University of Qom

Engineering Management and Soft Computing

JEMSC.QOM
Online ISSN: 2538-2675

Improve security monitoring knowledge management in IOT applications based on user behavior analysis

Hossein Amoozadkhalili

Assistant Prof. ,Department of Industrial Engineering, Nowshahr Branch, Islamic Azad University, Nowshahr, Iran. Email: Amoozad92@yahoo.com

Article Info

Article type:
Research Article

Article history:
Received 2023 May 22
Received in revised 2023 June 26
Accepted 2023 June 30
Published online 2023 September 16

Keywords:
IoT,
knowledge management,
user information and content retrieval.

ABSTRACT

Content retrieval and knowledge management services In IoT applications, user-aware applications always contain different information and require a lot of resources to meet user demand, and this requires a high cost to implement content retrieval and management monitoring services. Is knowledge. This article presents a way to monitor knowledge management as well as to store and retrieve user information in the Internet of Things. Using the proposed method, users can transfer their data to IoT storage servers with more security than similar methods without knowing how and where to store it. The purpose of this article is to create a user-centric system for security monitoring of knowledge management in IoT applications that can be easily used. In this regard, reducing the cost of resource allocation and knowledge management by intelligently reducing the amount of data received and the use of appropriate factors to increase the quality of IoT applications have been addressed.

Cite this article: Amoozadkhalili, H. (2023). Improve security monitoring knowledge management in IOT applications based on user behavior analysis. *Enginiiring Management and Soft Computing, 9* (1). 123-139. **DOI**: https://doi.org/10.22091/JEMSC.2022.7056.1154

© The Author(s)
DOI: https://doi.org/10.22091/JEMSC.2022.7056.1154

Publisher: University of Qom

JEMSC.QOM
شاپا الکترونیکی: ۲۶۷۵-۲۵۳۸

مدیریت مهندسی و رایانش نرم

دانشگاه قم

بهبود امنیت نظارت بر مدیریت دانش در برنامه‌های کاربردی اینترنت اشیا مبتنی بر تحلیل رفتار کاربر

حسین عموزادخلیلی

استادیار، گروه مهندسی صنایع، واحد نوشهر، دانشگاه آزاد اسلامی، نوشهر، ایران. رایانامه: Amoozad92@yahoo.com

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت: ۱۴۰۲/۰۳/۰۱

تاریخ بازنگری: ۱۴۰۲/۰۴/۰۵

تاریخ پذیرش: ۱۴۰۲/۰۴/۰۹

تاریخ انتشار: ۱۴۰۲/۰۶/۲۵

کلیدواژه‌ها:
اطلاعات کاربران و بازیابی محتوا،
اینترنت اشیا،
مدیریت دانش.

چکیده

خدمات بازیابی محتوا و نظارت بر مدیریت دانش در برنامه¬های کاربردی اینترنت اشیاء آگاه از کاربر، همواره دارای اطلاعات مختلف هستند و برای برآوردن تقاضای کاربر، نیاز به منابع زیادی دارند و این کار نیاز به هزینه بالا برای اجرای خدمات بازیابی محتوا و نظارت بر مدیریت دانش دارد. در این مقاله روشی جهت نظارت بر مدیریت دانش و همچنین ذخیره و بازیابی اطلاعات کاربران در اینترنت اشیا ارائه گردید. با استفاده از روش پیشنهادی کاربران می‌توانند اطلاعات خود را با امنیت خاطر بیشتر نسبت به روش‌های مشابه و بدون اطلاع از نحوه و مکان ذخیره‌سازی، داده‌هایشان را به سرورهای ذخیره‌سازی اینترنت اشیا بسپارند. هدف این مقاله ایجاد یک سیستم کاربرمحور برای امنیت نظارت بر مدیریت دانش در برنامه‌های کاربردی اینترنت اشیاست که به سهولت قابل استفاده باشد. در این راستا به کاهش هزینه در تخصیص منابع و مدیریت دانش با استفاده از کاهش هوشمند حجم داده‌های دریافتی و استفاده از فاکتورهای مناسب برای افزایش کیفیت نظارت بر برنامه‌های کاربردی اینترنت اشیا پرداخته شده‌است.

استناد: عموزادخلیلی، حسین. (۱۴۰۲). «بهبود امنیت نظارت بر مدیریت دانش در برنامه‌های کاربردی اینترنت اشیا مبتنی بر تحلیل رفتار کاربر». *مدیریت مهندسی و رایانش نرم*، دوره ۹ (۱). صص: ۱۳۹-۱۲۳. https://doi.org/10.22091/JEMSC.2022.7056.1154

ناشر: دانشگاه قم

© نویسندگان.

۱) مقدمه

اینترنت اشیا[1] مفهومی جدید در دنیای فناوری اطلاعات و ارتباطات بوده و به‌طور خلاصه فناوری مدرنی است که در آن برای هر موجودی (انسان، حیوان و اشیا) قابلیت ارسال و دریافت داده از طریق شبکه‌های ارتباطی اعم از اینترنت یا اینترانت فراهم می‌شود. دستگاه‌های هوشمند در دسته‌ای کلی به نام اینترنت اشیا قرار می‌گیرند. در سطح پایه‌ای، اینترنت اشیا درواقع به ارتباط اشیاء مختلف از طریق اینترنت و برقراری ارتباط با یکدیگر می‌پردازد تا هدف آن یعنی فراهم‌کردن تجربه کاراتر و هوشمندتر محقق شود. همانند دیگر فناوری‌های جدید، اینترنت اشیا نیز می‌تواند در ابتدا مفهومی سردرگم‌کننده به‌نظر برسد(توماس ۲۰۲۱). همچنین این واژه به‌ویژه هنگامی که صحبت از استانداردهای مختلف و همچنین ایمنی و امنیت آن می‌شود، می‌تواند مفاهیم جدید و ویژه‌ای پیدا کند. به‌عبارت‌دیگر ایده طراحی دستگاه‌های مختلف با امکان برقراری ارتباط بی‌سیم به‌منظور رهگیری و کنترل از طریق اینترنت و یا حتی از طریق یک برنامه ساده مخصوص گوشی‌های هوشمند، اصطلاح اینترنت اشیا را توصیف می‌کند. تکنولوژی‌های شناسایی و ردیابی، حسگرهای سیمی و بی‌سیم و شبکه‌های فعال، پروتکل‌های افزایش ارتباط و هوشمندی اشیا مهمترین قسمت‌های اینترنت اشیا هستند. اینترنت اشیا یک مفهوم است که حضور گسترده‌ای در محیط‌های مختلف اعم از اتصالات بی‌سیم و سیمی و طرح‌های نشانی‌دهی منحصر به فرد اشیا داشته و قادر به تعامل و همکاری اشیا با یکدیگر و دیگر چیزها برای ایجاد برنامه‌ها یا خدمات جدید و رسیدن به اهداف مشترک را درنظر گرفته‌است. چالش‌های فراوانی در زمینه تحقیق و توسعه برای ایجاد یک جهان هوشمند وجود دارد.

