ششمین همایش پژوهش های نوین در علوم و فناوری
6th Conference on Recent Research in Science and Technology
تابستان ۱۳۹۵
Summer 2016

پارادایم امنیت در پلت فرم اینترنت اشیا

Security Paradigm in the internet of things platform

آیه عطاریان

دانشجوی کارشناسی ارشد فناوری اطلاعات –شبکه ، دانشگاه آزاد ورامین ، تهران، ایران

Ay.attarian@yahoo.com

چکیده

اینترنت اشیا یک توانمند سازی مبتنی بر هوش را به ویژگی های جهان مدرن امروزی مانند شبکه ها ، سازمانها افزوده است امنیت و حریم خصوصی از مسایل عمده ای است که از تصویب همگانی شدن و گسترش IOT به صورت جهانی را جلوگیری کرده است . در این مقاله به بررسی و ارایه راه حل برای حملات امنیتی در لایه ، حفره های امنیتی و بخشهای دیگر وهمچنین بررسی محدودیت های پیش روی این تکنولوزی در پایان نیز چهارچوبی را به عنوان توصیه مطرح شده است.

واژه های کلیدی : اینترنت اشیا ، انکارسرویس، انکارسرویس،RFID، حمله DOS

۱. مقدمه

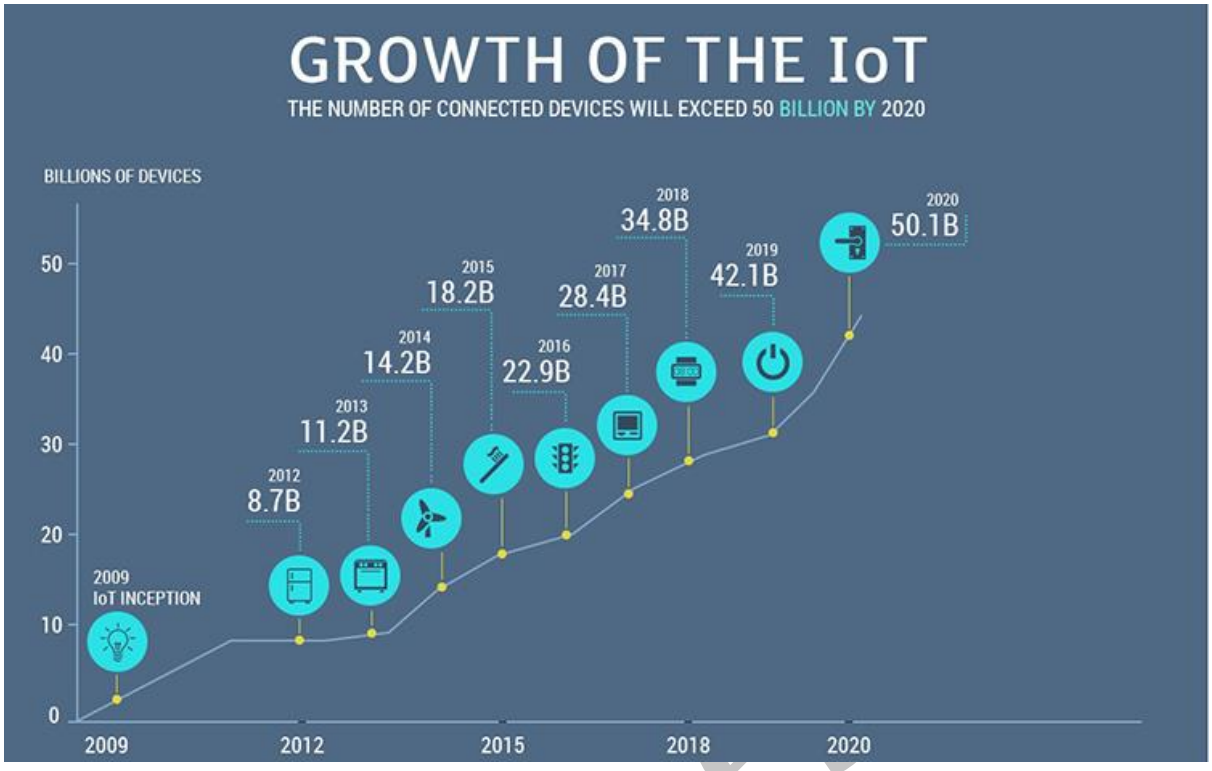
اینترنت اشیا [1]دستگاههای مختلف را قادر می سازد که بصورت روزانه از طریق اینترنت با یکدیگر در ارتباط باشند .این دستگاهها به صورت هوشمند به ارسال اطلاعات به سیسنم منمرکز می پردازتد و تضمین میکنند که با نظارت اقدامات لازم صورت میگیرد . اینترنت اشیا ء با هدف فراهم کردن حالت پیشرفته ارتباط بین دستگاهها و سیستم های مختلف و همچنین تسهیل تعامل انسان با محیط مجازی ، کاربرد خود را تقریبا در هر زمینه ای پیدا کرده است . افزایش نمایی در سالهای آینده در استفاده از IOT این انتظار را ایجاد میکند که به عنوان یک کاتالیزر برای نوآوری های تکنولوزیک اینده عمل کند.آنچه در این میان نگرانی را به همراه داشته مباحث امنیتی ، اینترنت اشیا است . در واقع درجه مقاومت و حفاظت از زیرساخت های امنیتی اینترنت اشیا ، سوال برانگیز است . از آنجایی که تمامی اشیا از زیرساخت اینترنت برای مبادله اطلاعات بهره میگیرند ، موضوع امنیت و محرمانگی آن توجه بسیاری را به سوی خود جلب نموده و به موضوعی بحث برانگیز در این حوزه تبدیل شده است . اینترنت اشیا با تمام قابلیت های پیشرفته خود در مبادله اطلاعات از نظر مباحث امنیتی یک مفهوم ناقص به حساب می آید . [1]این اتفاق تازه ظهور ،که در رده تکنولوزی سیمی قرار میگیرد ، چالش های متعددی را به همراه دارد.که

1-Internet of thing
2- The digital Divide

به تفصیل باید به ان پرداخته شود چالش های دیگری که مطرح میشود امنیت سایبری،محدودیت های فرهنگی کشورها،نقص در اشتراک گذاری دیتاها و ایجاد شکاف دیجیتالی [۲] و مسائلی پیرامون این موضوعات است که در این مقاله مروری کوتاه بر انان خواهیم داشت.

