

## بررسی مدل های امنیت اینترنت اشیاء در شبکه حمل و نقل هوشمند

بابک توکلیان<sup>۱</sup>، b.tavakolian@gmail.com

<sup>۱</sup>مدیر فن آوری اطلاعات و ارتباطات شهرداری کازرون

**چکیده:** امروزه اینترنت اشیاء و کاربرد های آن با استفاده از هوشمند سازی تجهیزات مختلف بیش از پیش مورد توجه قرار گرفته است. در این پژوهش به بررسی یکی از اساسی ترین دغدغه های کاربران و شرکت های تولید کننده تجهیزات IoT یعنی امنیت پرداختیم. به طور کلی بخش عمده ای از این کاربردها، کاربردهای حساس و پراهمیت هستند. استفاده از این فناوری، همچنین فناوری های حساس باعث شده تا اهمیت امنیت و پیاده سازی آن در این شبکه ها بیشتر از سایر شبکه ها مورد توجه و بررسی قرار گیرد. این در حالی است که مسائلی همچون توپولوژی و مقیاس پذیری جغرافیایی شبکه به این مشکلات دامن زده و بحث برقراری امنیت را امری دشوار و پیچیده نموده است. در مجموع وجود این مسائل برای شبکه های اینترنت اشیاء باعث ایجاد تفاوت ها و پیچیدگی های خاص در حوزه امنیت و برقراری امنیت ارتباطات این شبکه ها شده است. بر همین اساس و با توجه به اهمیت بالای بحث امنیت در شبکه های اینترنت اشیاء، تا کنون مقالات گسترده ای برای بهبود این مقوله حیاتی معرفی شده اند. در این مقاله به بررسی امنیت در سیستم حمل و نقل هوشمند پرداخته ایم.

**واژه های کلیدی:** امنیت اینترنت اشیاء، حمل و نقل هوشمند، امنیت، هوشمند سازی، اینترنت اشیاء

### ۱. مقدمه

درون شهری برای انجام فعالیت های روزمره در سطح شهر با مسافت های مختلف صورت می گیرد که همین موارد باعث ایجاد ترافیک و آلودگی هوا می شود. اینترنت اشیاء این امکان را دارد که با استفاده از سنسور های فعال خود موجب کاهش این مشکلات گردد. اما مسئله ای که مدیران در کشور های در حال توسعه همچون ایران برای بکار گیری این فناوری نوین بعنوان مانع با آن رو به رو شده اند ایجاد اعتماد کاربران برای پذیرش فناوری اینترنت اشیاء جهت استفاده در امور زندگی شهروندان می باشد. این در حالی است که میزان فعالیت های کاربران در نقاط شهری کشور های توسعه یافته به فناوری اینترنت اشیاء را می توان از شمار دستگاه های متصل به اینترنت که در سال های اخیر اعلام شده است سنجید. پیش بینی می شود در سال ۲۰۲۵ این تعداد بالغ بر ۴۵ میلیارد دستگاه در جهان برسد. این روند رو به رشد نشان دهنده گسترش روز افزون و تاثیرات عمیق کاربرد فناوری اینترنت اشیاء در زندگی روز انسان ها است [۳]. از این رو صنعت نیز علاقه زیادی به IoT نشان داده و به آن توجه زیادی نموده

اینترنت اشیاء (Internet of things (IoT)) شبکه ای است که هر شیء را به اینترنت متصل می کند و از ادغام و ترکیب چندین فناوری از جمله شناسایی خودکار امواج رادیویی، حسگر، سیستم موقعیت یاب جهانی و اسکترهای لیزری تشکیل شده است که باعث برقراری تبادل اطلاعات و ارتباطات می شود و هدف اصلی آن شناسایی هوشمند، ردیابی محل، نظارت و مدیریت است. [۲،۱]. تکنولوژی های تحت وب با سرعت بالایی در حال پیشرفت است و دستیابی به ایده های شهر هوشمند را تحقق پذیر کرده است. مفهوم جدید اینترنت اشیاء امکانات غیرقابل تصویری را برای توسعه مفهوم شهر هوشمند بوجود آورده است. با این وجود سرعت تکنولوژی هایی که امنیت کاربران و اطلاعات آنها را تضمین کند، به مراتب از تکنولوژی اینترنت اشیاء عقب تر است و مطالعات کمتری در این حوزه مهم صورت گرفته است. امروزه تکنولوژی اینترنت اشیاء بیشترین اهمیت و کاربرد خود را در حوزه ترافیک و حمل و نقل شهری نشان داده است. تعداد بسیار زیادی سفرهای

است. در بخش سوم نتایج حاصل از تحلیلها مورد بررسی قرار می گیرد و در بخش نهایی به جمع بندی تحلیل نتایج می پردازیم.

## ۲. مرور و ادبیات تحقیق

امروزه تکنولوژی های مختلفی به سرعت در حال پیشرفت هستند که فن آوری اینترنت اشیاء و کاربرد آن در حمل و نقل هوشمند هم یکی از آنهاست و بخش قابل توجهی از فن آوری اینترنت اشیاء در این حوزه کار شده است. با این وجود سرعت تکنولوژی که امنیت کاربران و اطلاعات آن ها تضمین کند، به مراتب عقب تر از خود تکنولوژی است. در سالهای اخیر نگاه ویژه تری به این موضوع شده اما همچنان خلع های بسیاری در این حوزه دیده می شود. عوامل مختلفی در این حوزه تاثیر گذار است که در این پژوهش سعی می شود فاکتور های اثر گذار امنیت اینترنت اشیاء در حمل و نقل هوشمند شناسایی و مورد بررسی قرار گیرد. در سالهای اخیر با توجه به رشد تکنولوژی های 4G,5G,cloud computing و ... اینترنت اشیاء به تدریج به صورت فراگیر وارد زندگی ما شده است تا برای کنترل و نظارت هوشمند و قوی تر و زندگی آسان تر مورد استفاده قرار گیرد.

