بررسی امنیت در رایانش ابری براساس فناوری IoT

زهرا شفیع پور مطلق، دکتر امیر هوشنگ تاجفر، محمد قیصری
دانشجوی ارشد دانشگاه پیام نور، تهران غرب shm-1439@yahoo.com
عضو هیأت علمی دانشگاه پیام نور a.tajfar@yahoo.com
کارشناس ارشد فناوری اطلاعات و مدرس دانشگاه پیام نور mohammad-gheysari@yahoo.com

چکیده

اینترنت از اشیاء و دستگاه‌هایی هستند که با گسترش آن‌ها و افزایش تعداد وسایل متصل به اینترنت پیش‌بینی می‌شود. در تمام جنبه‌های زندگی از جمله بهداشت و درمان، هوشمندسازی منازل، خودروها و محل‌های کار نفوذ خواهد کرد. با توجه به میزان های متفاوت اطلاعاتی که توسط یک دستگاه‌ها جمع‌آوری می‌شوند کاربران زیادی در خطر افشا یا سوءاستفاده اطلاعات قرار می‌گیرند. در چنین شرایطی جبران تخریب‌های وارده بسیار دشوار و حتی ناممکن است چون با جان انسان‌ها ارتباط پیدا می‌کند. مفهوم دیگر رایانش ابری است که بعنوان پشتیبان اینترنتی از اشیاء می‌باشد. در واقع رایانش ابری تکنولوژی نوظهوری است که قابلیت‌های مبتنی بر فناوری اطلاعات به عنوان خدماتی که بدون نیاز به دانش دقیق از فناوری های زیر ساختی و کمترین تلاش مدیریتی در دسترس قرار می‌گیرد ارائه می‌شود.

ابرها به دلیل مزایای بسیار مورد استقبال قرار گرفتند ولی مسائل مربوط به امنیت و حفظ حریم خصوصی اصلی‌ترین نگرانی در مورد این فناوری می‌باشد. زیرا ارائه‌دهندگان سرویس‌های ابر می‌توانند کنترل و نظارت کامل قانونی و یا غیر مقانونی برداده ها و ارتباطات بین کاربران سرویس و میزبان ابر داشته باشند. پس از مقدمه‌ای بر رایانش ابری، مفهوم کلی امنیت و اینترنتی از اشیاء، بر روی امنیت و رایانش ابری و اینترنت اشیاء و چالک های آن‌ها تمرکز کرده‌ایم.

کلمات کلیدی: رایانش ابری- اینترنت اشیاء- امنیت- اعتماد

۱- مقدمه

۱-۱- اینترنت اشیاء

اینترنت اشیاء یک مفهومی است که اشاره به حضور اشیاء در اطراف ما که قادر به تعامل و همکاری با یکدیگر هستند دارد. رشد اینترنت در طول سه دهه اخیر بسیار سریع بوده است به طوری که به تازگی به جای کامپیوترها از تلفن همراه برای اتصال به اینترنت استفاده می‌شود. گام بعدی در ادامه این توسعه تکامل از کامپیوترهای به هم پیوسته به سمت یک شبکه از اشیاء به هم پیوسته و در نتیجه یاجاد اینترنتی از اشیاء است.

اشیاء می‌توانند با داشتن آدرس‌هایی از خودشان ی اینکه به صورت ی سنسور در یک سیستم پیچیده تعبیه شوند تا بتوانند اطلاعات زیست محیطی را به دست آوردند. شبکه‌های سنسور می‌توانند درجه حرارت، اندازه‌گیری مسافت و ... را گزارش دهند یا حتی حضور مردم را حس کنند. اطلاعات جمع‌آوری شده از طریق سنسورها می‌توانند برای ایجاد برنامه‌های کاربردی برای مراقبت‌های بهداشتی، کنترل ترافیک، تجارت، تدارات یا خانه‌های هوشمند بری ایجاد محیط‌های تکاملی مورد استفاده قرار گیرند. در واقع می‌توان گفت اینترنتی از اشیاء شامل مجموعه‌ای ناهمگن از دستگاه‌ها و استراتژی ارتباطات است.

۱-۲- رایانش ابری

تعاریف و تفاسیر بی شماری در مورد رایانش ابری از منابع مختلف یافت می‌شود. اصطلاح رایانش ابری به احتمال زیاد از نمودار شبکه گرفته شده است. در نمودار شبکه برای توصیف انواع خاصی از شبکه‌ها نظیر اینترنت و انترانت از شکل ابر استفاده می‌شود. برخی منابع به محاسبات ابری به صورت مجموعه‌ای از برنامه‌های کاربردی که ترکیبی از مراکز داده سخت‌افزار و نرم‌افزار است، مراجعه می‌کنند. برخی دیگر رایانش ابری را یک مدل کسب و کار به جای یک تکنولوژی و یا خدمات خاص می‌دانند. به نظر ما محاسبات ابری متشکل از هر دو اجزای فن آوری و کسب و کار است. تکنولوژی‌هایی وجود دارد که به شکل قابل توجهی به ابر کمک می‌کند و بعید است که محاسبات ابری بتواند بدون آن‌ها وجود داشته باشد. برخی این توانمندسازها عبارتنداز: نرم‌افزارهای منبع باز، مجازی سازی، ذخیره‌سازی توزیع شده، پایگاه داده توزیع شده و سیستم‌های نظارت که بر اساس زیر ساخت های ابر هستند. به طور کلی فرض می‌شود رایانش ابری هر نرم‌افزار کاربردی یا بخشی از یک سیستم خدماتی باشد.

۱-۳- امنیت

از زمانی که اینترنت برای اتصال به کامپیوترها و به اشتراک گذاشتن اطلاعات در سراسر جهان طراحی شده است موضوع حملات و تهدیدات امنیتی از جمله ربودن اطلاعات جلسه، محرومیت از خدمات، استراق سمع، جعل هویت و غیره مطرح شده است. به منظور حفاظت در برابر مهاجمان و برای تأمین امنیت ارتباطات از فایروال ها، احراز هویت و رمز نگاری استفاده می‌شود. از آنجایی که امواج برای حمله مهاجمان باز هستند از دست دادن اطلاعات محرمانه و تهدید محرومیت از خدمات خطرناکترین مسئله‌ای است که در شبکه‌های بی سیم مطرح است. اتصال میلیارها دستگاه هوشمند قابل شناسایی و قابل آدرس دهی که به اصطلاح اینترنتی از اشیا و نامیده می‌شود باعث چالش‌های امنیتی جدیدی شده است. استقرار سیستم تهایی با توانایی جمع‌آوری، پردازش و برقراری ارتباط برای تبادل اطلاعات در مورد اشخاص و محیط نزدیک آن‌ها نگرانی هایی برای حریم خصوصی و اطلاعات شخصی افراد به وجود آورده است.

