یازدهمین کنگره ملی سراسری
فناوریهای نوین در حوزه توسعه پایدار ایران
11th National Congress of
the New Technologies in Sustainable Development of Iran
senaconf.ir

بررسی امنیت در IoT

بهزاد سارانی [1]

[1] دانشگاه ملی زابل، زابل، behzadsarani۶۲@gmail.com

چکیده

امروزه نصب و راه اندازی شبکه و ارتباط بین کامپیوترها و اشیا نیازی رایج و مرسوم است که به بهبود کیفیت زندگی افراد کمک شایانی می‌کند. اینترنت اشیا (IoT) یعنی اتصال دستگاه‌های مختلف به یکدیگر از طریق اینترنت. به کمک اینترنت اشیا برنامه‌ها و دستگاه‌های مختلف می‌توانند از طریق اتصال اینترنت با یکدیگر و حتی انسان تعامل و صحبت کنند، به عنوان مثال یخچال‌های هوشمندی که به اینترنت متصلند و شما را از موجودی و تاریخ انقضا مواد خوراکی داخل آن با خبر می‌کنند. در واقع، اینترنت اشیا شما را قادر می‌سازد تا اشیا مورد استفاده خود را از راه دور و به کمک زیرساخت‌های اینترنتی مدیریت و کنترل کنید.

لازم به ذکر می باشد امنیت نرم افزارها و سخت افزارها باید تامین شود تا وسایل IoT بتوانند کار خود را به خوبی انجام دهند. بدون امنیت، هر وسیله‌ای ممکن است هک شود و کنترل آن به دست هکر بیفتد و یا اطلاعات دیجیتالی کاربر دزدیده شود.

وقتی امنیت هنگام طراحی در نظر گرفته شود دیگر نیازی نیست که پس از وقوع هک و رخنه اقدام به تامین امنیت کرد. تامین امینت در طراحی، مساله مهم و حیاتی برای مشتری و سازمان‌ها است. از آنجایی که وسایل اینترنت اشیا به اینترنت وصل هستند پتانسیل هک شدن دارند و از طرفی بسیاری از آنها به صورت تعبیه شده امنیتی ندارند و انها را تبدیل به هدف خوبی برای هک می‌کند. در این مقاله به بررسی امنیت اینترنت اشیا (IOT) می پردازیم و راهکارهای افزایش امنیت را بررسی می کنیم.

واژه‌های کلیدی: اینترنت اشیاء، تکنولوژی، امنیت اینترنت اشیاء، IOT.

۱.۱. مقدمه

نظریه اینترنت اشیا برای نخستین بار در سال ۱۹۹۹ توسط کوین اشتون بیان شد اما چند سالی است که پیدایش اینترنت اشیا به طور جدی روی دنیای IT تاثیر گذاشته و در حال حاضر اکثر کسب وکارها در حال حرکت به سمت استفاده وسیع از این تکنولوژی هستند [۱]. Internet of Things به اختصار IOT و یا همان اینترنت اشیا چیز جدید و نا آشنایی نیست چون اولین نمونه استفاده از این تکنولوژی؛ تولید و رونمایی از توستر متصل به اینترنت توسط یک کمپانی در کنفرانسی در سال ۱۹۸۹ بود. اینترنت اشیا به عنوان انقلاب صنعتی بعدی نامیده می‌شود و پیاده سازی پروژه‌های اینترنت اشیا، روش تعامل تمام کسب و کارها، دولت‌ها و مصرف کنندگان را با دنیای فیزیکی تغییر خواهد داد.