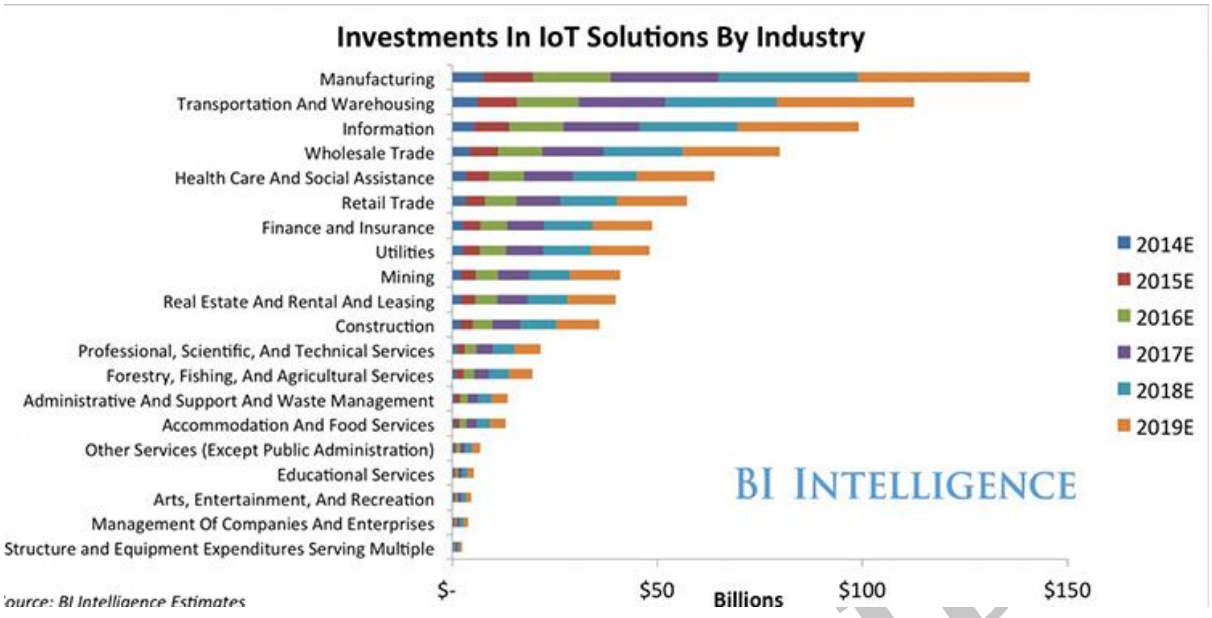
۲. اینترنت همه چیز

"جهانی که در آن اشیاء فیزیکی یکپارچه با اطلاعات شبکه ای یکپارچه ملحق میشوند و این اشیا فیزیکی میتوانند به شرکت کنندگان فعال در فرایند کسب و کار تبدیل شوند. [1]Haller.et.al .فعالیت در حوزه فناوری اینترنت اشیا از اوایل دهه ۹۰ میلادی آغاز شد ، اما اصطلاح "اینترنت اشیا" را کوین اشتون در سال ۱۹۹۹ پیشنهاد داد. بسیاری از دانشمندان بر این نظر هستند که توسعه محاسبات تعبیه شده فناوری های دیجتالی تحول ویزه ای را همراه خواهدداشت .که پیامد آن افزایش امنیت ، سلامت، ارایه خدمات و بهره وری بالا برای سازمانها و بشر می باشد.از سویی دیگر چالش هایی در حیطه محرمانگی شخصی ،امنیت سایبری ، به وجود امدن شکاف دیجیتالی و ساختار ناهمگن داده ها و انکار سرویس است.طبق گزارشات مرکز تحقیقاتی پو (Pew research center) در می سال ۲۰۱۴ ،اینترنت اشیا تا سال ۲۰۲۵ رشد فزاینده ای خواهد داشت. Anderson et al.2014 . به دلیل وجود عوامل وسایل پوشیدنی موبایلی ، سرعت های اتصال به اینترنت بالا و بهبود تکنولوزی های باتری ها شاهد رشد Iot بوده ایم به طوریکه به گفته گارتنر بیش از ۵۰ درصد اتصالات بین اینترنت بین اینترنت اشیا می باشد ، که در سال ۲۰۱۱تعداد انها بیش از ۱۵ بیلیون تخمین زده شد و پیش بینی می شود تا سال ۲۰۲۰ به ۳۰ بیلیون دستگاه میرسد. Abomhara,2014 . در شکل ۱ به تفضیل شاهد رشد این فناوری در صنعت و زندگی بشر خواهیم بود .



شکل ۱. حضور اینترنت اشیا در صنعت

تعداد صنایعی که بدنبال آوردن تکنولوژی های جدید برای بهبود کسب و کارشان هستند، بسیار قابل توجه است. همه صنایع مجبور خواهند بود بخش عظیمی از سرمایه هایشان را روی این موضوع سرمایه گذاری نمایند. [2کاربردهای اینترنت اشیاء برای شرکت ها، فروشگاه های خرده فروشی، بخش انرژی و قدرت و .... بعنوان راهکارهای اصلی محسوب می شوند و قطعا بیشتر مورد توجه در کسب و کارهای مجتمع قرار خواهند گرفت. درواقع عمده محصولات و ارزش معنوی و مادی سرمایه گذاری شده در تکنولوژی اینترنت اشیاء به بخش های صنعتی بزرگ برمیگردد که نمود اصلی آن در زندگی شخصی همه ما منعکس خواهد شد. پس خیلی هم شاید حضور اینترنت اشیاء در صنعت در آینده ما را از فواید مستقیم شخصی دور نمی کند.



شکل ۲.

۲-۱ پلتفورم اینترنت اشیا

شناسایی خودکارادیویی ، فناوری های ارتباطات بی سیم ، شبکه های حسگر ،شبکه تجهیزات تعبیه شده و شبکه محرک(Seaشبکه) شالوده اینترنت اشیا را تشکیل میدهد. براساس پیشرفت های سریع در ارتباطات سیار ، شبکه های حسگر بیسیم و RFID، مکانیزم های IOT می توانند با یکدیگر درهر مکان ،هرزمان و به هر شکلی یکپارچه شوند. Bandyopadhyay,2011. فرایند ارسال داده ها در فناوری اینترنت اشیا بدین ترتیب است که به سوزه ی مورد نظر یک شناسه یکتا و یک پروتکل اینترنتی تعلق میگیرد که داده های لازم را برای پایگاه داده ی مربوطه ارسال میکند.

.این حلقه بازخورد به شما اجازه می دهد تا بتوانید مانیتورینگ و کنترل اشیاء را از راه دور و از طریق اینترنت انجام دهید(نظیر بهبود عملیات مستمر) .تصمیم گیری در یک فضای تاریک در خصوص رویدادهای واقعی ، جای خود را به تصمیم گیری بر اساس داده صحیح ، به روز و بلادرنگ می دهد و فرد یا نهاد تصمیم گیرنده دارای هوشمندی لازم جهت

اتخاذ بهترین تصمیم و واکنش سریع در قبال مسایل خواهد بود . بدیهی است با نگاهی این چنین به مسایل و روش برخورد با آنها ، رسیدن به اهداف از پیش تعیین شده در حد یک آرزو باقی نخواهد ماند .

