ارائه یک چارچوب مفهومی برای دسته‌بندی تهدیدهای امنیتی در اینترنت اشیاء

حمیدرضا خدمتگزار[۱*]، ساناز قربانلو[۲]
[۱] استادیار پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)، khedmatgozar@irandoc.ac.ir
[۲] پژوهشگر پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)، sghorbanloo@gmail.com

چکیده: یکی از موضوعات مهم در حوزه اینترنت اشیاء، مدیریت مخاطرات امنیت اطلاعات است. یکی از اقدامات کلیدی در این حوزه، شناسایی و تحلیل تهدیدهای امنیتی اینترنت اشیاء است. در این مطالعه مبتنی بر مرور پیشینه و نظر متخصصات چارچوب مفهومی پیشنهادی به منظور دسته‌بندی تهدیدهای امنیتی حوزه اینترنت اشیاء ارائه شده است. مبتنی بر این چارچوب تهدیدهای حوزه اینترنت اشیاء بر پایه معیار انگیزه‌های حملات احتمالی و نوع صدمه به قربانی، در سه دسته اصلی شامل تهدیدهای امنیتی سیستم (شامل سه دسته تهدیدهای دستکاری، اختلالی و تصرفی)، حریم خصوصی (شامل چهار دسته تهدیدهای نظارت ناخواسته/غیرقانونی، نمایه‌سازی کاربر، نفوذ فعال، و ردپای ماندگار)، و اعتماد انعکاسی و شهرت (شامل سه دسته تهدیدهای سوءرفتار موجودیت‌های وابسته، سوءاستفاده از کالا یا خدمات، و ارائه نادرست) جای گرفتند. این چارچوب مفهومی پیشنهادی می‌تواند مورد استفاده پژوهشگران و متخصصان حوزه مدیریت مخاطرات امنیت اطلاعات در حوزه اینترنت اشیاء قرار گیرد.

کلید واژه‌ها: اینترنت اشیاء، امنیت اطلاعات، تهدید

۱- مقدمه

اینترنت اشیاء با سرعت خیلی زیادی درحال رشد است. بنابراین دور از ذهن نیست که در آینده‌ای نزدیک در انتظار یک دنیای فوق‌العاده متصل باشیم. همان‌طورکه اینترنت اشیاء گسترشی از معماری اینترنت است، بسیاری از مسائل دیگر مانند امنیت و حریم‌خصوصی نیز توسط اینترنت اشیاء از اینترنت به ارث گرفته شده است [1]. طبیعی است که ایجاد چنین شبکه‌ای، مخاطرات فراوانی را به همراه دارد. شبکه جهانی اینترنت که از همگانی شدن آن سال‌ها می‌گذرد، هنوز دارای ضعف‌های امنیتی بسیاری است که موجب به خطر افتادن اموال و حتی جان انسان‌ها نیز شده است.

در چنین شرایطی، برقراری امنیت در یک شبکه جهانی از اشیاء که هر کدام با ویژگی‌ها و محدودیت‌های خود به ارتباط با یکدیگر و با انسان‌ها می‌پردازند، طبیعتاً از پیچیدگی بسیار بالاتری برخوردار خواهد بود. شرایط جدید محیط و ویژگی‌های مختلف دستگاه‌ها، سبب می‌شود تا امنیت اینترنت اشیاء به طور ویژه موردتوجه قرار گیرد.

اینترنت اشیاء با تهدیدهای امنیتی جدیدی همراه است که وضعیت کلی مخاطره امنیت اطلاعات را تغییر می‌دهد. اگرچه بکارگیری راه‌حل‌های فناورانه ممکن است به تهدیدها و آسیب‌پذیری‌های اینترنت اشیاء پاسخ دهد، اما امنیت اینترنت اشیاء در درجه اول یک مسأله مدیریتی است. مدیریت مؤثر تهدیدهای مرتبط با اینترنت اشیاء، نیازمند ارزیابی کامل از مخاطرات باتوجه به محیط و تدوین برنامه‌ای برای کاهش تهدیدهای شناسایی شده است. از این‌رو، در این مقاله سعی شده است تا با تحلیل فضاهای تهدید مشخص، یک دسته‌بندی کاربردی در قالب یک چارچوب مفهومی از تهدیدهای اینترنت اشیاء ارائه شود.