۲.۱. اینترنت اشیا چگونه کار می کند؟

دستگاه‌های مجهز به تکنولوژی IOT مجهز به سنسورهایی هستند که به پلتفرم IOT وصلند و اطلاعات دستگاه‌های مختلف را یکپارچه می‌کنند و ارزشمندترین اطلاعات را بر اساس نیاز تعیین شده، آنالیز می‌کنند. اینترنت اشیا دقیقا می‌داند کدام اطلاعات مفید هستند و کدام اطلاعات را با خیال راحت می‌تواند کنار گذارد. این اطلاعات برای تشخیص الگوها، ارایه توصیه و تشخیص مشکلات احتمالی قبل از وقوع استفاده می‌شوند. نتیجه این است که می‌توانیم تصمیمات هوشمندانه‌تری بگیریم. پس از دریافت اطلاعات توسط سنسورها، اطلاعات به سرور اینترنت اشیا منتقل می‌شوند تا ذخیره، دسته‌بندی و آنالیز شوند. برای انجام این کارها نیاز به پلتفرم اینترنت اشیا است تا دریافت، تبدیل و انتقال اطلاعات، تامین امنیت و سازگاری با پلتفرم‌های دیگر برای دریافت و تبدیل اطلاعات و ... تامین شود. از جمله پلتفرم‌های اینترنت اشیا عبارتند از Google IoT Cloud و AWS IoT Core و Artik Cloud وMicrosoft Azure IoT.

۳.۱. امنیت در IoT

با توجه به ابعاد وسیع و گسترده‌ی زیرساخت‌های مبتنی بر اینترت اشیا، سازمان‌ها باید برنامه‌های امنیتی خود را به سطح کاملا جدیدی برای بهره مندی از مزایای IoT بیاورند. طبق تحقیقات شرکتGartner، در سال ۲۰۱۷، ۸/۴ میلیارد دستگاه متصل شده در سراسر دنیا مورد استفاده قرار گرفته است که این تعداد نسبت به سال ۲۰۱۶ تا ۳۱ درصد افزایش داشته است. انتظار می‌رود این عدد تا سال ۲۰۲۰ به ۲۰/۴ میلیارد برسد. بنابراین وجود امنیت در دستگاه های IoT امری حیاتی خواهد بود.

۴.۱. لزوم امنیت درIOT

به تازگی ، برخلاف پژوهش های صورت گرفته مرتبط با IOT و امنیت آن ، حملات مختلفی معرفی می شوند که فضای این مفهوم فناوری های مرتبط با آن را درگیر کرده است . معرفی این حملات بیشتر در کنفرانس هایی مثل BlackHat و دیگر انجمن های غیر امنیتی صورت میگیرد . این نشان میدهد که فناوری به پرتگاه بسیار پیچیده ای نزدیک شده و اقدامات متقابل اغلب ، فقط واکنشی است . بنابراین نیاز است اندکی به عقب برگردیم ، زمانی که فناوری های موثر بر زندگی ، در حال توسعه بودند و به سمت ابعاد خوبی از فناوری تمایل داشتند و امنیت را در هر سطحی بازتعریف کنیم . اگرچه این مسایل به خاطر اجبار های نظارتی در حال تغییر است ، اما با این حال تایید مراکز دولتی به معنای امنیت نخواهد بود.

مساله امنیت در IOT را می توان مهمترین چالش توسعه این فناوری در نظر گرفت . در این رابطه استاندارد های مختلفی در حال توسعه است ، ولی همچنان نیازمندی های امنیتی IOT و حتی مخاطرات آن به خوبی شناسایی و تحلیل نشده است[۲] . همان طور که گسترش دنیای اینترنت اشیا مزایای بیشماری را به همراه خود می‌آورد، در مقابل به میزان مخاطرات همراه آن نیز افزوده می شود. چرا که هکرها می‌توانند از هر یک از دستگاه‌های جدید به عنوان یک دروازه‌ی نو به دنیای هک و حملات سایبری استفاده کنند. مجرمان سایبری انگیزه می‌گیرند تا روش‌های جدید و حیرت انگیزی را برای هک کردن دستگاه‌های بی‌خطر بدست آورند تا به وسیله‌ی آنها به دستگاه‌های با ارزش‌تر راه یابند. پلو پز شاید به ظاهر برای امنیت خانه ی شما مشکل ساز نباشد، اما اگر به عنوان یک دروازه به دستگاه-های مهم تر در شبکه عمل کند، ممکن است به آسیب پذیرترین نقطه‌ی امنیتی خانه‌ی شما بدل شود. از عملیات تولید جهانی به