۳. چالش های امنیتی و انواع حملات در اینترنت اشیاء

از زمان پیدایش اینترنت اشیا و اذعان به تسهیلاتی که این فن اوری به همراه داشته و خواهد داشت اما شاهد دغدغه های گسترش یافته ای همچون مسایل امنیتی نیز بوده ایم ،که سازندگان بدان اهمیت کمتری داده اند و تعاریف ضعیف امنیتی برای اینترنت اشیا شده است و انچه مابین ۲۳ دسامبر ۲۰۱۳ تا ۶ زانویه ۲۰۱۴ رخ داد این موضوع را ثابت می کند . قرار دادن پسورد های ضعیف به صورت دیفالت Default برای اینترنت اشیا و بعضا درج پسورد رو ی دفترچه راهنما و ضعف برنامه نویسی مناسب برای تغییر پسورد توسط کاربر و نوع پسورد ، باعث شده تا هکرها به آسانی کنترل اینگونه ابزار را از راه دور به دست بگیرند . مشکلات ناشی شده از انتقال و پردازش داده های ناخواسته، حملات سایبری موجب نگرانی‌های کاربران و مسائل قانونی شده است ..Whitmore,Agarwa,2014 . اگر فعالیت روزانه افراد نظارت شده وآن‌ها تولید کننده خروجی‌های اطلاعاتی باشند، فعالیت‌های سیاسی، اقتصادی و اجتماعی تحت تأثیر قرار می‌گیرند. در صورت نقض امنیت، رخداد حمله و اختلال در عملکرد ، مزایای IoT کمرنگ می‌شود. در آینده ای نزدیک حجمی وسیع از اطلاعات توسط وسایل متصل و سیستم‌های مدیرتی دریافت و ارسال خواهد شد. به اعتقاد Sopho در سال ۲۰۱۵ سوءاستفاده از آسیب‌پذیری‌های نرم‌افزاری کاهش خواهد یافت. با توجه به کاهش تعداد آسیب‌پذیری‌های نرم‌افزاری، معدودی آسیب‌پذیری‌ها به شدت مورد استفاده قرار خواهند گرفت. اینترنت اشیاء، بزرگ‌ترین نگرانی امنیتی سال ۲۰۱۵ به نظر می‌رسد. در یکی از بررسی‌های اخیر واحد پژوهشی شرکت اچپی نشان می‌دهد هر ابزار عادی متصل به اینترنت اشیا ۲۵ ضعف امنیتی دارد که رقم شگفت‌انگیزی است و ۷۰ درصد ابزارها دست‌کم یکی از چنین ضعف‌هایی را دارند. اینترنت اشیاء با چالش‌های زیادی رو به رو است. SHahid.reza2013. از نظر مقیاس پذیری برنامه های کاربردی IoT به تعداد زیادی از دستگاه‌ها نیاز دارد که پیاده سازی آن‌ها به دلیل محدودیت‌های زمان، حافظه و پردازش مشکل است. محدودیت ادرس های اینترنتی در نسخه ۴ پروتکل اینترنتی این سیستم هاراوادار کرده حداکثر تا حدود ۴ میلیارد ادرس را پشتیبانی کند که با توجه به حجم اتصال تا سال ۲۰۲۰ باید از امکانات پیشرفته تری استفاده کرد .Raj.Samani2014.

درواقع می توان گفت برخلاف کامپیوترهای تجاری که چند دهه است به وسیله فایروال‌ها و سامانه‌های تشخیص نفوذ و بازدارنده (IDPS) محافظت می‌شوند، دستگاه‌های کنونی متصل به اینترنت از چنین تمهیداتی برخوردار نیستند. دانشگاه کلمبیا در راستای یکی از پژوهش‌های خود با حمله به سیستم‌های تجاری و نیز سامانه‌های نهفته موجود در دستگاه‌های مصرفی از جمله سامانه‌های سرگرمی خانگی، وب‌کم‌ها و اکسس‌پوینت‌های وای‌فای دریافت که تنها ۲,۴۶ درصد محصولات تجاری مشکل امنیتی دارند، در حالی که این مورد برای دستگاه‌های مصرفی ۴۱,۶۲درصد بود. حتی در آن دسته از محصولات مصرفی که تمهیدات امنیتی دارند نیز امکانات بازدارنده یا فعال نشده‌اند یا گذرواژه پیش‌فرض یا ناکارآمد دارند Zhibo.Pang2013 .

بسیاری از تولیدکنندگان این کالاها بیش‌تر به این می‌اندیشند که محصول خود را سریع‌تر وارد بازار کنند، اما به امنیت آن چندان توجهی ندارند. تولیدکننده در برخی موارد دستگاه طراحی شده برای شبکه‌های خصوصی را به‌سادگی فقط به اینترنت متصل می‌کند و درون آن هیچ‌گونه تمهیدات امنیتی خاصی را در نظر نمی‌گیرد. در بسیاری از این وسایل امکان دسترسی به تنظیمات امنیتی و سیستم‌عامل وجود ندارد. خیلی ساده می‌توانیم برنامه‌های امنیتی موردنظرمان را روی کامپیوتر و یا اسمارت فون نصب کنیم، اما با یک گاز، یخچال و...هوشمند که کیبورد و نمایشگر ندارد چگونه عمل کنیم؟

از چالش های دیکر امنیت Iot، سیستم‌عامل‌ها و نرم‌افزارهایی که باید به‌روزرسانی شوند . بیشترین منفعت ان اسودگی ما از بابت امنیت محصول است از سویی دیگر تولیدکنندگان محصولات هوشمند به سه دسته اند گروهی که که تضمین می‌کنند

محصولشان به‌روزرسانی می شود و گروه دیگر که این کار را زمان‌بر دانسته و از آن صرف‌نظر می‌کنند ، برخی دیگر از تولیدکنندگان، نه به‌روزرسانی را مدنظر می‌گیرد و نه مسائل امنیتی، با این حال قابلیت کنترل از راه دور محصول خود را بسیار مهم میدانند. درجمع بندی این بخش دغدغه های امنیتی اینترنت اشیاء می توان موارد ذیل را ذکر کرد:

۳-۱ قوانین و مقررات امنیتی : در حال حاضر، قانون و مقررات امنیت، همچنان در مرکز توجهات قرار ندارد و هیچ استاندارد تکنولوژی ای در مورد IOT وجود ندارد. IOT مربوط به اطلاعات امن ملی، اسرار تجاری و حریم شخصی افراد می باشد. در نتیجه، کشور ما نیاز به دیدگاه قانونی جهت توسعه IOT است. مقررات و قوانین به صورت بلا انکاری مورد نیاز است. Sen,jaydip 2013

۳-۲ ساختار معماری : IOT در طول کل بازه زمانی، پایدار باقی می ماند و مکانیزم امنیت در هر لایه منطقی نمی تواند سیستم دفاع کامل را پیاده سازی کند، در نتیجه، این موضوع یک چالش بوده و حوزه های تحقیقاتی فراوانی جهت ایجاد ساختار امن با ترکیب کنترل و اطلاعات، مورد نیاز است.