مدیریت دانش، مدیریت دانایی یا مدیریت اندوخته‌های علمی به‌معنای دردسترس قراردادن نظام‌مند اطلاعات و اندوخته‌های علمی است به‌گونه‌ای که به هنگام نیاز در اختیار افرادی که نیازمند آنها هستند، قرار گیرند تا آنها بتوانند کار روزمره خود را با بازدهی بیشتر و موثرتر انجام دهند. در این دنیا، اقتصاد به سمت اقتصاد دانش محور حرکت کرده و بسیاری از معادلات کنونی کشورها را با چالش مواجه ساخته که این امر، خود حاصل فناوری اطلاعات و ارتباطات است (چوپرا و ساینی ۲۰۲۱). سازمان‌های کنونی اهمیت بیشتری جهت درک، انطباق‌پذیری و مدیریت تغییرات محیط پیرامون قائل شده و در کسب و بکارگیری دانش و اطلاعات روزآمد به‌منظور بهبود عملیات و ارائه خدمات و محصولات مطلوب‌تر به ارباب رجوعان پیشی گرفته‌اند. چنین سازمان‌هایی نیازمند بکارگیری سبک جدیدی از مدیریت به‌نام مدیریت دانش و برنامه‌های کاربردی اینترنت اشیا می‌باشند. برخی از سازمان‌ها براین باورند که با تمرکز صرف بر افراد، فناوری و فنون برنامه‌های کاربردی اینترنت اشیا می‌توان دانش را مدیریت کرد. خدمات بازیابی محتوا و نظارت بر مدیریت دانش در برنامه‌های کاربردی اینترنت اشیا آگاه از کاربر، همواره دارای اطلاعات مختلف هستند و برای برآوردن تقاضای کاربر، نیاز به منابع زیادی دارند و این کار نیاز به هزینه بالا برای اجرای خدمات بازیابی محتوا و نظارت بر مدیریت دانش می‌باشد (شوارتز ۲۰۲۰).

۲) پیشینه پژوهش

اینترنت اشیا در حال تبدیل‌شدن به یک عنصر کلیدی از اینترنت آینده و یک زیرساخت حیاتی ملی و بین‌المللی می‌باشد.

---

[1]. Internet of Things

با این شرایط تامین امنیت کافی برای زیرساخت‌های اینترنت اشیا، اهمیت روزافزونی پیدا می‌کند. برنامه‌های کاربردی مقیاس بزرگ و خدمات براساس اینترنت اشیا به‌طور فزاینده‌ای در برابر هرگونه اختلال، حملات و یا سرقت اطلاعات، آسیب‌پذیر هستند. پیشرفت‌ها در برخی حوزه‌ها برای ایجاد اینترنت اشیاء امن، موردنیاز است. ازجمله هدف‌های بدخواهانه و مخرب می‌توان به حملات DDOS/DOS که در حال حاضر به خوبی برای اینترنت فعلی قابل درک است، اشاره نمود. لیکن اینترنت اشیا نیز مستعد ابتلا به چنین حملاتی است. تکنیک‌های خاص و سازوکارهایی برای حصول اطمینان از حمل‌ونقل، انرژی، زیرساخت‌های شهرها که نمی‌تواند غیرفعال یا واژگون شوند، موردنیاز است. همچنین تشخیص حمله عمومی و بازیابی یا تاب‌آوری برای مقابله با تهدیدات خاص اینترنت اشیا موردنیاز است. مانند ایستگاه‌ها و گره‌های درمعرض خطر، کدهای مخرب و حملات هک.

امیرپور و همکاران (۱۳۹۶) ضمن اشاره به نقش اینترنت اشیا در محیط‌های فیزیکی و دیجیتال به تاثیر شگرف این تکنولوژی در مبحث مدیریت دانش در شهر هوشمند پرداخته تا بتوان به‌عنوان نمونه‌ای برای استفاده در سازمان‌های مختلف مورد استفاده قرار گیرد. همچنین مشکل مدیریت منابع محاسباتی در شبکه‌های محاسباتی لبه- ابر بررسی شده‌است. سرورهای لبه تلفن‌های همراه ابتدا باید درخواست‌های موردنیاز کاربران تلفن‌همراه و دستگاه‌های اینترنت اشیا (IoT) را برآورده کنند سپس منابع محاسباتی را به‌صورت عمده و در بستر شبکه‌های ابری تولید کنند تا سود آنها به حداکثر برسد. با توجه به زمان‌گیربودن مدیریت منابع محاسباتی ممکن است برای مقابله با ترافیک بالا، منابع دچار مشکل شوند. بنابراین سرورهای تلفن‌همراه در بستر ابر، باید برای سود حاصل از عمده‌فروشی، هزینه بازپرداخت کنند. گل‌دوزی و تاجفر(۱۳۹۵) بیان کردند اینترنت اشیا در تولید داده‌های فرآیندهای دانشی به‌ویژه کشف دانش در محیط‌های فیزیکی و دیجیتال، به‌شدت درحال‌توسعه است. طرح‌های پژوهشی و پروژه‌های کاربردی متعددی درخصوص اینترنت اشیا توسط دانشگاه‌ها و یا کنسرسیوم‌های مشترک صنعت و دانشگاه در سال‌های اخیر انجام شده‌است. به‌طور کلی دستاوردهای حوزه فناوری اطلاعات و ارتباطات به‌طور قابل توجهی باعث تغییر در روش ارائه اطلاعات در زمینه مدیریت شرایط اضطراری شده و در حوزه‌هایی نظیر تصمیم‌گیری، حافظه سازمانی، مدیریت دانش، به اشتراک گذاری اطلاعات، ارتباطات، هماهنگی و هوشیاری لحظه‌ای (مبتنی بر وضعیت و موقعیت) باعث افزایش و بهبود کارآیی مدیریت در شرایط اضطراری گردیده‌است. فرازمند و همکاران (۱۳۹۷) سیستمی مبتنی بر موبایل را پیشنهاد داده‌است که موبایل به‌طور خودکار با استفاده از ارتباط بلوتوثی با حسگرها، داده‌های مختلفی مانند ضربان قلب، موقعیت مکانی و فشارخون شخص را دریافت کرده و این داده‌ها را جمع‌آوری می‌کند سپس آنها را به یک مرکز مراقبت فرستاده و تصمیم‌گیری در مرکز مراقبت ویژه صورت می‌گیرد. این روش موقعیت مکانی را چشم‌پوشی نموده‌است و برای سوابق شخص هیچ‌گونه یادگیری انجام نمی‌گیرد و در موقعیت هیچ‌نوع تصمیمی نمی‌پذیرد. فرج‌زاده و همکاران (۱۳۹۸) نشان دادند که فناوری‌های اطلاعاتی به‌عنوان یک ابزار با ارزش برای انتشار اطلاعات شناخته شده‌است. تحقیقات نشان از توان بالای فناوری‌های جدید اطلاعاتی در افزایش سطوح دانش مرتبط با سلامت افراد دارد. فناوری اینترنت اشیا به‌عنوان یک فناوری اطلاعاتی جدید، برای اتصال منابع پزشکی موجود و ارائه مراقبت‌های بهداشتی قابل اعتماد، موثر و هوشمند برای سالمندان و بیماران مبتلا به بیماری مزمن استفاده می‌شود. در این راستا بررسی‌های جامع درمورد دستاوردهای محققان و پیشرفت اینترنت اشیا در سیستم‌های بهداشتی از دیدگاه

