ششمین همایش بین‌المللی افق های نویـن در
مهندسی برق، کامپیوتـر و مکانیک
6th International Conference on the New Horizons in
Electrical Engineering, Computer and Mechanical
www.mhconf.ir

ارائه یک روش امنیت داده جهت لباس های سلامتی هوشمند

احسان حیدری[1]

[1]گروه کامپیوتر، واحد دورود، دانشگاه آزاد اسلامی، دورود، ایران heidaari@gmail.com

چکیده

محیط زندگی کمکی باهدف حمایت از افراد ضعیف و سالمندان برای زندگی روزانه خود، بر اساس وضعیت آنها ارائه می‌شود. برای این منظور، دستگاه‌ها و خدمات که کاربر محور و سازگار با نیازها و قابلیت‌های افراد نیازمند به مراقبت موردنیاز می‌باشد. ادغام مداوم فن‌آوری‌های پیشرو، مانند فن‌آوری‌های ابر و ارتباطات بی‌سیم، درزمینه اینترنت اشیاء، می‌تواند شکل جدیدی از ارتباطات بین افراد ضعیف و مسن، محیط‌زیست خود و گروه‌های مربوط به مراقبت به وجود آورد. بایستی بتوان افرادی که دارای بیماری‌های خاصی بوده و یا افراد ناتوان را در هرلحظه تحت نظارت داشت تا در هنگام بروز اتفاقی به‌سرعت تحت درمان قرار داده شوند. این نظارت توسط حسگرها و دستگاه‌هایی داده‌های مربوط به جمع‌آوری حالات بیماران در منزل و سایر محل‌های به‌دوراز مراکز درمانی را به مراکز درمانی ارسال می‌کنند تا در موارد ضروری اقدام شود. این اطلاعات ارسالی بایستی بدون تغییر و با حفظ جامعیت و یکپارچگی خود به سرورهای مراکز درمانی ارسال شوند. در اینجا ما طراحی مفهومی و پیاده‌سازی نمونه اولیه از یک سیستم مبتنی بر دروازه‌های اینترنت اشیاء که داده‌های حسگر سلامت را جمع‌آوری کرده و مسائل امنیتی را از طریق گواهینامه‌های دیجیتال و رمزگذاری داده‌های PKI انجام می‌دهند را ارائه کردیم. در نتیجه این روش رمزنگاری پیشنهادی باعث می‌شود که اطلاعات به‌سرعت و بصورت امن در اختیار مراکز درمانی موردنظر قرار گیرند تا با اقدام به‌موقع مراکز درمانی بتوان به سرعت به بیماران و سالمندان رسیدگی نمود که این امر آمار مرگ‌ومیر را کاهش خواهد داد.

واژه‌های کلیدی

اینترنت اشیا، دستگاه‌های سلامت همراه، حفاظت داده‌ها، رمزگذاری داده‌ها، کلید عمومی و متقارن.

۱. مقدمه

اینترنت اشیاء مفهومی جدید در دنیای فناوری اطلاعات و ارتباطات بوده و به‌طور خلاصه فناوری مدرنی است که در آن برای هر موجودی اعم از انسان، حیوان و یا اشیاء قابلیت ارسال و دریافت داده از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترانت، فراهم می‌شود. دستگاه‌های هوشمند در دسته‌ای کلی به نام اینترنت اشیاء قرار می‌گیرند. اینترنت اشیاء درواقع به ارتباط اشیای مختلف از طریق اینترنت و برقراری ارتباط با یکدیگر می‌پردازد تا هدف آن یعنی فراهم کردن تجربه کاراتر و هوشمندتر محقق شود. به‌عبارت‌دیگر ایده طراحی دستگاه‌های مختلف با امکان برقراری ارتباط بی‌سیم به‌منظور رهگیری و کنترل از طریق اینترنت و یا حتی از طریق یک برنامه ساده مخصوص گوشی‌های هوشمند، اصطلاح اینترنت اشیاء را توصیف می‌کند. با توسعه کلی اینترنت اشیاء، انواعی از فن‌آوری‌های مختلف ارتباطات بی‌سیم و ساختار شبکه جمع‌آوری می‌شوند و محیط شبکه ارتباطی به‌طور فزاینده پیچیده خواهد شد.[۵-۱] اینترنت اشیاء بین دنیای مجازی و دنیای فیزیکی قابلیت همکاری ایجاد می‌کند بنابراین با توجه به این قابلیت همکاری، بحث امنیت اطلاعات و حفظ حریم خصوصی در صنایع ملی و خدمات اجتماعی مطرح می شود. اگر مسائل امنیتی و حفظ حریم خصوصی موردتوجه قرار نگیرد، یک خطر بزرگ در برنامه‌های کاربردی اینترنت اشیاء وجود خواهد داشت؛ بنابراین، مسائل امنیتی اینترنت اشیاء موظف به افزایش به سطح ملی هستند و این مسئله برای بهبود امنیت اینترنت اشیاء بسیار مهم می‌باشد. با استفاده از روش‌های رمزنگاری می‌توان انتقال داده‌های امنی را در حوزه‌های مختلف اینترنت اشیاء داشته باشیم که با استفاده از زیرساخت کلید عمومی می‌توان به این سطح از امنیت دست‌یافت. در زیرساخت کلید عمومی فرستنده اطلاعات داده را با استفاده از کلید عمومی رمزگذاری می‌کند در این صورت است که تنها با کلید خصوصی که در دست گیرنده می‌باشد داده‌ها رمزگشایی می‌شوند بنابراین عوامل غیرمجاز نمی‌توانند در بین راه و در حین انتقال داده‌ها به محتوای داده‌ها دسترسی داشته باشند و تنها با کلید خصوصی می‌توان محتوای اطلاعات را رمزگشایی نموده و مورداستفاده قرار داد. [۹-۶] درحالی‌که امنیت در اینترنت بسیار مهم است، امنیت در اینترنت اشیاء را باید در تمامی سطوح کاملاً بررسی کرد. امنیت باید به‌صورت ابتدا تا انتها در نظر گرفته شود: امنیت در رمزگذاری داده‌ها در دستگاه‌ها، امنیت در رمزگذاری داده‌ها در مسیر انتقال (شبکه)، امنیت برای داده جمع‌آوری‌شده توسط حس‌گرها، امنیت در جمع‌آوری داده از طریق شبکه و امنیت داده‌های ذخیره‌شده روی پایگاه‌های داده و امنیت در سرویس مورد ارائه. حفاظت از اطلاعات سلامت جمع‌آوری‌شده از حس‌گرها و دستگاه‌های مختلف از دسترسی‌های غیرقانونی بسیار مهم است. در غیر این صورت اطلاعات مهم شهری، سلامت و خانه‌ها در اختیار هکرها قرار می‌گیرد؛ بنابراین، سیاست‌های دقیق و معیارهای امنیتی فنی باید برای به اشتراک‌گذاری داده‌های بهداشتی با کاربران مجاز، سازمان‌ها و برنامه‌های کاربردی معرفی شود. معرفی یک الگوریتم بهینه برای همکاری بین حفاظت، تشخیص و انجام واکنش برای جلوگیری از حملات مختلف، تهدید و آسیب‌پذیری یک چالش است. [۱۴-۱۰] بازار دستگاه‌های نظارت بر سلامت در حال حاضر توسط راه‌حل‌های نرم‌افزاری خاص که متقابلاً غیر سازگار بوده و از معماری متنوع ساخته‌شده‌اند، تشکیل شده است. درحالی‌که محصولات منحصربه‌فرد طراحی‌شده باهدف بلندمدت برای دستیابی به هزینه‌های فناوری پایین در سراسر بخش‌های فعلی و آینده، ناگزیر به چالش‌های بسیاری خواهد بود، مگر اینکه یک رویکرد منسجم‌تر به کار گرفته شود. هدف اصلی سلامت هوشمند، ارتقاء کیفیت زندگی برای افرادی که نیاز به پشتیبانی یا نظارت دائم دارند، می‌باشد. همچنین برای کاهش موانع نظارت بر پارامترهای مهم سلامت، برای جلوگیری از هزینه‌های درمانی غیرضروری و ارائه حمایت‌های پزشکی مناسب در زمان مناسب می‌باشد. در سرتاسر فرآیندهای تخصصی زیرساخت‌های سایبر فیزیکی در نقطه اتصال کنترل و سنجش، ترکیب حس‌گرها و تصمیم‌گیری، امنیت و دستگاه‌های سایبر فیزیکی ترکیبی، چالش‌هایی وجود دارد. به‌طورکلی دستگاه‌های اختصاصی پزشکی برای برقراری ارتباط با دیگر دستگاه‌های پزشکی و یا دستگاه‌های محاسباتی طراحی نشده‌اند و نیاز به پیشرفت در شبکه شدن و ارتباطات توزیع‌شده درون معماری‌های سایبر فیزیکی دارند. به نظر می‌رسد قابلیت همکاری و دستگاه‌های حلقه بسته، کلید موفقیت باشند. هنگامی‌که اطلاعات فردی بیمار بر روی شبکه‌های سایبر فیزیکی ارسال می‌شود، امنیت سیستم حیاتی خواهد بود. [۱۷-۱۵]