اوین اشاتون در سال 1999 برای نخستین بار نظریه اینترنت اشیاء را مطرح نمود، اینترنت اشیاء مقوله جدید و نا آشنایی نیست اولین نمونه استفاده از این تکنولوژی، تولید و رونمایی از توستر متصل به اینترنت توسط یک کمپانی طی یک کنفرانس در سال 1989 بود [۳]

اینترنت اشیاء بعنوان مفهومی جدید در دنیای فن آوری و ارتباطات، فن آوری مدرنی است که در آن برای هر موجودی (انسان، حیوان و یا اشیاء) قابلیت ارسال داده از طریق شبکه ها ارتباطی، اعم از اینترنت یا اینترنت، فراهم می گردد. بستر اینترنت اشیاء بر امواج رادیویی بی سیم قرارداده شده که به دستگاه های مختلف این امکان را می دهند تا از طریق اینترنت با یکدیگر به برقراری ارتباط بپردازند.

در حال حاضر دامنه کاربردهای IoT تنها به تصورات ما محدود می شود بر اساس بررسی مقالات انجام شده، کاربرد ها به حوزه های اصلی زیرساخت هوشمند، بهداشت، لجستیک/ زنجیره تامین، کاربردهای اجتماعی و سایر کاربردها تقسیم می شود که در ادامه با توجه به مبحث مقاله به تعاریف مختصری در حوزه لجستیک و حمل و نقل هوشمند خواهیم پرداخت.

است [۱۴]. این علاقه موجبات توسعه هزاران حسگر برای اپلیکیشن های مختلف مثل حس کردن مکان، پیش بینی آب و هوا، اپلیکیشن های بیومدیکال و موارد دیگر را فراهم آورده است. اما یکی از مهم ترین کاربرد های این فناوری در دنیای امروزه که نقش مهمی را نیز ایفا می کند بحث حمل و نقل هوشمند است. از چالش برانگیز ترین مباحث در حوزه اینترنت اشیاء بحث امنیت در اینترنت اشیاء می باشد، امنیت در ابعاد و تکنولوژی های مختلف یکی از موارد اساسی و مهم می باشد. این مهم در تکنولوژی های نو ظهور با توجه به تازه بودن و فراگیر بودن مورد اهمیت ویژه ای قرار می گیرد. اما برای کارشناسان شرکت های بزرگ تجاری، مدیران شهری و کاربران اینترنت اشیاء بیش از آن که مفهوم اینترنت اشیاء مهم باشد، مفهوم چالش های معماری و تهدیدات امنیتی در فن آوری اهمیت دارد [۴]. لذا برای پذیرش فن آوری اینترنت اشیاء به صورت شبکه، ابتدا بایستی به موضوع امنیت و محرمانگی آن توجه شود. به عبارت دیگر مسئله اصلی و چالش پیش روی فناوری اینترنت اشیاء به ویژه در کشورهای در حال توسعه، فقدان امنیت در ارتباطات میان اشیاء متصل به اینترنت می باشد. این مشکل می تواند برای پذیرش فن آوری برای کاربران مانع بزرگی محسوب شود و هزینه های زیر ساختی که از سوی دولت های برای راه اندازی این شبکه در نظر گرفته می شود بی حاصل گرداند. بسیاری از سفر های درون شهری برای انجام کارهای اداری یکی از مواردی است که باعث ایجاد ترافیک و آلودگی هوا می شود. اینترنت اشیاء این امکان را فراهم می کند که این آلودگی ها به حد زیادی کاهش یابد. لذا در این پژوهش مدلی برای امنیت اینترنت اشیاء در حمل و نقل هوشمند را مورد بررسی قرار می دهیم.

بخش اول این مقاله مرور و ادبیات می باشد با توجه به ماهیت بین رشته ای نیاز است برخی مفاهیم بررسی و دیدگاه مشترکی حاصل گردد. لذا این پژوهش فصل مشترکی از مباحث حوزه های حمل و نقل هوشمند، اینترنت اشیاء و امنیت را در بر می گیرد. در بخش دوم روش تحلیل عواملی که با عنوان روش تحقیق برای آزمون فرضیه های مدل پیشنهادی برای افزایش امنیت اینترنت اشیاء در حوزه حمل و نقل شهر هوشمند به کار رفته معرفی شده

فصل و بحث های امنیتی از این معماری به عنوان اساس کار مسایل امنیتی اینترنت اشیا مورد استفاده قرار بگیرد.