فناوری‌ها و روش‌های فعال انجام می‌گیرد. همچنین سیستم‌های مبتنی بر اینترنت اشیا و کاربردهای متنوع این فناوری در صنایع بهداشتی بررسی می‌گردد. درنهایت چالش‌ها و چشم‌انداز توسعه سیستم‌های مراقبت‌های بهداشتی مبتنی بر اینترنت اشیا به‌طور دقیق بحث می‌شود. ماریه پییر (۲۰۱۵) در تحقیقی سیستم مراقبت هوشمند سلامت که داده‌های ورودی را از سنسور مناسب دریافت می‌کند و از ارتباطات مختلف و تحلیل داده‌ها بهره می‌گیرد، ارائه نمود. این روش قابل اتکا، دقیق و لحظه‌ای داده‌ها، اشخاص درمعرض خطر را با روش‌های مناسب ارتباطی گزارش می‌کند. بهره‌گیری از روش‌های مناسب برای برقراری ارتباط پایدار و هوشمندی مناسبی با یادگیری ANFIS انجام می‌گیرد. این روش یک ماژول سخت‌افزاری مجزایی برای دریافت داده‌ها ارائه می‌کند. بهره‌گیری از فاکتورهای مختلف علائم حیاتی و قابل انعطاف بسیار حائز اهمیت است. همچنین استفاده از روش‌های هوشمندی برای دریافت داده‌های لحظه‌ای با حجم مناسب جهت افزایش سرعت این سیستم می‌تواند توانایی‌های سیستم را افزایش دهد. سون کیم (۲۰۱۸) سیستمی برای مدیریت از سلامت مبتنی بر برنامه‌های کاربردی اینترنت اشیا ارائه نمود که در آن یک میکروکنترلر به‌عنوان دروازه ارتباطی بین حسگرهای متعددی است که برای نظارت بر پارامترهایی ازقبیل شمارنده نبض، حسگر دما، شتاب‌سنج و غیره درنظر گرفته شده‌اند. میکروکنترلر اطلاعات را از حسگرها به‌دست آورده، آنها را پردازش نموده و از طریق پروتکل مناسب ارسال داده‌ها در شبکه (در اینجا از پروتکل Wi-Fi استفاده شده‌است) ارسال می‌کند و بدین‌ترتیب یک نظارت بی‌درنگ پارامترهای مراقبت از سلامت را برای متخصصان مراقبت از سلامتی فراهم می‌کند. سروری برای ذخیره و به‌روزرسانی داده‌ها با توجه به زمان و همچنین صفحه وبی برای نمایش داده‌های فعلی توسعه داده شده‌است. بدین‌ترتیب در هر زمان می‌تواند به‌سادگی با وارد شدن به یک صفحه وب HTML یا با تایپ‌نمودن آدرس IP منحصربه‌فرد مربوطه در مرورگر اینترنت، به اطلاعات دسترسی داشته باشد. این مقاله درمورد جزئیات پیاده‌سازی و ارزیابی روش خود اطلاعات بیشتری نداده‌است. داک نالی (۲۰۱۹) در تحقیقی مسئله مدیریت منابع را به‌عنوان سود حداکثری مدل کرده‌است. برای حل این مساله، ابتدا رابطه بین منابع محاسبه محفوظ، وظایف محاسباتی کاربران تلفن همراه و دستگاه‌های IoT و هزینه بازپرداخت را تحلیل نمود. سپس یک طرح عمده‌فروشی کارآمد را برای تعیین میزان منابع محاسبه عمده‌فروش طراحی کرد که با استفاده از آن می‌توان سود کل پیش‌بینی‌شده از سرور لبه موبایل را به‌حداکثر رساند. با توجه به منابع محاسباتی در این مقاله یک طرح بازپرداخت سریع برای سرورهای لبه تلفن‌همراه پیشنهاد شده‌است تا هزینه بازپرداخت به‌حداقل برسد. کولومتس (۲۰۱۹) به‌صورت خاص به پردازش‌ها و تحلیل‌هایی که در برنامه‌های کاربردی در حوزه سلامت در IoT انجام می‌شود، پرداخته است. لزوم استفاده از داده‌های این حوزه در کاهش مرگ‌ومیر و ابتلا به بیماری‌های مختلف باعث کاهش شدید هزینه‌های درمانی می‌شود. یکی از روش‌های پردازشی که در این مقاله به آن پرداخته شده‌است، شناسایی داده‌های نویز و یا داده‌های متفاوت با اغلب داده‌ها می‌باشد. این داده‌ها پتانسیل لازم برای بررسی بیشتر و توجه لازم را دارند زیرا الگوی رفتاری آنها با سایر افراد جامعه متفاوت است و شناسایی زودهنگام این نوع از داده‌ها موجب صرفه‌جویی هزینه‌های درمانی می‌شود. جین و همکاران (۲۰۱۶) درمورد یک روش کارآمد برای تجمیع داده‌ها و تحویل قابل اطمینان داده‌ها براساس روش بی‌سیم اینترنت اشیا مطالعه و ارائه نمودند که یک سناریوی قابل استقرار در نقاط انتهایی شبکه‌های اینترنت اشیا ازقبیل حسگرهاست که این نقاط مجبور به ارسال داده‌های خود بر روی پیوندهای پُراتلاف به‌سمت دیگر نقاط انتهایی اینترنت اشیا هستند. به‌طورخاص، بی‌سیم اینترنت

اشیا یک رویکرد توزیع شده‌است که کاهش سود ترافیک به‌دست‌آمده از تجمیع داده‌ها براساس محتوا و مسیریابی ترافیک بر روی پیوندهای قابل اعتماد را با ترکیب اطلاعات کیفیت پیوند درنظر می‌گیرد. هدف مقاله ایجاد یک سیستم کاربرمحور برای امنیت نظارت بر مدیریت دانش در برنامه‌های کاربردی اینترنت اشیاست که به‌سهولت قابل استفاده باشد. در این راستا به کاهش هزینه در تخصیص منابع و مدیریت دانش با استفاده از کاهش هوشمند حجم داده‌ها دریافتی و نیز استفاده از فاکتورهای مناسب برای افزایش کیفیت نظارت بر برنامه‌های کاربردی اینترنت اشیا پرداخته شده‌است. همچنین نتایج حاصل از روش پیشنهادی برای احراز هویت و کنترل دسترسی با تحلیل رفتار کاربر براساس معیارهای مختلف مورد بررسی قرار گرفته‌شد. نتایج حاصل از روش پیشنهادی در مقایسه با روش‌های مشابه نشان‌دهنده عملکرد قابل قبول روش می‌باشد.