۲. کارهای گذشتگان

اینترنت اشیاء در حال تبدیل جهانی است که ما در آن زندگی می‌کنیم. اینترنت اشیاء اغلب به‌عنوان شبکه‌ای از اشیاء فیزیکی تعریف‌شده است که می‌تواند با دیگر دستگاه‌های فعال اینترنتی و دستگاه‌های اشتراک‌گذاری اطلاعات ارتباط برقرار کند و اقداماتی مبتنی بر ورودی کاربر یا یک سیستم کنترل خودکار اجرا کند. اینترنت اشیاء دستگاه‌های متصل، داده‌ها و دستگاه‌های بین جهان فیزیکی و جهان آنلاین

برای افزایش بهره‌وری و رشد کسب‌وکار و همچنین بهبود کیفیت زندگی را عده می‌دهد. اینترنت اشیاء انتظار می‌رود که اتصال دستگاه‌های پیشرفته، دستگاه‌ها و خدماتی که فراتر از ارتباطات ماشین به ماشین هستند را ارائه دهد و تنوعی از پروتکل‌ها، دامنه‌ها و برنامه‌های کاربردی را پوشش می‌دهد.

همان‌طور که تعداد دستگاه‌های شبکه، تنوع قابلیت‌های سیستم اینترنت اشیاء در نوع دستگاه‌های شبکه همچنان رو به رشد است نیاز به امنیت بهتر برای ارتباطات دستگاه‌های حمل‌ونقل، شبکه‌های زیرساخت‌های انرژی و مانیتور بهداشت و درمان برای جوامع در همه‌جا بیشتر دیده می‌شود. باوجود مشخصات و قابلیت‌های این دستگاه‌های و دستگاه‌های مختلف، نیاز اساسی برای احراز هویت و امنیت برای همه مشترک و حیاتی می‌باشد. [۱۸]

ژیانگ لی در سال ۲۰۱۱ یک طرح از معماری امنیتی قابل‌اعتماد برای اینترنت اشیاء را پیشنهاد دادند. نقاط ضعف این سیستم را می‌توان به‌صورت زیر بیان شود:

اینترنت اشیاء باوجود یک انسان متصل می‌شود که عامل مهمی نیست. مهم‌ترین عوامل داده‌ها و دستگاه‌های اینترنت اشیاء هستند.

تکنیک‌ها و الگوریتم‌های امنیتی قدیمی را نشان می‌دهد که برای اینترنت اشیاء مناسب نیستند و یک ایده نوآورانه را نشان نمی‌دهد.

الگوریتم‌ها و تکنیک‌هایی که در هر لایه سیستم نشان داده می‌شوند، برای اجرا در سیستم اینترنت بیش‌ازحد بزرگ هستند. این به خاطر قدرت محدود ماشین‌ها از قبیل حس‌گرها و RFID که به‌عنوان اسکلت دستگاه‌های اینترنت اشیاء در نظر گرفته می‌شوند. [۱۹]

آریجیت در سال ۲۰۱۱ یک دنباله برای ساخت دستگاه‌های امنیتی برای اینترنت اشیاء پیشنهاد کردند. این دنباله تهدیدها و مشکلات سرویس‌های اینترنت اشیاء با ایمنی کم را نشان داده است. سیستم درباره برخی از ابزار که ممکن است به سرقت رفته باشند بحث می‌کند. این ابزار را می‌توان با استفاده از مانیتور یا دوربین‌های اتومبیل‌ها مشاهده شوند. این راه‌حل می‌تواند به‌عنوان سنتی در نظر گرفته و با طبیعت اینترنت اشیاء در یک راستا نیستند چون دستگاه‌هایی که برای نظارت از قبیل دوربین استفاده می‌شود، ممکن است هک شده یا به سرقت روند. [۲۰]

لیانگ ژو در سال ۲۰۱۱ یک معماری امنیتی برای اینترنت اشیاء بر اساس ترافیک چندرسانه‌ای پیشنهاد کردند. این دنباله ایده با ترافیک‌های چندرسانه‌ای مرتبط است که بیشتر اینترنت اشیاء را منتقل می‌کند؛ بنابراین، می‌تواند به‌عنوان یک راه‌حل پیشنهادی ویژه در نظر گرفته شود به‌طوری‌که آن می‌تواند فقط برای چندرسانه‌ای قابل‌اجرا باشد. علاوه بر این مبتنی بر تکنیک‌های قدیمی و سنتی می‌باشد که تاکنون تحت بحث و اجرا یا ارزیابی نبوده است. [۲۱]