۲- مروری بر ادبیات تحقیق

۲-۱- محاسبات ابری

اجازه دهید در ابتدا مهم‌ترین فاکتورهایی که مشوق کلیدی سازمان‌ها برای استفاده از رایانش ابری هستند را بررسی کنیم ؛

انعطاف‌پذیری

توانایی برای مقیاس ظرفیت محاسباتی بالا یا پائین تقاضا بسیار مهم است به عنوان مثال تصور کنید یک شرکت نرم‌افزار به عنوان یک سرویس (saas) آنلاین برای خدمات مالی تهیه می‌کند. بدیهی است با چنین مدل کسب و کاری تقاضای منابع محاسباتی این سازمان در طول فصل مالیات، تنها دو تا سه ماه در سال به اوج خواهد رسید.

Pay – as – you – grow [۱]

ارائه‌دهندگان ابر عمومی همانند آمازون اجازه می‌دهند که از سرمایه‌گذاری های بزرگ شرکت‌ها برای زیر ساخت اولیه دقیق و خرید منابع محاسباتی جدید که به صورت پویا مورد نیاز است جلوگیری شود در این حالت شرکت‌ها نیاز به برنامه‌ریزی و تعهد مالی اولیه ندارند این مدل به ویژه برای شرکت‌های کوچک و نو۱۱ که منابع زیادی را نمی‌توانند صرف کسب و کار خود کنند مفید است.

هزینه‌ها و مسئولیت زیر ساخت خانگی

اجرای فناوری اطلاعات داخل شرکت‌ها، هزینه‌ها و مسئولیت قابل توجهی را باعث می‌شود، در حالی که برخی استدلال می‌کنند لزوماً چنین نیست و اجرای ساخت را داخل سازمان امن تر و ارزان‌تر است. با توجه به بودجه IT شرکت، مهارت کارکنان و برخی دیگر فاکتورها ارزش اجرای زیر ساخت ابر عمومی می‌تواند مشخص شود. ارائه‌دهندگان ابر عمومی باید موافقت نامه سطح خدمات (SLA) قابل قبولی را پیشنهاد دهند و مراقب و مسئول دردسرهایی باشند که شرکت ممکن است با آن مواجه شود.

مدل‌های توسعه ابر

به طور معمول سه مدل استقرار ابر وجود دارد: خصوصی، عمومی، ترکیبی

علاوه بر آن یک مدل ابر انجمنی نیز وجود دارد که کمتر مورد استفاده قرار می‌گیرد.

ابر خصوصی در یک سازمان واحد ساخته و مدیریت می‌شود. سازمان‌ها نرم افزاری یک استفاده می‌کنند که قابلیت‌های ابر را توانمند سازد.

ابر عمومی مجموعه‌ای از منابع محاسباتی که توسط سازمان‌های شخص ثالث تهیه شده است. معروفتری ابرهای عمومی شامل خدمات وب آمازون، Google Appengin , Microsoft Azure .

ابرهیبرید یا ترکیبی، ترکیبی از منابع محاسباتی تهیه شده به وسیله هر دو ابر عمومی و خصوصی است .

ابر انجمنی منابع محاسباتی یک سراسر چندین سازمان تسهی می‌کند و می‌تواند توسط هر دو منابع IT سازمان و تهیه‌کنندگان شخص ثالث اداره شود.

[۱]. اصطلاح pay – as – you – grow یعنی پرداخت به شما در مقابل رشد اقتصادی شرکت که شما در آن رشد دخیل بوده آید.

مدل های خدماتی محاسبات ابری

مدل‌های خدمات ابر توضیح می‌دهند که چطور سرویس‌های ابر در دسترس مشتریان قرار می‌گیرند. مدل‌های خدمات اصلی شامل ترکیبی از Iaas (زیر ساخت به عنوان سرویس) و Paas (پلت فرم به عنوان سرویس) و Saas (نرم‌افزار به عنوان سرویس) است.

Iaas (زیرساخت به عنوان سرویس):

این مدل مؤلفه‌های زیر ساخت را برای مشتریان فراهم می‌کند مؤلفه‌ها ممکن است شامل موارد زیر باشند: ماشین‌های مجازی، ذخیره‌سازی، شبکه‌ها، دیواره‌های آتش، متعادل کننده‌های بارگیری و غیره خدمات وب آمازون یک از بزرگ‌ترین تهیه‌کنندگان Iaas است.

Paas (پلت فرم به عنوان سرویس)

این مدل یک پلت فرم کاربردی از پیش ساخته شده به مشتری ارائه می‌دهد به این صورت مشتری‌ها نیاز ندارند زمانی را برای ساختن زیر ساخت اساسی برای برنامه‌های کاربردی شان صرف کنند. به طور معمول راه‌حل Paas یک API[1] تهیه می‌کند که شامل مجموعه‌ای از توابع برای برنامه‌ریزی مدیریت پلت فرم و توسعه راه‌حل آن است. google Appengine یک تهیه‌کننده معروف Paas است.

خدمات وب آمازون نیز بعضی راه‌حل‌های Paas را علاوه بر ارائه Iaas تهیه می‌کند.

Saas (نرم‌افزار به عوان سرویس)

این مدل راه‌حل‌های فرم افزار انلاین را ارائه می‌دهد.

۲-۲- اینترنت اشیاء

چشم‌انداز اینترنتی اشیاء

چشم‌انداز آینده اینترنت اشیاء این است که اشیاء قادر باشند به حوادث فیزیکی با رفتار مناسب عکس‌العمل نشان دهند و همچنین قادر به درک و انطباق با محیط خود و قادر به همکاری و مدیریت با اشیاء دیگر باشند و همه این ها مستقل از مداخله کردن یا نکردن انسان باشد. برای رسیدن به چنین هدفی تحقیقات متعددی از جنبه‌های مختلف بر روی IOT انجام شده است.

موارد زیر سه جنبه از چشم‌انداز اصلی IOT هستند که در پژوهش‌ها بیشترین تمرکز بر روی آن‌ها بوده است.

چشم‌انداز شی دگرا

در اصل IOT با توسعه بر چسب RFID[2] آغاز شده است، RFID همراه با کد الکترونیکی محصول (EPC) در چارچوب جهانی یکی از مؤلفه‌های کلیدی در معماری IOT است. یک سیستم EPC جهانی از برچسب‌های RFID اشیاء قابل شناسایی و قابل ردیابی را تهیه می‌کند. بته هر حال چشم‌انداز به RFID محدود نمی‌شود. بسیاری تکنولوژی‌های دیگر در چشم‌انداز شئ گرا در اینترنت اشیاء درگیر هستند این تکنولوژی‌ها عبارتند از:

---

۱. API مخفف Application Programming Interface رابط های نرم افزاری هستند که ارتباط بین نرم‌افزار های مختلف را پیاده‌سازی می‌کنند.