۳) روش تحقیق

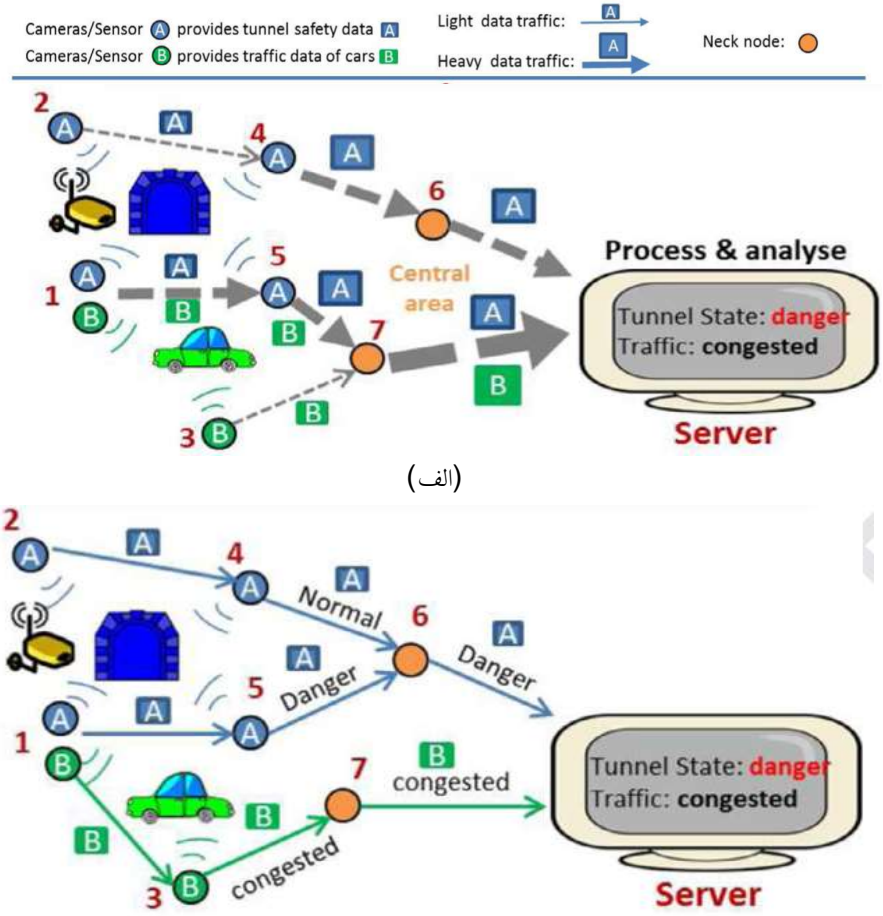
در این تحقیق ضمن مشخص نمودن مولفه‌های موردنیاز برای یک چارچوب نظارت مدیریت دانش به تعیین الزامات این چارچوب برای برنامه‌های کاربردی اینترنت اشیا براساس رفتار کاربر و حل چالش‌های این نوع از نظارت‌ها (امنیت و کیفیت سرویس) پرداخته شده‌است. همچنین ارائه روشی امن برای ارسال اطلاعات و تعیین ابزار و وسایل لازم برای تجزیه‌وتحلیل سیستم پیشنهادی بیان گردید. در این تحقیق برای گردآوری و تدوین مبانی نظری مربوط به موضوع تحقیق و بررسی سوابق تحقیق، از روش کتابخانه‌ای استفاده می‌شود. بدین‌منظور از کتب و مقالات موجود در کتابخانه‌ها و مقالات لاتین موجود در پایگاه‌های اینترنتی در رابطه با موضوع تحقیق، استفاده شد. جامعه آماری نیز مجموعه داده‌هایی که برای این منظور اضافه می‌شود، مجموعه داده‌های Healthdata.gov می‌باشد که طیف وسیعی از داده‌های پزشکی را شامل می‌شود. علاوه‌براین، در اجرای الگوریتم پیشنهادی از دیتاست nasa ناسا استفاده خواهد شد. ابزار گردآوری اطلاعات شامل مصاحبه و مشاهده می‌باشد. روش تجزیه‌وتحلیل نیز از نرم‌افزارMATLAB استفاده گردید و همچنین مقایسه نتایج روش ارائه‌شده در این مقاله با روش‌های مشابه صورت پذیرفت و تجزیه‌وتحلیل اطلاعات به دو صورت کمی و کیفی ارائه گردید.

۴) روش پیشنهادی

در این مقاله مشکل امنیت نظارت بر مدیریت دانش با هدف پایین‌آوردن هزینه استقرار و تضمین کیفیت خدمات به‌طور همزمان ارائه خواهد شد. به عبارتی توابع هدف در این تحقیق عبارتنداز هزینه، کیفیت سرویس و با توجه به عدم قطعیت در دستیابی به یک راه‌حل بهینه، از الگوریتم تقریبی استفاده گردید و نسبت تقریبی آنها را نیز تجزیه‌وتحلیل شد.

فرض می‌شود که گره‌ها، داده‌ها را به یک گره دروازه در مرکز توپولوژی ارسال می‌کنند. گره دروازه (به‌عنوان مثال از نظر پردازش قدرت، حافظه و غیره) نسبت به گره‌های جداگانه خود و دسترسی به تغذیه اصلی بسیار تواناتر است. گره‌ها دارای باتری و منبع اولیه و ناهمگن E (i) هستند. کنترل توان انتقال ممکن نیست و بنابراین تمام گره‌ها یک دامنه ارتباط ثابت دارند. ما همچنین فرض می‌کنیم که گره‌ها قابلیت پردازش ناهمگن دارند. برای مثال یک گره تنها قادر به پردازش یک یا چند نوع خاص از محتوا، به‌علت محدودیت‌های سخت‌افزاری یا نرم‌افزاری است. درصورتیکه یک گره، بسته داده‌ای را دریافت کند که قادر به پردازش آن نیست، به راحتی بسته را بازپخش می‌کند. برای شروع؛ گیت، یک پیام

