طراحی مدلی به منظور امنیت اطلاعات و حفظ حریم خصوصی در اینترنت اشیاء

تاریخ دریافت: ۱۳۹۶/۱۱/۲۴ تاریخ پذیرش: ۱۳۹۷/۰۲/۰۲

محمد جمالو،[۱] علی رجب زاده قطری،[۲] رضا رادفر[۳]

از صفحه ۲۱ تا ۴۸

چکیده

زمینه و هدف: اینترنت اشیاء یک پارادایم جدید است که ایده اولیه آن بر اساس تعامل مستمر انواع چیزهایی که در اطراف ما هستند ایجاد شده است، این تعامل مستمر باعث به خطر افتادن امنیت اطلاعات و حریم خصوصی افراد گردیده، زیرا سازوکارهای مؤثری برای شخصی‌سازی حریم خصوصی در این پارادایم، پیاده‌سازی نشده است.

روش شناسی: ابتدا از طریق مطالعه پژوهش‌های گذشته، شناخت نسبتاً جامعی در خصوص پژوهش به دست آمده و مدل مفهومی اولیه طراحی گردید، سپس با استفاده از روش دلفی در چهار مرحله، مدل مورد ارزیابی خبرگان قرار گرفت و پس از به‌روزرسانی و اصلاح، مدل ثانویه ارائه شد.

یافته‌ها: بیش از ۵۰درصد خبرگان، تقسیم‌بندی سه گانه مدل اولیه و عوامل اصلی تأثیرگذار در امنیت اطلاعات و حریم خصوصی افراد را در هر طبقه، تائید نمودند. همچنین ضریب هماهنگی کندال برای پاسخ‌های اعضاء، در دور چهارم ۰/۵۲۲ بود، که با توجه به اینکه تعداد اعضای نشست بیش از ۲۲ نفر است این میزان از ضریب کندال، کاملاً معنادار به حساب می‌آید.

نتیجه‌گیری: این پژوهش با در نظر گرفتن ابعاد مختلف حریم خصوصی و کیفیت داده‌های محتوایی و الزامات آن‌ها در پارادایم اینترنت اشیاء، مدل مفهومی ارائه نمود، که بر اساس آن، امکان شخصی‌سازی «حریم خصوصی» و «کیفیت داده‌ها» فراهم گردیده و امنیت اطلاعات در اینترنت اشیاء افزایش می‌یابد و براساس نظر خبرگان، مدل اولیه تأیید شده و پس از اصلاح به‌روزرسانی، مدل ثانویه ارائه گردید.

واژه‌های کلیدی: اینترنت اشیاء، حریم خصوصی، کیفیت داده‌های محتوایی، اعتماد.

۱- دانشجوی دکتری مدیریت فناوری اطلاعات، دانشکده مدیریت، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، تهران، ایران.
۲- دانشیار گروه مدیریت صنعتی، دانشگاه تربیت مدرس، تهران، ایران (نویسنده مسئول) alirajabzadeh@gmail.com
۳- استاد گروه مدیریت صنعتی، دانشکده مدیریت دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، تهران، ایران.

مقدمه

اینترنت اشیاء در بازه زمانی بین سال‌های ۲۰۰۸ و ۲۰۰۹ متولد شده است و پیش‌بینی می‌شود تعداد ابزارهای متصل در سال ۲۰۲۰ به ۵۰ میلیارد برسد(ایوانس،[۱] ۲۳۲:۲۰۱۱).

در چنین شرایطی توجه به مکانیزم‌های امنیتی اهمیت ویژه‌ای یافته است و نگرانی‌های زیادی برای به خطر افتادن حریم خصوصی به وجود آمده، تا آنجایی که به عقیده بسیاری از پژوهشگران موفقیت و رشد بیشتر اینترنت اشیاء در آینده، در گرو رفع این نگرانی‌ها می‌باشد.

به عنوان مثال در یکی از کلان شهرهای اروپایی برنامه ضد آلودگی هوا در حال اجرا می‌باشد و شهرداری در نقاط مختلف شهر و حومه‌ی آن، ایستگاه‌های دوچرخه قرار داده که افراد می‌توانند از آن‌ها به مدت دو ساعت و به صورت رایگان دوچرخه دریافت کنند.

هر دوچرخه به یک سیستم متمرکز با نام «bike&all» برای کنترل دوچرخه‌ها متصل است و در آن مجموعه‌ای از برنامه‌های کاربردی فراگیر که از جدیدترین حسگرها و فنّاوری‌های مخابراتی استفاده می‌نمایند، وجود دارد (مارکز،[۲] ۱۲۲:۲۰۱۵). به‌منظور جذاب کردن این سیستم برای شهروندان، به دوچرخه‌سواران امکان بهینه‌سازی زمان و لذت بردن هر چه بیشتر از تجربه‌ی دوچرخه‌سواری، با توجه به تمایلات هر یک از افراد در این سیستم ارائه می‌گردد. شهر با استفاده از تعداد زیادی حسگر[۳] به‌منظور تشخیص شرایط محیطی، حضور دوچرخه‌سواران و تصادفات تجهیز شده است. ازآنجا که اغلب شهروندان دارای یک گوشی هوشمند با قابلیت مکان‌یابی و حسگرهای دیگر هستند، سیستم از این قابلیت‌ها به‌منظور ارتباط با کاربران و دریافت اطلاعات آن‌ها استفاده می‌کند. هر چراغ راهنمایی دارای حسگری است که عبور دوچرخه را تشخیص داده و این اطلاعات را به سیستم مرکزی ارسال می‌کند تا از این طریق حجم ترافیک در یک خیابان برای سیستم قابل محاسبه باشد.

۱- Evans
۲- Marquez
۳- Sensor

این سطح از تعامل مستمر انواع چیزهایی که در اطراف انسان‌ها هستند باعث به خطر افتادن امنیت اطلاعات و حریم خصوصی افراد گردیده است، زیرا سازوکارهای مؤثری برای شخصی سازی حریم خصوصی در این پارادایم، پیاده سازی نشده است.

به عنوان مثال: آقای دیوید[۱] در حال راندن دوچرخه به سمت بازگشت به خانه است. او تصمیم می‌گیرد که مکان دقیق خود را به آشنایانش درصورتی‌که به او نزدیک هستند اعلام کند و آن‌ها را در بین مسیرش ببیند. سیستم با استفاده از موقعیت مکانی آقای دیوید و موقعیت مکانی آشنایانش یک مسیر جدید را محاسبه و پیشنهاد می‌دهد، مسیری که دوستانش می‌توانند به او ملحق شده و با هم حرکت کنند و یا برعکس، مسیر جدیدی که در آن‌ها با هم روبه‌رو نشوند. سیستم به منظور شناخت آشنایان آقای دیوید، از لیست مخاطبان گوشی هوشمند او استفاده می‌کند. بنا به دلایل مرتبط با حریم خصوصی، آقای دیوید نمی‌خواهد که این قضیه برای تمام اعضای لیست مخاطبانش صدق کند، بنابراین او نیاز دارد تا این امکان در سیستم فراهم شود تا اعضای لیست مخاطبانش را در گروه‌های متفاوت دسته‌بندی کرده و برای هر گروه، سطوح مختلفی از کیفیت و رزولیشن محتوایی داده‌ها[۲] در مورد موقعیت مکانی‌اش ارائه نماید. برای نمونه، دوستان نزدیک او مکان دقیقش را دریافت کنند، برخی از همکارانش یک موقعیت مکانی باکیفیت پایین (برای مثال با خطای $\pm$ ۱۰km) دریافت نمایند و سایر افراد لیست مخاطبانش اصلاً موقعیت مکانی‌ای دریافت نکنند.

مثال فوق، تنها نمونه‌ای از نیاز به تبیین و ارائه مدل‌های جدید ارتباطی، به جهت حفظ حریم خصوصی و امنیت اطلاعات افراد در اینترنت اشیاء می‌باشد و با در نظر گرفتن تنوع اشیائی که پیرامون افراد را فراگرفته‌اند و تنوع الزامات حریم خصوصی و امنیت اطلاعات برای هریک از آن‌ها و صاحبانشان، اهمیت و پیچیدگی مدل بیش از پیش نمایان می‌گردد.