زیرساخت‌های تولید برق و توزیع ملی، دستگاه‌های متصل می‌توانند به طور چشمگیری مخاطرات عملیات را افزایش دهند. حمله‌ی اخیر هکرهای روسی به سیستم‌های کنترل نیروگاه‌های آمریکا، نیاز به هوشیاری را به شدت برجسته می‌کند.

۵.۱. امنیت دستگاه‌ها

یکی از موارد ایجاد امنیت در IoT، امن کردن دستگاه‌ها است. بعضی از دستگاه‌ها یا قطعات تجهیزات ممکن است به طور مداوم به درستی عمل کنند و نیازی به مراقبت و نظارت مستقیم برای برقراری امنیت نداشته باشند. وجود چنین دستگاه‌های سخت افزاری که می‌توانند جلوی دستیابی اطلاعات را توسط افراد نادرست بگیرند، بسیار مفید می‌باشد. همچنین در برابر هکرها، امور سایبری و از دستگاه‌های تسلیحاتی دفاع می‌کنند. یکی از روش‌های مناسب برای افزایش امنیت، استقرار یک رویکرد لایه‌ای است، به این ترتیب مهاجمان باید موانع متعددی را که برای محافظت از دستگاه‌ها و جلوگیری از ورود اطلاعات و دسترسی‌های غیرمجاز طراحی شده‌اند، دور بزنند. شرکت‌ها باید از آسیب پذیری‌های شناخته شده نظیر پورت‌های باز TCP / UDP، پورت‌های سریال باز، درخواست رمز عبور باز، مکان‌هایی برای تزریق کد از جمله سرورهای وب، ارتباطات بدون رمزگذاری و اتصالات رادیویی محافظت کنند.

یکی دیگر از اقدامات خوب برای محافظت از دستگاه‌ها، ارتقاء آنها با نصب پچ‌های امنیتی مورد نیاز است. اما به یاد داشته باشید که بسیاری از فروشندگان دستگاه در هنگام ساخت و فروش دستگاه‌ها بر امنیت تمرکز نمی‌کنند. طبق مطالعات انجام شده، بسیاری از دستگاه‌های اینترنت اشیا unpatchable هستند و به همین علت از امنیت لازم برخوردار نیستند. پس قبل از سرمایه گذاری در دستگاه-هایی که از طریق IIoT متصل می‌شوند، قابلیت‌های امنیتی دستگاه‌ها را ارزیابی کنید و مطمئن شوید که توسعه دهندگان از ابزارهای کافی برای ارزیابی عملکرد امنیتی دستگاه‌های خود برخوردارند. یکی دیگر از مسایل مهمی که باید مورد توجه قرار بگیرد، دقت در مدیریت و اطمینان از هویت دستگاه‌های IOT است که در تلاش برای اتصال به شبکه و استفاده از سرویس‌های موجود هستند.

۶.۱. امنیت متحرک/سیار در اینترنت اشیاء (IoT)

گره های متحرک در IoT اغلب از یک خوشه به خوشه ی دیگر حرکت می کنند، که در آن پروتکل های مبتنی بر رمزنگاری لازم است تا شناسایی سریع، احراز هویت، و حفظ حریم خصوصی فراهم شود. یک پروتکل موقتی در [۳] ارائه شده است که زمانی استفاده می شود که یک گره متحرک به خوشه ی جدید می پیوندد. چنین پروتکلی شامل یک پیام درخواست معتبر و یک پیام پاسخ اهراز هویت است، که به سرعت شناسایی، احراز هویت، و حفظ حریم خصوصی را پیاده سازی می کند. آن می تواند نسبت به حملات مجدد، استراق سمع، و ردیابی یا حملات حریم خصوصی مکانی قوی شود. در مقایسه با سایر پروتکل های مشابه همانند پروتکل برهم زنی مبنا ، آن دارای سربار ارتباطی کمتر، امنیت بیشتر، و خواص حفاظتی حریم خصوصی بیشتر است.