رادیویی را ارسال می کند تا به گره‌ها اطمینان دهد که از چند دروازه عبور می کنند. گره‌هایی که این پیام را دریافت می کنند با شناسه لایه ID مشخص می‌شوند. بعد از انتصاب شناسه لایه، گره موردنظر، این پیام را با شناسه لایه خود در این پیام پیوند می‌دهد. چنین موجی همانند انتشار، منجر به تشکیل یک نوع توپولوژی می‌شود. اخیرا محاسبات توزیع‌شده در شبکه‌های بی‌سیم، توجه زیادی را به خود جلب کرده‌است. به‌خصوص با پدیدارشدن اینترنت اشیا (IoT) که به دستگاه‌های IoT با پردازش بالا، ارتباطات و قابلیت‌های ذخیره‌سازی مستقل مجهز شده‌اند. ایده کلیدی این است که به‌جای ارسال تمام داده-های خام به‌طور مستقیم در یک شبکه بی‌سیم گران‌قیمت (چندمنظوره) که معمولا با مصرف کیفیت بالا و تاخیر زمانی همراه است، یک روش ارزان‌تر برای اولین بار حجم داده را به‌صورت محلی با پردازش شبکه کاهش می‌دهد و سپس نتایج پردازش را انتقال می‌دهد. در بسیاری از موارد، داده‌هایی که برای یک برنامه کاربردی جمع‌آوری می‌شوند، به‌شدت همپوشانی دارند و به‌همین دلیل می‌توانند در هنگام انتقال به چاهک، ترکیب شده یا به‌طور مشترک پردازش شوند. برای مثال؛ خواندن حسگرهای چندگانه با یک رویداد فیزیکی یکسانی همراه است. چنین پروسه جمع‌آوری داده‌ها می‌تواند کل پیام‌های ارسال‌شده توسط لینک‌های گران‌قیمت بی‌سیم را کاهش دهد که تاثیر قابل توجهی بر مصرف کیفیت و همچنین بهره‌وری شبکه عمومی دارد. چنین پروسه جمع‌آوری داده‌ها می‌تواند کل پیام‌های ارسال‌شده توسط لینک‌های گران‌قیمت بی‌سیم را کاهش دهد که تاثیر قابل توجهی بر مصرف کیفیت و همچنین بهره‌وری شبکه عمومی دارد. از سوی دیگر، بسته‌های غیرمجاز ممکن است به‌سادگی از نقطه نظر پردازش جمع نشوند مثلا این رویکرد برای محاسبه میانگین دما و خواندن رطوبت معنی ندارد. بنابراین یک مسئله مهم در جمع‌آوری داده‌ها، تعیین یک جریان اطلاعات بهینه‌شده و توپولوژی ارتباطی است تا به‌طور موثر مسیر داده‌های متقابل به گره‌های پردازش درنظر گرفته‌شده در شبکه فراهم شود. بیایید به‌عنوان مثال، سیستم مانیتور تونلی را بررسی کنیم. همانطورکه در شکل ۱ نشان داده شده‌است، انواع گره‌ها و دوربین‌های حسگر برای نظارت بر دو برآورد تونل کلیدی نصب شده‌اند: ایمن ساختن تونل و مدیریت ترافیک. جایی که مقدار زیادی از داده‌های حسی حقیقی ازجمله تصاویر و جریان‌های تصویری باید به یک سنت کنترل از راه دور منتقل شود. به‌طور سنتی، سرور برای اولین بار تمام داده‌ها را از طریق همان توپولوژی مسیریابی، صرفنظر از اینکه آیا داده‌ها برای ایمنی تونل یا مدیریت ترافیک استفاده می‌شوند، جمع‌آوری می کند. این مورد در شکل ۱-الف نشان داده شده‌است. به‌عنوان مثال با درنظر گرفتن گره ۱، اطلاعات ایمنی تونل A و داده های ترافیکی B را به گره ۵ ارسال می کند که با آنها به‌صورت یکسان برخورد می‌شوند. هنگامی که تمام داده‌ها به مقصد می‌رسند، نتایج نهایی در سمت سرور محاسبه می‌شود. با این حال، این احتمال بسیار زیاد است که یک مشکل "نقطه عطفی" ایجاد شود که در آن ترافیک شبکه سنگین در ناحیه مرکزی سبب افزایش مصرف کیفیت در گره‌های گردن می‌شود و همچنین به حوادث احتمالی ترافیک منجر می‌شود. این به خاطر این واقعیت است که گره‌های گردن به لحاظ جغرافیایی به نقطه دسترسی/ سرور نزدیک‌تر است. بنابراین باید پیام‌هایی را که از مناطق بیرونی می‌آیند، منتقل کنند (شکل ۱-الف).



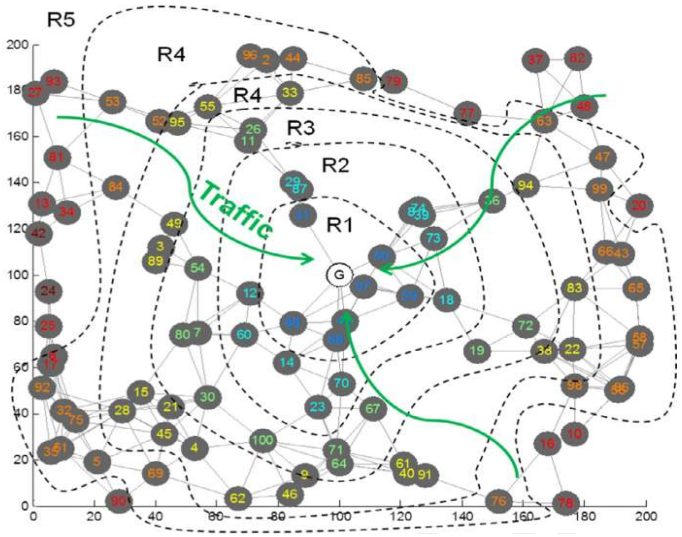
شکل ۱. مسیریابی سنتی در مقابل رویکرد بی‌سیم اینترنت اشیا؛ (الف) مسیریابی سنتی با پردازش متمرکز؛ (ب) بی‌سیم اینترنت اشیا و پردازش توزیع‌شده

برای غلبه بر چنین مشکلی، پروتکل مسیریابی مرکزی کاربرمحور(بی‌سیم اینترنت اشیا) برای جمع‌آوری داده‌های کارآمد در شبکه‌های چندتایی IoT پیشنهاد شده‌است. همانطورکه در شکل ۱-ب نشان داده شده‌است، ازآنجاکه هر دو گره ۱ و ۳ اطلاعاتی را برای شرایط ترافیک فراهم می‌کنند، به‌جای ارسال محتوا B به گره ۵ (نشان داده‌شده در شکل ۱-ب)، گره ۱ آن را به گره ۳ می‌فرستد که می‌توان آنها را در هنگام ارسال به سرور ترکیب و یا جمع‌بندی کرد. نتایج متوسط مانند هشدارهای ترافیکی سنگین را می‌توان در شبکه محاسبه کرد. درنتیجه، دو توپولوژی مسیریابی متمایز براساس محتویات A و B در بی‌سیم اینترنت اشیا ایجاد می‌شود. این می‌تواند منجر به کاهش میزان داده‌های فرستاده‌شده در شبکه و همچنین تاخیر زمانی در سیستم ارتباطی، صرفه‌جویی در کیفیت محدود گره و افزایش طول عمر شبکه شود. بی‌سیم اینترنت اشیا یک تغییر رویکرد را از روش‌های سنتی جمع‌آوری داده‌ها به روش جدید جمع‌آوری داده‌ها و بازیابی محتوا فراهم می‌کند. این تغییر می‌تواند چندین مزیت همچون بهره‌وری کیفیت، پاسخ سریع سیستم، طول عمر طولانی شبکه و غیره را به همراه داشته باشد و راه‌حلی برای حل مشکل انفجار اطلاعات برای شبکه IoT آینده فراهم می‌کند. یک تابع هدف چندگانه پیشنهاد شده‌است تا تجمیع داده‌های بهینه در شبکه با هدف کاهش تاخیر، تعادل بار و گسترش طول عمر

شبکه وجود داشته باشد. با استفاده از این، هر گره می‌تواند استراتژی مسیریابی خود را براساس الگوهای ترافیکی همسایه و دسترسی کیفیت گره‌های همسایه اصلاح کند. علاوه‌براین، یک مکانیزم انتخاب نامزد مسیریابی برای جلوگیری از حلقه‌های ارتباطی توسعه داده شد و هزینه انتقال سیگنال‌های پیام محلی برای کنترل گره و منابع محدود می‌شود.