۱- Daivid
۲- QOC

بیان مسأله

اینترنت اشیاء یک پارادایم جدید است که ایده اولیه آن بر اساس تعامل مستمر انواع چیزهایی که در اطراف ما هستند ایجاد شده است، این تعامل مستمر در به اشتراک‌گذاری داده‌ها، که تقریباً در تمامی ابعاد زندگی انسان‌ها وجود دارد، باعث به خطر افتادن حریم خصوصی افراد گردیده، زیرا سازوکارهای مؤثری برای شخصی‌سازی حریم خصوصی و حفاظت گسترده از امنیت اطلاعات، وجود ندارد. علاوه بر این، دغدغه‌های مصرف‌کنندگان محتوا در خصوص کیفیت داده‌های محتوایی نادیده گرفته شده و چالش بین «حریم خصوصی تولیدکننده محتوا» و «کیفیت داده‌های محتوایی مصرف کننده محتوا» همچنان باقی است.

با توجه به گستردگی دامنه استفاده از اینترنت اشیاء و برنامه‌های متعدد کاربردی آن در حوزه‌های گوناگون مثل برنامه‌های روزمره، رفتارها، مسائل بهداشت و یا مسائل عاطفی، ضرورت و پیچیدگی توجه به موضوعات مرتبط با حریم خصوصی و امنیت اطلاعات در این فضا بیش از پیش مورد توجه همگان قرار گرفته است.

این پژوهش بر آن است تا با در نظر گرفتن ابعاد مختلف حریم خصوصی و کیفیت داده‌های محتوایی و الزامات آن‌ها، به مدل‌سازی چهارچوب اینترنت اشیاء بپردازد تا امکان شخصی‌سازی «حریم خصوصی» و «کیفیت داده‌های محتوایی» تولیدکنندگان و مصرف‌کنندگان محتوا در اینترنت اشیاء فراهم گردد.

مبانی نظری پژوهش

اینترنت اشیاء: تا پیش از این، تصور عموم مردم این بود که تنها این انسان‌ها هستند که قرار است با ابزارهایی که در اختیار دارند توسط شبکه اینترنت به هم متصل شوند و شخصاً از قابلیت‌های آن بهره ببرند. اما بیش از یک دهه است که مفاهیم جدیدی شکل گرفته است. این مفاهیم در چند سال اخیر در قالب محصولات هوشمند به بازار راه پیدا کرده‌اند. اکنون در مورد ایده‌هایی صحبت می‌کنیم که بر اساس آن هر شی فیزیکی قادر است با اتصال به اینترنت یا به کمک سایر ابزارهای ارتباطی، با سایر

اشیاء تعامل داشته باشد. عبارت اینترنت اشیا، برای اولین بار در سال ۱۹۹۹ توسط کوین اشتون[۱] مورد استفاده قرار گرفت.

او جهانی را توصیف کرد که در آن هر چیزی، از جمله اشیاء بی‌جان، برای خود هویت دیجیتال داشته و به کامپیوترها اجازه دهند آن‌ها را سازماندهی و مدیریت کنند. او ابتدا که اینترنت اشیاء را پایه نهاد، احتمالاً تنها استفاده از چیپ‌های شناسایی مبتنی بر فرکانس‌های رادیویی، موسوم به ار.اف. ای دی را در ذهن داشت. پس از گذشت حدود ۱۵ سال ایده بنیادین «کوین اشتون»، جنبه‌های عملی‌تر و گسترده‌تری به خود گرفته است.

اساس داستان این است که دستگاه‌ها (اشیاء) در یک پلتفرم عظیم با کمک حسگرهای مختلف به جمع‌آوری اطلاعات پرداخته و از طریق ترکیبی از تکنولوژی‌های ارتباطی زمان خود (به طور مثال زمانی ار.اف. ای دی[۲] و زمانی وای فای[۳]) با یکدیگر به تبادل داده بپردازند (ایوانس،[۴] ۲۳۲:۲۰۱۱).

حریم خصوصی:[۵] پذیرش حریم خصوصی به عنوان یک حق انسانی ریشه‌ای تاریخی دارد. در انجیل و قوانین یهود و در چین باستان مصونیت‌هایی در این زمینه وجود داشته است (بروجردی،[۶] ۲۰۲:۲۰۰۴). برخی نویسندگان سابقه این حق را به دوران رم و یونان باستان نسبت می‌دهند و منشأ آن را همان لزوم رعایت حق مالکیت نسبت به اموال مادی می‌دانند (محسنی،[۷] ۱۴۰:۲۰۰۱). اولین بار که نظریه حریم خصوصی و تقاضای حمایت از آن مطرح شد، تا حدودی ناشی از سوء استفاده مطبوعات و رفتارهای مداخله‌گرایانه روزنامه‌نگاران، در زندگی خصوصی افراد بود (هارلو،[۸] ۱۴۵:۲۰۰۳). اینترنت رسانه ایده‌آل نشر الکترونیکی با سه ویژگی قابلیت تعامل، سرعت عمل و نامحدود بودن فضاست (وارد،[۹] ۲۳۲:۲۰۰۵). که در آن کاربران، مخاطبان مراوده‌ای

۱- Kevin Ashton
۲- RFID
۳- Wi-Fi
٤- Evans
٥- Privacy
٦- Borojerdi
۷- Mohseni
۸- HarLow
۹- Ward

هستند که با یکدیگر تعامل مشترک و رابطه‌ای کاملاً دوسویه دارند (ام سی کوالی،[1] ۱۴۸:۲۰۰۴). شبکه‌های رایانه‌ای تاکنون چالش‌های اجتماعی شدیدی در حوزه مالکیت معنوی و حریم خصوصی ایجاد کرده‌اند. با آن‌که فناوری و خدمات رایانه‌ای دائماً در حال تکامل‌اند بسیاری از این چالش‌ها همچنان باقی مانده‌اند به همین دلیل دولت‌ها باید اهداف، اصول و ارزش‌هایی را تعریف کنند که نظام‌های ارتباطی‌شان را فعال سازد (استین و سینها،[2] ۹۸:۲۰۰۶). خط و مشی حریم خصوصی در یک ارائه دهنده خدمات اینترنت، رعایت مسائل مرتبط با استفاده از اطلاعات شخصی کاربران می‌باشد (کوستا و دامورتییر،[3] ۱۶۸:۲۰۰۸).

امنیت در اینترنت اشیاء: اینترنت اشیاء بخشی جدایی‌ناپذیر از آینده اینترنت است. پروتکل‌های ارتباطی جدید هم به عنوان بنیاد این شبکه پیچ درپیچ ایفای نقش می‌کنند. وظیفه این پروتکل‌ها این است که تعامل و یکپارچگی کامل اشیاء مجازی و فیزیکی جهان پیرامون‌مان را تضمین کنند. کامپیوترها، گوشی‌ها، تلویزیون‌ها، حسگرها، خودروها، یخچال‌ها، حتی بسته‌های غذا و دارو، در این شبکه متشکل از اشیاء قرار می‌گیرند.

لیکن خطراتی در خصوص اینترنت اشیاء وجود دارد و به همین دلیل نمی‌توان امنیت آن را صد در صد دانست. در اینترنت اشیاء دستگاه‌ها اطلاعاتی را فرستاده و دستوراتی را دریافت می‌کنند، از این رو نفوذ هکر و سوءاستفاده آن چندان هم دور از انتظار نیست. اخیراً آزمایشگاه مکآفی اینتل گزارش امنیتی را ارائه کرده است که طی آن به خطراتی که دستگاه‌های اینترنت اشیاء را تهدید می‌کنند، اشاره کرده است. در این گزارش آمده که با افزایش دستگاه‌های متصل به هم در اینترنت اشیاء، خطر نفوذ هکرها نیز افزایش می‌یابد، شاید برخی دستگاه‌ها از امنیت کافی برخوردار نباشند (ایوانس،[4] ۲۳۵:۲۰۱۱).