۳-۳ مدیریت کلان : مدیریت اساسی، پایه مهمی از مکانیزم امن می باشد، این موضوع همواره یک موضوع تحقیقاتی داغ می باشد. این مورد همچنان مشکلترین جنبه امنیت رمزنگاری است. در حال حاضر، محققان راه حل ایده آل برای این موضوع را پیدا نکرده اند.Bianchi2010. G . الگوریتم رمزنگاری سبک یا عملکرد بالاتر گره سنسور، همچنان اعمال نشده است. در نتیجه، شبکه سنسور مقیاس بزرگ همواره به صورت قابل اجرا باقی می ماند. مسائل امنیت شبکه بیشتر مورد توجه قرار گرفته و تبدیل به یک نکته مهم شده و مشکلاتی را در حوزه تحقیقات محیط شبکه ایجاد می کند.

۳-۴ نیازمندی ها برای کاربرد های نوظهور: با توسعه WSNها، تشخیص فرکانس رادیویی(RFID)، تکنولوژی محاسبات فراگیرنده، تکنولوژی مخابرات سبکه، و تئوری کنترل بلادرنگ توزیع شده، CPS، یک شکل بُروز پیدا کرده از IOT تبدیل به واقعیت شده است در این سیستم، امنیت بالا برای تضمین عملکرد سیستم مورد نیاز است. ایجاد ساختارهای شبه امن نیز بسیار ضروری می باشد. مدیریت اساسی در یک شبکه سنسور مقیاس بزرگ واقعی نیز همواره از مسائل چالشی بوده و مقررات و قوانین این حوزه که مربوط به IOT استف نیز جزو موضوعات چالشی می باشد.Mary R .Schurgot2012

۳-۵ استاندارد سازی : پاسی آئوری از شرکت Finnish و عثمان حق از Pachube با این نظریه موافق هستند و اعلام کردند ترجیح می‌دهند به‌جای آن‌که استانداردهای سخت‌گیرانه مانع پیش‌رفت شود، اجازه داده شود فناوری خود رشد کند. پاتریک وترولد از شرکت سیسکو پس از آن اعلام کرد اینترنت اشیا بهتر است با استانداردهای باز ساخته شود. این منبع باز بودن عمل‌پذیری متقابل را به وجود می‌آورد. اما در نقطه مقابل محافظه‌کاران درباره این ایده تکاملی تدریجی به ما یادآوری می‌کنند بهتر است تأمل کنیم چه کسی خواستار استانداردها است؟ موضوع به پاسخ‌گویی استانداردها باز می‌گردد. وبر پیشنهاد می‌کند استانداردها باید به صورتی ارائه شوند که چهارچوب‌های مدیریتی را به وجود آورند و اطلاعات را به‌سرعت در اختیار ما قرار دهند. پیاده‌سازی استانداردها پاسخ‌گویی آن‌ها را همراه خواهد داشت. بهبود پاسخ‌گویی با ایجاد چنین چهارچوبی بهبود امنیت اینترنت اشیا را به دنبال دارد.

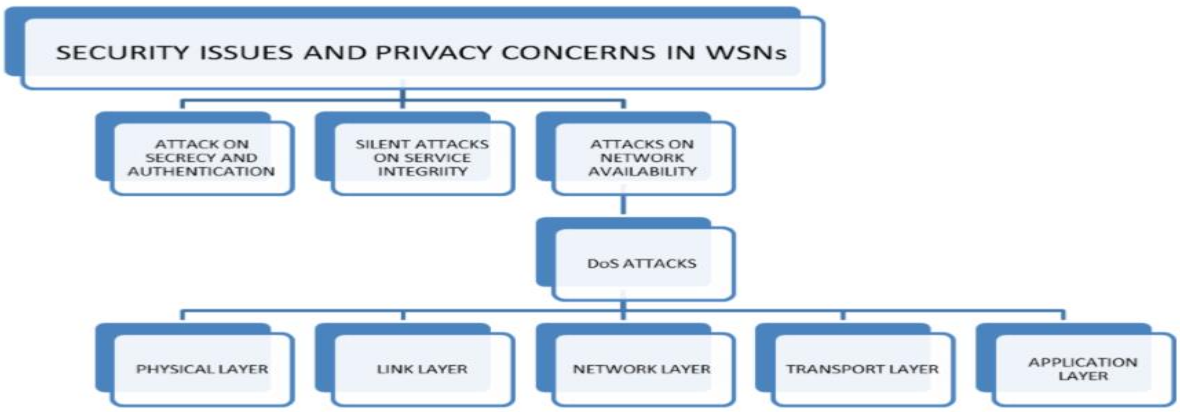
۳-۶ حریم خصوصی : از مهمترین مسائل امنیتی که کل سیستم IOT در حال توسعه را مورد آزار قرار میدهد ناشی از مسائل امنیتی موجود در تکنولوژی های ست که در IOT برای باز بخش اطلاعات از یک دستگاه به دستگاه دیگر بکار گرفته می شوند. که همین مسله حریم خصوصی افراد را تحت شعاع خود قرار میدهد. برای مثال دونمونه از حملات به دستگاههای ارتباطی بیان می کنیم :

۳-۶-۱ مسائل امنیتی در شبکه های حسگربیسیم(WSNs)

روابط سلسله مراتبی مسائل مختلف امنیتی که شبکه های حسگربیسیم را تهدید میکند در شکل ۴ نشان داده شده است.

عملیات سرکوبگرایانه ای که میتوانند در شبکه های حسگربیسیم اجرا شوند را میتوان به سه دسته تقسیم کرد:

- حملات بر محرمانگی و هویت
- حملات خاموش بر جامعیت سرویس
- حملات بر در دسترس بودن شبکه (انکار سرویس((Denial of service(DOS))
- حملاتی که رخ میدهددر این ۳ دسته قرار میگیرند. جلوگیری از دسترسی کاربران قانونی به اطلاعات توسط نفوذگران شخص ثالث ناشناس میتواند در لایه های مختلف شبکه اتفاق بیافتند.