۵) مدل‌سازی سیستم و فرضیات

فرض می‌شود که گره‌ها، داده‌ها را به یک گره دروازه[۲] در مرکز توپولوژی ارسال می‌کنند. گره دروازه (به‌عنوان مثال ازنظر پردازش قدرت، حافظه و غیره) نسبت به گره‌های جداگانه خود و دسترسی به تعزیه اصلی بسیار تواناتر است. گره‌ها دارای باتری و منبع اولیه و ناهمگن E (i) هستند. کنترل توان انتقال، ممکن نیست و بنابراین تمام گره‌ها یک دامنه ارتباط ثابت دارند. ما همچنین فرض می‌کنیم که گره‌ها قابلیت پردازش ناهمگن دارند. برای مثال یک گره تنها قادر به پردازش یک یا چند نوع خاص از محتوا، به‌علت محدودیت‌های سخت‌افزاری یا نرم‌افزاری است. درصورتیکه یک گره، بسته داده‌ای را دریافت کند که قادر به پردازش آن نیست، به راحتی بسته را بازپخش می‌کند. برای شروع؛ گیت، یک پیام رادیویی را ارسال می‌کند تا به گره‌ها اطمینان دهد که از چند دروازه عبور می‌کنند. گره‌هایی که این پیام را دریافت می‌کنند با شناسه لایه ID مشخص می‌شوند. بعد از انتساب شناسه لایه، گره موردنظر، این پیام را با شناسه لایه خود در این پیام پیوند می‌دهد. چنین موجی، همانند انتشار، منجر به تشکیل یک نوع توپولوژی می‌شود که در شکل ۲ نشان داده شده‌است.



شکل ۲. فاصله هاپ مبتنی بر توپولوژی رینگ

۶) مد جمع‌آوری و کاربرد

ما برنامه‌های نظارت و تحلیل رفتارکاربر(سناریوی جمع‌آوری داده‌ها از چند نقطه به یک نقطه) را برای هدف جمع‌آوری اطلاعات درنظر می‌گیریم. تمام بسته‌های داده مرتبط با یک پردازش مشابه، به‌عنوان یک بسته از همان محتوا درنظر گرفته می‌شود که می‌تواند توسط یکی از گره‌ها پردازش شود. به‌عنوان مثال یک نوع داده (خواندن درجه حرارت) در یک ساختمان

[2] .Gateway

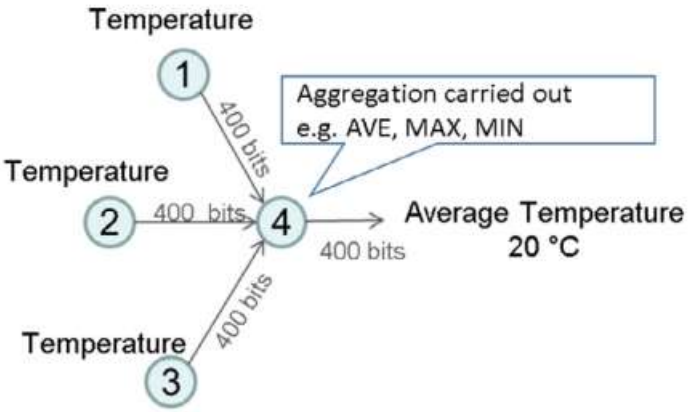
جمع‌آوری می‌شود، محتوای لازم برای یک برنامه که به دمای متوسط ساختمان نیاز دارد را فراهم می‌کند. فرض کنیم که هر برنامه در حال اجرا در شبکه تنها یک هدف پردازش واحد دارد اما برنامه‌های متعدد، می‌تواند وجود داشته باشد.

تعداد کل برنامه‌های کاربردی $K = \{ak \mid k = 1، 2، 3، \ldots\}$ دارای نرخ ورودی پوایسون[3] λ است اما با طول اجرای مختلف $T = \{tk \mid k = 1، 2، 3، \ldots\}$ و داده‌های ترافیکی ترافیک ناهمگن Rk. تابع تجمعی داده‌های مختلف را می‌توان با توجه به فرآیندهای تجمعی ازدست‌رفته یا تلفات اعمال کرد.

برای هر گره i با تابع پردازش s یک مدل عمومی جمع‌آوری داده در ادامه تعریف شده‌است:

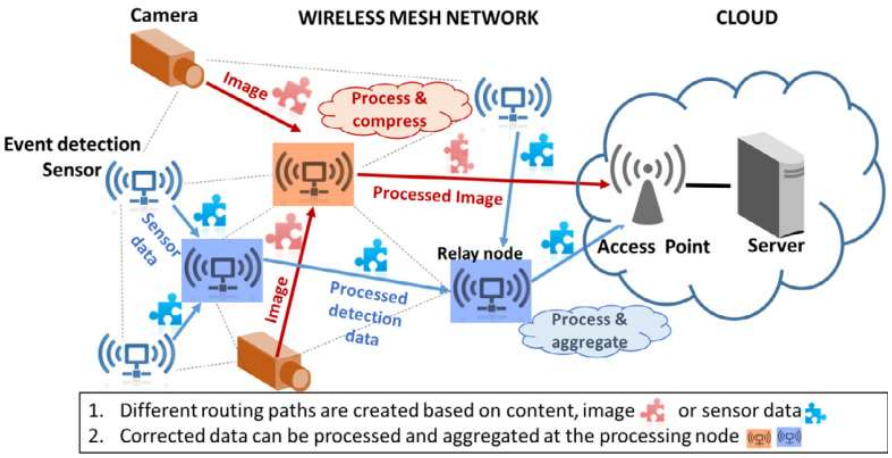
$$R_i^{out} = \omega_s * R_i^{in}$$
$$0 < \omega_s \leq 1$$