اینترنت اشیا در واقع شبکه ای از اشیا قابل شناسایی، اتصال و جمع آنها با اینترنت و نمایش<sup>۵</sup> آن ها در دنیای دیجیتال یا مجازی می باشد. برای ایجاد یک شبکه اینترنت اشیا، طیف وسیعی از تکنولوژی ها درگیر می باشند. به عنوان مثال شناسه های RFID برای شناسایی تجهیزات و مکان یابی آنها، پروتکل های بهبود یافته برای پوشش های شخصی<sup>۶</sup> و گسترده، تکنولوژی های وب و غیره برای تکامل شبکه اینترنت اشیا درگیر خواهند بود. این تکنولوژی ها در کنار یکدیگر منجر به ایجاد دنیای مجازی<sup>۷</sup> از اشیا بر روی دنیای حقیقی فیزیکی خواهد شد که در آن اشیا با استفاده از مخابرات ماشین به ماشین (M2M)<sup>۸</sup> قابلیت صحبت با هم خواهند داشت. با این وجود، این اشیا با هدایت انسان قادر به جمع آوری داده برای انسان یا انجام برخی دستورات انسان در محیط پیرامون یا به عنوان یک سری واحدهای منفعل قادر به جمع آوری داده برای واحدهای هوشمندتر خواهند بود. شبکه های حسگر بی سیم<sup>۹</sup> (WSN) یکی از تکنولوژی های اتصال دنیای مجازی و فیزیکی است که در آن حسگرها به عنوان گره های شبکه قادر به برقراری ارتباط خودکار بین خودشان و سیستم های هوشمندتر هستند. شبکه های حسگر ابتدایی مجموعه ای از تجهیزات حسی است که داده های محیطی را حس، جمع آوری و با همکاری یکدیگر به یک گره اصلی برای پردازش ارسال می کند. این نسل از شبکه های حسگر فاقد استاندارد خاصی بوده و معمولاً برای مانیتور کردن محیط های دور از دسترس از قبیل جنگل ها، بیابان ها یا میدان های جنگی مورد استفاده قرار می گیرند.

شبکه های حسگر فعلی یا پیشرفته در محیط های نزدیکتر به انسان و برای اهدافی از قبیل کنترل ترافیک، مانیتورینگ پل ها و تونل ها، کنترل و انتقالات صنعتی پیاده سازی شده اند. بطور کلی IoT می تواند به سه لایه کلی تقسیم شود. شکل ۱، معماری لایه های اینترنت اشیا را نشان می دهد [۸].

-سطح اول لایه ادراک: اساسی ترین لایه، لایه ادراک یا لایه تشخیص می باشد که تمامی اطلاعات را از طریق تجهیزات فیزیکی

لجستیک و زنجیره تامین: از گذشته تا بحال از RFID و شبکه های حسگر استفاده گسترده می شده است. از حسگرها در خطوط مونتاژ امکان تولیدی و نیز از RFID برای رهگیری محصولات در طول بخشی از زنجیره تامین آن توسط هر شرکت استفاده می شود. اگرچه استفاده از این تکنولوژی ها در زنجیره تامین امری جدید نیست، اما IoT امکان استفاده از این تکنولوژی ها را در کل مرزهای جغرافیایی و سازمانی ممکن می کند. بویژه IoT می تواند کارایی زنجیره تامین را از طریق اطلاعاتی که دارای جزئیات بیشتر و به روزتر است بیشتر از قبل بهبود بخشد که این امر منجر به بهبود قابلیت رهگیری محصولات می شود. برای مثال مدتی است که از RFID برای رهگیری محصولات و بخشهای مختلف آنها در زنجیره تولید استفاده می شود با این حال هنگامی که محصول از فروشگاه خارج می شود دیگر تولید کننده توانایی خود برای رهگیری آن را از دست می دهد. به همین شکل، مصرف کنندگان نمی توانستند به چرخه زندگی محصولات خریداری شده دسترسی پیدا کنند. به واسطه ی اختصاص یک شناسه منحصر به فرد برای هر محصول و امکان دسترسی به داده های آن از طریق وب، IoT امکان رهگیری محصولات را در طول کل چرخه عمر آنها امکانپذیر می کند [۷].

صنعت حمل و نقل: اینترنت اشیا در بحث حمل و نقل و مدیریت تردد به کمک حکومت می آید و مانیتور تردها و ترافیک را تسهیل سازی می کند. وسایل نقلیه مستقل می توانند پویایی حمل و نقل و تدارکات تحت پوشش شهر را تغییر دهند. بعنوان نمونه هواپیمای بدون سرنشین تجهیزات پزشکی می تواند به نجات زندگی انسان در مناطق دسترسی سخت و صعب العبور کمک نماید و تاکسی های بدون راننده می تواند با استفاده از تشخیص مسیر های بدون ترافیک به مسافران خود کمک کنند [۸].

## ۱.۲. معماری و پروتکل های اینترنت اشیا

در این بخش یک معماری کلی مورد استفاده برای اینترنت اشیا مورد بررسی قرار می گیرد و یک معماری مبتنی بر استاندارد هفت لایه ISO و پروتکل های مرتبط معرفی می شود تا در ادامه این

<sup>۵</sup> Machine to machine (M2M)

<sup>۹</sup> Wireless sensor networks (WSN)

<sup>۵</sup> Representation

<sup>۶</sup> Personal area network

<sup>۷</sup> Virtual world

مبتنی بر تحلیل تهدیدهای اتخاذ شده، مدل تهدید را بعنوان روشی برای تحلیل تأثیر تهدیدها در کاربردهای مختلف ارائه می نماید. از این مدل تهدید، ویژگی های حریم خصوصی و امنیت استنباط می شود. این ارزیابی ما را در مشخص نمودن تلاشها و توجهات بیشتر در فعالیتهای آینده که باید در توسعه مکانیزمهای امنیتی در اینترنت اشیاء سرمایه گذاری شود راهنمایی خواهد کرد [۹].