در کنفرانس هکرهای کلاه سفید سال ۲۰۱۳، محققان امنیتی نشان دادند که چگونه دوربین‌های امنیتی به راحتی هک می‌شوند. هنگامی که هکرها نفوذ کردند می‌توانند ویدئوهای ضبط شده را سرقت کرده و به شبکه کل دوربین‌ها نفوذ کنند. در

۱- MCQuail
۲- Stein and Sinha
۳- Kosta and Dumortier
٤- Evans

سال۲۰۱۴ هکرهایی توانستند به دوربین‌های موجود در اتاق کودکان نفوذ کرده و از این طریق ترس و وحشت را در آن‌ها ایجاد کردند.

به هر صورت مسئله حریم خصوصی در اینترنت اشیاء بسیار پیچیده‌تر از ارتباطات اینترنت است، زیرا اساس ارتباطات در اینجا به صورت دوسویه و چند سویه بوده و شکل سابق ارائه‌کننده محتوا از بین رفته است، لذا حریم خصوصی در اینترنت اشیاء می‌بایست بیان کند مدیریت داده‌های محتوایی جمع‌آوری شده برای بخش مصرف‌کننده محتوا نیز باشد.

پیشینه پژوهش

پژوهش‌های انجام شده در حوزه حریم خصوصی و امنیت اطلاعات بیشتر متمرکز بر فرآیندهای رمزنگاری اطلاعات بوده است.

- در سال ۲۰۱۳ تحقیقی با عنوان «امنیت مشترک در اینترنت اشیاء»[۱] در دانشگاه یو پی ام اس[۲] پاریس انجام گردیده است. این تحقیق بر ارتباط پایان به پایان امن[۳] تمرکز دارد و پیشنهاد می‌نماید کلید امنیتی مشترکی بین هر دوطرف در اینترنت اشیاء طراحی گردد. در این تحقیق، روش‌های گروهی جدیدی، برای طراحی کلید دسترسی به منظور کاهش الزامات در پروتکل‌های امنیتی موجود برای پشتیبانی شدن دستگاه‌ها با منابع محدود پیشنهاد شده است. این رساله، نگه‌داشتن نشانه «پروتکل امنیتی لایه انتقال[۴]» در مبادله کلید اینترنت و «پروتکل‌های شناسایی میزبان بر اساس تبادل پایه‌ای[۵]» را به عنوان بهترین پشتیبان برای پر کردن الزامات امنیتی پایان به پایان در اینترنت اشیاء معرفی می‌کند. این پژوهش اقدام به طراحی مجدد این کلیدها نموده است به صورتی که رقیب محدود شده امکان دارد، با احتمال کمتری در فضای ناهمگن گره‌ها در اینترنت اشیاء، در گره‌های محدود که در همسایگی قرار دارند، بارگذاری نماید. سطح اعتماد درونی در یک گره، به وسیله بررسی مکانیزم‌های امنیتی شناخته

۱- Access Control in IoT/M۲M – Cloud Platform
۲- UPMC
۳- end to end SECURE
٤- Transport Layer Security(TLS)
٥- Host Identity Protocol base exchange (HIP BEX)

شده به عنوان سیستم مدیریت اعتماد تخمین زده می‌شود. این هدف‌های سیستم، رفتارهای گره‌ها را برای یافتن عناصر غیر قابل اعتماد و انتخاب گره‌های قابل اطمینان برای کمک به سرویس‌های گروهی پیگیری می‌کند. در عوض یک سیستم مدیریت اعتماد، بر اساس یک پایه هماهنگی گروهی عمل می‌کند، به صورتی‌که چندین گره، اسنادی را درباره اعتمادشان به دیگری به اشتراک می‌گذارند. در این پژوهش با انجام تجزیه و تحلیل گسترده در سیستم‌های مدیریت اعتماد مجموعه‌ای از بهترین اقدامات اجرایی که راهنمای مناسبی برای طراحی یک سیستم مدیریت اعتماد کارا در پروتکل‌های کلیدی مشترک را فراهم می‌کند، شناسایی شده است. این کارایی ارزیابی شده، چگونگی برآورده کردن نیازمندی‌های خاص در نگرش‌های پیشنهاد شده برای ساخت کلید در مفهوم اینترنت اشیاء، ارزیابی شده است (ساعید،[۱] ۲۰۱۳: ۱۲۰).

- در سال ۲۰۱۵ تحقیقی با عنوان «کنترل دسترسی در اینترنت اشیاء ماشین با ماشین با پلت‌فرم رایانش ابری»[۲] توسط باین انگوراجاتی[۳] در دانشگاه آلبورگ دانمارک اجرا گردیده است. با توجه به اینکه در اینترنت اشیاء، ارتباطات ماشین با ماشین[۴] مطرح است و کمترین دخالت را انسان‌ها در آن دارند، مشکل و مسأله مورد بررسی در این پژوهش «طراحی مقیاس‌پذیری، انعطاف و مکانیزم کنترل دسترسی اجزاء کوچک شبکه[۵] برای اینترنت اشیاء ماشین با ماشین با پلت‌فرم رایانش ابری» می‌باشد.

این پژوهش به دنبال پاسخگویی به سوالات زیر بوده است:

- آماده کردن یک اجزاء کوچک شبکه، برای انتساب کارآمد سیاست و کنترل دسترسی سازگار در میان افزار[۶] اینترنت اشیاء ماشین با ماشین چگونه است؟
- پشتیبانی کردن از مقیاس‌پذیری و کارآمدی مدیریت متحرک، همراه با کنترل دسترسی در میان‌افزار اینترنت اشیاء ماشین با ماشین چگونه است؟

۱- Saied
۲- Access Control in IoT/M۲M – Cloud Platform
۳- Bayu Anggorojati
٤- IOT M۲M
٥- fine-grained
٦- middleware

- غلبه کردن بر تضاد بین ماهیت پویا و مقیاس‌پذیری در مسائل اینترنت اشیاء و آماده کردن یک سطح معینی از احراز هویت در مدل‌سازی کنترل دسترسی چگونه است؟

مدل کردن سیستم تشخیص نفوذ در سیستم کنترل دسترسی برای اینترنت اشیاء ماشین با ماشین با پلت فرم رایانش ابری، به صورتی‌که، جایی برای محافظت از مجموعه دارایی‌های امنیتی باشد، در مقابل عدم قطعیت در مخرب بودن حریف و برخی دیگر از محدودیت‌های منابع، چگونه است؟ (انگوراجاتی،[۱] ۳۵:۲۰۱۵)

محقق در پایان این پژوهش سیستم کنترل دسترسی بخش مبتنی بر قابلیت همراه با مدیریت محلی مقیاس‌پذیر در سیستم اینترنت اشیاء در شبکه محلی ار.اف.ای.دی را طراحی نموده است.

مهم‌ترین ویژگی سیستم طراحی شده، تمرکز ویژه بر مقیاس‌پذیری، کارایی و انعطاف به دلیل ناهمگون بودن منابع شبکه می‌باشد.

این پژوهش با استفاده از تعریف دسترسی گروهی از طریق انتشار قابلیت در زیر مجموعه تحت کنترل و حفظ دسترسی آن‌ها، این مدل را طراحی نموده است.

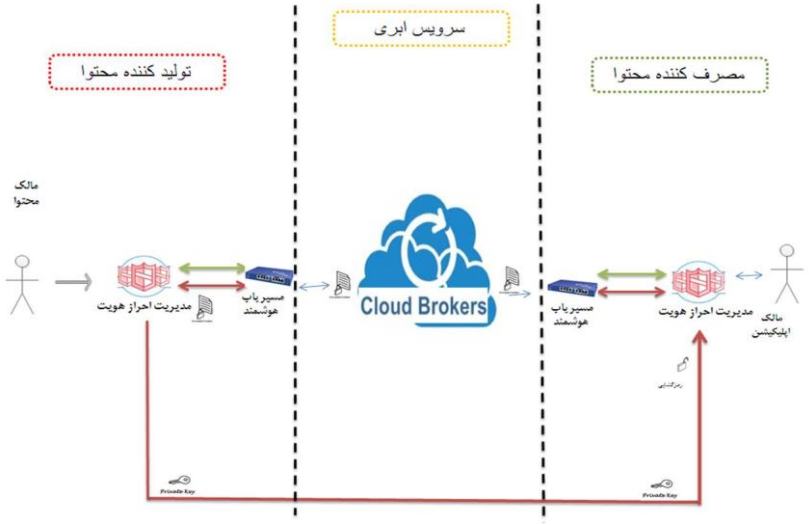
همچنین این پژوهش اقدام به طراحی سیستم تشخیص نفوذ جهت شناسایی و کاهش تهدیدهای درونی در شبکه‌های اینترنت اشیاء ماشین با ماشین با پلت‌فرم رایانش ابری نموده است.