مرجع [۴] چالش های امنیتی را برای معماری HIMALIS (ورودی ناهمگن و انطباق تحرک از طریق تعیین محل تفکیک ID) با توجه به ویژگی های IoT و پیام های مدیریت تعیین محل/ID، که نسبت به حملات آسیب پذیر هستند، تجزیه و تحلیل کرد. این تحقیق یک طرح مدیریتی متحرک مقیاس پذیر و امنی را پیشنهاد می کند که محدودیت های IoT را در نظر می گیرد، و قابلیت های آسیب پذیری حریم خصوصی و امنیتی ممکن معماری HIMALIS را حل می کند. طرح پیشنهادی از احراز هویت میان حوزه ای مقیاس پذیر، به روز رسانی مکانی امن، و انتقال محدود برای فرایند متحرک پشتیبانی می کند.

علاوه براین، سیستم های شناسایی فرکانس رادیویی (RFID)، بر مبنای محیط شبکه ای EPC (کد الکترونیکی محصول)، به طور خودکار اشیاء برچسب زده را با استفاده از سیگنال های Rf بدون تماس مستقیم شناسایی می کند، که یکی از فناوری های فعال کننده ی IoT است. در تحقیق [۵]، یک شبکه متحرک RFID بر مبنای EPC شرح داده شد و تهدیدهای سیستم متحرک RFID تجزیه و تحلیل شد. چنین معماری امنیت و کارآمدی را تضمین می کند.

علاوه براین، برای امنیت و حریم خصوصی سیستم های متحرک RFID، مدل دیگر امنیتی و حریم خصوصی در مورد IoT در تحقیق [۶] پیشنهاد شد. این مدل نه تنها حریم خصوصی برچسب ها و خوانندگان را در نظر می گیرد، بلکه همچنین از خرابی برچسب ها، خرابی خواننده، خوانندگان متعدد، و پروتکل های کلید تبادل تصدیق شده دوجانبه پشتیبانی می کند.

تقویت شده توسط سرویسهای مبتنی بر مکان، سیستم های IoT دارای این پتانسیل هستند تا یک بررسی انبوه سیستماتیک را انجام دهند تا حریم خصوصی کاربران، بخصوص حریم خصوصی مکانی شان،نقض شود. مرجع [۷] برخی از مسائل حریم خصوصی مکانی موجود یافته شده در دستگاه های متحرک را بررسی کرد. توجه خاصی به مکانیزم های مجوزی دسترسی کنونی استفاده شده در سیستم عامل های اندروید، آی فون، و ویندوز داده شده است. توجه داتشه باشید که مسائل حریم خصوصی واقعی در سیستم عامل های متحرک باید توسط IoT کسب شود و با سایر سیستم عامل های ثابت یکپارچه شود.

در تحقیق [۸] یک طرح دست دهی امنیتی میان گره های متحرک در یک سیستم حمل و نقلی هوشمند پیشنهاد شده است. بطور دقیق تر، یک گره متحرک، در یک کانال ارتباطی ناامن، مشروعیت یک گره حسگر معمولی را از طریق مذاکره خصوصی معماری دست دهی تایید می کند؛ به این شیوه، یک سلسله مراتبی متحرک ایجاد می شود تا یک WSN مستقر شده به شیوه ای امن جستجو شود.