اودریگو در ۲۰۱۱ یک تجزیه‌وتحلیل کلی برای مشکل امنیتی اینترنت اشیاء ارائه دادند. آن درباره برخی از ویژگی‌های عمومی مانند شناسایی و کنترل حس‌گر از راه دور بحث می‌کند. علاوه بر این، در برابر حملات انکار سرویس (DOS) به گره‌های حسگر یک دفاع ایجاد می‌کند.[۲۲]

هوی در سال ۲۰۱۲ تکنیک‌های احراز هویت و کنترل دسترسی برای دستگاه‌های اینترنت اشیاء را ارائه دادند. این دنباله بر روی سادگی و کارآمد بودن رمزنگاری منحنی بیضوی متمرکز تمرکز کرد. علاوه بر این، روش مجوز کنترل دسترسی مبتنی بر نقش بر اساس برنامه‌های کاربردی شیء و نقش‌ها با توجه به ماهیت اینترنت اشیاء اقتباس شده است. این سیستم احراز هویت سه مشکل دارد؛ [۲۳]

۱) آن مبتنی بر الگوریتم‌های امنیتی قدیمی می‌باشد

۲) آن تنها با کاربران سیستم سروکار دارد و نه با دستگاه‌ها و داده‌های سیستم

۳) آن به‌عنوان یک تکنیک پیشنهادشده خاص در نظر گرفته می‌شود

۳. روش پیشنهادی

جهت جلوگیری از تغییر داده‌ها توسط عوامل غیرمجاز می‌توان از رمزنگاری داده‌ها استفاده نمود. در اینجا ما رمزنگاری داده‌های جمع‌آوری‌شده حسگرهای سلامت با استفاده از زیرساخت کلید عمومی را ارائه می‌کنیم.پیر شدن جمعیت افزایش جمعیت با اختلالات، ناتوانی یا بیماری‌های مزمن را در پی خواهد داشت. خدمات محیط زندگی کمکی (AAL) می‌تواند این افراد را در زندگی روزمره خود پشتیبانی کند و یک سبک زندگی مستقل و امن برای آنها تا زمانی که ممکن است فراهم کند. [۲۴]

بنابراین، مراقبت در حال حرکت به سمت جامعه‌ای است که با دستگاه‌های سلامت نیازمند به اطلاعات بلادرنگ برای فعال کردن عمل مراقبت از افراد با صرف‌نظر از محل هر دو (مراکز مراقبت‌های بهداشت و درمان و بیمار) است. برای این منظور، خدمات AAL توسط فن‌آوری‌های کمکی مبتنی بر خانه (به‌عنوان‌مثال خانه‌های هوشمند، اشیاء تعبیه‌شده در شبکه‌های شخصی مانند دستگاه‌های بی‌سیم و حس‌گرها) که در اطراف افراد ضعیف بوده و در حال خدمت‌رسانی به آنها به شیوه سفارشی می‌باشند. این فن‌آوری جریان‌های داده را ارائه می‌کند که رفتار و تندرستی این افراد را ترسیم می‌کند تا زمانی که حالت‌های جدیدی از تعامل بین آنها، خانواده خود، مراقبان و دیگر متخصصان مراقبت‌های بهداشتی ایجاد شود. اینترنت اشیاء در حال پدیدار نمودن یک معماری سرویس اطلاعات جهانی می‌باشد که به‌احتمال‌زیاد یکی از مهم‌ترین پیشرفت‌های فن‌آوری در این قرن می‌باشد تأثیر محدوده گسترده‌ای از حوزه‌ها ازجمله مراقبت‌های خانگی را شامل می‌شود. اساساً، آن را شروع یک دوره جدید می‌دانند که تمامی دستگاه با یکدیگر و با سرویس‌های واسط صحبت خواهند کرد. برنامه‌های کاربردی و ستون فقرات مدیریت دستگاه نیاز دارند که به دستگاه داخلی و ارتباطات اینترنتی دست یابند تا بتوانند توسط محاسبات ابری، تسهیل پیمایش و پشتیبانی از میلیاردها اشیاء متصل را فراهم کنند. در این زمینه، ظهور اینترنت اشیاء می‌تواند مزایای زیادی را در زندگی‌های شخصی و اجتماعی مردم به ارمغان بیاورد. بااین‌حال، وجود موانع قابل‌توجهی برای رشد و استفاده گسترده از آن وجود دارد که امنیت برجسته‌ترین آنها می‌باشد. عبارت امنیت شامل محدوده گسترده‌ای از مفاهیم مختلف، پیشرو ازجمله آنها احراز هویت، محرمانگی، یکپارچگی و مجوز می‌باشد. اشیاء جاسازی‌شده شبکه‌های باز، مانند دستگاه‌های بی‌سیم و حسگرها، برای اینترنت احتمالاً جرقه جدیدی باشد و مدل‌های مخرب مبتکرانه برای به دست آوردن دسترسی به این اشیاء محلی در مجاورت آن نیاز نخواهند داشت. ازاین‌رو، زیرساخت‌های امنیتی مناسبی برای همساز کردن ترکیب اینترنت اشیاء از حس‌گرها و دستگاه‌ها موردنیاز می‌باشد. به‌منظور جلوگیری از رشد چنین مدل‌های مخرب و یا حداقل برای کاهش تأثیر آنها، مکانیزم های رمزنگاری مختلف (به‌عنوان‌مثال الگوریتم امضاء) می‌تواند به کار گرفته شوند. برای این منظور یک نمونه اولیه سیستم مبتنی بر ابر ارائه می‌شود که با مفهوم اینترنت اشیاء مطابقت دارد [۲۵]. سیستم پیشنهادی داده‌های جمع‌آوری‌شده توسط حسگرهای لباسی قابل پوشیدن (به‌عنوان‌مثال سیگنال زیستی، داده‌های حرکت و داده‌های متنی مانند مکان، درجه حرارت محیط، وضعیت فعالیت و غیره) که به یک دروازه بکار رفته در تکنیک‌های تعیین‌شده برای ارتباطات اینترنت اشیاء و سپس به زیرساخت‌های ابر فرستاده شود. واسطهای مناسب انتشار داده‌ها را به برنامه‌های کاربردی خارجی (مانند دستگاه‌های پرونده پزشکی و یا سیستم‌عامل تشخیص اضطراری) فعال می‌کند و یک برنامه مبتنی بر وب برای نظارت و مدیریت بلادرنگ داده‌های ضروری فراهم می‌کند که بر چهارچوب امنیتی ثبت‌شده در این سیستم، تمرکز دارد.