مدل مفهومی پژوهش

برای تدوین مدلی جهت حفظ حریم خصوصی و امنیت اطلاعات در اینترنت اشیاء، مطالعه مبانی نظری پژوهش انجام شد و پژوهش‌های گذشته در حوزه، حریم خصوصی در فضای مجازی و ابعاد آن، اعتماد، امنیت اطلاعات، الگوریتم‌های رمزنگاری پارادایم اینترنت اشیاء و مکانیزم‌های ارتباطی آن، تفاوت‌های حریم خصوصی افراد در اینترنت با اینترنت اشیاء موردبررسی قرار گرفت. سپس با توجه به مطالب موجود، ملاک‌ها و

۱- Anggorojati

شاخص‌های مدل مفهومی تهیه و در نهایت پس از چندین بار اصلاح مدل اولیه پژوهش طراحی گردید، که در شکل زیر آورده شده است.



شکل ۱- مدل مفهومی حفظ حریم خصوصی و امنیت اطلاعات در اینترنت اشیاء

روش‌شناسی پژوهش

فرآیند معمول پژوهش در رویکرد کمی، مطالعه منابع برای انتخاب نظریه مناسب، ساخت فرضیه‌ها و سپس آزمون و تحلیل آماری آن‌ها می‌باشد. در مقابل رویکرد کیفی، ممکن است نظریه‌ای مرتبط با مطالعه وجود نداشته یا پژوهشگر تمایلی به محدود ساختن کار خود به نظریه‌های موجود نداشته باشد. به این ترتیب، رویکرد کیفی می‌تواند به منظور ساخت نظریه‌ای جدید برای توضیح پدیده یا توصیف الگوهای جدیدی به کار رود که در داده‌ها یافت می‌شوند. در رویکرد کمی لازم است داده‌ها مشخص و دقیق باشند، بنابراین داده‌های اصلی گردآوری شده کمی خواهند بود، اما رویکرد کیفی، تأکید بر کیفیت و عمق داده‌ها است در نتیجه، داده‌هایی که گردآوری می‌شوند اساساً کیفی می‌باشند (هوسی،[۱] ۱۹۹۷:۱۰).

۱- Hussey

تحقیقات انجام شده در این خصوص نشان می‌دهد که عوامل مؤثر بر امنیت اطلاعات و حریم خصوصی در اینترنت اشیاء در زمینه‌های متعدد و سطوح تحلیل متفاوت، تنوع بسیار زیادی دارند، بنابراین رویکرد کمی به این پژوهش ممکن است باعث کاهش عواملی گردد و یا حتی عواملی نادیده گرفته شود که بسیار می‌توانند در نتیجه پژوهش تأثیرگذار باشند.

زیرا ساخت چهارچوب‌های نظری در این رویکرد که مقدمه طرح فرضیه‌ها است، پژوهش را در قالب‌هایی قرار می‌دهد که انعطاف لازم را برای برخورد با وضعیت‌های جدید ندارند (نورث روف،[۱] ۲۰۰۵:۲۰۵).

بنابراین طراحی و ارزیابی مدل مفهومی جهت حفظ حریم خصوصی و امنیت اطلاعات در اینترنت اشیاء با رویکرد کیفی انجام پذیرفت زیرا در آن، چهارچوبی از پیش مشخص و تعیین شده وجود نداشت و مدل ارائه شده بر اساس داده‌های گردآوری شده طراحی شده است.

بنابراین با انجام مطالعه سوابق پژوهش‌های گذشته، شناخت نسبتاً جامعی از وضع موجود در این خصوص به دست آمد و مدل مفهومی اولیه طراحی گردید، سپس این مدل با استفاده از روش دلفی تکمیل و نهایی شد.

روش دلفی: هر چند روش دلفی در ابتدا برای پیش‌بینی به کار برده شد اما در گردآوری داده‌های مربوط به زمان حال یا گذشته که به درستی معلوم یا موجود نیستند و یافتن روابط علی در پدیده‌های پیچیده اجتماعی و اقتصادی نیز استفاده می‌شود (لینستون،[۲] ۱۹۷۵:۴).

در مراحل گوناگون فرآیند یک تحقیق نیز این روش می‌تواند به کار رود، از جمله این مراحل می‌توان به یافتن دیدگاهی نظری برای پژوهش، انتخاب متغیرها، شناخت اولیه روابط علی میان متغیرها و تعریف سازه‌ها اشاره کرد (اوکلی،[۳] ۲۰۰۴:۳۰). روش دلفی پیش از این در بخش عمومی و برای مقاصدی مانند پیش‌بینی، وفاق، فراهم‌آوری اطلاعات، برنامه‌ریزی، ارزیابی و هدف‌گذاری چندین دفعه به کار رفته است(کریبر،[۴] ۲۰۰۰:۱۳۲).

۱- Northrop
۲- Linston
۳- Okoli
٤- Cryer

این روش در حوزه فناوری و سیستم‌های اطلاعات نیز کاربردی فراوان داشته است. از جمله این کاربردها که به هدف این پژوهش نزدیک می‌باشد، می‌توان به شناخت ابعاد موضوع‌ها و عوامل مؤثر بر جنبه‌های گوناگون پدیده‌های حوزه فناوری اشاره نمود(اوکلی،[۱] ۲۰۰۴:۳۰).

تشکیل و ترکیب نشست خبرگان: روش دلفی با مشارکت افرادی انجام می‌پذیرد که در موضوع پژوهش دارای دانش و تخصص باشند. این افراد با عنوان پانل دلفی شناخته می‌شوند. گزینش اعضای واجد شرایط برای پانل دلفی از مهم‌ترین مراحل این روش به حساب می‌آید، زیرا اعتبار نتایج کار بستگی به شایستگی و دانش این افراد دارد (پاول،[۲] ۲۰۰۳:۳۸۲).

این افراد برخلاف آنچه در پیمایش‌های کمی معمول است، بر مبنای نمونه‌گیری احتمالی انتخاب نمی‌شوند، زیرا سازوکاری برای تصمیم‌گیری گروهی است و نیاز به متخصصان واجد شرایط دارد که درک و دانش عمیقی از موضوع پژوهش داشته باشند. روشن است که این افراد را نمی‌توان از این طریق انتخاب کرد. معمولاً انتخاب اعضای نشست از طریق نمونه‌گیری غیر احتمالی صورت می‌گیرد. یکی از روش‌های استفاده شده در این زمینه نمونه‌گیری هدف‌دار یا قضاوتی است. این روش بر این فرض استوار است که دانش پژوهشگر درباره جامعه برای دست‌چین کردن اعضای نشست قابل استفاده است (لینستون،[۳] ۱۹۷۵:۱۰۰۸).

در صورتی که پژوهشگر خود تمام افراد مناسب را برای عضویت در نشست نشناسد، می‌تواند از روش نمونه‌گیری زنجیره‌ای نیز استفاده کند که نوعی از روش‌های غیر احتمالی به حساب می‌آید. در این روش پژوهشگر کار تعیین اعضاء را با شناسایی فرد یا گروهی از افراد آگاه آغاز و از این طریق به دیگر افراد مناسب برای کار دست می‌یابد (بنیس،[۴] ۲۰۰۴:۱۰۵).