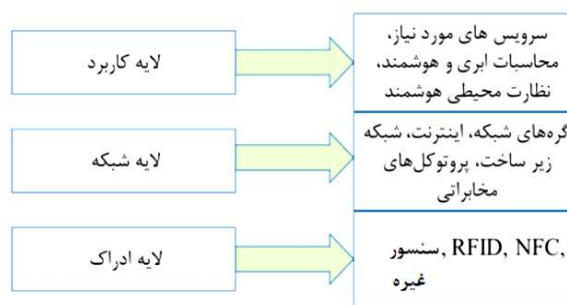
ژی کای ژانگ<sup>۱۲</sup> و همکارانش در سال ۲۰۱۱ بر روی موضوع تهدیدهای امنیتی و اقدامات متقابل در حال ظهور در اینترنت اشیاء تحقیق نموده اند. این مقاله، سناریوهای ارتباطات اینترنت اشیاء را برشمرده و تهدیدها را در مقیاس بزرگ، فضای غیر قابل اعتماد و در محیط محاسبات فراگیر بررسی نموده است. برای مقابله با این چالش های جدید، معماری امنیتی متعارف بازبینی خواهد شد. به خصوص، الگوهای احراز هویت مختلفی برای اطمینان از محرمانه بودن و صحت داده های مبادله شده ارزیابی می شود. علاوه بر موضوع تهدیدهای امنیتی و اقدامات متقابل در حال ظهور در اینترنت اشیاء، بطور ویژه چالش های تبادل اطلاعات حساس و خصوصی بین اشیاء در حال جابجایی، اشیاء در منزل و اشیاء در سازمان ارزیابی شده اند. نامگذاری، مدیریت و احراز هویت اشیاء در IoT از مسائل کلیدی برای برقراری ارتباطات امن و ارزیابی داده ها هستند. براساس سناریوهای مختلف ارتباطات در IoT، چند الگوی احراز هویت بالقوه که قابل اجرا هستند عنوان شده است [۱۰].

کی جینگ<sup>۱۳</sup> و همکارانش در سال ۲۰۱۷ بر روی موضوع چشم اندازها و چالش های اینترنت اشیاء پژوهش نمودند که تمرکز آنها بر روی مشکلات امنیتی در میان دیگر چالش ها می باشد. همانطور که IoT براساس اینترنت ساخته شده است، مشکلات امنیتی اینترنت نیز در IoT نشان داده خواهد شد. این مقاله مشکلات امنیتی هر سه لایه ادراک، انتقال و کاربرد را به صورت جداگانه تجزیه و تحلیل نموده و سعی شده مشکلات جدید و راه حل آنها را بیابد. این مقاله همچنین مسائل یکپارچگی در بین لایه های غیرهمگن و جزئیات مسائل امنیتی را تجزیه و تحلیل می کند و بطور کلی در مورد مسائل امنیتی IoT بحث و تلاش می کند برای آنها راه حل هایی بیابد. همچنین این مقاله به مقایسه

جمع آوری کرده و دنیای فیزیکی را شناسایی می کند، این اطلاعات شامل خصوصیات اشیاء، شرایط محیطی و ... و تجهیزات فیزیکی شامل خواننده، RFID تمامی انواع سنسورها، GPS و دیگر تجهیزات می باشد. مولفه اساسی در این لایه، سنسورها برای دریافت و بیان دنیای واقعی در دنیای دیجیتال است.

-سطح دوم، لایه شبکه: مسئول ارسال اطلاعات از لایه ادراک، پردازش اولیه اطلاعات، دسته بندی و پردازش می باشد. در این لایه، ارسال اطلاعات مبتنی بر چندین شبکه پایه بوده که شامل اینترنت، شبکه مخابرات سیار، گره های ماهواره ای، شبکه بیسیم و شبکه زیرساخت بوده و پروتکل های مخابراتی نیز جهت تبادل اطلاعات بین تجهیزات ضروری است.

-لایه کاربرد: که مدیریت نقش و کاربرد اینترنت اشیاء را مشخص می کند و ممکن است از یک زیر لایه برای ایجاد یک بستر قابل اطمینان استفاده کند.



شکل ۱- معماری لایه ای اینترنت اشیاء

## ۲.۲. پیشینه تحقیق

احمد اتملی<sup>۱۴</sup> و اندرئو مارتین<sup>۱۵</sup> در سال ۲۰۱۵ بر روی موضوع تحلیل امنیتی مبتنی بر تهدید در اینترنت اشیاء تحقیق و یک مدل تهدید در IoT ارائه نمودند که برای تعیین محل سرمایه گذاری به منظور امن شدن این سیستم ها با توجه به تلاشهای انجام شده در این زمینه استفاده می شود. آنها به این نتیجه رسیدند که اقدامات توصیه شده در ارائه تأمین امنیت و تضمین حفظ حریم خصوصی هنگام استفاده از IoT به ماکمک خواهند کرد. چشم انداز اینترنت اشیاء و ارتباط آن با سایر پژوهش ها در زمینه امنیت و حریم خصوصی در اینترنت اشیاء بحث شده است. همچنین رویکردهای مختلفی که توسط بسیاری از محققین در امنیت و حریم خصوصی نشان داده شده ارائه گردیده است. رویکرد

<sup>۱۲</sup> zhi kai zhang

<sup>۱۳</sup> Qi Jing

<sup>۱۴</sup> Ahmad Atamli

<sup>۱۵</sup> Andrew Martin

مسائل امنیتی بین IoT و شبکه های سنتی و بحث در مورد باز کردن مسائل امنیتی IoT می پردازد [۱۱].