به‌طور خاص، مفهوم دروازه اینترنت اشیاء برای جمع‌آوری سیگنال و داده‌های بیمار و استفاده از رمزگذاری داده‌ها مناسب، کنترل دسترسی کاربر و تکنیک‌های انتقال امن برای ایجاد حریم خصوصی ضروری و امنیتی موردنیاز توسط دستگاه‌های نظارت بر سلامتی معرفی می‌شود. در طول چند سال گذشته علاقه رو به رشدی در استفاده از دستگاه‌های مبتنی بر اینترنت اشیاء در طیف گسترده‌ای از برنامه‌های کاربردی، ازجمله برنامه‌های کاربردی مراقبت‌های خانگی دیده شده است. این تغییر از دستگاه‌های کاربر پایانی متصل به اینترنت و اینترنت برای برقراری ارتباط با همدیگر و یا با انسان‌ها استفاده می‌کند که شامل چالش‌های امنیتی جدید می‌باشد و مکانیزم‌های محافظت سنتی دیگر کفایت نمی‌کند درنتیجه نیاز به زیرساخت‌های امنیتی قوی مطرح می‌شود. چالش‌های امنیتی توسط تعدادی از دستگاه‌ها و محدودیت مورد انتظار در واسطهای کاربر تشدید می‌شود؛ که در میان آنها، جنبه‌های امنیتی خاص، مانند احراز هویت و حریم خصوصی داده‌ها، رویکردهای نوآورانه موردنیاز وجود دارند. با توجه به احراز هویت، نیاز به تعریف یک مکانیزم احراز هویت شیء به‌منظور اینکه اطمینان حاصل شود که تنها اشیاء مجاز می‌توانند دسترسی به بخش‌های خاصی از داده‌های مبادله شده در یک محیط اینترنت اشیاء را به دست آورند. به‌مراتب برای اینکه یک مکانیزم در یک سیستم مبتنی بر اینترنت اشیاء مؤثر باشد، یک جنبه که

باید قبل از طراحی آن در نظر گرفته شود، مدیریت هویت است. این موضوع با توجه به ماهیت اینترنت اشیاء بحرانی در نظر گرفته می‌شود که در اصل به‌منزله یک تلفیقی از دنیای دیجیتال و فیزیکی است. اگرچه مدیریت هویت کاربر یک موضوع است که به‌خوبی در ادبیات موردبررسی قرارگرفته است، مدیریت هویت اشیاء دربرگیرنده یک محیط اینترنت اشیاء است که یک تعداد از موضوعات جدید را نشان می‌دهد که بایستی با آنها برخورد شود. با توجه به حریم خصوصی داده‌ها، ماهیت دستگاه‌های مبتنی بر اینترنت اشیاء و فن‌آوری‌های ثبت‌شده در آن، رمزنگاری را در ارتباطات ضروری تشکیل می‌دهند؛ بنابراین، از حملات امنیتی مانند استراق سمع، می‌توان جلوگیری کرد. در دستگاه‌های مبتنی بر اینترنت اشیاء، داده‌ها معمولاً توسط منابع اطلاعاتی متعدد، یعنی حسگرها و دستگاه‌های به دست می‌آیند. در شبکه‌های حسگر بی‌سیم (WSN) معمولاً یک دروازه (گره جمع‌آوری) قبل از ارسال آنها به سرور، یک زیرساخت ابر و غیره داده‌ها را جمع‌آوری می‌کند. به‌منظور حفظ حریم خصوصی، داده‌ها باید قبل از انتقال آنها رمزگذاری شوند. به‌عنوان‌مثال، بسیاری از راه‌حل‌ها جمع‌آوری داده‌ها را آدرس‌دهی می‌کنند تا زمانی که امنیت حفظ شود. رمزنگاری کلید عمومی یک جفت از کلیدهای وابسته ریاضی استفاده می‌کند. اگر یک کلید برای رمزگذاری اطلاعات استفاده شود، پس تنها کلید وابسته می‌تواند این اطلاعات را رمزگشایی کند.

درصورتی‌که کلید عمومی به خطر بیافتد می‌شود، انجام محاسبات برای بازیابی کلید خصوصی امکان‌پذیر نمی‌باشد. در مورد اینترنت اشیاء و مراقبت‌های بهداشتی، دستگاه‌هایی که اطلاعات مربوط به بیمار (مانند خواندن حسگر بدنی) را تولید می‌کنند، می‌توانند داده‌ها را با استفاده از یک کلید عمومی رمزگذاری کنند و برنامه‌های کاربردی نظارت بر سلامت رمزگذاری (به‌عنوان‌مثال، ابر و یا دستگاه‌های وب توسط مراقبان و یا بستگان اداره شوند) می‌توانند از کلید خصوصی برای رمزگشایی اطلاعات استفاده کنند. همچنین با استفاده از گواهی‌های دیجیتال زیرساخت کلید عمومی می‌توان به احراز هویت مناسب دستگاه‌ها و علاوه بر این به انتقال داده‌ها امن دست‌یافت. بهر حال ایجاد زیرساخت کلید عمومی در سیستم اینترنت اشیاء یک چالش عمده را مطرح می‌کند بدین شرح که حتی فرآیند رمزگذاری با کلید عمومی به محاسبات و منابع حافظه نیاز دارد که فن‌آوری‌های حسگر بی‌سیم موجود آن را فراهم نمی‌کند، به‌ویژه هنگامی‌که انتقال داده‌های مکرر موردنیاز است. (به‌عنوان‌مثال، انتقال سیگنال قلب)

سیستم پیشنهادی این مسئله را با معرفی دروازه‌های فعال اینترنت اشیاء نشانه‌گذاری می‌کند. دروازه‌های اینترنت اشیاء دستگاه‌هایی با توان محاسباتی قابل‌مقایسه با کامپیوترهای رومیزی هستند، با سیستم‌عامل کاملاً یکپارچه (معمولاً لینوکس) که واسط‌های ارتباطی بسیاری دارد. این دروازه‌ها همچنین می‌توانند یک مسئله امنیتی اضافی را برای دستگاه‌های اینترنت اشیاء آدرس‌دهی کنند: ثبت دستگاه‌های حسگر جدید و مدیریت کلید. هنگامی‌که یک دستگاه جدید نظارت که داده‌ها از طریق اینترنت انتقال می‌دهد معرفی می‌شود، دستگاه نیاز به دسترسی به کلید عمومی برای رمزنگاری مناسب داده‌ها دارد که فرآیندهای بعدی مدیریت کلید و مسائل توزیع را افزایش می‌دهد.