۲. RFID مخفف radio freguency identification که به عنوان جدیدترین تکنولوژی شناسایی به نحوی گسترده در دنیا مورد توجه قرار گرفته است.

ارتباطات میدانی نزدیک (NFC)، شناسه منحصر به فرد خارجی (uuID) حسگر بی سیم و شبکه‌های محرک چیزهایی کـه در ارتباط با RFID هستند اجزای اصلی اینترنتی از اشیاء را تشکیل می‌دهند. استفاده از این فناوری در واقع به مفهـوم گسـترش یافتن هرچیزی از هر نوعی است همانند: انسان به دستگاه‌های الکترونیکی چون کامپیوترها، حسگرها، محرکها، تلفن.

در واقع هر شیء روزمره ممکن است به طور هوشمند ساخته شود و تبدیل به یک شیء در شبکه شود برای مثال تلویزیون هـا، وسایل نقلیه، کتاب‌ها، لباس‌ها، داروها یا مواد غذایی می‌توانند به دستگاه‌های حسگر مجهز شوند و آدرس منحصر بفـردی بـرای خود داشته باشند و به این صورت قادر به جمع‌آوری اطلاعات، اتصال به اینترنت و ایجاد شبکه‌ای از شبکه‌های اشیاء اینترنتی از اشیاء هستند .

چشم‌انداز اینترنت گرا

تمرکز دید اینترنت گرا بر روی IP برای اشیاء هوشمند است و پیشنهاد می‌کند از پروتکل های اینترنت برای حمایـت از اتصـال اشیاء هوشمند در سراسر جهان استفاده شود. به عنوان یک نتیجه این دیدگاه چالش‌های توسـعه زیرسـاخت اینترنـت بـا یـک فضای آدرس IP که می‌تواند تعداد زیادی از اشیاء متصل به هم را در خود جای دهد مطرح می‌کنـد. توسـعه IP v6 بـه عنـوان یک مسیر برای مواجهه با این موضوع شناخته شده است.

تمرکز دیگر این دیدگاه توسعه وبی از اشیاء است که در آن استانداردهای وب و پروتکل ها برای اتصال دستگاه‌های تعبیه شـده که بر روی اشیاء روزمره نصب شده‌اند به کار گرفته می‌شوند.

این موضوع با استفاده از استانداردهای فعلی معروف امکان‌پذیر می‌باشد استانداردهایی چـون URL ، HTTP ، Rest ful API که برای دسترسی به دستگاه‌های فیزیکی و یکپارچه کردن اشیاء در وب به کار می‌روند.

چشم‌انداز معناگرا

ناهمگونی در بین اشیاء IOT همراه با تعداد زیادی از اشیاء درگیر چالش‌های قابل توجهی در مـورد قابلیـت همکـاری در بـین آن‌ها به وجود می‌آورد. فناوری های بالقوه راه‌حلی برای نشان دادن، تبادل، ادغـام و مـدیریت اطلاعـات در یـک روشـی کـه بـا ماهیت جهانی اینترنتی از اشیاء سازگار است نشان می‌دهند.

در واقع در این دیدگاه ایده اصلی ایجاد یک تعریف استاندارد شده برای منابع ناهمگون، توسعه مدل‌های اطلاعـات بـه اشـتراک گذاشته شده جامع، تهیه واسطه معنایی و محیط‌های اجرایی است و در نتیجه انطباق معنایی ادغـام و قابلیـت همکـاری بـرای داده‌هایی تکه از منابع مختلف به دست آمده است.

انواع داده در اینترنت اشیاء

RFID Data : سیستم‌های RFID یک مفهوم اصلی از اینترنت اشـیاء هسـتند در واقـع روش اسـتفاده امـواج رادیـویی بـرای شناسایی و ردیابی اهداف مشخص است .

Sensor Data: شبکه‌های سنسور در حال حاضر به طور گسترده از مقیاس کوچک به بزرگ گسـترش یافتـه اسـت. همچنـین حسگرها یک جزء کلیدی در اینترنتی از اشیاء هستند. استفاده از تحسگرها با توجه به پارامترهای محیط زیست و یا هر برنامـه کار بردی متفاوت است.

Multimedia Data: داده‌های چندرسانه ای اصطلاحاً به همگرایی متن، تصویر، صدا، ویدئو داخل یک فرم تنها اشاره دارد.

Positional Data: داده‌های وابسته به موقعیت نشان‌دهنده محل یک شی در یک سیستم موقعیت یاب است بـه عنـوان مثـال یک سیستم تعیین موقعیت جهانی (GPS) .

Command Data: بعضی از دیتاهای داخل شبکه فرمان می‌دهند. ویتاهایی تکه برای کنترل دستگاه‌هایی از قبیل محـرک هـا مورد استفاده قرار می‌گیرند.

۳- بررسی امنیت در رایانش ابری و اینترنتی از اشیاء

۳-۱- تعریف اعتماد در IOT

اعتماد در تفاهم مشترک خود یک احساس انسانی است که تصمیم و رفتار را تحت تأثیر قرار می‌دهد. حضور اعتقاد احساس راحتی، تمایل به همکاری (و یا در صورت نیاز عمل) و بی‌دقتی بالقوه را فراهم می‌کند، در حالی که عدم اعتماد منجر به احتیاط، احساس نا امنی، عدم همکاری می‌شود. در میان بسیاری از تعاریف و مفاهی مختلف اعتماد ما در تحال حاضر تمرکز ختود را بته درک انسان از اعتماد با توجه به IOT محدود می‌کنیم. اقدامات ما چند تعریف را به اعتماد اختصاص داده است، به عنوان مثال موضوعی که در آن اعتماد تجربه می‌شود و یا از اندازه‌گیری که از طریق آن درجه اعتماد اختصاص داده است، به عنوان مثال موضوعی که در آن اعتماد تجربه می‌شود، و یا اندازه‌گیری که از طریق آن درجه اعتماد را می‌توان در یک وضعیت خاص (مانند پول) ارزیابی کرد، به طور کلی اعتماد انتظار رفتاری خاص از یک مورد است یا این‌که یک رویداد مرتبط با آن رخ می‌دهد یا نه.

۳-۲- تعریف امنیت در IOT

ما همچنین مفهوم اعتماد را با تجربه به کاربر IOT از امنیت آن‌ها گسترش دادی. در تعریف امنیت IOT ما از مفهوم یک سیستم کلی از دستگاه‌های به هم پیوسته شروع می‌کنیم .