مرجع [۹] بیان می کند که سرویس مراقبت های بهداشتی یک نیاز جدید برای راه حل های متحرک است. برای حفاظت از حریم خصوصی و امنیت بیماران در بافت مراقبت های بهداشتی با استفاده از یک زیرساخت IoT، مکانیزیمی امن و خصوصی پیشنهاد شده است. از دیدگاه قابلیت اعتماد، فراهم اوردندگان سرویس باید احراز هویت را از یک مقام عمومی دریافت کنند، که مسئول تحویل گواهی های رمزنگاری شده به هر کنشگر است تا یک ارتباط امن میان دستگاه های پایانی و دلالان برنامه ایجاد شود؛ هدف ایجاد یک بازار برنامه ای IoT مورد اعتماد است، بطوریکه اطلاعات در دستگاه های پایانی بتوانند مبادله شوند تا یک ارتباط امن میان بازار و کاربران ایجاد شود.

در تحقیق [۱۰]، یک معماری امنیتی قابل راه اندازی بر روی سیستم عامل های متحرک برای برنامه های بهداشتی الکترونیکی تعریف شده است. به خصوص، شناسایی برچسب RFID در بافت پزشکی و راه حل های ساخته شده و امن شده ی IoT ترکیب شده اند، تا دسترسی آسان و موجود در همه جا به سوابق مرتبط پزشکی میسر شود، درحالیکه کنترل و امنیت برای تمامی تعاملات فراهم می شود.

همچنین در [۶، ۱۱] فناوری متحرک RFID استفاده شد تا مسائل امنیتی و حریم خصوصی زیر حل شوند: تمامی برچسب های موجود از عملکرد برهم زنی در طراحی پروتکل های RFID پشتبانی نمی کنند و کانال های بین خواننده و سرور همیشه در بافت متحرک امن نیستند. بنابراین، یک پروتکل احراز هویت بسیار سبک و حفظ کننده حریم خصوصی برای سیستم های متحرک RFID تعریف شد، که تنها ازXOR بیتی و چندین مولدهای اعداد شبه تصادفی ساخته شده خاص استفاده می کند. این تحقیق ویژگی های حریم خصوصی متعددی (بطور مثال، ناشناسی برچسب، حریم خصوصی مکان برچسب، حریم خصوصی خواننده، احراز هویت دوجانبه) را فراهم می آورد و از متحمل شدن تعدادی از حملات (بطور مثال، حملات پخش مجدد، حملات عدم همگام سازی) اجتناب می کند.

در تحقیق [۱۲] سیستم های پیشگیری نفوذی –متحرک (m-IPS) کارآمد و امن برای فعالیت های تجاری با استفاده از دستگاه های متحرک برای محاسبه انسان محور پیشنهاد شده است. چنین سیستمی اطلاعات، پروفایل ها و اطلاعات نقشی فضایی و زمانی کاربر را بررسی می کند تا کنترل دسترسی دقیقی را فراهم آورد.

مرجع [۱۳] یک سیستم جمع آوری اطلاعات متحرک را بر مبنای IoT طراحی کرده است، که یک دروازه ی دسترسی را از طریق دستگاه های تلفن های هوشمند پیاده سازی می کند. همچنین، علاوه بر احراز هویت پایانه های متحرک از طریق دروازه، نیقش کلیدی توسط استراتژی جمع آوری انجام می شود که مسیرهای حرکت داده های تاریخی را مشخص می کند تا مشکلزمان بیش از حد طولانی اتصال دستگاه کاهش یابد و کارآمدی انتقال اطلاعات بهبود یابد.

در تحقیق [۱۴]، توجه خاصی به امنیت و تحرک در IoT شده است. در حقیقت، افراد و کمپانی هایی که می خواهند برای داده های شان تامین امنیت کنند از دیوار اتش استفاده می کنند که به ناچار منجر به اختلاف چالش برانگیزی بین امنیت داده و قابلیت استفاده ی آن می شود. از آنجاییکه اکثر محصولات بطور فزاینده ای در حال متحرک شدن هستند، نویسندگان [۱۴] یک استاندارد پیام دهی مدیریت

چرخه زندگی کوانتومی (QLM) را طراحی کرده اند تا رابط های در سطح برنامه ای استاندارد شده و عمومی را فراهم آوردند تا یک ارتباط دو طرفه را از طریق هر نوعی از دیوار آتش، برای مثال برای اجرای کنترل زمان واقعی، تضمین کنند.