که در آن R_i^{in} و R_i^{out} به‌ترتیب نرخ ترافیک ورودی و خروجی را نشان می‌دهند. ωs جمع‌آوری داده یا میزان فشرده‌سازی را نشان می‌دهد که بستگی به تابع پردازش s دارد. اگر $\omega s = 1$ به این معنی است که محتوای کنونی توسط تابع s قابل پردازش نیست. ωs نیز می‌تواند متغیر و وابسته به تابع پردازش باشد. به‌عنوان مثال ممکن است همبستگی قابل توجهی از جریان داده‌ها شامل گزارش‌های داده‌ای از میانگین یا ماکسیمم خواندن برای نظارت بر برنامه‌های کاربردی،که می‌تواند پیام‌های چندین ورودی را به یک پیام خروجی تنها تبدیل کند، وجود داشته باشد. در چنین مواردی بسته به تعداد کل پیام دریافت شده (فرض M) بر روی گره تجمعی ωs می‌تواند M1 باشد. با این وجود ما فرض می‌کنیم که تنها پیام‌هایی از برنامه‌های مشابه، می‌توانند جمع شوند. به‌دلایلی داده‌ها با نوع مختلف ممکن است به‌راحتی پردازش نشوند و یا فقط در بعضی موارد امکان‌پذیر نباشد. به‌عنوان مثال محاسبه میانگین دما و رطوبت ارزش چندانی ندارد. یک نمونه از تجمع داده‌ها را می‌توان در شکل ۳ مشاهده کرد.



(الف)

[3] .Poisson



(ب)

شکل ۳. مدل‌های جمع‌آوری در کاربردهای مختلف

در آزمایش‌های صورت‌گرفته در این مقاله فرض شده‌است که سیستم دارای ۵۰ شی می‌باشد که به‌طور تصادفی در ۱۰ خوشه توزیع شده‌اند. هر یک از ۱۰ خوشه در یک منطقه محلی بر روی یک صفحه مربع شکل ۴ به اندازه ۱۰۰ × ۱۰۰ واقع شده‌است. در میان ۱۰ خوشه، یکی به‌عنوان خوشه مرکزی به سازماندهی تمام ۱۰ خوشه و به‌صورت یک توپولوژی درخت مشخص شده‌است. در هر خوشه، اشیا به‌طور تصادفی در منطقه محلی واقع در خوشه مستقر شده‌اند. علاوه‌براین، یک سوئیچ در هر خوشه برای ارائه ارتباطات درون‌خوشه‌ای و ارتباط بین‌خوشه‌ای بین اشیا وجود دارد.

براساس معماری سیستم، آزمایش‌های شبیه‌سازی بر روی پارامترهای زیر انجام شده‌اند.

الف) مقدار منابع در دسترس به‌صورت سه‌گانه (واحد پردازش مرکزی دردسترس برحسب گیگاهرتز، فضای حافظه موجود برحسب گیگابایت، فضای ذخیره‌سازی موجود برحسب گیگابایت) می‌باشد. بازه منبع [(۲۰۰، ۱۲۹، ۱۲)، (۹۶۰۰، ۳۰۰۰، ۹۶)] به‌طور تصادفی برای تصمیم‌گیری منابع دردسترس هر شی استفاده می‌شود.

ب) پهنای باند که در بازه [۱۰ گیگابایت در ثانیه، ۴۰ گیگابایت در ثانیه] فرض شده‌است.

برای شبیه‌سازی و ارزیابی الگوریتم پیشنهادی از نرم‌افزار c استفاده شده‌است. همچنین نتایج حاصل از روش پیشنهادی با نتایج روش‌های مشابه مقایسه شده‌است. مقادیر پارامترهای بسیار زیاد متاثر می‌شوند؛ این پارامترها به‌شدت به همگرایی بهتر بستگی دارند.

۷) معیارهای ارزیابی

ما برای ارزیابی روش پیشنهادی از چندین معیار استفاده کرده‌ایم. همچنین برای مقایسه از روش ارائه‌شده در مقاله هینزلمان (۲۰۰۲) استفاده کرده‌ایم که نتایج مقایسه در ادامه توضیح داده شده‌اند.

۷–۱) معیار FMR

نرخ تطابق جعلی یا FMR برابر است با احتمال قبول یک نمونه نادرست به‌عنوان نمونه‌ای اصلی. از این معیار به نسبت قبول

نادرست یا FAR نیز یاد می‌شود. به‌بیان ساده‌تر این معیار یعنی احتمال اینکه اثر فرد B به‌اشتباه به‌عنوان اثر فرد A شناخته شده باشد.

رابطه (۱)

$$\mathrm{FMR} = \frac{TP}{TP\ +\ FN}$$

۷-۲) معیار FNMR

FNMR احتمال ردشدن اشتباه یک نمونه از فرد قانونی یا اصلی است. در بسیاری از موارد به FNMR به‌عنوان نسبت ردشدن نادرست یا FRR نیز اطلاق می‌شود.

رابطه (۲)

$$\mathrm{FNMR} = \frac{TN}{TN\ +\ FP}$$

۷-۳) معیار دقت

این معیار نشان می‌دهد که روش پیشنهادی تا چه حد می‌تواند هویت را به‌درستی نمایش دهد.

رابطه (۳)

$$acc = \frac{TP + TN}{TP + FP + FN\ +\ TN}$$

۷-۴) معیار عدم پذیرش اشتباه

این خطا زمانی رخ می‌دهد که یک سیستم بیومتریک کاربر دارای مجوز را به اشتباه نپذیرد. FRR[4] به معنی نرخ عدم پذیرش اشتباه که خطای شماره یک هم نامیده می‌شود و درصد دفعاتی که عدم پذیرش اشتباه رخ می‌دهد را نشان می‌دهد.

۷-۵) معیار نرخ خطای مساوی EER[5]

کاهش نرخ پذیرش اشتباه باعث افزایش غیرتعمدی نرخ عدم پذیرش اشتباه می‌شود. نقطه‌ای که میزان نرخ عدم پذیرش اشتباه با نرخ پذیرش اشتباه برابر می‌شود، نقطه نرخ خطای مساوی است. هرچه میزان این پارامتر کمتر باشد نمایانگر این است که سیستم دارای یک حساسیت بهتر و توازن خوبی است.

۷-۶) معیار زمان اجرا

در این معیار مدت زمانی که طول کشیده تا نظارت بر مدیریت دانش به‌طور کامل انجام شود مورد مقایسه قرار گرفته است.

۸) امنیت روش پیشنهادی

در رمزنگاری مبتنی بر ویژگی کل، اطلاعات رمز نمی‌شوند و فقط ویژگی که از اطلاعات استخراج شده‌است، رمزنگاری می‌گردد. چون رمزنگاری سمت سرور صورت می‌گیرد، در حین انتقال اطلاعات در بستر شبکه از سیستم سرویس‌گیرنده به سرور ذخیره‌سازی، امنیت اطلاعات به خطر می‌افتد و اخلال‌گران می‌توانند با استراق سمع به اطلاعات کاربر دسترسی پیدا کنند. در روش پیشنهادی این مشکل حل شده‌است. احراز هویت و رمزنگاری اطلاعات قبل از ارسال، هر دو با استفاده از تحلیل رفتارکاربر که یک رمزنگاری با سطح امنیت بالا و روشی نامتقارن است، صورت می‌گیرد. این روش در مقایسه

[4]. False Reject Rate
[5]. Equal Error Rate

با روش‌های قبل، سطح امنیت بالاتری دارد زیرا در مرجع نامبرده از RSA تنها برای تولید کلید استفاده شده و برای رمزنگاری الگوریتم Blowfish که جز الگوریتم‌های متقارن و حتی ضعیف‌تر از DES عمل می کند، استفاده شده‌است. پس روش پیشنهادی امنیت بالاتری نسبت به روش‌های قبلی دارد و امنیت اطلاعات در آن نسبت به مراجع نامبرده عملکرد بهتری دارد.

