رمزنگاری از حمله استراق سمع و تداخل فرکانس های رادیویی جلوگیری می کند و میتوان اطمینان حاصل کرد که اطلاعات حساس در فرایند انتقال داده به دست فرد غیرمجاز نمی رسد. این در حالی است که برای رمزگذاری داده ها نیاز به مبادله کلید معتبر و طرح های مدیریت کلید است.

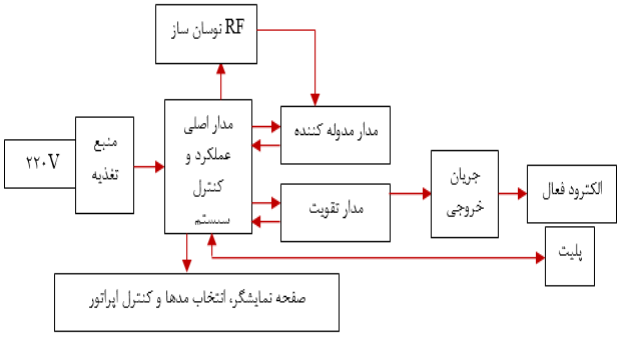


شکل ۲: مدل رایج رمزنگاری و رمزگشایی

در دنیای واقعی مدیریت کلید سخت ترین قسمت رمزنگاری محسوب می شود و حفاظت از کلیدهای سری کار بسیار دشواری است. از آنجا که احتمال حمله به دستگاه های رمز کلید عمومی و الگوریتم های رمزنگاری وجود دارد از این رو طراحی مطمئن و قدرتمند مدیریت کلید نقش بسزائی در امنیت تبادل داده دارد. در این رابطه وجود زیر ساخت کلید عمومی(PKI)[۲۷] جهت تولید ، نگهداری، عملیات صدور و توزیع گواهینامه برای کلید عمومی، نگهداری و انتشار لیست گواهی های لغو شده امری حیاتی است . قابل ذکر است که دومین عامل مهم امنیت IoT توافق کلید است که قبل از رمزنگاری داده به عنوان فرآیند مهم شناخته می شود، از این رو حصول اطمینان از احراز هویت اهمیت است. ایجاد یک کلید نشست امن بین اشیا در محیط IoT می تواند ارتباط ایمن بین کاربر و گره های حسگر را تضمین نماید. [۱۰]

نکته مهم دیگر آن است که امنیت IoT فقط با تکیه بر مکانیسم رمز عبور و الگوریتم های رمزنگاری تأمین نمی شود. برای حفاظت از احراز هویت موجودیت ها[۲۸] و تمامیت داده[۲۹] نیاز است که گره های حسگر قانونی باشد. بنابراین، مکانیسم مدیریت اعتماد برای اطمینان از اعتماد در روابط بین دستگاه های IoT و کاربران ضروری است، درحالی که حسگرها و دستگاه های پزشکی IoT در محیط های باز و کنترل نشده تعبیه شدند. وجود مکانیسم های اعتماد برای غلبه بر محیط های نا امن و پرخطر در استفاده از خدمات و برنامه هایIoT اساسی است. اخیراً بسیاری از دستگاه-های سلامت الکترونیک از طریق مکانیسم های امنیتی ایستا نظیر دیواره آتش[۳۰] و دستگاه های تشخیص نفوذ حفاظت می شود. درحالی که این مکانیسم ها به تنهایی نمی توانند اهداف و الزامات امنیتی را در محیط پویای IoT تأمین نمایند. اگر معماری IoT بتواند مسئله امنیت سایبری[۳۱] و تابآوری سایبری[۳۲] را تامین کند، این دستگاه ها به بالاترین سطح اعتماد پذیری خواهند رسید. سیستم مدیریت اعتماد باید برای تضمین اهداف و مکانیسم های امنیتی به طور موفقیت آمیزی اعمال شود. [۱۱]

تصورکنید که یک بیمار ناگهان در وضعیت اضطراری قرار گیرد تأخیر طولانی در به دست آوردن این اعتبارنامه، می تواند موجب از دست رفتن جان او شود، بنابراین تمام دستگاه های IoT باید مطابق با استانداردهای امنیتی باشند. علاوه براین، داده های موجود در برچسب RFID برای تبادل داده باید از یک استاندارد رمزگذاری واحد تبعیت کند.



شکل ۳: اجزای سیستم RFID

[23] . Brute force
[24] . Dictionary
[25] . Social engineering
[26] . Phishing
[27] . Public Key Infrastructure
[28] . Entity Authentication
[29] . Integrity
[30] . FireWall
[31] . Cyber Security
[32] . Cyber Resilience

اگر چه محدودیت توان مصرفی یکی از موانع مهم در شبکه IoT است اما تدابیر و راهکار امنیتی چندانی برای آن ذکر نشده است. این فناوری از دستگاه های کوچک با باتری محدود تشکیل شده است و دارای قدرت کم و ذخیره سازی پائین هستند. بنابراین، الگوریتم های رمزنگاری سنتی نمیتوانند مستقیماً روی چنین دستگاه هایی با توان پایین قرار گیرد. این دستگاه ها در زمانی که نیازی به پردازش و ارسال داده نیست باید در حالت ذخیره مصرف انرژی قرار گیرند دستگاه هایی که انرژی کافی ندارند، اساساً نمی توانند به طور عادی کار کنند. بنابراین، محدودیت انرژی، یافتن راه حل امنیتی را به چالش میکشد. دستگاه های تعبیه شده IoT متشکل از دستگاه ها و پشته های پروتکل شبکه ضعیف و فاقد ماژول های امنیتی هستند. [۱۲]

۴-۳-۳- چالش های اینترنت اشیاء

چالشهای تحقیقاتی اصلی درزمینه اینترنت اشیاء شامل حریم خصوصی، محرمانگی داده و اعتماد میشود که حریم خصوصی و امنیت از مهمترین چالش ها در اینترنت اشیاء به حساب می آیند.