امروزه، نگرانی های حریم خصوصی و امنیت به یک مانع و عامل کاهش پیشرفت بسیاری از فن آوری ها تبدیل شده است. بسیاری از فنآوری ها در ارائه مناسب مکانیزم های امنیتی و حریم خصوصی شکست خورده اند، در نتیجه باعث آزدگی و آسیب شده اند. به منظور به دست آوردن اعتماد عمومی در اینترنت اشیاء ما نیاز داریم بپذیریم که حریم خصوصی و امنیت این سیستم ها پذیرفته نمی شود، مگر با اعمال مکانیزم های مناسب به منظور تضمین امنیت اشیائی که از ابتدا در IoT وجود دارند. هدف اصلی این مقاله بررسی و شناسایی تهدیدات امنیتی استفاده از اینترنت اشیاء در حمل و نقل هوشمند است.

### ۳. چالش های امنیتی اینترنت اشیاء

به منظور برآورده کردن مسئله امنیت، اینترنت اشیاء با چالش های بیشتری نسبت به شبکه های موجود مواجه است. با توجه به تعداد تجهیزات متصل شده به شبکه، ارتباط این تجهیزات و اشیاء با یکدیگر و توسعه اینترنت اشیاء در بستری از شبکه های موجود از قبیل اینترنت، شبکه موبایل و شبکه حسگرها و ... اینترنت اشیاء با چالشهای امنیتی بیشتری مواجه است. در نتیجه، برخی از تکنولوژی ها و روش های جدید، باید جهت برآورده کردن نیازمندی های بیشتر بر حسب قابلیت اطمینان، امنیت و حریم خصوصی، توسعه داده شود. امنیت اطلاعات و شبکه باید با خصوصیتی از جمله شناسایی، قابلیت اعتماد، رمزنگاری و غیرقابل انکار بودن و ... برآورده شود. در نتیجه، امنیت در حوزه IoT در مسئله قابل دسترسی بودن و مستقل بودن، دارای اهمیت بیشتری است.

چالش های این حوزه بسیارند، که هم اجتماعی اند و هم فنی و باید آنها را رفع کرد تا IoT مورد استفاده و پذیرش عمومی قرار گیرد. می توان این چالش ها را به سه دسته امنیت ارتباط، حریم خصوصی و مسئولیت پذیری/مسائل حقوقی تقسیم بندی کرد [۱۲، ۱۳ و ۱۴].

#### -امنیت ارتباط

دستگاههای IoT غالباً وایرلس هستند و ممکن است در مکانهای عمومی واقع شوند. ارتباط وایرلس از طریق رمزنگاری کردن امن تر می شود و در نتیجه رمزنگاری کردن داده برای اشیاء

یک روش افزایش امنیت اطلاعات است. با این وجود، بسیاری از دستگاههای IoT فعلی به اندازه ای قوی نیستند که از روش رمزنگاری مناسب پشتیبانی کنند. پس، برای ممکن کردن رمزنگاری در این شبکه، لازم است در دستگاههای IoT از الگوریتم های کارتر و با مصرف انرژی کمتر استفاده کرد و همچنین به روشهای کارآمد تری از نظر توزیع کلید رو آورد. علاوه بر رمزنگاری، احراز هویت هم مسئله امنیتی مهمی بوده و برای دست یافتن به آن، وجود شناسه های یکتا برای دستگاه های IoT امری مهم می باشد. این شناسه ها حتی ممکن است برای تعیین کردن هویت شیء در نهادهای ملی، شناسایی فعالیت های قانونی و سایر عملکردها استفاده شوند. از اینرو، حصول اطمینان از اینکه اشیاء هوشمند دقیقاً همانهایی هستند که ادعا می کنند، برای موفقیت امنیت IoT حیاتی است. بطور کلی فرض می شود ساختار اینترنت اشیاء در طول کل بازه زمانی، پایدار باقی می ماند و نشان داده شده است که مکانیزم امنیت در هر لایه منطقی نمی تواند سیستم امن کاملی را پیاده سازی کند، در نتیجه، این موضوع و استفاده از الگوریتم های بین لایه ای هنوز به عنوان یک چالش در اینترنت اشیاء مطرح است. این مساله در مرحله بعدی منجر به لزوم داشتن یک مکانیزم امن مدیریت اساسی کل شبکه می شود.