۱-۳ - معماری رمزنگاری کلید عمومی

سیستم پیشنهادی توانایی جمع‌آوری داده‌ها پزشکی را از حس‌گرهای مختلف تلفن همراه و پوشیدنی، داده‌های متنی (مانند شرایط اتاق، عادات کاربر و غیره) دارد. جمع‌آوری و انتقال امن به مراقبان و اعضای خانواده با استفاده از یک زیرساخت مبتنی بر ابر انجام می‌شود. معماری به‌طور عمده متشکل از سه جزء است:

حس‌گرهای متنی و تلفن همراه

دروازه‌های اینترنت اشیاء

زیرساخت Back- end

۱-۱-۳- حس‌گرهای متنی و موبایل

دستگاه‌های حس‌گر تلفن همراه و متنی به‌طور مداوم و یا دوره‌ای می‌توانند در مورد وضعیت بیمار (برای مثال، ضربان قلب / نبض، درجه حرارت و غیره) و زمینه آنها (به‌عنوان‌مثال، دمای اتاق، کیفیت هوا، شرایط نور و غیره) حس کنند. معمولاً این دستگاه‌های حسگر دارای

یک واحد میکروکنترلر می‌باشند که داده‌های حسگر آنالوگ یا دیجیتال را دریافت می‌کند، آنها را به ارزش کمی تفسیر می‌کند و آنها را به یک دستگاه جمع‌آوری داده‌ها و نظارت با استفاده از یک رابط بی‌سیم انتقال می‌دهد (مانند بلوتوث یا ZigBee). فن‌آوری‌های بی‌سیم بعدی زیرساخت‌های مبتنی بر گره‌های شبکه و یا شبکه‌های مش را پشتیبانی می‌کنند. این به این معنی است که ماژول‌های که چنین فناوری‌هایی را پشتیبانی می‌کنند می‌توانند به‌طور خودکار خود را پیکربندی نموده و به شبکه‌های بی‌سیم موجود که توسط دروازه‌های اینترنت اشیاء ایجادشده‌اند متصل شوند.

۲-۱-۳- دروازه اینترنت اشیاء

دروازه اینترنت اشیاء ابزارهای محاسباتی مبتنی بر لینوکس هستند که واسط‌های شبکه ضروری برای برقراری ارتباط با حس‌گرها را دارند (به‌عنوان‌مثال، واسط‌های بلوتوث و Zigbee) و همچنین می‌توانند با استفاده از بی‌سیم (به‌عنوان‌مثال، وای فای) و یا رابط‌های سیمی با اینترنت ارتباط برقرار کنند. دروازه‌ها منابع محاسباتی بهتری دارند (معمولاً با حداقل پردازنده با سرعت 1GHz ARM و 512MB یا حافظه) RAM و میزبان یک سیستم‌عامل کامل می‌باشد که ابزار PKI (مانند OpenSSL) را فراهم می‌کند. از طریق پیکربندی مناسب واسط‌های شبکه و شبکه سیستم‌عامل لینوکس دروازه‌ها می‌توانند رمزنگاریPKI را به داده‌های ورودی اعمال کنند و سپس با استفاده از سرویس‌های وب و یا سایر فن‌آوری‌های ارتباطی بلادرنگ به سمت برنامه‌های کاربردی پزشکی مبتنی بر وب هدایت کنند .

یک ویژگی اضافی توانایی انجام برخی پردازش داده‌های اولیه می‌باشد (به‌عنوان‌مثال، فیلتر کردن داده، فشرده‌سازی و یا تجزیه‌وتحلیل الگو)، قبل از اینکه داده‌ها با استفاده PKI رمزگذاری شده و با استفاده از WiFi و یا یک واسط شبکه اترنت به اینترنت فرستاده شود. بسیاری از بوردهای توسعه لینوکس مذکور با واسط شبکه (مانند فای و یا اترنت) یکپارچه می‌شوند و همچنین قابلیت ورودی خروجی‌های محیط عمومی GPIOs را دارند. بعداً می‌تواند به ماژول‌های RF مختلف (مانند بلوتوث، ZigBee و غیره) متصل شود. درنتیجه ارتباط دستگاه با حس‌گرهای مختلف متنی و تلفن همراه که بر وضعیت بیمار نظارت می‌کند فعال می‌شود.

۳-۱-۳- زیرساخت Backend ابر

رایانش ابری یک مدل برای فعال‌سازی راحت، هنگام درخواست دسترسی شبکه به یک گروه مشترک از منابع محاسباتی قابل تنظیم (به‌عنوان‌مثال، شبکه‌ها، سرورها، ذخیره‌سازی، برنامه‌های کاربردی و خدمات) می‌باشد که می‌تواند به‌سرعت و با حداقل تلاش مدیریتی یا فعل‌وانفعالات ارائه‌دهنده خدمات تهیه کرده و پخش نماید. ویژگی‌های بعدی رایانش ابری یک مدل بسیار مناسب برای ساختن زیرساخت back-end ایجاد می‌کند که مدیریت داده‌ها و مجازی‌سازی دستگاه‌های سلامت همراه اینترنت اشیاء را پشتیبانی می‌کند. علاوه بر این، منابع ابری می‌تواند نیازهای ضروری برای رمزگذاری / رمزگشایی اطلاعات PKI (مانند منابع محاسباتی) و مدیریت کلید رمزگذاری / رمزگشایی فراهم می‌کند. باید توجه داشت که این رمزنگاری باعث افزایش طول پیام و در کاهش سرعت انتقال داده‌ها خواهد شد.

۳-۲-روش پیشنهادی استفاده از رمزنگاری کلید عمومی و متقارن

با توجه به مطالب گفته‌شده به‌درستی می‌توان فهمید که ارسال و دریافت داده‌های جمع‌آوری‌شده از حسگرها و دستگاه‌های مورداستفاده در درمان و سلامت همراه امری بسیار حساس می‌باشد و بایستی محیطی امن بوده و جامعیت و یکپارچگی و حریم خصوصی به‌طور کامل حفظ شود. این ایمن بودن با استفاده از رمزنگاری کلید عمومی انجام خواهد شد ولی با توجه به اینکه رمزنگاری کلید عمومی از دو کلید جهت رمزنگاری و رمزگشایی استفاده می‌کند و همچنین به دلیل پیچیدگی تولید کلید رمزنگاری، عملیات رمزگذاری و رمزگشایی داده‌ها مقداری تأخیر در پی خواهد داشت، در مقابل رمزنگاری کلید عمومی رمزنگاری متقارن را داریم که جهت رمزنگاری و رمزگشایی از یک کلید خصوصی استفاده می‌کند.