یک موتور پردازشگر داده های حسگر متحرک (MOSDEN) در تحقیق [۱۵] ارائه شد که یک میان افزار اجرا شونده در IoT برای دستگاه های متحرک با منابع محدود است (تا به حال بر روی سیستم عامل اندروید ایجاد شد)، که سب جمع آوری و پردازش داده های حسگر بدون تلاش های برنامه نویسی می شود. آن از مکانیزم فشار و کشش جریان داده ای و همچنین متمرکز سازی و پراکنده سازی (بطور مثال نظیر به نظیر) ارتباط داده ای حمایت می کند.

از این رو، از آنجاییکه تعداد زیادی از دستگاه های IoT احتمالا متحرک هستند، یک پروتکل مدیریت تحرک به منظور حفظ اتصال IP لازم است، برای مثال از طریق استاندارد 6LoWPAN، همانطوریکه در [۱۶] پیشنهاد شد. آثار دیگر، همانند [۱۷]، به انتشار ویدئویی کارآمد در برنامه های IoT چند رسانه ای متحرک پرداخته است، درحالیکه [۱۸] تعامل چیزهای هوشمند با فناوری های سنتی وب را از طریق یک سیستم عامل بلوتوث متحرک بررسیکرده است. روابط اجتماعی در گره های متحرک در IoT از طریق یک مدل شناختی در [۱۹] مورد بررسی قرار گرفت، درحالیکه استفاده از NFC برای پرداخت ها از طریق دستگاه های متحرک در محیط به اصطلاح وب اشیاء (WoT) در [۲۰] مورد بررسی قرار گرفت، که یک معماری سبک مبتنی بر رویکردهای RESTful را پیشنهاد کرده است.

در مجموع،اگرچه مسئله امنیتی دستگاه های متحرک (یعنی، شناسایی، احراز هویت، مبادله و ذخیره سازی کلید و گواهی) توسط جوامع علمی تحت بررسی است، راه حل های کنونی تاحدی به رفع این نیازها می پردازند، بنابراین نیازمند تلاش های بیشتری هستیم تا این یکپارچگی با فناوری های IoT ایجاد شود.