تعداد مناسب برای اعضاء نکته مهم دیگری است که در تشکیل نشست باید به آن توجه کرد. مانند هر نوع نمونه‌گیری دیگر حجم نمونه به عواملی مانند امکان دسترسی

۱- Okoli
۲- Powell
۳- Linston
٤- Benis

به افراد، زمان لازم و هزینه گردآوری اطلاعات بستگی دارد. در روش دلفی که اعضاء نشست باید از متخصصان موضوع پژوهش باشند، این محدودیت‌ها افزایش پیدا می‌کند. از طرف دیگر ایجاد اتفاق نظر میان اعضاء به عنوان هدف از کاربرد این روش با افزایش آن دشوارتر می‌شود. هر چند تعداد اعضای نشست در پژوهش‌هایی از این دست بین ۱۰ تا ۱۶۸۵ نفر متغیر بوده است، اما هنگامی که میان اعضای نشست تجانس وجود داشته باشد، حدود ۱۰ تا ۲۰ عضو توصیه شده است (پاول،[۱] ۳۸۲:۲۰۰۳).

بر این اساس اعضای نشست دلفی برای این پژوهش به صورت نمونه‌گیری غیر احتمالی و ترکیبی از نمونه‌گیری غیر احتمالی و ترکیبی از روش‌های هدفدار و زنجیره‌ای برگزیده شدند.

بر این اساس ابتدا یازده نفر از افرادی نامزد شدند که در شبکه اجتماعی لینک‌دین متخصص حوزه بوده و واجد یک یا چند ویژگی زیر بودند:

الف)عضو هیات علمی دانشگاه یا موسسه پژوهشی فعال در زمینه اینترنت اشیاء؛

ب)مدیر، مشاور ارشد و یا متخصصین فعال در حوزه اینترنت اشیاء و امنیت اطلاعات در فضای مجازی.

گام بعدی جلب مشارکت نامزدها برای انجام پژوهش است که باید به صورت جداگانه و تا حد امکان با انجام مکاتبات مجازی مستمر انجام شود.

بهتر است در تماس با نامزدها پس از توضیح پژوهش و انتظاری که از آن‌ها می‌رود دعوت‌نامه‌ای نیز در اختیارشان قرار گیرد که شامل چگونگی انجام پژوهش و دریافت موافقت آن‌ها برای مشارکت باشد(کرییر،[۲] ۱۳۲:۲۰۰۰).

برای دعوت نامزدها به مشارکت، طرحی طراحی و برای اظهار نظر در اختیار دو نفر از متخصصان موضوع قرار گرفت و ویرایش شد. سپس با تک‌تک نامزدها به صورت مجازی تماس گرفته شد و هدف و موضوع پژوهش و چگونگی انجام کار به آگاهی ایشان رسید و از آن‌ها دعوت شد که در نشست دلفی به صورت مجازی مشارکت کنند.

۱- Powell
۲- Cryer

سپس فرمی برای ایشان ارسال شد که شامل موضوع پژوهش، هدف‌های آن، تعریف‌ها تعداد دوره‌ها، زمان لازم برای مشارکت در هر دوره و مشخصات افراد بود.

در این فرم از آن‌ها خواسته شد که تمایل و موافقت خود را با مشارکت در این نشست اعلام کنند، همچنین از هر یک از این افراد درخواست شد که افراد دیگری را معرفی کنند که بر اساس معیارهای یاد شده برای مشارکت در این پژوهش مناسب باشند.

از میان افراد معرفی شده، ۱۵ نفر دیگر واجد شرایط تشخیص داده شدند که همین فرایند برای آن‌ها نیز تکرار شد. از این میان در مجموع ۲۲ نفر تمایل و توافق خود را برای مشارکت در نشست دلفی اعلام کردند .

جدول سه نیز سابقه کار اعضاء را به تفکیک نوع، تعداد، بیشترین، کمترین و میانگین آن‌ها نشان می‌دهد. از میان ۲۲ نفر، تحصیلات ۱۲ نفر از اعضای نشست دکتری تخصصی،۷ نفر کارشناسی ارشد و ۳ نفر کارشناسی بود.

۱۵ نفر تحصیلاتی در زمینه فناوری اطلاعات داشتند و تحصیلات سایر افراد عبارت بودند از،۳ نفر در زمینه مدیریت،۲ نفر در زمینه حقوق خصوصی و یک نفر صنایع و یک نفر اطلاع رسانی بود.

جدول شماره ۱- ویژگی‌های اعضای نشست پژوهش

نوع کار	تعداد افراد	سابقه (به سال)		
		بیشترین	کمترین	میانگین
عضو هیات علمی دانشگاه یا موسسات پژوهشی فعال در زمینه اینترنت اشیاء	۱۰	۱۲	۳	۴
مدیر، مشاور ارشد در پروژه‌های مرتبط با اینترنت اشیاء	۱۵	۸	۲	۳
متخصصین فعال در حوزه‌های مرتبط با اینترنت اشیاء	۱۴	۱۰	۴	۵
متخصصین فعال در حوزه مرتبط با امنیت اطلاعات و حریم خصوصی مجازی	۴	۱۷	۵	۹

مقیاس اتفاق نظر: یکی از مهم‌ترین مقیاس‌ها برای تعیین درجه هماهنگی و موافقت میان چندین دسته رتبه مربوط به N شی یا فرد، ضریب هماهنگ کندال است. برای تعیین میزان اتفاق نظر میان اعضای نشست خبرگان در این تحقیق، از ضریب کندال استفاده شده است، زیرا با کاربرد این مقیاس می‌توان همبستگی رتبه‌ای میان K مجموعه را یافت. چنین مقیاسی به ویژه در مطالعات مربوط به «روایی میان داوران» مفید است.

ضریب هماهنگی کندال نشان می‌دهد که افرادی که چند مقوله را بر اساس اهمیت آن‌ها مرتب کرده‌اند به طور اساسی معیارهای مشابهی را برای قضاوت درباره اهمیت هر یک از مقوله‌ها به کار برده‌اند و از این لحاظ با یکدیگر اتفاق نظر دارند (کندلوال،[۱] ۶۸:۲۰۰۱). این مقیاس با استفاده از فرمول زیر محاسبه می شود:

$$W = \frac{S}{\frac{1}{12}K^2(N^3 - N)}$$

که در آن:

S= $\sum\left[RJ - \frac{\sum RJ}{N}\right]^2$ حاصل جمع مربعات انحراف های RJ ها از میانگین RJ ها

Rj= مجموع رتبه‌های مربوط به یک عامل

K= تعداد مجموع رتبه‌ها (تعداد داوران)

N= تعداد عوامل رتبه‌بندی شده

$\frac{1}{12}k^2(N^3 - N)$ = حداکثر حاصل جمع مربعات انحراف‌های از میانگین Rj ها

یعنی حاصل جمع S که در صورت وجود موافقت کامل بین K رتبه‌بندی مشاهده می‌شود. مقدار این مقیاس هنگام هماهنگی با موافقت کامل، برابر با یک است و در زمان نبود هماهنگی برابر با صفر می‌باشد.

«اشمیت» برای تصمیم‌گیری درباره توقف یا ادامه دوره‌های دلفی، دو معیار آماری ارائه می‌کند. اولین معیار، اتفاق نظری قوی میان اعضای نشست است که بر اساس مقدار ضریب هماهنگی کندال تعیین می‌شود و در صورت نبود چنین اتفاق نظری ثابت ماندن

۱- Khandelwal

این ضریب یا رشد ناچیز آن در دو دور متوالی نشان می‌دهد که افزایشی در توافق اعضاء صورت نگرفته است و فرآیند نظرخواهی باید متوقف شود. شایان ذکر است که معناداری آماری ضریب W برای متوقف کردن فرآیند دلفی کفایت نمی‌کند برای نشست‌های با تعداد بیشتر از ۱۰ عضو حتی مقادیر بسیار کوچک W نیز معنادار به حساب می‌آیند (اشمیت،[۱] ۷۷۳:۱۹۹۷).