۲- مبانی نظری پژوهش

۲-۱- اینترنت اشیاء

اینترنت اشیاء، به اشیایی که به‌طور منحصربه‌فرد قابل شناسایی هستند و نمایش مجازی آن‌ها در ساختاری مانند اینترنت شکل می‌گیرد، اشاره دارد [1]،[2] ،[3] . عبارت اینترنت اشیاء نخستین بار توسط کوین اشتون در سال ۱۹۹۹ و دیوید ال.بروک در سال ۲۰۰۱ مطرح شد [4]،[5] . در جدول ۱ تعاریف متفاوتی از منابع مختلف نقل شده است. با درنظرگرفتن این جدول، اینترنت اشیاء را می‌توان به عنوان پارادایمی فراگیر در محیط‌های متنوع از اشیاء تعریف کرد که از طریق بی‌سیم و یا باسیم قادر به تعامل و همکاری با سایر اشیاء متصل شده به‌منظور ایجاد ارتباطات یکپارچه و ارائه خدمات بافت‌آگاه و نیل به اهداف مشترک باشند.

جدول ۱ تعاریف اینترنت اشیاء

منبع	تعریف
[6]	اشیاء دارای هویت و شخصیت‌های مجازی هستند که در فضای هوشمند با استفاده از واسطهای هوشمند برای اتصال و ارتباط در بافت‌های اجتماعی، محیط زیستی و کاربری فعالیت می‌کنند.
[7]	از لحاظ معنایی، اینترنت اشیاء به معنای یک شبکه جهانی گسترده از اشیاء متصل شده و به‌طور یکتا قابل شناسایی، براساس پروتکل‌های ارتباطی استاندارد است.
[7]	اینترنت اشیاء به مردم و اشیاء این امکان را می‌دهد که در هر زمان و مکانی با هر شیء و شخصی، در حالت ایده‌آل با استفاده از هر مسیر یا شبکه و هر سرویسی، در ارتباط باشند.
[8]	اینترنت اشیاء به نمایش مجازی انواع مختلفی از اشیاء در اینترنت و یکپارچگی آن‌ها در اینترنت یا سرویس‌های مبتنی بر وب می‌پردازد.

۲-۲- امنیت در اینترنت اشیاء

در اینترنت اشیاء، اصطلاح امنیت شامل طیف گسترده‌ای از مفاهیم است که شامل مؤلفه‌های اساسی محرمانگی، احرازهویت، صحت، مجوز، عدم انکار و حتی دسترس‌پذیری اطلاعات و سیستم را نیز دربرمی‌گیرد [10]. همچنین برخی از مفاهیم مانند تشخیص تکراری و به موقع بودن را نیز شامل می‌شود [11].