رویکرد کلی ما حفظ تعادل بین وضعیت واقعی امنیت سیستم و امنیت درک شده کاربر (و درنتیجه اعتماد آن‌ها) در هنگام استفاده از سیستم بوده است. هدف از این روش جلوگیری از اعتماد بیش از حد کاربرد به سیستم در ۳صورت ناامنی (که اغلب منجر به افشای داده‌های حساس در حضور افراد غیر قابل اعماد می‌شود)، وجلب اعتماد کاربر در صورت امنیت سیستم است. با حفظ چنین تعادلی بین اعتماد و امنیت، ما انتظار پذیرش اجتماعی بهتر IOT و کاهش ضررهای کسب و کار ارائه‌دهندگان خدمات IOT در دراز مدت را داریم .

۳-۳- ساخت مدل امنیتی IOT

هنگام تجزیه و تحلیل روابط امنیت و اعتماد درون IOT، با فدراسیون دستگاه‌های IOT سروکارداریم فدراسیون ها مانند ابرهای خصوصی (که در ۲-۱ توضیح داده شد) توسط یک گروه از دستگاه‌های مرتبط متصل به یک زیر شبکه شکل می‌گیرند. شبکه‌ها توسط یک مرز اعتماد، که توسط به اشراک گذاری یک دایره اعتماد مشخص و یا بالینک دادن به زنجیره‌ای از اعماد شکل می‌گیرد، محدود شده‌اند.

تشکیل شبکه ممکن است بر مبنای تسهیلات، یک فرد و یا نزدیکی فیزیکی دستگاه‌ها باشد. برخی از منابع داخل شبکه ممکن است میان بسیاری از کاربران با ریشه اعتماد متمایز و یا همپوشانی شده به اشتراک گذاشته شود. مرزهای اعتماد موانع سخت و ثابتی نیستندف اما ممکن است یا ترک یا وارد شدن دستگاه به فدراسیون دچار تغییر شوند. نمونه نخست فدراسیون ها خانه‌ها و دفاتر هوشمند می‌باشد. این فدراسیون ها به یک مرکز و سازمان و یا یک فرد دارای بسیاری از دستگاه‌ها، مانند مورد خانه‌های هوشمند مطابقت دارند. علاوه بر این دستگاه ممکن است بخشی از چندین فداراسیون مستقل باشد.

مسائل امنیت و اعتماد از دو دیدگاه مختلف به وجود می‌آیند، ناز دیدگاه سوژه و شیء

از نظر فدراسیون، دارایی های داخلی باید از تهدیدهای خارجی محافظت شود. اهداف مشترک امنیت در این مورد محرمانه، یکپارچه و در دسترس هستند.

دیدگاه دیگر این است که یک دستگاه با فدراسیون های موجود تعهد داشته باشد. گذشته از حفاظت از دارایی های داخلی، ملاحظات حریم خصوصی به یک نگرانی تبدیل شده است.

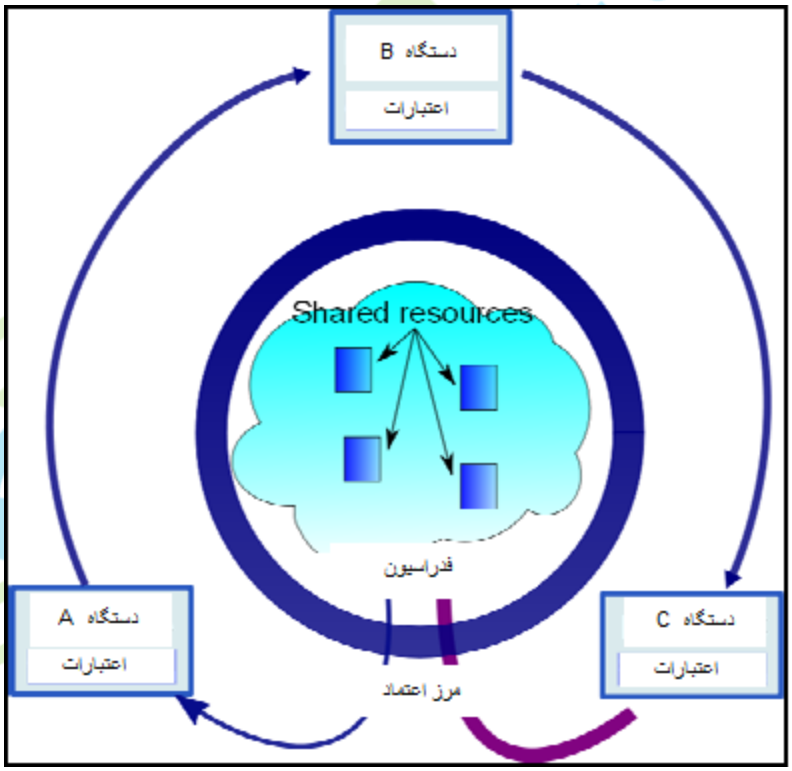
نگرانی دیگر پروفایل منابع است تکه در آن فدراسیون منطبق شده در موقعیتی است که مشخصات استفاده منابع عوامل تازه پیوسته شده را پروفایل می‌کند و در نتیجه احتمالاً حریم تخصوصی نقض می‌شود.

یکی دیگر از مجموعه مشکلات مربوط به عملیات درون IOT می‌باشد. عوامل ممکن است دیگر شرکت‌کنندگان را برای پیوستن به فدراسیون دعوت کنند، یا دسترسی به دارایی فدراسیون را در اختیار آن‌ها قرار دهند . به عنوان مثال اثر یک انجمن صاحب خانه‌ها دارای یک رویدارد رأی دادن الکترونیکی باشد، شرکت‌کنندگان به وجود آید که صاحب خانه در خارج از کشور باشد و نمی‌توانند رویداد حضور داشته باشد.

مثال دیگر مدیریت یک مرکز چند رسانه‌ای هوشمند است. اعضای خانواده از یک سطح آشکارتر بیشتر از مهمانان لذت می‌برند. با این وجود یک مهمان ممکن است منظور کنترل پخش و به اشتراک گذاری موسیعی سطح آشکارتری توسط یکی از اعضای خانواده داده شود.

تجزیه و تحلیل سناریوهای کار uTRUSTit مجموعه‌ای از ویژگی‌های مشترک را تولید کرد تکه در اغلب موارد به نظر می‌رسند. بعضی سناریوها کاربردهای ممکن IOT را که ممکن است در آسنده به کار گرفته شوند پیش‌بینی کرده است. به منظور تجزیه و تحلیل این سیستم‌ها، برخی از فرضیات معماری در مورد آن‌ها در نظر گرفته شده است. ما باید از یک مدل معماری استفاده کنیم که به طور کلی و به اندازه کافی برای تحقیقات ما غیر محدود باشد.