۴- محدودیت های پژوهش

اندک بودن تعداد مطالعات امنیت IoT در صنعت مراقبت. پیشنهاد می شود برای طراحی و پیاده سازی معماری امن IoT به تهدیدات و مکانیسم های امنیتی این حوزه توجه شود.

۵- نقاط قوت پژوهش

از نقاط قوت این پژوهش مرور جامع و طبقه بندی مفهومی از مکانیسم های امنیت IoT بود که بینش وسیعی را برای محققان ، مدیران و متخصصان امنیت اطلاعات در جهت مقابله با تهدیدات و حملات امنیت IoT فراهم می کند.

۶- نتیجه گیری

با توجه به پیچیدگی و جدید بودن مباحث مدیریت و آمادگی در برابر حملات بیولوژیک و همان طور که از قبل انتظار می رفت میزان آمادگی بیمارستان ها در سطح ضعیف ارزیابی شده است ، که نیازمند توجه مسئولین به این موضوع و ایجاد راه کارها و تمهیدات جدی و سریع جهت افزایش این آمادگی ها می باشد، لذا بررسی میزان آمادگی مراکز درمانی کل کشور ، یک ضرورت دایمی است. با گسترش روز افزون دستگاه های با قابلیت ارتباطی عملکردی، به بینش اینترنت اشیا که در آن توابع ادراکی و عملکردی به صورت بدون مرز در محیط ادغام می شوند و امکان ایجاد قابلیت های جدید با دسترسی به منابع اطلاعاتی غنی، فراهم شده است، بسیار نزدیک خواهیم شد. تکامل نسل بعدی سیستم های سیار وابسته به خلاقیت کاربران در طراحی برنامه های کاربردی جدید است . اینترنت اشیا یک فناوری در حال رشد ایده آل جهت تأثیرگذاری بر این دامنه با فراهم کردن داده ها و منابع محاسباتی برای ایجاد برنامه های انقلابی است.

جهت به کارگیری مفید و مؤثر از اینترنت اشیا می توان از یک چارچوب مبتنی بر ابر استفاده کرد تا علاوه بر کاهش هزینه ها، قابلیت مقیاس پذیری نیز مهیا شود. چارچوب مبتنی بر ابر امکان انجام محاسبات، تجزیه و تحلیل، ذخیره سازی و مصورسازی را به صورت جداگانه برای کاربران فراهم می کند، بنابراین امکان گسترش هر بخش به صورت جداگانه و در نهایت، تکامل یکدیگر در یک محیط اشتراکی فراهم خواهد بود. با پیشرفت های حاصل شده در چند سال اخیر، پیش بینی می شود در ۵ تا ۱۱ سال آینده، اینترنت اشیا به مرحله ای که توسط عامّه مردم مورد پذیرش واقع شود، خواهد رسید. بررسی های انجام شده در این مقاله ممکن است به توسعه دهندگان و کارآفرینان کمک کند تا راه حل هایی برای تمام جامعه ارائه دهند.

مراجع

[۱] محمد مصلحی،مصطفی قبائی آرانی "رویکرد مبتنی بر الگوریتم رمزنگاری AES برای امنیت اینترنت اشیاء" ۱۳۹۵، صفحات ۱-۳.

[۲] امیر پناهی "اینترنت اشیاء، بایدها و نبایدها" فصلنامهٔ مطالعات حفاظت و امنیت انتظامی، شماره چهل ونهم،۱۳۹۷، صفحات ۴-۱۰.

[3] S. Nasiri and F. Sadoughi, *Security and privacy mechanisms of Internet of things in healthcare and non-healthcare industry* , pp. 88-97, 2019.

[4] W. Sun, Z. Cai, Y.Li, *Security and Privacy in the Medical Internet of Things* ,pp.1-6, 2018.

[5] Yap Sy Yuan and Dr. Tan Chye Cheah, *A Study of Internet of Things Enabled Healthcare Acceptance In Malaysia*, pp.25-27 ,2020.

[6] R. Roman, J. Zhou and J. Lopez, *On the features and challenges of security and privacy in distributed internet of things*, pp. 2267-2268 , 2013.

[7] Gubbi, *Vision, constructive elements and future trends of the Internet of Things*,pp. 8-10, 2013.

[8] Y. Yin, *The internet of things in healthcare*, pp.1-3, 2016

[9] L.Yu, *Smart Hospital based on Internet of Things*, pp 1654-1658, 2012

[10] D. Kouicem, A. Bouabdallah and H. Lakhlef, *Internet of things security: A top-down survey* , pp.7-11, 2018.

[11] K. Habib, W. Lesister, A. Torjusen, *Security Analysis of a Patient Monitoring System for the Internet of Things in eHealth*, pp. 73-75, 2015

[۱۲] محبوبه درافشانیان "کاربردهای اینترنت اشیاء در مراقبت از بیماران" ۱۳۹۵، صفحات ۱-۵.