حال بایستی توجه کرد که برای بیمارانی که شرایط حادی دارند، به‌عنوان‌مثال بیمار قلبی که هرلحظه در معرض حمله قلبی قرار دارد، سریع بودن ارسال داده‌های حسگرها و اعزام سریع نیروی درمانی به محل بیمار اهمیت ویژه‌ای خواهد داشت. رمزنگاری کلید عمومی روشی مناسب برای حفظ امنیت و حریم خصوصی داده‌ها می‌باشد ولی بایستی میزان تأخیر را به حداقل رساند. به همین خاطر بجای اینکه داده‌های جمع‌آوری‌شده را با رمزنگاری کلید عمومی به رمز درآورد می‌توان داده‌های جمع‌آوری‌شده را با رمزنگاری متقارن به رمز

درآورده و سپس کلید متقارن را با روش رمزنگاری کلید عمومی به رمز درآورد. در رمزنگاری کلید عمومی از یک کلید عمومی برای رمزگذاری و از یک کلید خصوصی برای رمزگشایی استفاده می‌شود ولی در رمزنگاری متقارن فرستنده و گیرنده تنها از یک کلید خصوصی جهت رمزنگاری و رمزگشایی استفاده می‌کنند. رمزنگاری کلید عمومی تقریباً ۵۰۰ برابر کندتر از رمزنگاری متقارن می‌باشد، جهت سرعت بخشیدن به عملیات رمزنگاری در ارسال داده‌ها، پیام توسط رمزنگاری متقارن به رمز درآمده و سپس کلید رمزنگاری متقارن توسط رمزنگاری زیرساخت کلید عمومی رمز شده و ارسال می‌شود که در وهله اول امنیت داده‌ها حفظ می‌شود و در وهله دوم عملیات رمز شدن و ارسال سریع‌تر انجام خواهد شد.

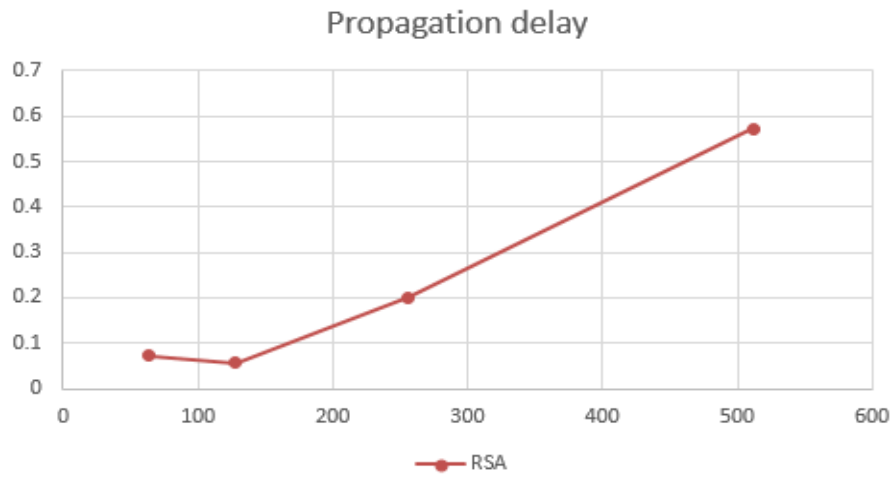
رمزنگاری کلید عمومی الگوریتم‌های متفاوتی دارد که الگوریتم AES تاکنون شکسته نشده است و به همین خاطر الگوریتمی مناسب می‌باشد. الگوریتم AES حداکثر با ۲۵۶بیت رمزنگاری را انجام می‌دهد. کلید خصوصی متقارن در ابتدای رمزنگاری به‌صورت تصادفی تولیدشده و بین فرستنده و گیرنده مبادله می‌شود ولی زمان آن بسیار کوتاه‌تر از کلید عمومی می‌باشد زیرا دیگر پیچیدگی‌های توابع ریاضی را برای تولید کلید ندارد.

درنهایت پس از رمز شدن متن توسط رمزنگاری متقارن، کلید خصوصی متقارن با استفاده از رمزنگاری کلید عمومی رمز شده و مبادله می‌شود. در سخت‌افزار این نوع رمزنگاری‌ها از چندپردازنده‌های قوی استفاده می‌شود که اعمال ترکیبی رمزنگاری به‌موازات هم و سریع انجام شوند.

۴. شبیه سازی

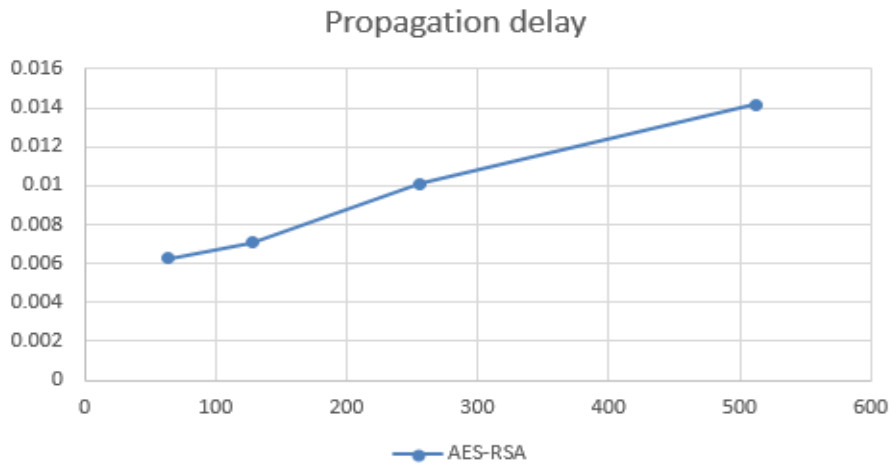
برای شبیه سازی رمزنگاری زبانهای برنامه نویسی مختلفی وجود دارد که در اینجا ما از زبان NS استفاده کرده ایم تا تأخیر انتشار در روش رمزنگاری ترکیبی کلید عمومی و کلید متقارن و روش کلید عمومی را باهم مقایسه کنیم. پس از اجرای شبیه سازی نتایجی برای تأخیر انتشار بسته ارسالی به دست آمد که این نتایج بخوبی نشان دهنده برتری روش ترکیبی پیشنهادی با روش کلید عمومی می باشد.

در نمودار شکل ۱ تأخیر انتشار را برای روش رمزنگاری کلید عمومی مشاهده می کنید، همانطور که ملاحظه می کنید با افزایش طول بسته ارسالی مقدار تأخیر انتشار به نسبت زیادی افزایش می یابد.