۲-۳- تهدید

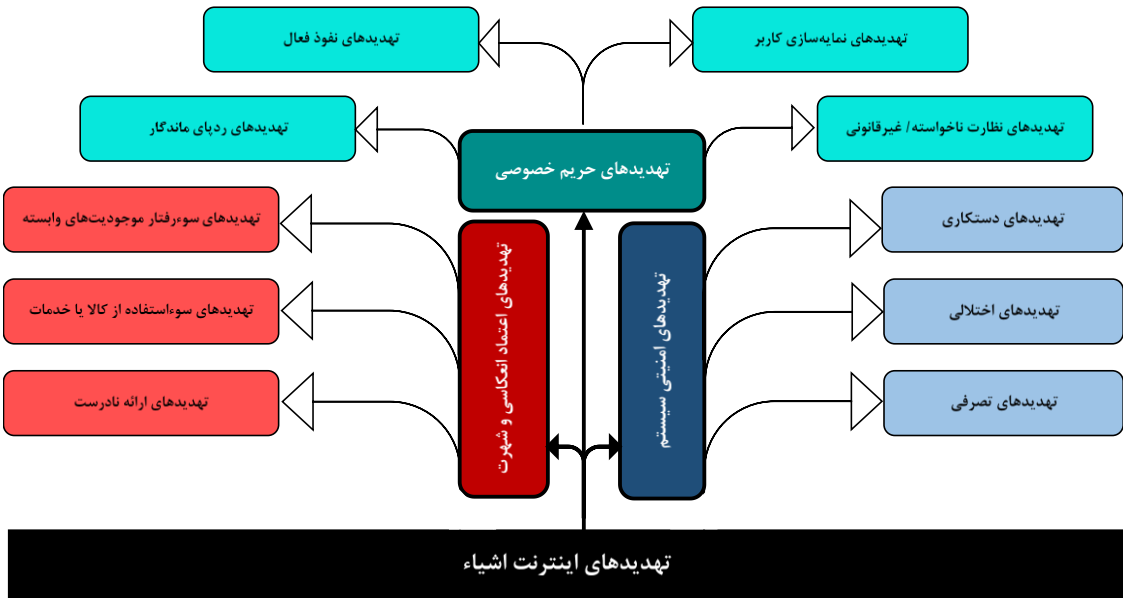
در چارچوب اینترنت، تهدید (یا تهدید سایبری) به‌عنوان "احتمال تلاش مخرب برای مختل کردن یا تخریب یک شبکه یا سیستم رایانه‌ای" تعریف شده است [9]. از دیدگاه امنیت سیستم و اطلاعات، تهدید یک موجودیت (شیء، شخص یا شرایط) است که عمداً یا غیرعمد خطری برای سیستم ایجاد می‌کند [10]. تعریف تهدید برای اینترنت اشیاء می‌تواند شکل گسترده این تعریف باشد. فضای یکپارچه سایبری-فیزیکی، پیامدهای تهدیدهای اینترنت اشیاء را حتی شدیدتر می‌کند، زیرا تحقق آن‌ها ممکن است جهان فیزیکی را نیز تحت تأثیر قرار دهد [10].

۳- روش پژوهش

به منظور شناسایی چارچوب تهدیدهای اینترنت اشیاء، دو گام اصلی مدنظر قرار گرفت. در گام اول مبتنی بر مرور پیشینه چارچوبی اولیه از تهدیدهای اینترنت اشیاء بدست آمد. در گام دوم نیز با برگزاری دو جلسه مصاحبه گروه متمرکز با دو گروه متخصصان حوزه‌های اینترنت اشیاء و همچنین امنیت اطلاعات و سپس تحلیل محتوا، چارچوب پیشنهادی مورد اعتباریابی قرار گرفت و نهایی شد.

۴- چارچوب پیشنهادی

در این چارچوب مفهومی تهدیدها براساس معیار انگیزه‌های حملات احتمالی و نوع صدمه به قربانی دسته‌بندی شده‌اند. شکل ۱ چارچوب تهدید پیشنهادی در حوزه اینترنت اشیاء را به تصویر کشیده است. همان‌طور که در شکل نشان داده شده است، سه دسته کلی از تهدیدهای مطرح برای اینترنت اشیاء پیشنهاد شده است که در ادامه شرح داده خواهد شد:



شکل ۱: چارچوب مفهومی پیشنهادی دسته‌بندی تهدیدهای اینترنت اشیاء

تهدیدهای امنیتی سیستم، هر فعالیت بالقوه‌ای که ممکن است به صورت عمدی یا غیرعمدی ارکان امنیت را نقض کند و اشیاء را به صورت فردی یا کل یک شبکه را به خطر بیاندازد به‌عنوان یک تهدید امنیتی سیستم برای اینترنت اشیاء شناخته می‌شود [10]. با الهام از [12]، تهدیدهای امنیتی سیستم را می‌توان براساس اهداف حملات سایبری به سه دسته تهدیدهای تصرفی، تهدیدهای اختلالی و تهدیدهای دستکاری دسته‌بندی کرد.