ورودی و خروجی هر دور نشست خبرگان به روش دلفی

دور اول نشست خبرگان

در این دوره اعضاء نشست ۱۰ عامل را از میان ۲۰ عامل موجود در مدل مفهومی دارای تأثیر زیاد و خیلی زیاد بر امنیت اطلاعات و حریم خصوصی افراد در اینترنت اشیاء تشخیص دادند و علاوه بر این ۳۹ عامل را برای تکمیل مدل مطرح کردند که با ترکیب برخی از آنها تعداد ۳۰ عامل باقی ماندند.

از این میان ۱۲ عامل به نوعی با عوامل ارائه شده در پژوهش‌های قبلی یکسان بودند که پس از حذف آن‌ها ۱۸ عامل موفقیت منحصر به فرد باقی ماندند.

دور دوم نشست خبرگان

در این دور اعضای نشست ۱۰ عامل را از میان ۱۸ عامل که در دور اول از طرف اعضاء ارائه شده بودند، دارای تأثیر زیاد و خیلی زیاد تشخیص دادند. به این ترتیب اعضای نشست در مجموع و از میان عواملی که در مدل اولیه ارائه شده بود ۲۴ عامل را دارای تأثیر زیاد و خیلی زیاد تشخیص دادند.

دور سوم و چهارم نشست خبرگان

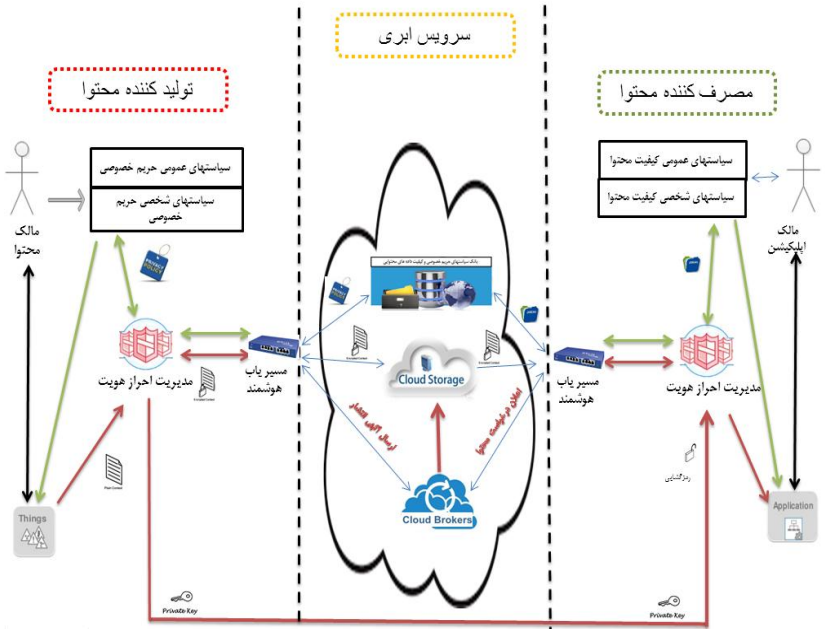
در دورهای سوم و چهارم، اعضاء باید مجدداً اظهارنظر خود را درباره میزان تأثیر هر یک از عوامل اعلام می‌کردند.

آن‌ها علاوه بر این باید ترتیب اهمیت عوامل را از نظر خود اعلام می‌کردند، این عوامل در دور سوم به ترتیب میانگین میزان اهمیت آن‌ها در دور اول و دوم و در دور چهارم ارائه شدند که اعضاء در دوره سوم تعیین کرده بودند.

۱- Schmidt

مدل نهایی پژوهش

پس از اجرای نظر اعضای نشست خبرگان در دوره‌های چهارگانه روش دلفی مدل نهایی پژوهش، به صورت شکل زیر ارائه گردید.



شکل ۲- مدل نهایی پژوهش، جهت حفظ حریم خصوصی و امنیت اطلاعات در اینترنت اشیاء

این مدل از سه بخش اصلی زیر تشکیل شده است:

- بخش تولیدکننده محتوا یا «مالک محتوا[۱]»؛
- بخش مصرف‌کننده محتوا یا مالک اپلیکیشن؛
- بخش سرویس ابری با الگوریتم انطباقی.

مهم‌ترین عناصر مورد تأیید خبرگان در هر بخش در جدول شماره سه ارائه گردیده است.

۱- Context Owner

جدول ۲- مهم‌ترین عناصر مورد تأیید خبرگان در هر بخش مدل

عناصر مورد تأیید خبرگان بخش مالک محتوا	عناصر مورد تأیید خبرگان بخش مصرف کننده محتوا	عناصر مورد تأیید خبرگان بخش سرویس ابری
مالک محتوا	مالک اپلیکیشن[۱]	*بانک اطلاعاتی و موتور استنتاج سیاست‌های حریم خصوصی و کیفیت محتوا*[۲]
اشیاء (تولید کنند گان محتوا)[۳]	اپلیکیشن (مصرف کننده محتوا[۴])	سرویس ذخیره سازی ابری[۵]
سیاست‌های حریم خصوصی تولید کننده محتوا[۶]	سیاست‌های کیفیت محتوا[۷]	سرویس کارگزار ابری[۸]
مدیریت احراز هویت سمت تولید کننده محتوا[۹]	*مدیریت احراز هویت سمت مصرف کننده محتوا*[۱۰]	
مسیریاب هوشمند[۱۱]	مسیریاب هوشمند	

تشریح مهم‌ترین عناصر مورد تایید خبرگان در هر بخش مدل:

- **بخش تولید کننده محتوا:** به مجموع اطلاعات استخراج شده و به اشتراک گذاشته شده و فرآیندهایی که اشیاء درگیر آن‌ها هستند، داده محتوایی[۱۲] گفته می‌شود (مارکز، ۲۰۱۵). تولیدکننده محتوا به دنبال کاهش کیفیت محتوا و افزایش حریم خصوصی خود است زیرا حریم خصوصی مانند قدرتی است که روی تکه‌های اطلاعاتی که متعلق به فرد است قرار دارد (اگری و رتنبرگ، ۱۹۹۸).

۱. **مالک محتوا:** یک شخص، یک سازمان یا گروهی از افراد هستند که قوانین حریم خصوصی داده‌های محتوایی متعلق به خودشان را تعریف می‌کنند، تا تصمیم بگیرند که این داده‌ها به چه کسی یا تحت چه

۱- Application Owner
۲- Privacy & QOC Policy Database
۳- Context Producer
٤- Application
٥- Cloud Storage
٦- Privacy Policy
۷- Quality of context policy
۸- Cloud Broker
۹- Authentication maneger Producer
۱۰- Authentication maneger Consumer
۱۱- Smart Routers
۱۲- CONTEXT

شرایطی به اشتراک گذاشته شوند. آن‌ها مجموعه سیاست‌هایی را تعیین می‌کنند که تنظیمات حریم خصوصی‌شان را برقرار می‌نماید.

۲. **اشیاء (تولید کنند گان محتوا):** شیء یا مجموعه‌ای از اشیاء هوشمند هستند که با توجه به سیاست‌های تعیین شده توسط مالکشان اقدام به تولید داده‌های محتوایی می‌نمایند.

۳. **سیاست‌های حریم خصوصی تولید کننده محتوا:** این سیاست‌ها مجموعه تدابیر و دستوراتی است که مالک یا تولیدکننده محتوا برای حفاظت از حریم خصوصی خود، ارائه می‌نماید. به عنوان مثال، به مباحث ذیل می-توان اشاره نمود:

- تعیین ویژگی‌های مصرف‌کنندگان مجاز؛
- تعیین کاربردهای مجاز از محتوا؛
- تعیین مجاز یا غیرمجاز بودن، انتشار محتوا برای زنجیره مصرف‌کنندگان بعدی؛
- میزان رزولوشن و دقت محتوا.