نگرانی اصلی ما امنیت و اعتماد بوده بنابراین مدل ارائه شده تنها چشم‌انداز امنیت و اعتماد IOT را توصیف می‌کند.



شکل۱ – مدل امنیتی IOT

۳-۴- امنیت برای محاسبات ابری چیست؟

کنترل‌های امنیتی در رایانش ابری با کنترل‌های امنیتی در هر محیط دیگر IT تفاوتی ندارد. با این حال به دلیل استخدام مدل‌های خدمات ابری، مدل‌های عملیاتی و تکنولوژی‌های مورد استفاده برای فعال خدمات ابر، محاسبات ابری ممکن است خطرات متفاوتی غیر از راه‌حل‌های سنتی IT ارائه دهد. رایانش ابری به آرامی در حال از دست دادن کنترل است در حین اینکه در حال حفظ پاسخگویی است حتی اگر مسئولیت عملیاتی بر عهده یک یا چند شخص ثالث باشد.

وضعیت امنیتی یک سازمان با بلوغ، اثر بخشی و کامل بودن اجرای کنترل‌های امنیتی و تنظیم ریسک مشخص می‌شود. این کنترل‌ها در یک یا چند لایه اجرا می‌شوند اعم از امکانات (امنیت فیزیکی)، زیر ساخت شبکه (امنیت شبکه) سیستم‌های IT (امنیت سیستم)، همه روش‌های اطلاعاتی و برنامه‌های کاربردی (امنیت برنامه‌های کاربردی)، علاوه بر کنترل تها تفکیک وظایف و مدیریت تفسیر نیز به ترتیب اجرا شده‌اند.

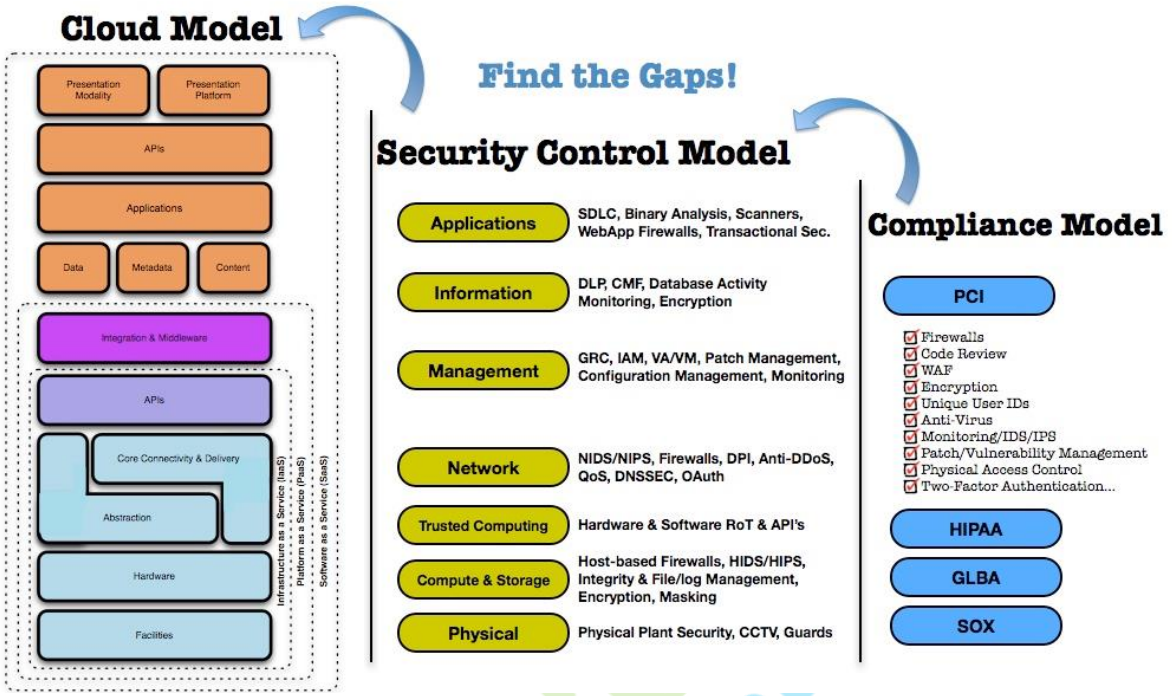
مسئولیت‌های امنیتی ارائه‌دهنده مشتری تا حد زیاد بین مدل‌های خدمات ابر متفاوت است. به عنوان مثال زیر ساخت های AWSEC2 امازون به عنوان یک ارائه‌دهنده خدمات شامل مسئولیت فروشنده برای امنیت بالا تا هایپروژن است. به این معنی که آن‌ها تنها می‌توانند رسیدگی به کنترل‌های امنیتی مانند امنیت فیزیکی، امنیت زیست محیطی و امنیت مجازی سازی را انجام دهند.

مشترک نیز به نوبه خود مسئول کنترل‌های امنیتی است که به سیستم IT مربوط می‌شود از جمله سیستم عامل برنامه‌های کاربردی و داده‌ها .

بر عکس ارائه‌دهنده saas مدیریت منابع مشتری Sales firce. com (CRM) است چون کل پشته بوسیله salesforce.com تهیه شده است و تهیه‌کننده نه تنها مسئول کنترل‌های امنیتی، فیزیکی و زیست محیطی است همچنین باید به کنترل‌های امنیتی روی زیر ساخت، برنامه‌های کاربردی و دیتا نیز بپردازد.

این مسئولیت‌های عملیاتی مستقیم مشتری یک بسیار کاهش می‌دهد. یکی از جذابیت های رایانش ابری بازده هزینه است که به وسیله اقتصاد مقیاس، استفاده مجدد استانداردسازی فراهم شده است. براین به وجود آمدن این بازده مؤثر تهیه‌کنندگان مجبور به ارائه خدماتی هستند که به اندازه کافی برای خدمت به بزرگ‌تری پایگاه مشتری ممکن انعطاف‌پذیر باشند و آدرس پذیری بازار خود را به حداکثر برسانند. متأسفانه یکپارچه سازی امنیت با این راه‌حل‌ها اغلب به صورت انعطاف پذیرتر کردن آن‌ها مشاهده شده است.

این انعطاف ناپذیری اغلب در ناتوانی برای به دست آوردن تعادل برای استقرار کنترل امنیتی در محیط‌های ابر در مقایسه با IT سنتی آشکار می‌شود. این محور ها عمدتاً ناآگاهی از کیفیت واقعی زیر ساخت و فقدار دیر و توانایی ادغام بسیاری از کنترل‌های امنیتی آشنا به‌خصوص در لایه شبکه است. شکل زیر موارد زیر را نشان می‌دهد .