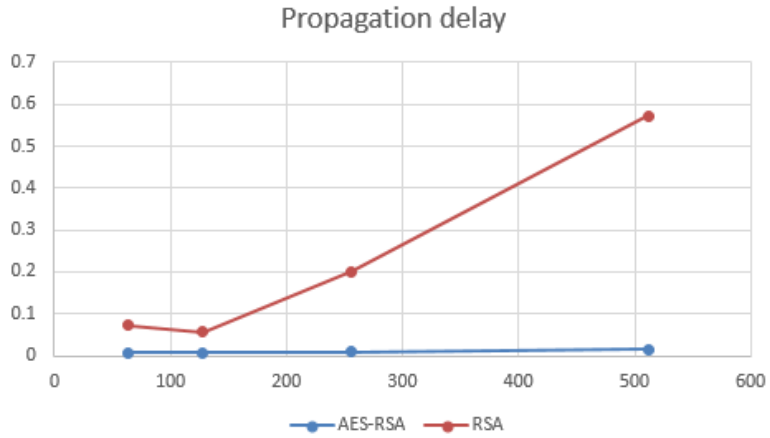
شکل ۱ - نتایج تأخیر انتشار برای روش رمزنگاری

در نمودار شکل ۲ مقادیر تأخیر انتشار بدست آمده از شبیه سازی روش ترکیبی را می بینید. همانطور که ملاحظه می کنید در این روش با افزایش طول بسته تأخیر انتشار به مقدار بسیار کمی افزایش می یابد.



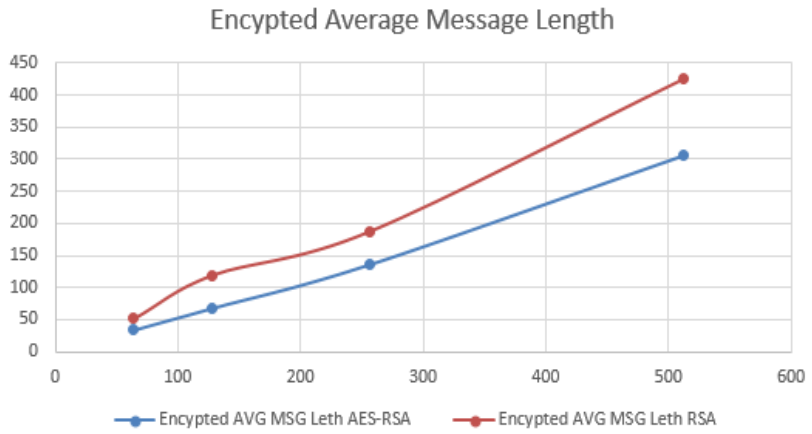
شکل ۲- تأخیر انتشار برای روش ترکیبی کلید متقارن و نامتقارن

با توجه به نمودار شکل۳ و با مقایسه نتایج این دو روش به‌خوبی می‌توان تفاوت آن‌ها در تأخیر انتشار بسته‌های ارسالی را ملاحظه نمود. همان‌طور که می‌بینید درروش اول یعنی رمزنگاری کلید عمومی، با افزایش طول رمزنگاری تأخیر بیشتری در ارسال پیام خواهیم داشت درصورتی‌که درروش دوم یعنی رمزنگاری ترکیبی با استفاده کلیدعمومی و متقارن با افزایش طول رمزنگاری تأخیر بسیار کمی خواهیم داشت.



شکل۳- مقایسه دو روش ترکیبی و کلید عمومی ازنظر تأخیر انتشار پیام

همان‌طور که در شکل ۴ مشاهده می‌کنید رمزنگاری با استفاده از روش ترکیبی بر طول پیام نیز تأثیر خواهد داشت بدین‌صورت که طول پیام ارسالی درروش ترکیبی کلید عمومی و متقارن کمتر از حالت کلید عمومی می‌باشد که این امر باعث افزایش سرعت انتقال و کاهش تأخیر انتشار خواهد شد.



شکل ۴- مقایسه دو روش ترکیبی و کلید عمومی ازنظر طول پیام رمز شده

۵. نتیجه گیری

اینترنت اشیاء قادر است انبوهی از داده‌ها و اطلاعات بیمار را جمع‌آوری کند که می‌تواند به تشخیص دقیق‌تر و آنی حوادث سلامتی کمک بسیاری نماید. دستگاه‌های سلامت همراه از تکنولوژی‌های ارتباطی مختلف استفاده می‌کنند (بلوتوث کم انرژی، ZigBee، بی‌سیم و غیره) و پروتکل‌های داده‌ها مختلف در این راه موضوعات مختلف قابلیت همکاری را معرفی می‌کنند. حفاظت داده‌ها نیز بسیار ضعیف است چون‌که دستگاه‌های حسگر فاقد منابع برای حفاظت از گمنامی کاربر و ارائه احراز هویت مناسب و رمزگذاری داده‌ها در همان زمان می‌باشند. چندین راه‌حل‌های امنیتی درگذشته ارائه‌شده است، اما در اغلب موارد دستگاه‌ها و دستگاه‌های حسگر فردی در نظر گرفته‌شده یا اعتبارنامه‌های امنیتی (مانند کلیدهای رمزگذاری) می‌توانند هنگام دسترسی داشتن به دستگاه‌ها به خطر بیافتد. در اینجا ما طراحی مفهومی و پیاده‌سازی نمونه اولیه از یک سیستم مبتنی بر دروازه‌های اینترنت اشیاء که داده‌های حسگر سلامت را جمع‌آوری کرده و مسائل امنیتی را از طریق گواهینامه‌های دیجیتال و رمزگذاری داده‌ها را انجام می‌دهند را ارائه کردیم. دروازه اینترنت اشیاء می‌تواند هر دو موضوع قابلیت همکاری ارتباطات حسگر و ارائه یک مفهوم کمتر آسیب‌پذیر و ایمن برای تصدیق هویت برای خدمات و ارسال داده‌های بیمار را حل نماید. معماری اینترنت اشیاء برای داشتن قابلیت آسیب‌پذیری‌های امنیتی در نظر گرفته می‌شود، درنتیجه طرح پیشنهادی می‌تواند به‌ویژه برای توسعه‌دهندگان اینترنت اشیاء در حوزه سلامت و درمان الکترونیکی بسیار مفید باشد. جهت تسریع عملیات درمان و نجات بیماران، از ترکیب رمزنگاری کلید عمومی و متقارن به صورتی استفاده می‌کنیم که پیام را توسط رمزنگاری متقارن رمزگذاری می‌کنیم و کلید متقارن را با روش رمزنگاری کلید عمومی رمز می‌کنیم. این روش رمزنگاری ترکیبی، تأثیر بسزایی در کاهش طول پیام رمزشده و در پی آن کاهش تأخیر انتشار بسته های ارسالی خواهد داشت. در نتیجه این روش رمزنگاری پیشنهادی باعث می‌شود که اطلاعات به‌سرعت و بصورت امن در اختیار مراکز درمانی موردنظر قرار گیرند تا با اقدام به‌موقع مراکز درمانی بتوان به سرعت به بیماران و سالمندان رسیدگی نمود که این امر آمار مرگ‌ومیر را کاهش خواهد داد.