۴. **مدیریت احراز هویت سمت تولید کننده محتوا:** این بخش نقش بسیار مهمی را در چهارچوب ارائه شده ایفا می‌کند و مهم‌ترین نتایج آن، ایجاد اعتماد بین تولیدکننده و دریافت‌کننده محتوا می‌باشد. زیرا مورد اعتماد بودن مقادیر مربوط به مالکان، کاربران نهایی و اپلیکیشن‌های مصرف‌کننده، در برقراری تبادل داده‌ها و پایداری آن‌ها در اینترنت اشیاء بسیار اهمیت دارد. مدیریت احراز هویت تولیدکننده از چهار بخش اصلی، به شرح ذیل تشکیل گردیده است:

- مدیریت اعتماد[۱]: در این بخش صحت، دقت و کامل بودن داده‌های محتوایی ارسال شده از تولیدکننده محتوا، مورد کنترل قرار می‌گیرد.

۱- Trust Manager

- مدیریت شناخت[1]: در این بخش داده‌های لازم جهت افزایش شناخت از تولیدکننده محتوا جمع‌آوری می‌گردد تا سطح شناخت موجود از تولیدکننده محتوا افزایش یافته و امکان پیاده‌سازی، سیاست‌های «حریم خصوصی» و «کیفیت محتوا» فراهم گردد.
- مدیریت رمزنگاری و رمزگشایی داده‌ها:[2] در این قسمت داده‌های ارسال شده از سوی تولیدکننده محتوا رمزنگاری می‌گردد. همچنین پس از تبادل سیاست‌ها و برقراری توافق‌نامه کلید رمزگشایی به مصرف‌کننده محتوا ارسال می‌گردد.
- تطبیق محتوای در حال ارسال با سیاست‌ها: در این قسمت به بررسی و تطبیق داده‌های محتوایی در حال ارسال با سیاست‌های تدوین شده توسط «مالک محتوا » اقدام می‌گردد.

۵. **مسیریاب هوشمند:** در صورت انجام موفقیت‌آمیز همه مراحل فوق، در این قسمت اطلاعات به بخش‌های مختلف سرویس رایانش ابری،[3] ارسال می‌گردد. مهم‌ترین این تراکنش‌ها عبارتند از:

- ارسال محتوای کدگذاری شده به سرویس ذخیره‌سازی ابری،[4] جهت ذخیرش داده‌ها؛
- ارسال آگهی انتشار محتوا به کارگزار ابری، جهت یافتن مشتری منطبق با سیاست‌ها؛
- ارسال سیاست‌های تدوین شده به «بانک سیاست‌های حریم خصوصی و کیفیت داده‌های محتوایی» جهت ذخیره و استفاده از آن‌ها در موارد مشابه.

○ **بخش سرویس‌های مبتنی بر ابر**: در این چهارچوب از رایانش ابری استفاده شده و چهار سرویس به شرح ذیل در آن تعریف می‌گردد:

۱- Visibility Manager
۲- Encription/ Decryption manager
۳- CLOUD computing
٤- Cloud Storage

۱. **بانک اطلاعاتی و موتور استنتاج سیاست‌های حریم خصوصی و کیفیت محتوا:** در این سرویس، تمامی سیاست‌های اتخاذ شده در یک شبکه مشخص از اینترنت اشیاء، در این قسمت ثبت، ذخیره و به‌روزرسانی می‌گردند تا برای اتخاذ سیاست‌های مشابه، مالکان و مصرف‌کنندگان محتوا پیشنهاد داده شود.

۲. **سرویس ذخیره سازی ابری:** در این سرویس داده‌های کدگذاری شده اشیاء، ثبت و ذخیره می‌گردند.

۳. **سرویس کارگزار ابری:** در این سرویس تبادل داده‌های محتوایی با توجه به شرایط کیفیت داده‌های محتوایی مصرف‌کننده و حریم خصوصی تولیدکننده محتوا انجام می‌گیرد. در حقیقت وجود یک فرآیند انطباق بین درخواست تولیدکننده و مصرف‌کننده صورت می‌گیرد.

- **بخش مصرف‌کنندگان محتوا:** مصرف‌کننده محتوا به دنبال افزایش کیفیت داده محتوایی می‌باشد.

کیفیت داده محتوایی مجموعه‌ای از معیارهای کیفی قابل اندازه‌گیری مانند دقت، احتمال خطا، و یا بروز بودن می‌باشد (باچلوز و دیگران، ۲۰۰۳).

این بخش از پنج قسمت به شرح ذیل تشکیل شده است:

۱. **مالک اپلیکیشن:** یک شخص، گروهی از اشخاص یا یک سازمان که مالک اپلیکیشن‌ها بوده و از طریق آن‌ها، به داده‌های محتوایی دسترسی داشته و بهره‌بردار اصلی می‌باشند. آن‌ها مجموعه سیاست‌ها در خصوص کیفیت محتوای مورد نیاز اپلیکیشن‌ها را تعیین می‌کنند.

۲. **اپلیکیشن (مصرف‌کننده محتوا):** شی یا مجموعه‌ای از اشیاء هوشمند هستند که جهت ارائه خدمت و سرویس، به داده‌های محتوایی، نیاز دارند.

۳. **سیاست‌های کیفیت محتوا:** این سیاست‌ها مجموعه تدابیر و دستوراتی است که مالک اپلیکیشن، جهت ارائه خدمت بهینه، در خصوص حداقل

کیفیت محتوای مورد نیاز، ارائه می‌نماید. مصرف‌کننده محتوا نیاز به داده‌های معتبر با حداقل سطح مشخصی از کیفیت و دقت محتوا دارد و در توافق نامه بین تولیدکننده و مصرف‌کننده محتوا می‌بایست این ملاحظات مصرف‌کننده رعایت شود. به عنوان نمونه در مثال دوربین مداربسته، جهت مراقبت از بیمار حاضر در منزل، سنسورها نیاز به بیشترین کیفیت داده در تمامی ساعات شبانه روز دارند اما حریم خصوصی مالک محتوا با این موضوع می‌تواند در تناقض باشد و دسترسی به کیفیت و دقت کامل محتوایی در همه زمان و همه مکان از نظر وی غیر ممکن است و مخل حریم خصوصی وی ارزیابی می‌گردد.

۴. **مدیریت احراز هویت مصرف کننده:** این بخش، نقش مکمل در سمت مصرف‌کننده ایفا می‌کند و از چهار بخش اصلی جهت مدیریت احراز هویت برای مصرف‌کننده محتوا تشکیل شده است.

- **مدیریت اعتماد:** در این بخش صحت، دقت و کامل بودن داده‌های محتوایی، مورد کنترل قرار می‌گیرد، تا مشخص شود داده‌ها دارای کیفیت مناسبی می‌باشد.
- **مدیریت شفافیت:** در این بخش، اطمینان از اینکه کاربران مجاز در صورت نیاز به اطلاعات و دارایی‌های مربوطه به آن‌ها دسترسی داشته باشند و همچنین سطح قابل‌مشاهده بودن تولیدکننده محتوایی تعیین می‌گردد. به عنوان مثال، میوه فروش محل برای تعیین میزان میوه مورد نیاز مشتریان محل برای روز آینده، نیاز به دسترسی به اطلاعات موجودی یخچال مشتریان دارد، در این قسمت دسترسی پایدار به این اطلاعات برای کاربران مجاز بررسی می‌شود.
- **مخزن اهداف:**[1] در این قسمت، بررسی‌های لازم در خصوص اهداف مالکان و مصرف‌کنندگان محتوا انجام می‌گیرد. هدف از این کار، ارائه داده‌های تکمیلی در خصوص اهداف مالکان و مصرف‌کنندگان محتوا

۱- Purpose Repository

به بخش «کارگزار ابری» می‌باشد تا تطبیق اهداف هر طرف با سیاست‌های حریم خصوصی طرف دیگر ارزیابی گردد. در این بخش، تقسیم‌بندیِ داده شده توسط مالک محتوا، در مورد ویژگی‌های کاربر نهایی و زنجیره کاربرانی که مجاز به استفاده از داده‌ها هستند بروزرسانی و اصلاح می‌شود.