شکل ۲- نقشه مدل ابر با کنترل امنیتی و مدل پذیرش

در saas محیط‌های کنترل‌های امنیتی و دامنه آن‌ها در قرار داد برای خدمات مذاکره کرده‌اند که سطح خدمات، حفظ حریم خصوصی و قبول همه موضوعاتی که در قرار داد هستند به صورت قانونی برخورد شود. در ارائه Laas در حالی که مسئولیت امنیت زیر ساخت اساسی و لایه‌های استزاع متعلق به تهیه‌کننده است، باقی مانده پشته مسئولیت مشتری است.
Paas یک تعادلی ارائه می‌کند مابین جایی که امنیت پلت فرم که بر عهده تهیه‌کننده است و امنیت برنامه‌های کاربردی که در مقابل پلت فرم توسعه می‌یابد و مطمئناً برنامه‌هایی که در حال توسعه اند بر عهده مشتری است. درک تأثیر تفاوت‌ها بین مدل‌های خدمات و چگونگی توسعه آن‌ها برای مدیریت ریسک یک سازمان حیاتی است.

۳-۵- مدل مرجع امنیت ابر

مدل مرجع امنیتی ابر نشان‌دهنده روابطی از کلاس‌ها و مکان‌های آن‌ها در متن با نگرانی ها و کنترل‌های امنیتی مربوطه شان برای سازمان‌ها و افرادی که با رایانش ابری برای اولین بار دست و پنجه نرم می‌کنند.
برای جلوگیری از مشکلات بالقوه و سردرگمی توجه به نکات زیر مهم است:
درک اینکه سرویس‌های ابری چگونه مستقر شده‌اند اغلب به جای اینکه چطور آن‌ها ارائه شده‌اند مورد استفاده قرار می‌گیرد و این منجر به گیجی می‌شود.
برای مثال ابرهای خصوصی یا عمومی ممکن است به صورت ابرهای داخلی یا خارجی بیان شوند که ممکن است در همه موقعیت‌ها درست باشد یا نباشد.
شیوه‌ای که خدمات ابری استفاده کرده است اغلب وابسته به موقعیت مدیریت یک سازمان یا محیط امنیتی (معمولاً به وسیله حضور یک دیواره آتش تعریف می‌شود) توصیف شده است. درحالی که از لحاظ رایانش ابری درک مرزهای امنیتی نادرست مهم است شیوه‌ای که در آن محیط به خوبی مشخص شده‌اند یک مفهوم بی مورد است.

Re-perimeterization و فرسایش از مرزهای اعتماد که در حال حاضر در سازمان‌ها در حال اتفاق افتادن است بوسیله رایانش ابری تقویت شده و سرعت گرفته است.

طبیعت بی‌نظمی از تبادل اطلاعاتبا ناکارآمدی کنترل‌های امنیتی ایستای سنتی که نمی‌توانند به طبیعت پویای سرویس‌های ابر منجر شوند همه با توجه به محاسبات ابری نیاز به تفکر جدیدی دارند.

بر روش‌های استفاده و استقرار ابر باید تفکر شود نه تنها در چارچوب داخلی بلکه در مقابل ارتباطات خارجی با مکان‌های فیزیکی از دارایی ها، منابع و اطلاعات این تفکر باید صورت گیرد.

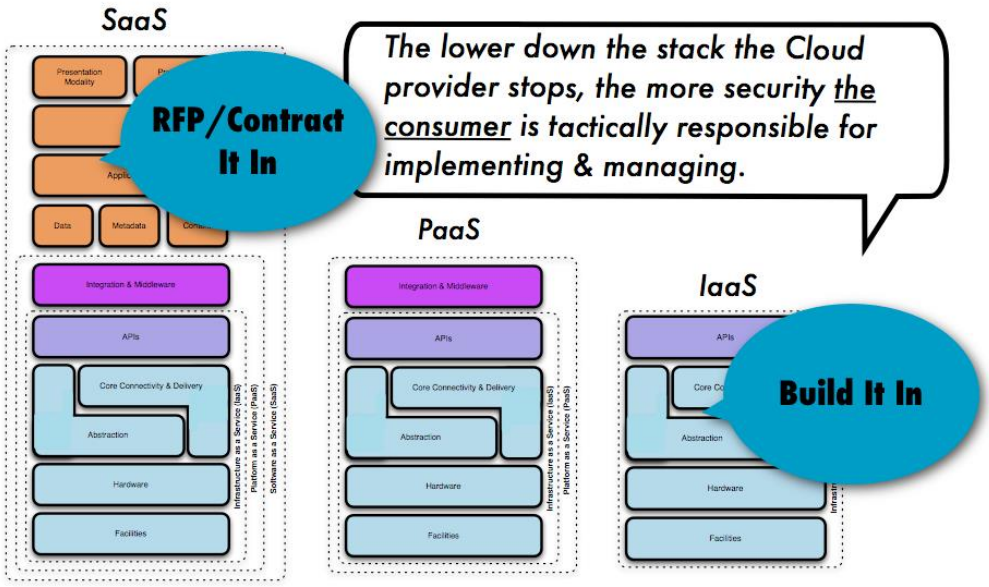
گذشته از این اینکه به وسیله چه کسی مورد استفاده قرار می‌گیرد و چه کسی مسئول حکومت و امنیت و انطباق با سیاست‌ها و استانداردهایشان است. تأکید بر ریسک همچنین بستگی به موارد زیر دارد:

انواع دارایی ها، منابع و اطلاعات مدیریت شده‌اند.

چه کسی و چگونه آن‌ها را مدیریت می‌کند.

چه کنترل‌هایی انتخاب شده و چگونه آن‌ها یکپارچه می‌شوند.