منابع

1. Zhang, Q.; Zhu, C.; Yang, L. T.; Chen, Z.; Zhao, L.; Li, P. An incremental CFS algorithm for clustering large data in industrial Internet of Things. IEEE Transactions on Industrial Inform`atics, 2017, 13, 1193-1201.doi: 10.1109/TII.2017.2684807.
2. Xuanxia Yao, Fadi Farha, Rongyang Li, Ismini Psychoula, Liming Chen, Huansheng Ning,Security and privacy issues of physical objects in the IoT: Challenges and

opportunities,Digital Communications and Networks,2020,ISSN 2352-8648,https://doi.org/10.1016/j.dcan.2020.09.001.

3. Conti, M.; Kaliyar, P.; Lal, C. REMI: A reliable and secure multicast routing protocol for IoT networks. In Proceedings of the 12th International Conference on Availability, Reliability and Security, 2017, August, p. 84. ACM.doi: 10.1145/3098954.3106070.
4. Mohammad Saeid Mahdavinejad, Mohammadreza Rezvan, Mohammadamin Barekatain, Peyman Adibi, Payam Barnaghi, Amit P. Sheth, Machine learning for internet of things data analysis: a survey, Digital Communications and Networks,Volume 4, Issue 3,2018, Pages 161-175, ISSN 2352-8648,https://doi.org/10.1016/j.dcan.2017.10.002.
5. Al-Turjman, F. Cognitive routing protocol for disaster-inspired internet of things. Future Generation Computer Systems, 2019, 92, 1103-1115.doi: 10.1016/j.future.2017.03.014.
6. Lim, J.; Ko, Y. B.; Kim, D.; Kim, D. A Stepwise Approach for Energy Efficient Trust Evaluation in Military IoT Networks. In 2018 International Conference on Information and Communication Technology Convergence (ICTC), 2018, October, pp. 689-692. IEEE. doi: 10.1109/ICTC.2018.8539353.
7. Ernst, T.; Guillemaud, R.; Mailley, P.; Polizzi, J. P.; Koenig, A.; Boisseau, S.; Gerbelot-Barillon, R. Sensors and related devices for IoT, medicine and s mart-living. In 2018 IEEE Symposium on VLSI Technology, 2018, June, (pp. 35-36). IEEE. doi: 10.1109/VLSIT.2018.8510692.
8. Ben Arbia, D.; Alam, M.; Kadri, A.; Ben Hamida, E.; Attia, R. Enhanced IoT-based end-to-end emergency and disaster relief system. Journal of Sensor and Actuator Networks, 2017, 6, 19.doi: 10.3390/jsan6030019
9. Turkmen, A.; Peng, A. S.; Miller, M.; Dassow, B.; Bauer, D.; Mills, L.; Batzler, R. Development of a Home Energy Monitoring System: A Capstone Project Experience. In 2019 IEEE Power and Energy Conference at Illinois (PECI), 2019, February, pp. 1-6. IEEE.doi: 10.1109/PECI.2019.8698778.
10. Chilipirea, C.; Ursache, A.; Popa, D. O.; Pop, F. Energy efficiency and robustness for IoT: building a smart home security system. In 2016 IEEE 12th international conference on intelligent computer communication and processing (ICCP), 2016, September, (pp. 43-48). IEEE.doi: 10.1109/ICCP.2016.7737120
11. Gupta, S. K.; Kuila, P.; Jana, P. K. Energy efficient multipath routing for wireless sensor networks: A genetic algorithm approach. In 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2016, September, pp. 1735-1740). IEEE.doi: 10.1109/ICACCI.2016.7732298
12. Akkaya, K.; Younis, M. A Survey on Routing Protocols for Wireless Sensor Networks, Ad Hoc Netw, 2005, 3, pp. 325-49,2005.doi: 10.1016/j.adhoc.2003.09.010
13. Heinzelman, W.; Chandrakasan, A.; Balakrishnan, H. Energy-Efficient Communication Protocol for Wireless Microsensor Networks, Proceedings of the 33rd International Conference on System Science (HICSS'00), Hawaii, USA, 2000, pp. 1-10.doi: 10.1109/HICSS.2000.926982
14. Tandon, A.; Srivastava, P. Location Based Secure Energy Efficient Cross Layer Routing Protocols for IoT Enabling Technologies. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2019, 8, 368-374.
15. Althunibat, S.; Khalifeh, A.; Mesleh, R. On the performance of wireless sensor networks with QSSK modulation in the presence of co-channel interference. Telecommunication Systems, 2018, 68, 105-113.doi: 10.1007/s11235-017-0382-4.
16. Heidari, E.; Movaghar, A. An efficient method based on genetic algorithms to solve sensor network optimization problem, GRAPH-HOC, arXiv preprint arXiv:1104.0355, 2011, 3, 18-33. DOI : 10.5121/jgraphoc.2011.3102 18.

17. Kharkongor, C.; Chithralekha, T.; Varghese, R. Trust and Energy-Efficient Routing for Internet of Things—Energy Evaluation Model. In Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications, 2017, pp. 585-597, Springer, Singapore. doi: 10.1007/978-981-10-3153-3_58
18. Sujithra M, Padmavathi G. Iot security challenges and issues–an overview. World Scientific News. 2016;41:214-21.
19. Kazmi A, Jan Z, Zappa A, Serrano M. Overcoming the heterogeneity in the internet of things for smart cities. InInternational workshop on interoperability and open-source solutions 2016 Nov 7 (pp. 20-35). Springer, Cham.
20. Ukil A, Sen J, Koilakonda S. Embedded security for Internet of Things. In2011 2nd National Conference on Emerging Trends and Applications in Computer Science 2011 Mar 4 (pp. 1-6). IEEE.
21. Zhou L, Chao HC. Multimedia traffic security architecture for the internet of things. IEEE Network. 2011 May 23;25(3):35-40.
22. Roman R, Alcaraz C, Lopez J, Sklavos N. Key management systems for sensor networks in the context of the Internet of Things. Computers & Electrical Engineering. 2011 Mar 1;37(2):147-59.
23. Suo H, Wan J, Zou C, Liu J. Security in the internet of things: a review. In2012 international conference on computer science and electronics engineering 2012 Mar 23 (Vol. 3, pp. 648-651). IEEE.
24. Doukas C, Maglogiannis I, Koufi V, Malamateniou F, Vassilacopoulos G. Enabling data protection through PKI encryption in IoT m-Health devices. In2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE) 2012 Nov 11 (pp. 25-29). IEEE.
25. Yoon S, Park H, Yoo HS. Security issues on smarthome in IoT environment. InComputer science and its applications 2015 (pp. 691-696). Springer, Berlin, Heidelberg.