تهدیدهای تصرفی، شامل تهدیدهایی است که منجر به کنترل مهاجم بر یک بخش فیزیکی یا منطقی زیرساخت اینترنت اشیاء یا دسترسی به اطلاعاتی که در سیستم ذخیره می‌شود، خواهد شد. تهدیدهای تصرفی ممکن است خسارت فوری یا مستقیم بر قربانی نداشته باشند. با این وجود، مفاهیم ضروری امنیت، یعنی محرمانگی داده (کسب‌وکار کنترل) و استفاده برای افراد دارای دسترسی مجاز را نقض می‌کند. علاوه‌براین، چنین کنترل یا دسترسی غیرمجازی، شانس تهدیدها شدیدتر و فعال‌تر، مانند اختلال، تخریب، انکار یا تخریب عملکرد هدف را بیشتر می‌کند. برای مثال، اگر مهاجم کنترل یک کنترل‌کننده شبکه هوشمند را در دست بگیرد، می‌تواند اطلاعات مربوط به مصرف برق هر مکان یا حتی تک‌تک لوازم منزل را مشاهده کند. در حقیقت، افشای اطلاعات خصوصی مانند الگوهای مصرف برق هر وسیله خانگی ممکن است مهاجم را قادر سازد تا به راحتی از اطلاعات برای اهداف مخرب استفاده کند.

تهدیدهای اختلالی شامل تهدیدهای مستقیمی است که از طریق حملات به منظور اختلال، تضعیف، انکار سرویس و نابودکردن سیستم هدف، باعث آسیب‌رساندن به سیستم و ذی‌نفعان می‌شود. برای مثال اگر کنترل‌کننده هوشمند شبکه توسط یک مهاجم تصرف شود، می‌تواند با تغییر عملکرد شبکه هوشمند، باعث اختلال در سیستم توزیع برق یا سیستم شارژ شود، یا باعث خراب‌کاری در منبع تغذیه برق شود، و یا حتی کل سیستم را خاموش کند.

تهدیدهای دستکاری شامل تهدیدهای اثرگذار بر چرخه تصمیم‌گیری هدف است [13]. در حقیقت یک تهدید دستکاری ممکن است خراب کردن داده قبل از ورود به سیستم اینترنت اشیاء باشد. در این حالت، حتی اگر محیط داخلی اینترنت اشیاء امن و کارآمد باشد، نگرانی‌های امنیتی همچنان ممکن است به دلیل اقدامات سیستم صحیح براساس اطلاعات نادرست افزایش یابند. برای مثال در یک سیستم گرمایش مرکزی برای یک خانه، کسی می‌تواند چرخه تصمیم‌گیری کنترل‌کننده را به سادگی با نگه داشتن یک فندک روشن در مقابل سنسورهای ترموستات، برای تشخیص و گزارش افزایش دمای غیرطبیعی تغییر دهد. براساس اطلاعات نادرست دریافت شده از این سنسور، کنترل‌کننده ممکن است دمای خانه را به شدت کاهش دهد تا دمای موردنیاز را حفظ کند. شکل نهایی تهدیدهای دستکاری زمانی خواهد بود که یکپارچگی و صحت داده‌های انتقالی بین دو موجودیت، به دلیل دخالت غیرمجاز دستکاری می‌شود. حملاتی مانند حمله شخص میانی[۱]، بازپخش[۲] و جعل[۳]، تهدیدهایی برای یکپارچگی و صحت داده هستند.