#### -حریم خصوصی

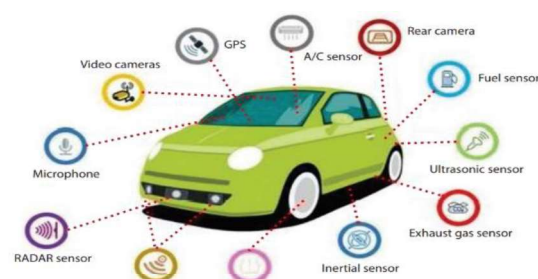
همچنانکه اشیاء بیشتری از طریق IoT قابل رهگیری می شوند، تهدیدها برای حریم خصوصی جدی تر شده اند علاوه بر اینم سازی داده ها جهت عدم قرارگیری آنها در اختیار افراد غیرهدف، لازم است مساله مالکیت داده ها نیز حل شود تا کاربران بتوانند راحت تر در IoT مشارکت کنند. از این رو، مالکیت داده های گردآوری شده از اشیاء هوشمند باید به وضوح مشخص شود. لازم است مالک داده را مطمئن کرد که داده ها بدون رضایت وی استفاده نمی شوند بویژه به هنگام به اشتراک گذاری داده ها. سیاستهای حریم خصوصی می تواند رویکردی برای حصول اطمینان از محرمانگی داده ها باشند. اشیاء هوشمند و دستگاههای خوانشگر در IoT را می توان به تنظیمات سیاستهای حریم مجهز کرد. پس، زمانی که شی و خوانشگر وارد ارتباط می شوند، آنها می توانند قبل از تکمیل فرآیند ارتباط، اقدام به بررسی سیاست حریم خصوصی یکدیگر جهت سازگاری کنند.

#### ۴. فناوری سنسور<sup>۱۴</sup>

استفاده از سنسور ها برای تبدیل حمل و نقل سنتی به هوشمند ضروری و از نیاز های اولیه است. در واقع سنسور عنصری است که عوامل خروجی را به شکل سیگنال و به عنوان ورودی دستگاه ها جهت پردازش و تصمیم گیری به مرکز پردازشی اینترنت اشیاء می فرستد، در شکل ۲ سنسور های موجود در یک خودرو هوشمند نشان داده شده است.

- در مواقع مشکل و خطا سنسور ها سریعاً به واحد های ترافیکی و امدادی اطلاع می دهند.
- نیاز به نیروی انسانی ماهر را کاهش می دهند.
- در نهایت محصول با کیفیت بهتری را می توانند ارائه دهند.

به طور کلی خروجی ها و تصمیم گیری های یک عامل هوشمند (چراغ ها، مسیر یابی، خودرو ها و...) در حمل و نقل هوشمند و تصمیم گیری عامل ها نقش موثری دارند [۱۴]. در صورت برآورده شدن این نقش ها به درستی، ایمنی حمل و نقل تضمین می شود که در نهایت باعث رضایت مسافران، رانندگان و کلیه استفاده کنندگان از سیستم حمل و نقل عمومی می شود. همانگونه که در تصویر شماره ۲ مشخص است برخی از سنسور ها برای نظارت و کنترل عملکرد، موقعیت، کارایی و سیستم ایمنی نصب شده اند به طور متوسط برای یک خودرو هوشمند بین ۵۰ تا ۱۰۰ سنسور



شکل ۲ - سنسور های موجود در خودرو های هوشمند

نصب گردیده است. برای یک خودرو هوشمند تر تعداد سنسور ها به ۲۰۰ سنسور نیز می رسد [۱۵].

#### ۵. امنیت در شبکه های اینترنت اشیاء مورد استفاده در حمل و نقل

همانگونه که در قسمت هایی از مقاله پیش رو بیان گردید شبکه های اینترنت اشیاء بنا بر مزایایی که فراهم می سازند، امروزه به یکی از مهم ترین تکنولوژی ها در عرصه های مختلف عنوان شده که روز به روز بر کاربرد این فناوری افزوده می شود [۱۶ و ۱۷]. به طور کلی بخش عمده ای از این کاربرد ها، کاربرد های حساس و پر اهمیت هستند و استفاده از این فن آوری باعث شده تا اهمیت امنیت و پیاده سازی امنیت در این شبکه ها بیشتر از سایر شبکه ها مورد توجه و بررسی قرار گیرد. این در حالی است که مسائلی همچون توپولوژی و مقیاس پذیری جغرافیایی شبکه به این مشکلات دامن زده و بحث برقراری امنیت را امری بسیار دشوار و پیچیده نموده است. در مجموع وجود این مسائل برای شبکه های اینترنتی اشیاء باعث ایجاد تفاوت ها و پیچیدگی های خاص در حوزه امنیت و برقراری امنیت ارتباطات این شبکه ها شده است.

وجود مسائل و مباحث عنوان شده، به ضرورت ارائه مدل هایی متمایز به جهت برقراری و پیاده سازی امنیت در شبکه های اینترنت اشیاء (به عنوان نیاز و ضرورتی انکارناپذیر) اشاره دارد. بر همین اساس و با توجه به اهمیت بالای بحث امنیت در شبکه های اینترنت اشیاء، تا کنون مقالات گسترده ای برای بهبود این مقوله حیاتی معرفی شده اند. در یک دسته بندی کلی این روش ها را می توان به دو دسته کلی به قرار زیر بخش بندی و ارزیابی نمود [۱۸ و ۱۹].

##### • روش های رمزنگاری

هدف این سیستم، رمزنگاری داده ها به جهت پیشگیری از دسترسی های غیرمجاز است. مهم ترین مسئله این روش عدم مقابله با حملات فعال است.

##### • روشهای مبتنی بر اعتماد<sup>۱۵</sup>

هدف ایجاد اعتماد بین گره های شبکه به جهت تشخیص انواع حملات مخرب است. مهم ترین مسئله این روش عدم وفق پذیری با پویایی و عدم قطعیت محاسبات اعتماد است.