مسائل مربوط به پذیرش



شکل ۳-

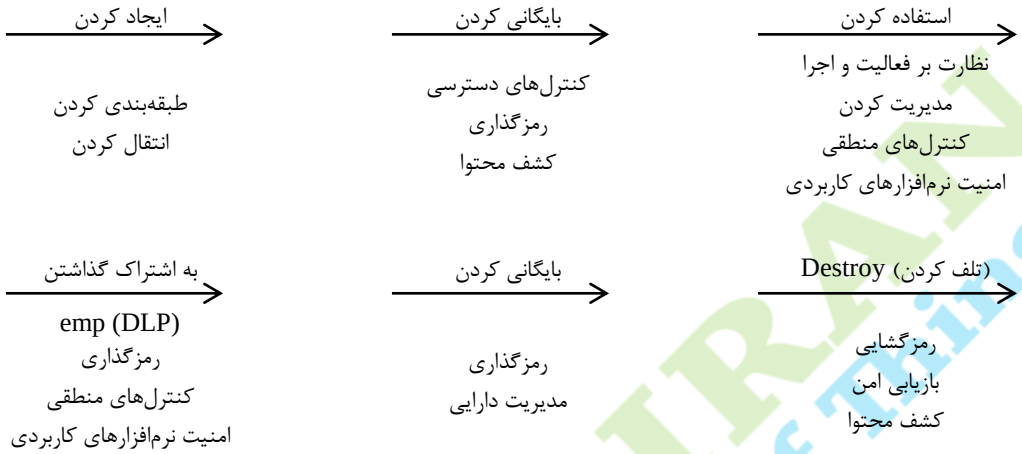
۳-۶- مدیریت چرخه عمر اطلاعات

یکی از اهداف اصلی امنیت اطلاعات محافظت از اطلاعات اساسی سیستم‌ها و برنامه‌های ما است. همان‌طوری که با انتقال سیستم‌ها به رایانش ابری، متدهای سنتی از امنیت اطلاعات به وسیله معماری مبتنی برابر به چالش کشیده شده‌اند. انعطاف‌پذیری، چند مالکیتی، معماری منطقی و فیزیکی جدید و کنترل‌های انتزاعی نیاز به استراتژی های جدید امنیت داده دارد.

بوسیله بسیاری مدل‌های استقرار ابر ما داده را به محیط‌های خارجی یا حتی عمومی انتقال می‌دهیم با روش‌هایی که تنها چند سال پیش غیر قابل قصور بود.

چرخه امنیت داده با چرخه مدیریت اطلاعات متفاوت است و این چرخه منعکس کننده نیازهای متفاوت از مخاطبان امنیتی است. چرخه عمر امنیت داده شامل شش مرحله است:

شکل ۴



چالش‌های کلیدی در مورد چرخه عمر امنیت داده‌ها در ابر شامل موارد زیر است:

- امنیت داده‌ها: محرمانه بودن، یکپارچگی، در دسترس بودن، اعتبار، مجوز، سندیت (قابل ارائه به صورت قانونی) و انکارناپذیری
- محل سکونت داده‌ها: باید در مورد داده‌ها اطمینان وجود داشته باشد از جمله نسخه‌های پشتیبان و کپی های آن‌ها که ذخیره شده‌اند در مکان‌های جغرافیایی مجاز به وسیله قرارداد، SLA و آیین‌نامه‌ها (مقررات)
- پس ماند داده‌ها یا تداوم: داده‌ها باید به طور مؤثر و به طور کامل حذف شده باشند تا از دست رفته شده تلقی شوند. بنابراین تکنیک‌هایی در این زمینه به طور کامل و مؤثر در ابر باید در دسترس باشند تا زمانی که مورد نیاز است مورد استفاده قرار گیرند از جمله این تکنیک‌ها: پاک کردن، از بین بردن داده‌ها یا ارائه غیر قابل جبران
- درآمیختن داده‌ها با دیگر مشتریان ابر: به طور ویژه داده‌های طبقه‌بندی شده و داده‌های حساس با داده‌های مشتریان دیگر بدون کنترل‌های جبرانی در حین استفاده از جمله ذخیره‌سازی یا انتقال نباید آمیخته شوند. مخلوط کردن یا درآمیختن داده‌ها تا زمانی که نگرانی ها در مورد امنیت داده‌ها و محل جغرافیایی مطرح شده است به چالش کشیده خواهد شد.

بازیابی و پشتیبان گیری داده‌ها طرح‌هایی برای بازیابی و بازگرداندن داده‌ها هستند داده‌ها باید در دسترس باشند و طرح‌های بازیابی و پشتیبان گیری داده برای ابر باید در محل مؤثر باشد.

- کشف داده‌ها: به عنوان یک سیستم قانونی همچنان تمرکز روی کشف الکترونیکی، ارائه‌دهندگان سرویس ابر و مالکان داده نیاز به تمرکز روی کشف داده‌ها، اطمینان قانونی و مقامات نظارتی که همه داده‌های درخواست شده بازیابی شده است خواهد داشت.

در یک محیط ابر پاسخ دادن به سؤالات بسیار مشکل است و کنترل‌های قانونی، تکنیکی و اجرایی مورد نیاز خواهد بود.

- استنباط و تجمیع داده‌ها: نگرانی هایی در ابر به خاطر استنباط و تجمع داده‌ها اضافه شده است که در نتیجه باعث نقض محرمانه بودن اطلاعات حساس و محرمانه می‌شود. از اینرو باید شیوه‌هایی باشد برای اطمینان مالکان داده و اطلاعات سهامداران که داده‌ها هنوز از نقض دقیق محافظت شده‌اند. موقعی که داده‌ها درآمیخته یا جمع شده‌اند در نتیجه

اطلاعات محافظت شده آشکار می‌شود. به عنوان مثال گزارش‌های پزشکی حاوی اسامی و اطلاعات پزشکی با اطلاعات بدون نام اما حاوی همان فیلد مخلوط شده‌اند.

۳-۶- امنیت نرم‌افزارهای کاربردی

محیط‌های ابر به واسطه مزیت انعطاف‌پذیری، باز بودن و اغلب در دسترس عموم بودن باعث شده است بسیاری مفروضات اصلی درباره امنیت نرم‌افزارهای کاربردی به چالش کشیده شود. برخی از این مفروضات به خوبی درک شده‌اند با این حال بسیاری هم هستند که درک نشده‌اند.

در این بخش بررسی می‌کنیم چطور رایانش ابری امنیت روی طول عمر یک برنامه کاربردی را از طراحی تا عملیات به انهدام نهایی تحت تأثیر قرار می‌دهد. این راهنمایی است برای همه ذینفعان از جمله طراحان برنامه، متخصصان امنیت، پرسنل عملیات و مدیریت فنی که بدانند چطور می‌توان بهترین مدیریت اطمینان و کاهش ریسک را در برنامه‌های رایانش ابری داشته باشند.

رایانش ابری یک چالش خاص برای برنامه‌های کاربردی در سراسر لایه نهایی از saas و paas و Iaas می‌باشد. برنامه‌های ابر مبتنی بر نرم‌افزار به یک طراحی دقیق شبیه به برنامه‌های ساکن در یک کلاس DMZ[1] نیاز دارند. این شامل یک تجزیه و تحلیل عمیق است که همه جنبه‌های سنتی از مدیریت اطلاعات به صورت محرمانه، یکپارچه و قابل دسترسی را پوشش دهد.