تهدیدهای حریم خصوصی شامل پنهان‌سازی اطلاعات شخصی و همچنین توانایی کنترل آنچه با این اطلاعات اتفاق می‌افتد، است [14]. براساس گزارش منتشرشده از سوی [15] در ارتباط با تعاریف حریم خصوصی، [10] تهدید حریم خصوصی را به عنوان یک رویداد احتمالی از افشای اطلاعات حساس به موجودیت‌هایی (شخص، شرکت، یا هوش مصنوعی) تعریف می‌کند که مجاز به داشتن آن نیستند یا نیازی به داشتن آن ندارند. این می‌تواند به شکل داده‌های غلط در اختیار موجودیت‌های غیرمجاز یا داده‌های بیشمار در اختیار موجودیت‌های مجاز باشد. تهدیدهای حریم خصوصی ممکن است بر صاحب واقعی داده تأثیر جدی و مؤثری نداشته باشند. در چارچوب پیشنهادی چهار نوع تهدید در این دسته جای گرفته‌اند که در ادامه شرح داده خواهد شد.

تهدیدهای نظارت ناخواسته/ غیرقانونی، اینترنت اشیاء می‌تواند به راحتی توسط یک گروه مخرب برای نظارت غیرقانونی مورد سوءاستفاده قرار گیرد. برای مثال یک فرد خرابکار می‌تواند از طریق دوربین‌هایی که در اسباب‌بازی‌ها نصب شده‌اند بر کودکان نظارت کند، حرکت افراد را از طریق سیستم تعبیه شده در کفش‌های هوشمند آنان رصد کند، و یا ورود و خروج اعضای یک خانواده را با متصل شدن به قفل درب خانه متصل به اینترنت و استفاده از منبع برق از طریق کنترل‌کننده‌های هوشمند تشخیص دهد.

تهدیدهای نمایه‌سازی کاربر می‌تواند به‌عنوان جمع‌آوری، تطبیق و تجزیه‌وتحلیل داده‌های کاربر تعریف شود که شناسایی، جدسازی، طبقه‌بندی و تصمیم‌گیری در مورد کاربر را تسهیل می‌کند. برای مثال فرض کنید یک بیمار مبتلا به بیماری قلبی دارای یک

[۱] Man-in-the-middle attack
[۲] Replay attack
[۳] Spoofing attack

دستگاه ضربان‌ساز بلوتوث است. هنگامی که دستگاه ضربان‌ساز ریتم نامنظمی را تشخیص می‌دهد، به تلفن همراه اطلاع می‌دهد. تلفن همراه پیشنهاد می‌کند که بیمار بنشیند، سپس به بیمارستان اطلاع داده و یک آمبولانس را فرا می‌خواند. در همین حال بیمار در زمان تلاش برای استراحت، تبلیغاتی را درباره داروهای شگفت‌انگیز برای بیماری‌های قلبی در گوشی خود دریافت می‌کند.

تهدیدهای نفوذ فعال، به نقض‌های امنیتی یا حریم خصوصی در یک شرکت یا فرد اشاره دارد که می‌تواند به عواقب فاجعه‌بار منجر شود. برای مثال در حالی که شما در حال رانندگی یک ماشین هوشمند هستید، هکرها قادر به نفوذ به سیستم‌عامل آن هستند و اطلاعاتی را که در داشبورد نشان داده می‌شود را دستکاری می‌کنند تا سرعت را پایین‌تر یا بیشتر از سرعت واقعی خودرو نشان دهند، اطلاعات سوخت را دستکاری می‌کنند و یا حتی بدتر از آن، کیسه‌های هوا را بدون رخ دادن تصادف فعال می‌کنند و یا فرمان خودروی در حال حرکت را می‌چرخانند.

تهدیدهای ردپای ماندگار، احتمال سوءاستفاده از شیء هوشمند حذف شده را برای انجام برخی از اقدام‌های مخرب درنظر می‌گیرد. برای مثال، هنگامی که افراد اشیاء هوشمند را جمع‌آوری می‌کنند، آن‌ها یک پایگاه اطلاعاتی مرتبط با هویت خود را در سیستم‌های اطلاعات شرکت ایجاد می‌کنند. این ارتباط ممکن است حتی پس از حذف آن شئ نیز ادامه یابد.