تمامی روش های پیشنهادی برای اینترنت اشیاء بر اساس دو روش رمزنگاری و یا مدل های اعتماد طراحی شده اند. این درحالی است که بیشتر این تحقیقات مبتنی بر مدل های اعتماد طراحی و توسعه یافته اند. این مدل ها برای برقراری اعتماد در اینترنت اشیاء بسیار کارا بوده و همچنین با خصوصیات این فناوری بسیار

<sup>۱۵</sup> Trust Mechanism

<sup>۱۴</sup> Sensor Technology

قابلیت های این روش ها طراحی گردیده اند. این روش ها اغلب به برقراری اعتماد توام با توسعه مسیر متمرکز شده و از این حیث موفق اند. اما این روش ها با افزایش سربار های کنترلی همراهند [۱۵].

- روش های متمرکز بر ارزیابی چند معیاره در روش های متمرکز بر ارزیابی چند معیاری، قابلیت اعتماد وابسته به چند عامل محاسبه شده و معمولا ترکیبی از QOS یا قابلیت اطمینان می باشد. برای مثال علاوه بر اعتماد به عملکرد گره ها، کیفیت اتصال و انرژی گره ها نیز در نظر گرفته شده که از آن ها با عنوان اعتماد به اتصال و اعتماد به انرژی یاد می شود [۱۹].

- روش های مبتنی بر خوشه بندی این روش ها بر مبنای خوشه بندی گره ها طراحی شده و بر این اساس سعی بر برقراری امنیت دارند. برای این منظور گره ها به خوشه هایی مجزا تقسیم شده و برای هر گره یک سر خوشه انتخاب می شود. معمولا انتخاب سر خوشه ها بر اساس انرژی باقی مانده بیشتر یا تلفیقی از این دو عامل انجام می شود. پس از خوشه بندی، اعتماد اعضا خوشه توسط گره سر خوشه ارزیابی و ذخیره شده و در ادامه بر مبنای این اعتماد برای تشخیص گره مخرب تصمیم گیری می شود. مزیت این روش ها را می توان بهینه سازی انرژی و مدیریت موثر اعتماد عنوان کرد. اما از محدودیت های این دسته از روش ها می توان به پیچیدگی و تاخیر بالا اشاره نمود [۱۵ و ۱۶ و ۱۹].

- روش های متمرکز بر حملات مسیریابی تمرکز این دسته از روش ها بر مقابله با حملات مسیریابی از جمله حمله رتبه، حمله سیاه چاله، حمله گودال کرم، حمله چاله خاکستری و غیره می باشد. اغلب این روش ها بر حوزه مسیریابی و ارزیابی فرایند های مسیریابی (مانند ارزیابی تعداد و محتویات پیام های DIO و DAO) متمرکز شده و بر اساس نتایج این ارزیابی سعی بر تشخیص حملات دارند. برترین قابلیت این روش ها را می توان مقابله با حملات مسیریابی و بزرگ ترین مشکل آن ها را می توان ناکارآمدی در مقابله با سایر حملات عنوان نمود [۱۶ و ۲۰].

سازگارتر هستند. روش های معرفی شده بر پایه این مدل قابلیت مقابله با هر دو نوع حملات عوامل خودخواه و عوامل بدخواه را فراهم ساخته و در شرایط مختلف شبکه، پاسخگوی نیازهای مختلف امنیتی هستند [۱۹ و ۲۰]. این مدل ها بر پایه اعتماد اجتماعی طراحی شده و منطبق با این اصل عمل می کنند. در این روش گره های شبکه با انجام رفتار های درست با افزایش اعتماد و اعتبارشان تشویق شده و در صورت سوء رفتارها با کاهش اعتماد مجازات خواهند شد. از نتایج این افزایش و کاهش اعتماد به منظور تفکیک عوامل خوش رفتار از عوامل مخرب استفاده می شود. به طوری که اگر اعتماد عاملی به زیر مقدار مشخصی سقوط کند، عامل مورد نظر مهاجم در نظر گرفته شده و به منظور مجازات در شبکه قرنطینه خواهد شد.

## ۶. مروری بر روش های پیشنهادی امنیت حمل و نقل هوشمند بر مبنای اینترنت اشیا

بنابر آنچه در ارتباط با اهمیت امنیت و اعتماد در اینترنت اشیا ارائه و عنوان شد، تا کنون مقالات و تحقیقات گسترده ای در راستای بهبود این مبحث کلیدی معرفی شده اند. در این بخش برخی از جدیدترین مدل های اعتماد و امنیت ارائه شده برای شبکه های اینترنت اشیا که در حمل و نقل هوشمند نیز بکار می رود را از لحاظ قابلیت و محدودیت ها بررسی خواهیم کرد.

- روش های رمز نگاری این روش ها بر مقابله با حملات دسترسی یا به اصطلاح حملات غیر فعال متمرکز شده و تمرکز آن ها بر رمزنگاری و پیشگیری از دسترسی غیر مجاز به اطلاعات است. برای این منظور اغلب این روش ها از تکنیک های رمزنگاری استفاده می گردد. [۱۴].

- روش های احراز هویت این روش ها بر احراز هویت گره ها متمرکز شده و هدف آن ها مقابله با حملات خارجی است. در واقع این روش ها با تدابیری که فراهم می سازند، قابلیت تشخیص گره های شبکه را فراهم می سازد و با همین روش قادر به مقابله با این سوء رفتار هستند [۱۵].