شکل ۴. روابط سلسله مراتبی امنیتی

۳-۶-۲ حملات انکار سروبس بر لایه های IOT

- حمله Dos به لایه فیزیکی:

لایه فیزیکی شبکه های حسگربیسیم انجام عملیات انتخاب و تولید فرکانس حامل، مدولاسیون و دمدولاسیون، رمزگذاری، رمزگشایی و انتقال و دریافت داده را برعهده دارد.. این لایه شبکه حسگر بی سیم اساسا از طریق موارد زیر مورد حمله قرار میگیرد:

- Jamming: این نوع از حمله DOS، کانال ارتباطی بین گره ها را اشغال میکند و بدین ترتیب از ارتباط آنها با یکدیگر جلوگیری بعمل می آورد.
- Node tempering (دستکاری گره): دستکاری فیزیکی گره برای استخراج اطلاعات حساس بعنوان دستکاری گره شناخته میشود.

راهکار : توافق بر کلید حفاظت از داده حسگر و پیاده سازی رمزنگاری ساده

– حمله DOS به لایه اتصال

لایه اتصال WSN، ارسال همزمان جریان داده های مختلف، تشخیص فریم داده، کنترل Mac و خطا را بر عهده دارد. علاوه بر این قابلیت اطمینان نقطه به نقطه (point-point) و یا نقطه به چندین نقطه (point-multiple point) را تضمین میکند. حملات DOS که در این لایه اتفاق میافتند به شرح زیر است:

- Collision(برخورد): این نوع حمله DOS میتواند زمانی آغاز شود که دو گره بصورت همزمان بسته های داده را در یک کانال فرکانسی انتقال دهند. برخورد بسته های داده به یکدیگر منجر به تغییرات کوچکی در بسته میشود، این امر موجب میگردد که در پایان دریافت، در شناسایی بسته با ناسازگاری مواجه شویم که موجب دور انداختن بسته داده آسیب دیده و فرستادن دوباره آن خواهد شد[22].
- Unfairness: همانطور که در [22] توضیح داده شده است، این حمله، یک حمله مبتنی بر تکرار برخورد (repeated Collision) است و میتواند بعنوان حملات مبتنی بر خستگی (exhaustion based attacks) مطرح شود.
- Battery Exhaustion: این نوع از حمله DOS، ترافیک بالای غیر معمولی را در یک کانال ایجاد میکند و بدین ترتیب قابلیت دسترسی پذیری را برای گره های دیگر بسیار محدود می سازد. چنین خرابکاری هایی در یک کانال از درخواست های بسیار زیاد(درخواست ارسال) و انتقال ها، در طول کانال حاصل میشود.

راهکار : با کمک انتی ویروس ها ،محسابات ابری

– حمله DOS به لایه شبکه

کاربرد اصلی لایه شبکه مسیر یابی است. حملات DOS ویژه ای که در این لایه اتفاق میافتند عبارتند از :

- Spoofing: بازپخش و هدایت نادرست ترافیک
- Hello flood attack: این حمله ترافیک بالایی را در کانال ها با فرستادن تعداد زیاد غیر معمولی از پیامهای بی فایده (useless) صورت می دهد. در اینجا یک گره مخرب مجزا یک پیام بی فایده را ارسال میکند، سپس این پیام توسط مهاجم برای ایجاد ترافیک بازپخش می شود.
- Homing: در حمله Homing، جستجو برای یافتن سرخوشه ها و مدیران کلیدی که توانایی خاموش کردن کل شبکه را دارند، صورت میپذیرد.
- Selective forwarding : همانطور که از نام این حمله پیداست، در حمله ارسال انتخابی، یک گره که در معرض خطر قرار دارد، تنها چند گره انتخاب شده را بجای تمامی گره ها میفرستد. این انتخاب گره ها بر اساس نیازمندی مهاجم در رسیدن به اهداف خرابکارانه خود صورت میگیرد، بنابراین چنین گره هایی بسته های داده را منتقل نمیکنند.
- Sybil: در این حمله، مهاجم یک گره مجزا را تکثیر میکند و آن را با هویت های چند گانه به دیگر گره ها نشان میدهد.
- Wormhole: این نوع از حمله DOS باعث جابجایی بیت های داده از جایگاه اصلی خود در شبکه میشوند. این جابجایی بسته داده از طریق تونل زنی بیت های داده در طول یک تاخیر کوتاه از اتصال اتفاق میافتد.

- Acknowledgement flooding: پیامهای تصدیق (Acknowledgement) ، زمانهایی که شبکه های حسگربیسیم الگوریتمهای مسیر یابی را بکار میگیرند مورد نیاز هستند. دراین نوع از حمله DOS، یگ گره مخرب پیامهای تصدیق جعلی را که اطلاعات نادرستی را به گره های مقصد همسایه میدهد، ارسال میکند.

راهکار: شناسایی مکانیز م های رمز نگاری ، بالا بردن امنیت ارتباطات و تصدیق هویت

- حملات DOS در لایه انتقال

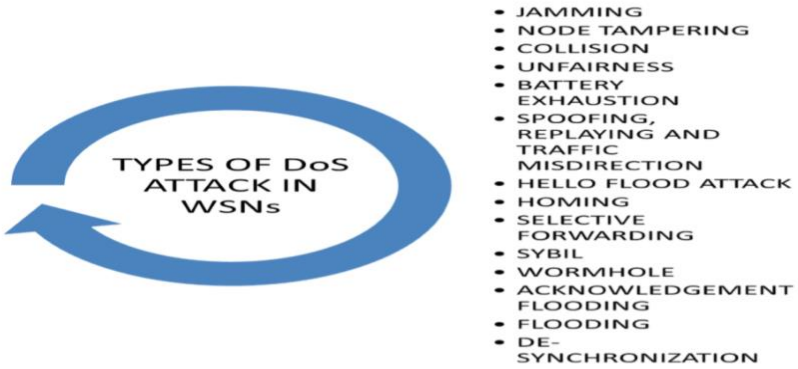
این لایه از معماری WSN، قابلیت اطمینان از انتقال داده ها را فراهم می سازد و از ازدحام ناشی از ترافیک بالا در روترها جلوگیری میکند. حملات DOS در این لایه بشرح زیر است:

- Flooding: به ازدحام عمدی در کانال های ارتباطی از طریق باز ارسال پیامهای غیر ضروری اشاره دارد.
- De-synchronization: در حمله De-synchronization، پیامهای جعلی در یک یا هردو نقطه ی انتهایی (endpoint) تولید میشوند و ارسال مجدد بسته را برای اصلاح خطایی که موجود نیست درخواست میکنند. این امر موجب از دست رفتن انرژی در یک یا هر دو نقطه انتهایی بخاطر انجام دستورالعملهای جعلی میشود.