تهدیدهای اعتماد انعکاسی و شهرت، این تهدیدها شامل هیچ‌گونه نفوذ در سیستم اصلی که امن است، نیستند. در واقع، ممکن است هیچ ارتباطی بین مهاجم و زیرساخت اصلی وجود نداشته باشد. این تهدیدها از نارسایی‌های موجود در رابط کاربری بین سیستم اینترنت اشیاء و کاربران، همچنین وابستگی یک ارائه‌دهنده خدمت به عوامل دیگر برای ارائه خدمات خود به کاربران سوءاستفاده می‌کنند. تهدیدهایی که در ذیل این دسته تعریف می‌شوند عبارتنداز:

تهدیدهای ارائه نادرست، در اکوسیستم اینترنت اشیاء کاربران توسط موجودیت‌هایی فریب می‌خورند که غیرقانونی هستند و به دروغ خود را به‌عنوان نماینده یک شرکت، ارائه‌دهنده خدمات یا سازنده دستگاه معرفی می‌کنند تا به مناقع شخصی دست پیدا کنند، حریم خصوصی کاربران را نقض کنند و یا حداقل یک تجربه کاری ناخوشایند را به کاربر ارائه دهند. در چنین مواردی، شهرت موجودیت واقعی که به نادرستی نمایانده شده‌است، دچار خدشه می‌شود. این نوع تهدید مشابه حملات فیشینگ در تعاملات وب است [16]. در یک حمله فیشینگ، مهاجم تلاش می‌کند تا اطلاعات حساس (مانند اطلاعات ورودی، جزئیات کارت اعتباری) را با وانمود کردن اینکه یک موجودیت قابل اعتماد است، به دست آورد. کاربران قربانی از طریق ارتباطاتی که ادعا می‌شود از وب‌سایت‌های اجتماعی، مؤسسات مالی و یا پورتال پرداخت آنلاین معتبر، هستند مورد کلاهبرداری قرار می‌گیرند.

تهدیدهای سوءاستفاده از کالا یا خدمات، اعتبار یک ارائه‌دهنده خدمات همچنین می‌تواند توسط استفاده از خدمات یا محصولاتش توسط یک موجودیت خارجی برای انجام فعالیت‌هایی که امنیت، حریم خصوصی و حتی شهرت افراد را نقض می‌کند، تضعیف شود. این تهدیدها می‌توانند اثرات منفی بر شهرت و موقعیت مالی ارائه‌دهندگان خدمت، به رغم عدم وجود کاستی در محصولات یا خدماتشان داشته باشند. برای مثال، کاربران خرابکار ممکن است از دستگاه‌هایی مانند عینک گوگل یا ساعت‌های هوشمند سوء استفاده کنند تا اطلاعات را از مکان‌هایی که چنین فعالیت‌های غیرقانونی یا غیرمجاز هستند، جمع‌آوری کنند. این موارد نقض حریم خصوصی ممکن است به تهدیدهای امنیتی و یا تهدیدهای شهرت تبدیل شوند.

در تهدیدهای سوءرفتار موجودیت‌های وابسته، استحکام امنیت و حریم خصوصی ارائه‌دهنده خدمات تحت تأثیر عملکرد موجودیت‌های مرتبط قرار می‌گیرد. کیفیت امنیت و حفظ حریم خصوصی حوادث مرتبط با موجودیت‌های مرتبط ممکن است تحت نظر ارائه‌دهنده خدمات قرار نگیرد. اگر رفتار این موجودیت‌ها ناسازگار یا مخرب باشد، در نهایت عملکرد و شهرت ارائه‌دهنده خدمات را تضعیف خواهد کرد.