- روش های مبتنی بر تکنیک های فرا ابتکاری<sup>۱۶</sup> این روش بر پایه الگوریتم های فرا اکتشافی مانند گرگ خاکستری و سایر الگوریتم های زیست محیطی گسترش یافته و بر پایه

## نتیجه گیری

در این مقاله به معرفی تکنولوژی نو ظهور اینترنت اشیا و در ادامه به بررسی امنیت در اینترنت اشیا و استفاده و کاربرد اینترنت اشیا در حمل و نقل پرداخته شد. همانگونه که بیان شد به طور کلی بخش عمده ای از این کاربرد ها حساس و پر اهمیت هستند و استفاده از این فناوری باعث شده تا اهمیت امنیت و پیاده سازی امنیت در این شبکه ها بیشتر از سایر شبکه ها مورد توجه و بررسی قرار گیرد. این در حالی است که مسائلی همچون توپولوژی و مقیاس پذیری جغرافیایی شبکه به این مشکلات دامن زده و بحث برقراری امنیت را امری بسیار دشوار و پیچیده نموده است. در مجموع وجود این مسائل برای شبکه های اینترنت اشیا باعث ایجاد تفاوت ها و پیچیدگی های خاص در حوزه امنیت و برقراری امنیت ارتباطات این شبکه ها شده است. وجود مسائل و مباحث عنوان شده ، به ضرورت ارائه مدل هایی متمایز به جهت برقراری و پیاده سازی امنیت در شبکه های اینترنت اشیا (به عنوان نیاز و ضرورتی انکارناپذیر) اشاره دارد . بر همین اساس و با توجه به اهمیت بالای بحث امنیت در شبکه های اینترنت اشیا، تا کنون مقالات گسترده ای برای بهبود این مقوله حیاتی معرفی شده اند که در این پژوهش مورد بررسی قرار گرفتند.

## مراجع

- [5] Ricci F, Rokach L, Shapira B (2015) Recommender systems: introduction and challenges. In: Recommender systems handbook. Springer, Berlin, pp 1–34
- [6] Kalai A, Zayani CA, Amous I, Abdelghani W, Sèdes F (2017) Social collaborative service recommendation approach based on user's trust and domain-specific expertise. *Future Gen Comput Syst* 80:355–367
- [7] Montori, Federico, et al. "Machine-to-machine wireless communication technologies for the Internet of Things: Taxonomy, comparison and open issues." *Pervasive and Mobile Computing* 50 (2018): 56-81.
- [8] Dey, Amlan Jyoti, and Hiren Kumar Deva Sarma. "Routing techniques in internet of things: a review." *Trends in Communication, Cloud, and Big Data* (2020): 41-50.
- [9] Marietta, J., and B. Chandra Mohan. "A review on routing in internet of things." *Wireless Personal Communications* 111.1 (2020): 209-233.
- [10] Asghari, Parvaneh, Amir Masoud Rahmani, and Hamid Haj Seyyed Javadi. "Internet of Things applications: A systematic review." *Computer Networks* 148(2019): 241-261.
- [11] Dhanvijay, Mrinai M., and Shailaja C. Patil. "Internet of Things: A survey of enabling technologies in healthcare and its applications." *Computer Networks* 153 (2019): 113-131.
- [12] Harbi, Yasmine, et al. "A review of security in internet of things." *Wireless Personal Communications* 108.1 (2019): 325-344.
- [13] Ogonji, Mark Mbock, George Okeyo, and Joseph Muliaro Wafula. "A survey on privacy and security of Internet of Things." *Computer Science Review* 38 (2020): 100312.
- [14] Wang, Lanjing, et al. "ISA evaluation framework for security of internet of health things system using AHP-TOPSIS methods." *IEEE Access* 8 (2020): 152316-152332.
- [15] Alshehri, Mohammad Dahman, and Farookh Khadeer Hussain. "A fuzzy security protocol for trust management in
- [1] Ashton K (2009) That 'internet of things' thing. *RFID J* 22(7):97–114
- [2] Kobayashi G, Quilici-Gonzalez JA, Broens MA, Quilici- Gonzalez ME (2011) Ubiquity of virtual disguisers and potential impact on ethical behavior. In: 2011 fourth international conference on Ubimedia computing. IEEE, Piscataway
- [3] Kobayashi G, Quilici-Gonzalez ME, Broens MC, Quilici-Gonzalez JA (2016) The ethical impact of the Internet of Things in social relationships: technological mediation and mutual trust. *IEEE Consumer Electron Mag* 5(3):85–89
- [4] Zheng S, Jiang T, Baras J (2011) Exploiting trust relations for nash equilibrium efficiency in ad hoc networks. In: IEEE international conference on communications (ICC), 2011. IEEE, Piscataway

- the internet of things (Fuzzy-IoT)." Computing 101.7 (2019): 791-818.
- [16] Fu, Yulong, et al. "An automata based intrusion detection method for internet of things." Mobile Information Systems 2017 (2017).
- [17] Suryani, Vera, Selo Sulistyo, and Widyawan Widyawan. "Two-phase security protection for the Internet of Things object." Journal of Information Processing Systems 14.6 (2018): 1431-1437.
- [18] Yan, Zheng, Peng Zhang, and Athanasios V. Vasilakos. "A survey on trust management for Internet of Things." Journal of network and computer applications 42 (2014): 120-134.
- [19] Mohammadi, Venus, et al. "Trust-based recommendation systems in Internet of Things: a systematic literature review." Human-centric Computing and Information Sciences 9.1 (2019): 1-6
- [20] Sharma, Avani, et al. "Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes." Computer Communications (2020)