- حملات DOS در لایه کاربرد

لایه کاربردWSN، مسئولیت مدیریت ترافیک را بر عهده دارد. این لایه همچنین بعنوان فراهم کننده نرم افزار برای برنامه ها ی کاربردی مختلف که ترجمه داده را به شکلی قابل فهم انجام میدهند، عمل میکند. و یا در جمع آوری اطلاعات با فرستادن کوئری ها، کمک میکند[20].در این لایه یک حمله مبتنی بر path (مسیر)، با تحریک گره های حسگر برای ایجاد یک ترافیک بزرگ در مسیر منتهی به ایستگاه پایه آغاز میشود[21] و [22]. شکل ، تمامی حملات DOS علیه لایه های مختلف شبکه ی حسگر بی سیم ذکر شده در بالا را نشان میدهد.

راهکار : میتوان با توافق بر کلید حفاظت ازحریم خصوصی و تصدیق هویت از طرف مدیریت امنیت تا حدود زیادی مقابله کرد



شکل ۵. انواع حملات انکار سرویس در شبکه های حسگربیسیم

برخی دیگر از حملات DOS، در ادامه نام برده میشوند[7] و[14]،[15]،[36]:

- Neglect and Greed Attack(حمله حریصانه و غفلت)

- Interrogation (بازجویی)
- Black Holes (سیاه چاله ها)
- Node Subversion (اختلال در عملکرد گره)
- Node malfunction (براندازی گره)
- Node Outage(قطع گره)
- Passive Information Gathering(جمع آوری اطلاعات مجهول)
- False Node(گره جعلی)
- Message Corruption (اختلال پیام)

برخی دیگر از مسائل امنیتی و حریم خصوصی در WSN، در [7]،[9] و[10]:

- . Data Confidentiality (محرمانگی داده)
- Data Integrity (صحت داده)
- Data Authentication (اعتبار داده)
- Data Freshness (تازگی داده)
- Availability (دردسترس پذیری)
- Self-Organization (خود سازماندهی)
- Time Synchronization (هماهنگ سازی زمانی)
- Secure Localization (محلی سازی ایمن)
- Flexibility (انعطاف پذیری)
- Robustness and Survivability (قابلیت مقاومت و بقا)

مطابق با [26]، تهدیداتی که در WSN مهمتر هستند، میتوانند در یک دسته بندی دیگر به شکل زیر باشند:

- External versus internal attacks (حملات داخلی در مقابل حملات خارجی)
- Passive versus active attacks (حملات فعال در مقابل حملات غیر فعال)
- Mote-class versus laptop-class attacks (حملات laptop-class در مقابل حملات Mote-class)

مطابق با [12]، حملات در WSNمیتوانند بشکل زیر دسته بندی شوند:

- Interruption (ایجاد وقفه)
- Interception (استراق سمع)
- Modification (تغییردادن)
- Fabrication (جعل کردن)

حملات در WSN، در یک دسته بندی دیگر میتوانند بشکل زیر باشند:

- حملات بر پایه میزبان
- حملات بر پایه شبکه

در حوزه IOT، تکنولوژی RFID، اساسا بعنوان تگ های RFID برای تبادل خودکار اطلاعات بدون هیچ گونه دخالت دستی بکار میرود. اما بعلت وضعیت ناقص تکنولوژیRFID، تگ های RFID در معرض حملات مختلفی از بیرون قرار دارند. چهار نوع از رایج ترین حملات و مسائل امنیتی تگ های RFID همانطور که در شکل ۳ نشان داده شده، عبارتند از:

- غیر فعال کردن غیر مجاز تگ (حمله بر اعتبار): حملات DOS در تکنولوژی RFID، منجر به غیر فعال شدن تگ های RFID بصورت موقت یا دائم میشوند. این حملات، به ارائه یک تگ RFIDکه باعث اختلال و سوء رفتار در عملکرد اسکن تگ خوان میشود، میپردازند. و EPC این تگ، اطلاعات اشتباهی را در مورد هویت ترکیبی عددی منحصر به فرد اختصاصی خود ارائه میکند. این نوع از حملات DOS میتوانند از راه دور انجام شوند، بطوریکه به مهاجم اجازه میدهند تا رفتار تگ را از راه دور دستکاری نماید.
- شبیه سازی غیر مجاز تگ (حمله بر صحت): بدست آوردن اطلاعات شناسایی (مانند EPC)، از طریق دستکاری تگ ها توسط Reader های سرکش(مخرب) در این دسته قرار میگیرند. هنگامی که اطلاعات شناسایی یک تگ به خطر بیافتد، تکرار تگ(شبیه سازی تگ) ممکن خواهد شد. این موضوع میتواند برای دور زدن اقدامات امنیتی ساخته شده و همچنین معرفی آسیب پذیری های جدید در هر صنعتی که از مراحل تایید خودکار تگ های RFID استفاده میکنند، بکار رود.
- مسیر یابی غیر مجاز تگ (حمله به محرمانگی): یک تگ می تواند از طریق Reader های مخرب ردیابی شود، این امر منجر به از دست دادن اطلاعات حساس مانند آدرس اشخاص خواهد شد. بنابراین از دیدگاه مصرف کننده، با توجه به اینکه خرید یک محصول که تگ RFID دارد، میتواند ردیابی شود، محرمانگی را برای آنها تضمین نمیکند و در واقع حریم شخصی آنها را بخطر می اندازد.
- حملات بازپخش(حمله بر دسترسی پذیری): در این نوع از حملات جعل هویت، مهاجم از واکنش تگ نسبت به تهدیدات Reader مخرب، برای جعل تگ استفاده میکند[25]. در حملات بازپخش، بمحض دریافت هر کوئری از Reader، سیگنال ارتباطی بین Reader و تگ مورد استراق سمع، و بعدا ثبت و بازبخش قرار میگیرد و بدین ترتیب در دسترس بودن تگ، جعل میشود.