برنامه‌های کاربردی در محیط ابر به وسیله جنبه‌های عمده زیر اثر خواهند داشت:

- معماری امنیت برنامه‌های کاربرد

باید توجه شود که واقعیت این است که بیشتر برنامه‌های کاربردی روی سیستم‌های مختلف وابستگی داده می‌شود. با رایانش ابری برنامه‌های وابسته می‌توانند بسیار پویا باشند حتی در نقطه‌ای که هر وابستگی یک ارائه‌دهنده سرویس شخص ثالث جدا از هم را نشان می‌دهد. ویژگی‌های ابر مدیریت پیکربندی و تأمین مداوم را می‌سازند که به طور قابل توجهی پیچیده تر از به‌کارگیری نرم‌افزار سنتی است. محیط درایوها برای اطمینان از امنیت برنامه‌ها نیاز به تغییرات معماری دارند.

- چرخه عمر توسعه نرم‌افزار (SDLC)

رایانش ابری بر تمامی جنبه‌های SDLC تأثیر می‌گذارد. محدوده معماری نرم‌افزار، طراحی، توسعه تضمین کیفیت، مستندسازی، استقرار مدیریت، نگهداری و انهدام

- پذیرش (مطلوبیت)

پذیرش به وضوح بر داده‌ها تأثیرگذار است اما برنامه‌های کاربردی را نیز تحت تأثیر قرار می‌دهد. به عنوان مثال تنظیم یک برنامه که چطور یک تابع رمزنگاری خاص را پیاده‌سازی کند.

پلت فرم‌ها (شاید با تعیین کنترل و تنظیمات سیستم عامل)

فرآیندها (از جمله گزارش مورد نیاز برای حوادث امنیتی)

- ابزارها و خدمات

رایانش ابری تعدادی از چالش‌های جدید در مورد ابزار و خدمات مورد نیاز برای ساخت و حفظ برنامه‌های کاربردی در حال اجرا را معرفی می‌کند. این ها شامل توسعه و آزمون ابزارها، مدیریت برنامه‌های خدمات شهری، اتصال به خدمات خارجی و وابستگی به کتابخانه‌ها و سرویس‌های سیستم عامل می‌باشد که ممکن است از ارائه‌دهندگان ابر ناشی شود. درک شاخه‌هایی که عملیات و مسئولیت‌های فرضی را فراهم می‌کند برای این ها بسیار اساسی است.

[1] DMZ مخفف demilitarized zone به معنی منطقه غیر نظامی است. هدف DMZ افزودن یک لایه امنیتی اضافی به یک LAN است. یک مهاجم تنها به تجهیزات موجود در DMZ دسترسی دارد و نمی‌تواند به کل شبکه دسترسی داشته باشد.

- آسیب‌پذیری: این مورد نه تنها شامل مستندات و تحولات مداوم و آسیب‌پذیری‌های مرتبط با برنامه‌های وب می‌شود بلکه آسیب‌پذیری های مرتبط با ماشین به ماشین، برنامه‌های کاربردی معماری سرویس گرا را نیز شامل می‌شود که این برنامه‌ها به طور فزاینده‌ای در ابر مستقر شده‌اند.

۴- نتیجه‌گیری

رایانش ابری یک فناوری بسیار امیدوارکننده است که در کاهش هزینه‌های عملیاتی و افزایش بازدهی سازمان کاربرد فراوان دارد و شاهد کاربرد آن در حوزه‌های مختلف هستیم. از جمله اینکه رایانش ابری به عنوان پشتیبان اینترنت اشیاء می‌باشد به صورتی که برخی کارشناسان پیش‌بینی کرده‌اند ابر عمومی به عنوان ستون فقرات اینترنت اشیاء به جایگاه تثبیت شده برسد. در نتیجه میلیون ها شیء متصل به اینترنت در فضای ابر عمومی قرار خواهد گرفت و اطلاعات مربوط به آن‌ها به شکل ساده‌تری از گذشته قابل ثبت ذخیره‌سازی و تحلیل خواهد بود. با وجود این مقوله امنیت هنوز در مرحله آغازین قرار دارد و نیاز به توجه تحقیقاتی بیشتری دارد. امنیت دستگاه‌های مبتنی بر IOT بسته به نیاز کسب و کار تعیین می‌شود و نقش مدیران در ایجاد امنیت بسیار حیاتی است مسئله محرمانه بودن داده‌ها در رایانش ابری بسیار با اهمیت تر از شبکه سنتی است زیرا داده‌ها در محیط رایانش ابری به مقدار زیادی وابسته به شبکه و سرور می‌باشند و مشتریان زیادی وجود خواهد داشت که به مسئله امنیت و محرمانه بودن اطلاعات مشتریان رایانش ابری اعتماد ندارند و نمی‌خواهند داده‌های خود را به طرح زیربنایی ابری انتقال دهند این مسائل مانع از رشد رایانش ابری شده‌اند و مسئله امنیت از جمله مسائل هسته‌ای در این ارتباط است.

در این مقاله به ساخت مدل امنیتی IOT ، امنیت برای رایانش ابری،مدل مرجع امنیت ابر، چرخه عمر امنیت داده و چالش‌های کلیدی در مورد آن و امنیت نرم‌افزارهای کاربردی اشاره شده است.

در پایان می‌توان خاطرنشان کرد که به طور برجسته نیاز به کار مشتری در زمینه‌های مختلف امنیت همچون مسئولیت ارائه‌دهندگان در قبال خدمات خود در ابرها مورد نیاز است تا خدمات شفاف و قابل اطمینانی برای افراد جامعه مهیا شود.

مراجع

[1] Thi Anh Mai Phan. Kongens lyngby 2013
IMM- M.S.C- 2013- 48. Cloud databases for internet- of- things data
[2] Eugene Gorelik. 2013 Massachusetts Institute of technology working paper CISL- 2013-01. Cloud computing models
[3] Janne Poikolainen. University of Jyvaskyla 2012. Internet of things- emergence of standards.
[4] Stefan Mussato, zurich, Switzerland. University zurich. Guidline for mapping security of wireless sensor networks to security fundamentals.
[5] Josep Balash. March 2014. Implementation aspects of security and privacy in embedded design
[6] Daniel Petro, Gyogry vesztergombi. Search- LAB security evaluation analysis and research laboratory Ltd, budafokiut 91., 1117 Budapest, Hungary. Security and trust challenges in the area of the internet of things
[7] Best regards, Jerry Archer, Alan Boehme, Dave Cullinane, Paul Kurtz Nils Puhlmann, Jim Reavis. Cloud security Alliance Desambr 2009. Security Guidance for critical areas of focus in cloud computing v2.1