- **رمز نگاری و رمز گشایی داده‌ها**[۱]: در این قسمت داده‌های دریافت شده از سوی تولیدکننده محتوا رمز گشایی می‌گردد.
- **تطبیق سیاست‌ها با داده‌های محتوایی:** در این قسمت به بررسی و تطبیق داده‌های محتوایی درخواست شده از «اپلیکیشن (مصرف کننده محتوا)» با سیاست‌های تدوین شده توسط «مالک اپلیکیشن» اقدام می‌گردد. در صورت عدم تطبیق، درخواست داده، برگشت داده می‌شود تا اصلاحات لازم در راستای سیاست‌های مصرف‌کننده محتوا انجام شود.

۵. **مسیریاب هوشمند:** در صورت انجام موفقیت‌آمیز همه مراحل فوق، در این قسمت اطلاعات به سرویس‌های رایانش ابری[۲] ارسال می‌گردد.

یافته‌های پژوهش

نتایج دوره‌های چهارگانه روش دلفی نشان می‌دهند که به دلایل زیر اتفاق نظر میان اعضای نشست حاصل شده است و می‌توان تکرار دوره‌ها را بیان داد:

- بیش از ۵۰درصد اعضا نشست، تقسیم‌بندی سه‌گانه مدل ارائه شده و چهار عامل اصلی تاثیر گذار در امنیت اطلاعات و حریم خصوصی افراد در اینترنت اشیاء را در طبقه بندی ارائه شده و عوامل اصلی مدنظر خود انتخاب کرده بوند.
- انحراف معیار اعضاء در مورد بخش‌های اصلی مدل از ۰/۷۸ در دوره‌های اول و دوم به ۰/۶۲ در دوره چهارم کاهش یافت و همچنین انحراف معیار پاسخ اعضاء

۱- Encription/ Decryption manager
۲- CLOUD computing

درباره میزان اهمیت عوامل اصلی مدل در هر بخش از ۷۳/ در دوره اول و دوم به ۰/۶۱ در دوره چهارم کاهش یافت .

- ضریب هماهنگی کندال برای پاسخ های اعضاء درباره بخش‌های اصلی مدل در دور چهارم ۰/۵۲۲ و برای عوامل اصلی مدل در هر بخش ۰/۵۳۲ است.
- با توجه به اینکه تعداد اعضای نشست بیش از نفر بود این میزان از ضریب کندال کاملاً معنادار به حساب می‌آید (اشمیت،[۱] ۷۷۳:۱۹۹۷).
- ضریب هماهنگی کندال در مورد بخش‌های اصلی مدل در دور چهارم نسبت به دور سوم تنها ۰۴۵/ و برای عوامل اصلی مدل در هر بخش ۰/۰۳۲ افزایش یافت که این ضریب یا میزان اتفاق نظر میان اعضای نشست در میان دو دور متوالی رشد قابل توجهی نشان نمی‌دهد[۲] (اشمیت، ۷۷۳:۱۹۹۷).

۱- Schmidt
۲- Schmidt

بحث و نتیجه‌گیری

این پژوهش با در نظر گرفتن ابعاد مختلف حریم خصوصی و کیفیت داده‌های محتوایی و الزامات آن‌ها در پارادایم اینترنت اشیاء، مدل مفهومی ارائه نمود، که بر اساس آن، امکان شخصی‌سازی«حریم خصوصی» و «کیفیت داده‌های محتوایی» تولیدکنندگان و مصرف‌کنندگان محتوا فراهم گردیده و امنیت اطلاعات در اینترنت اشیاء افزایش می‌یابد.

با مرور منابع و پژوهش‌های این حوزه و با توجه به پیچیدگی‌های امنیت اطلاعات و حریم خصوصی در اینترنت اشیاء، در مدل اولیه الگوریتم ارتباطی به سه بخش، سمت تولیدکننده، سمت مصرف‌کننده و بخش سرویس‌های ابری تقسیم‌بندی شد و برای هر یک از این بخش‌ها الزاماتی تعیین گردید.

جهت ارزیابی مدل ارائه شده و بهینه‌سازی آن از روش دلفی و نظر مجموعه خبرگان استفاده شد و در مجموع بیش از ۵۰ درصد اعضا نشست، تقسیم‌بندی سه‌گانه مدل ارائه شده و ۴ عامل اصلی تأثیرگذار در امنیت اطلاعات و حریم خصوصی افراد در اینترنت اشیاء را در هر طبقه ارائه شده، جزء عوامل اصلی مدنظر خود انتخاب کرده بودند و مدل اولیه مورد تأیید قرار گرفت و پس از جمع‌بندی نظر خبرگان، مدل ثانویه ارائه گردید.

منابع

- Agre, P. E. and M. Rotenberg (۱۹۹۸). Technology and privacy: The new landscape, Mit Press.
- Anggorojati, B. (۲۰۱۵). Access Control in IoT/M۲M - Cloud Platform. Department of Electronic Systems, Aalborg University.
- A. Linstone H, Turoff M. (۱۹۷۵). The Delphi Method: Techniques and Applications. london edited ed۱۹۷۵.
- Beins BC. (۲۰۰٤). Research Methods: A Tool for Life; boston.
- Borojerdi, M. (۲۰۰٤). "[Privacy in the Information Society] (in Persian)." ۲۰۱۷, from http://www.bashgah.net/fa/content/show/٦۹٥٤.
- Buchholz, T. (۲۰۰۳). Quality of Context Information: What it is and why wee need it. Proceedings of the ۱۰th International Workshop of the HP OpenView University Association (HPOVUA'۰۱).
- Cryer P. (۲۰۰۰). The research student's guide to success, ۲nd edn (Buckingham, Open University Press).
- Evans, D. (۲۰۱۱). "The internet of things: How the next evolution of the internet is changing everything." CISCO white paper ۱(۲۰۱۱): ۱-۱۱.
- Fink A, Kosecoff J, Chassin M, Brook RH. (۱۹۸٤). Consensus methods: characteristics and guidelines for use. American journal of public health;۷٤(۹):۹۷۹-۸۳.
- HarLow, C. (۲۰۰۳). [Understanding tort Law.] (in Persian). Tehran, Mizan.
- Hasson F, Keeney S, McKenna H. (۲۰۰۰). Research guidelines for the Delphi survey technique. Journal of advanced nursing;۳۲(٤):۱۰۰۸-۱٥.
- Hussey J, Hussey R. (۱۹۹۷). Business Research. London: Macmillan.
- Khandelwal VK.(۲۰۰۱).An empirical study of misalignment between Australian CEOs and IT managers. The Journal of Strategic Information Systems;۱۰(۱):۱٥-۲۸.
- Kosta, E. and Dumortier,J. (۲۰۰۸). Taxonomy. picos deliverabled۲.۱. ۳۲.
- Marquez, S. M. (۲۰۱٥). Models and algorithms for managing quality of context and respect for privacy in the Internet of Things, Université Paris-Saclay.
- MCQuail, D. (۲۰۰٤). [Audience analysis] (in Persian). Tehran, Ministry of Culture and Islamic Guidanc.
- Mohseni, M. (۲۰۰۱). Sociology Information Society. (in Persian). Tehran, Agah.

- Northrop A. (۲۰۰۲). Lessons for managing information technology in the public sector. Social science computer review;۲۰(۲):۱۹٤-۲۰٥.
- Okoli C, Pawlowski SD.(۲۰۰٤). The Delphi method as a research tool: an example, design considerations and applications. Information & management;٤۲(۱):۱٥-۲۹.
- Powell C.(۲۰۰۳). The Delphi technique: Myths and realities Methodological Issues. Nursing Research;٤۱(٤).
- Saied, Y. B. (۲۰۱۳). Collaborative security for the internet of things, Institut National des Télécommunications.
- Saunders M, Lewis P, Thornhill A. (۲۰۰۳). Research Methods for Business Students: Prentice Hall.
- Schmidt RC. (۱۹۹۷).Managing Delphi surveys using nonparametric statistical techniques. decision Sciences;۲۸(۳):۷٦۳-۷٤.
- Stein, L. and N. Sinha (۲۰۰٦). "New global media and the role of the state." The handbook of new media: ٤۱۰-٤۳۱.
- Ward, M. (۲۰۰٥). [Journalism online] (in Persian). Tehran, Iran Newspa