علاوه بر این دسته بندیها، به برخی از آسیب پذیریهای امنیتی مهم از تکنولوژی RFID اشاره خواهیم کرد:

- Reverse Engineering (مهندسی معکوس)
- Power Analysis (آنالیز توان)
- Eavesdropping (استراق سمع)
- Man-in-the-middle attack (حمله شخص ثالث)
- Denial of Service (DoS) (انکار سرویس)
- Spoofing (جعل کردن)
- Viruses (ویروس)
- Tracking (ردیابی)
- Killing Tag Approach (رویکرد کشتن تگ)

شکل ۳. مسائل امنیتی در RFID

۴. معرفی قابلیتهای اطمینان بخشی و تحلیل ریسک در مواجه با تهدیدات

بیان اینکه پروتکل PRI به عنوان کلیدی برای رمزگشایی و امنیت که شامل رمزنگاری مسیرهای گره به مثصد خود است ، ارایه داده است زمانی داده ها در طول راه به گره فرزندانشان فرستاده میشوند که پس از انتقال کلید به گره ، گره به مقصد رسیده باشد . li Zaui2014 . حال انکه R.Agroval عمل فیزیکی را از روشهای امنیتی حفاظت از داده ندانسته و معتقد است با استفاده از دستگاههای فراکانس رادیویی که در دستگاهها تعبیه شده که برای برقراری ارتباط دستگاه با دستگاه و انسان اجازه میدهد .یکی از دیگر روشهای تحلیل ریسک در مواجه با تهدیدات را می توان استفاده از سنسور سایبری و یا سنسوری که زمان واقعی حوادث را با داده هایی مانند دما و سرعت تشخیص داده و اقدام فوری صورت میدهد عنوان کرد .همچنین "ترجیح براساس مدل حریم خصوصی " با استفاده از یک شخص ثالث را یکی از روشها عتوان کرد که برای شناسایی با روش Eferences مجموعه ای از روابط را برای سطح ایمنی یک دستگاه فراهم میکند . سیستم های حمل و نقل هوشمند با استفاده از روش امنیتی دیگری به نام ITS به تجزیه و تحلیل خطر پرداخته که در آن یک زیرساخت کلید عمومی است ،پرداخته است . استفاده از میان افزارها برای ارتباط امن توسط دستگاههای رمزنگاری یکی از روش های امنیتی با محبوبیت رو به افزایش است . با احراز هویت و کنترل دسترسی در اینترنت اشیا ، نقاطع ضعف در دستگاهها و تمامیت داده ها را میتوان رفع کرد . در این روش یک کاربر برای اجازه از ثبت نام در سازمان (RA) درخواست احراز هویت برای دسترسی به دستگاه را می پرسد . (RA) برای کاربر سوالی را ارسال و در صورت پاسخ مثبت کاربر ،دسترسی او به دستگاه تصدیق میشود . leu la 2013. یک چهارچوب به نام کمک به محیط نواورانه زندگی (AAL) که اجازه میدهد تا افراد با تجربه یک شیوه مستقل و زندگی سالمی را به عنوان رهبری همه جانبه سیستم های فنی اینترنت آشیا ارایه دهند . اگرچه این روش کاملا عملی است ، میتواند مفید واقع شود اما اشکال اصلی این روش این است که انها در تلاش برای رفع مشکلات اتصال هستند در صورتیکه هیچ اشاره ای به ویزگی های همه جانبه حفظ حریم شخصی و امنیت ندارند .A Doh2015 .

۵. نتیجه گیری

در این مقاله سعی براین شدهاست که چالش های پیش روی یکی از مهمترین دغدغه های اینترنت اشیا از جنبه های مختلف بررسی شود . کاربرد فناوری های یاد شده به نفع بسیاری از کشورهای در حال توسعه است وبی شک اینترنت اشیا در کنار مزایایش مشکلاتی هم به همراه دارد که صرف تمرکز برروی وارد کردن این تکنولوزی به جامعه بدون فراهم کردن زیرساخت های اجتماعی –فرهنگی ، مالی و تکنولوزیکی ان به هدر دادن سرمایه است . در این مقاله، نقص های امنیتی موجود در اینترنت اشیا که ممکن است برای توسعه و پیاده سازی IOT در حوزه های مختلف بسیار زیان آور باشد را بررسی

کردیم. بنابراین، اقدامات امنیتی ([18]،[24]، [29] و[34]) در برخورد با مشکلات امنیتی ذکر شده در بالا و همچنین پیاده سازی سیستم های تشخیص نفوذ مختلف ([11] و[33]) رمزنگاری ([5]) در فرایند مبادله اطلاعات و استفاده از روشهای کارآمد برای ارتباط([13]) منجر به زیر ساخت های IOT امن تر و مقاوم تری می شود. در نتیجه علاقه مندیم نشان دهیم که تلاشهای بیشتر در توسعه اقدامات امنیتی برای زیر ساخت های IOT، قبل از توسعه بیشتر روشهای جدید پیاده سازی IOT در زندگی روزمره، یک روش ثمر بخش تر و سیستماتیک تر خواهد بود.

۶. منابع

[1] Jason Pontin: “ETC: Bill Joy's Six Webs”. In: *MITTechnology Review*, 29 September 2005. Retrieved 17November 2013.

[2] Shen, Guicheng, and Bingwu Liu. "The visions,technologies, applications and security issues ofInternet of Things."*E-Business and E-Government(ICEE), 2013 International Conference on*.IEEE,2011.

[3] Akyildiz, I.F. ; Georgia Inst. of Technol., Atlanta, GA,USA ; Weilian Su ; Sankarasubramaniam, Y. ; Cayirci,E "A survey on sensor networks." *Communicationsmagazine, IEEE* 40.8 (2002): 102-114.

[4] Z.G. Prodanoff, Optimal frame size analysis for framedslotted ALOHA based RFID networks, ComputerCommunications (2012), doi: 10.1016/j.comcom.2009.11.007.

[5] Dey, Sandipan, Ajith Abraham, and SugataSanyal."An LSB Data Hiding Technique Using PrimeNumbers."*Information Assurance and Security, 2007. IAS 2007.Third International Symposium on*.IEEE,2007.

[6] Rolf Clauberg. RFID and Sensor Networks: FromSensor/Actuator to Business Application, RFID6Workshop, University of St. Gallen, Switzerland,September 27, 2010.

[7] AashimaSingla, RatikaSachdeva, “Review onSecurity Issues and Attacks in Wireless SensorNetworks” International Journal of Advanced Researchin Computer Science and Software Engineering<www.ijarcsse.com>. Volume 3, Issue 4, April 2013ISSN: 2277 128X.

[8] Sen, Jaydip. "Security and privacy challenges incognitive wireless sensor networks." *arXiv preprintarXiv: 1302.2253* (2013).

[9] G. Bianchi, “A comparative study of the varioussecurity approaches used in wireless sensor networks,”*International Journal of Advanced Science andTechnology*, *vol. 17*, (2010) April, pp. 31-44.

[10] T. A. Zia, “A Security Framework for Wireless SensorNetworks”, ttp://ses.library.usyd.edu.au/bitstream/2123/2258/4/02whole.pdf, **(2008)**.