منابع

[۱] رزاقی، نسیم،۱۳۹۵،بررسی اینترنت اشیا،کنفرانس بین المللی مهندسی کامپیوتر و فناوری اطلاعات،تهران
[۲]سیارنخجیری، امیر،۱۳۹۸،امنیت در اینترنت اشیاء(IOT) ،سومین کنفرانس ملی ایده های نوین در فنی و مهندسی،رشت،
[۳] J. Mao, L. Wang, Rapid identification authentication protocol for mobile nodes in internet of things with privacy protection, J.Networks ۷ (۷) (۲۰۱۲) ۱۰۹۹–۱۱۰۵.
[٤] A. Jara, V. Kafle, A. Skarmeta, Secure and scalable mobility management scheme for the internet of things integration in the future internet architecture, Int. J. Ad Hoc Ubiquitous Comput. ۱۳(۳-٤) (۲۰۱۳) ۲۲۸–۲٤۲.
[٥] T. Yan, Q. Wen, A secure mobile rfid architecture for the internet of things, in: Proceedings ۲۰۱۰ IEEE International Conference on Information Theory and Information Security, ICITIS ۲۰۱۰, Beijing, China, ۲۰۱۰, pp. ٦۱٦–٦۱۹.
[٦] W. Zhu, J. Yu, T. Wang, A security and privacy model for mobile rfid systems in the internet of things, in: International Conference on Communication Technology Proceedings, ICCT, ۲۰۱۲, pp. ۷۲٦–۷۳۲.
[۷] M. Elkhodr, S. Shanhrestani, H. Cheung, A review of mobile location privacy in the internet of things, in: International Conference on ICT and Knowledge Engineering, Bangkok, Thailand, ۲۰۱۲, pp. ۲٦٦–۲۷۲.
[۸] S. Li, P. Gong, Q. Yang, M. Li, J. Kong, P. Li, A secure handshake scheme for mobile-hierarchy city intelligent transportation system, in: International Conference on Ubiquitous and Future Networks, ICUFN, Da Nang, ۲۰۱۳, pp. ۱۹۰–۱۹۱.
[۹] K.c. Kang, Z.-B. Pang, C.c. Wang, Security and privacy mechanism for health internet of things, J. China Universities Posts Telecommun. ۲۰ (SUPPL-۲) (۲۰۱۳) ٦٤–٦۸.
[۱۰] F. Goncalves, J. Macedo, M. Nicolau, A. Santos, Security architecture for mobile e-health applications in medication control, in: ۲۰۱۳ ۲۱st International Conference on Software, Telecommunications and Computer Networks, SoftCOM ۲۰۱۳, Primosten, ۲۰۱۳, pp. ۱–۸.
[۱۱] B. Niu, X. Zhu, H. Chi, H. Li, Privacy and authentication protocol for mobile rfid systems,Wireless Pers. Commun. ۷۷ (۳) (۲۰۱٤) ۱۷۱۳–۱۷۳۱.
[۱۲] Y.-S. Jeong, J. Lee, J.-B. Lee, J.-J. Jung, J. Park, An efficient and secure m-ips scheme of mobile devices for human-centric computing, J.Appl. Math. Special Issue ۲۰۱٤ (۲۰۱٤) ۱–۸.
[۱۳] J. Geng, X. Xiong, Research on mobile information access based on internet of things, Appl. Mech. Mater. ٥۳۹ (۲۰۱٤) ٤٦۰–٤٦۳.
[۱٤] S. Kubler, K. Frmling, A. Buda, A standardized approach to deal with firewall and mobility policies in the iot, Pervasive MobileComput. (۲۰۱٤).
[۱٥] C. Perera, P. Jayaraman, A. Zaslavsky, D. Georgakopoulos, P. Christen, Mosden: An internet of things middleware for resource constrained mobile devices, in: Proceedings of the Annual Hawaii International Conference on System Sciences, Washington, DC, USA, ۲۰۱٤, pp. ۱۰٥۳–۱۰٦۲.
[۱٦] J. Montavont, D. Roth, T. Nol, Mobile {IPv٦} in internet of things: analysis, experimentations and optimizations, Ad Hoc Netw. ۱٤ (۰) (۲۰۱٤) ۱٥–۲٥.
[۱۷] D. Rosario, Z. Zhao, A. Santos, T. Braun, E. Cerqueira, A beaconless opportunistic routing based on a cross-layer approach for efficient video dissemination in mobile multimedia IoT applications,Comput. Commun. ٤٥ (۰) (۲۰۱٤) ۲۱–۳۱.
[۱۸] J.P. Espada, V.G. Daz, R.G. Crespo, O.S. Martnez, B.P. G-Bustelo, J.M.C. Lovelle, Using extended web technologies to develop bluetooth multi-platform mobile applications for interact with smart things, Inf. Fusion ۲۱ (۰) (۲۰۱٤) ۳۰–٤۱.
[۱۹] J. An, X. Gui, W. Zhang, J. Jiang, J. Yang, Research on social relations cognitive model of mobile nodes in internet of things, J. Network Comput. Appl. ۳٦ (۲) (۲۰۱۳) ۷۹۹–۸۱۰.
[۲۰] T.-M. Gronli, P. Pourghomi, G. Ghinea, Towards NFC payments using a lightweight architecture for the web of things, Computing (۲۰۱٤).