۵- نتیجه‌گیری

در ادبیات حوزه امنیت اطلاعات، دارایی اطلاعاتی هر آن چیزی تعریف شده است که در تولید، پردازش، انتقال و استفاده اطلاعات مورد استفاده قرار می گیرد و برای سازمان مهم است. یکی از انواع این دارایی‌ها، دارایی‌های اطلاعاتی کاربردی در حوزه اینترنت اشیاء هستند. از سوی دیگر مبتنی بر ادبیات این حوزه، یک حادثه امنیت اطلاعات هنگامی رخ می‌دهد که یک تهدید از یک یا چند آسیب‌پذیری استفاده می‌کند و به یک یا چند دارایی اطلاعاتی صدمه وارد می‌کند. یک حادثه بالقوه با نام مخاطره امنیت اطلاعات معرفی شده است [17]. بنابراین یکی از اجزای مهم در حوزه مدیریت مخاطره امنیت اطلاعات شناسایی و دسته‌بندی تهدیدها است. در این پژوهش چارچوبی پیشنهادی برای دسته‌بندی

تهدیدهای موجود در اینترنت اشیاء پیشنهاد شد. در این چارچوب تهدیدهای فضای اینترنت اشیاء در سه دسته اصلی تهدیدهای امنیت سیستم، حریم خصوصی و اعتماد انعکاسی و شهرت جای گرفتند.

در مجموع این پژوهش پنجره‌های تازه‌ای برای پژوهش‌های میان‌رشته‌ای در شناسایی و دسته‌بندی تهدیدهای اینترنت اشیاء باز می‌کند. تمرکز بر پژوهش به منظور توسعه دسته‌بندی ارائه انجام شده در این چارچوب می‌تواند مورد توجه پژوهشگران این حوزه قرار گیرد.

مراجع

[1] S. Misra, M. Maheswaran and S. Hashmi, Security challenges and approaches in internet of things, Cham: Springer International Publishing, 2017.

[2] A. Arabsorkhi, M. Haghighi and R. Ghorbanloo, "A conceptual trust model for the internet of things interactions," in *In 2016 8th International Symposium on Telecommunications (IST)*, 2016.

[3] "ETICA: Ethical Issues of Emerging ICT Applications," 2014.

[4] J. Van Den Hoven, Â. Guimarães Pereira, F. Dechesne, J. Timmermans and H. Vom Lehn, "Fact Sheet-Ethics Subgroup IoT-Version 4.0," *Delft University of Technology, Chair Ethics Subgroup IoT Expert Group*, 2012.

[5] L. Atzori and I. a. G. Morabito, "The internet of Things: A survey," *Computer Network*, vol. 54, no. 15, pp. 2787-2805, 2010.

[6] H. Sundmaeker, P. Guillemin, P. Friess and S. Woelfflé, "Vision and challenges for realising the Internet of Things," *Cluster of European research projects on the internet of things, European Commision*, vol. 3, no. 3, pp. 34-36, 2010.

[7] L. Tan and N. Wang, "Future internet: The internet of things," in *In 2010 3rd international conference on advanced computer theory and engineering (ICACTE)*, 2010.

[8] A. Bassi, G. H. Sintef and E. Hitachi, "Internet of Things in 2020: A Roadmap for the future," European Commission/ EPoSS Expert workshop on RFID/ Internet of Things, Brussels, 2008.

[9] "Internet of Things," *World Wide Web Consortium (W3C)*, 2014.

[10] "Oxford Dictionaries Online," 2014.

[11] O. Garcia-Morchon, S. Kumar, S. Keoh, R. Hummen and R. Struik, "Security Considerations in the IP-based Internet of Things draft-garciacore-security-06," *Internet Engineering Task Force*, 2013.

[12] M. Covington and R. Carskadden, "Threat implications of the internet of things," in *In 2013 5th International Conference on Cyber Conflict (CYCON 2013)*.

[13] S. Applegate, "The principle of maneuver in cyber operations," in *In 2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 2012.

[14] "Privacy, 2014; http://plato.stanford.edu/entries/privacy/," 2014.

[15] "Privacy and Security, 2014; http://msdn.microsoft.com/en-us/library/ms976532.aspx," 2014.

[16] Z. Ramzan, "Phishing Attacks and Countermeasures," *Handbook of information and communication security*, pp. 433-448, 2010.

[17] International Organization for Standardization, "IOS/IEC 27005- Information technology — Security techniques — Information security risk management," International Organization for Standardization, 2018.