[11] Bhattasali, Tapalina, RituparnaChaki, and SugataSanyal. "Sleep Deprivation Attack Detection inWireless Sensor Network." arXiv preprint arXiv:1203.0231(2012).

[12] Xiangqian Chen, Kia Makki, Kang Yen, NikiPissinou,“Sensor network security: a survey” IEEECommunications Surveys and Tutorials 01/2009;11:52-73. DOI: 10.1109/SURV.2009.090205

[13] Roy, Bibhash, SumanBanik, ParthiDey, SugataSanyaland NabenduChaki, "Ant colony based routing formobile ad-hoc networks towards improved quality ofservices." *Journal of Emerging Trends in Computingand Information Sciences* 3.1 (2012): 10-14.

[14] M. Saxena, “Security in Wireless Sensor Networks-ALayer based classification”, Technical Report, Centerfor Education and Research in Information Assurance& Security-CERIAS, Purdue University. pages.cs.wisc.edu/~msaxena/papers/2007-04-cerias.pdf, **(**2007).

[15] J. Sen, “A Survey on Wireless Sensor networkSecurity”, *International Journal of CommunicationsNetwork and Information Security*, *vol. 1*, *no. 2*, **(2009)**August, pp. 59-82.

[16] M. Sharifnejad, M. Shari, M. Ghiasabadi and S.Beheshti, “A Survey on Wireless Sensor NetworksSecurity”, SETIT, (2007).

[17] B. T. Wang and H. Schulzrinne, “An IP tracebackmechanism for reflective DoS attacks”, *CanadianConference on Electrical and Computer Engineering*,*vol. 2*, (2004) May 2-5, pp. 901-904.

[18] VipulGoyal, Virendra Kumar, Mayank Singh, AjithAbraham and SugataSanyal: A New Protocol toCounter Online Dictionary Attacks, Computers andSecurity, Volume 25, Issue 2, pp. 114-120, ElsevierScience, March, 2006. This paper is now listed in thetop 25 articles of the COMPUTER SCIENCE(Computer and Security)
[19] http://sensors-and-networks.blogspot.in/2011/08/physical-layer-for-wireless-sensor.html
[20] Ahmad AbedAlhameedAlkhatib, and Gurvinder SinghBaicher. "Wireless sensor networkarchitecture." *International conference on computernetworks and communication systems (CNCS 2012)IPCSIT.Vol. 35*. 2012, pp. 11-15.
[21] Al-Sakib Khan Pathan, "Denial of Service in WirelessSensor Networks: Issues and Challenges", Advances inCommunications and Media Research, Vol. 6 (Editedby Anthony V. Stavros), ISBN: 978-1-60876-576-8,Nova Science Publishers, Inc., USA, 2010.
[22] Sunil Ghildiyal, Amit Kumar Mishra, Ashish Gupta,NehaGarg, "Analysis of Denial of Service (DoS)Attacks in Wireless Sensor Networks" IJRET:International Journal of Research in Engineering andTechnology; eISSN: 2319-1163 | pISSN: 2321-7308
[23] Khoo, Benjamin. "RFID as an enabler of the internet ofthings: issues of security and privacy." *Internet ofThings (iThings/CPSCom), 2011 InternationalConference on and 4th International Conference onCyber, Physical and Social Computing*.IEEE, 2011.
[24] VipulGoyal, Ajith Abraham, SugataSanyal and SangYong Han, "The N/R One Time Password System."Information Assurance and Security Track (IAS'05),IEEE International Conference on InformationTechnology: Coding and Computing (ITCC'05), USA,April, 2005. pp 733-738, IEEE Computer Society.
[25] Burmester, Mike, and Breno De Medeiros. "RFIDsecurity: attacks, countermeasures andchallenges." *The 5th RFID Academic Convocation,The RFID Journal Conference*. 2007.
[26] C. Karlof and D. Wagner, "Secure Routing in SensorNetworks: Attacks and Countermeasures", Elsevier's*AdHoc Networks Journal*, Special Issue on SensorNetwork (SNPA), (2003) September, pp. 293-315.
[27] Zhou, Wei, and Selwyn Piramuthu. "Security/privacyof wearable fitness tracking IoT devices."*InformationSystems and Technologies (CISTI), 2014 9th IberianConference on*.IEEE, 2014.
[28] Aggarwal, Charu C., and TarekAbdelzaher."Integrating sensors and social networks."*SocialNetwork Data Analytics*.Springer US, 2011.379-412.
[29] VipulGoyal, Virendra Kumar, Mayank Singh, AjithAbraham and SugataSanyal, CompChall: AddressingPassword Guessing Attacks Information Assuranceand Security Track (IAS'05), IEEE InternationalConference on Information Technology: Coding andComputing (ITCC'05), USA. April 2005, pp 739-744,IEEE Computer Society.
[30] W. Drira, Renault, E., Zeghlache, D. "Towards aSecure Social Sensor Network." *Proceedings of theIEEE International Conference on Bioinformatics andBiomedicine*, pp. 24-29, 2013.
[31] N. Eagle, Pentland, A., and Lazer, D. "Inferring SocialNetwork Structure using Mobile Phone Data."*Proceedings of the National Academy of Sciences(PNAS),* 2009. vol. 106 no. 36 Nathan Eagle, 15274–15278, doi: 10.1073/pnas.0900282106
[32] M. Rahman, Carbunar, B., Banik, M. 2013. "Fit andVulnerable: Attacks and Defenses for a HealthMonitoring Device." *34th IEEE Symposium onSecurity and Privacy (IEEE S\&P),* 2013
[33] Animesh Kr Trivedi, Rishi Kapoor, RajanArora, SudipSanyal and SugataSanyal, "RISM - Reputation BasedIntrusion Detection System for Mobile Ad hocNetworks", Third International Conference onComputers and Devices for Communications,CODEC-06, pp. 234-237. Institute of Radio Physicsand Electronics, University of Calcutta, December 18-20, 2006, Kolkata, India
[34] R. A. Vasudevan, A. Abraham, S. Sanyal and D. P.Agrawal, "Jigsaw-based Secure Data Transfer overComputer Networks," IEEE International Conferenceon Information Technology: Coding and Computing,2004. (ITCC '04), Proceedings of ITCC 2004, Vol. 1,pp 2-6, April, 2004, Las Vegas, Nevada.
[35] Xiao, Qinghan, Thomas Gibbons, and Hervé Lebrun."RFID Technology, Security Vulnerabilities, andCountermeasures."*Supply Chain the Way to FlatOrganization, Publisher-Intech*(2009): 357-382.
[36] G. Padmavathi, and D. Shanmugapriya. "A survey ofattacks, security mechanisms and challenges inwireless sensor networks." arXiv preprint arXiv:0909.0576 (2009).