۹) بار کاری سرویس‌دهنده

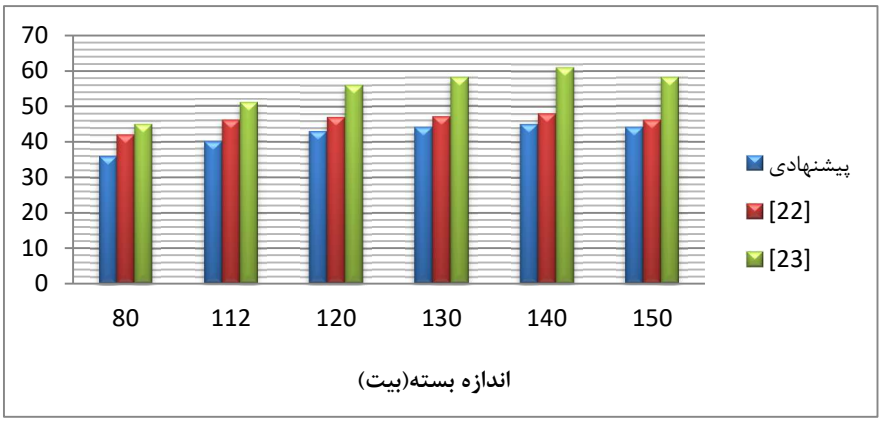
در روش پیشنهادی سرورهای ذخیره‌سازی تنها وظیفه ذخیره و بازیابی اطلاعات را برعهده دارند و درگیر مسائل دیگری مانند رمزنگاری و مدیریت حساب کاربری نمی‌شوند. پس بار کاری سرور کاهش می‌یابد و مشکل گلوگاه نیز برطرف خواهد شد.

جایگذاری فایل: در روش پیشنهادی اطلاعات به بخش‌های کوچکتری شکسته شده و روی چندین رسانه توزیع می‌شوند. بدین شکل ریسک ازبین‌رفتن اطلاعات کاهش می‌یابد و با مورد حمله قرارگرفتن یک سرور، کل اطلاعات فاش نخواهد شد. همچنین برای واکشی اطلاعات نیز چون اطلاعات همزمان از چندین سرور واکشی می‌شوند، سرعت نیز بالا می‌رود.

همچنین در قسمت پردازش، چون اطلاعات به‌صورت رمزنگاری‌شده از سیستم سرویس‌گیرنده به سرور اینترنت اشیا ارسال می‌شود در حین ارسال اطلاعات نیز اخلال‌گران به اطلاعات دسترسی نخواهند داشت. همچنین با تبادل کلید با استفاده از RSA عملیات احراز هویت کاربر صورت می‌گیرد.

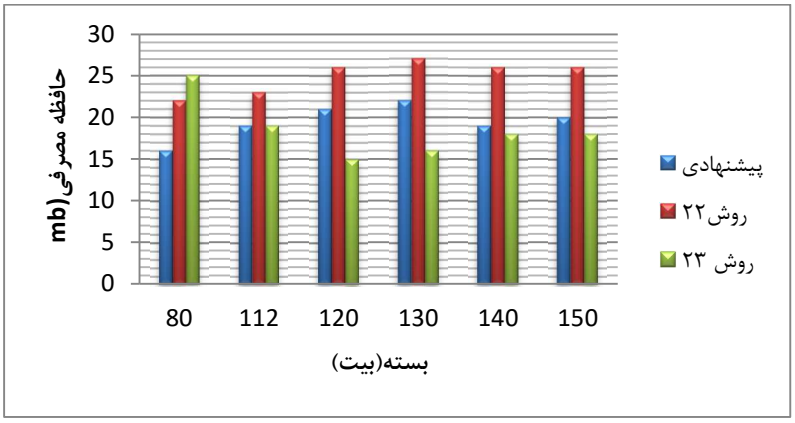
شکست فایل: همانطورکه گفته شد قبل از شروع آپلود فایل، ابتدا آن فایل به بخش‌های کوچکتری شکسته می‌شود. برخی روش‌های ذخیره‌سازی کل فایل را روی سرورها آپلود کرده و تنها به رمزکردن محتویات فایل اکتفا می‌کنند. این‌گونه روش‌ها به‌دلیل عدم شکست فایل، با مشکل روبرو خواهند بود.

معیار زمان اجرا: در این معیار مدت زمانی که طول کشیده‌است تا نظارت بر مدیریت دانش به‌طور کامل انجام شود، مورد مقایسه قرار گرفته‌است. در هر مرحله، اندازه بسته‌ها بیشتر شده‌است که در شکل ۴ قابل مشاهده می‌باشد.



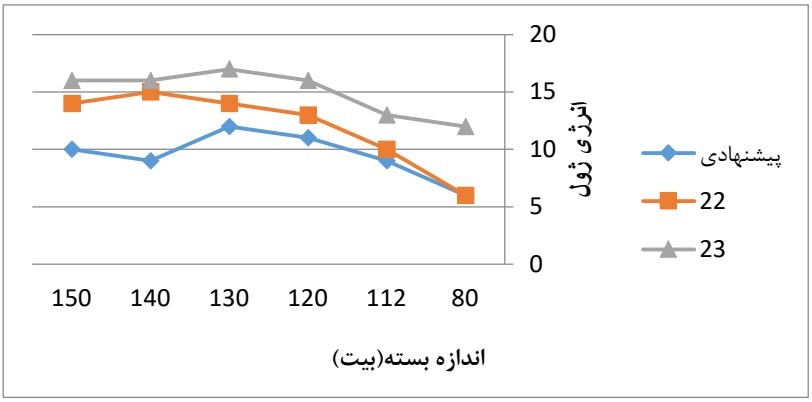
شکل ٤. زمان اجرا

معیار حافظه مصرفی: همانطورکه در شکل ۵ در این معیار میزان حافظه مصرفی (برحسب مگا بایت) بررسی شده‌است تا نظارت بر مدیریت دانش به‌طور کامل انجام شود. براساس تعداد بسته‌ها ارسالی، مورد مقایسه قرار گرفته است. نتایج نشان می‌دهد که روش‌های قبل به ازای بسته‌های بیشتر، کمترین میزان مصرف حافظه را دارد و روش پیشنهادی نتوانسته‌است به ازای بسته‌های بالا حافظه مصرفی را کاهش دهد.



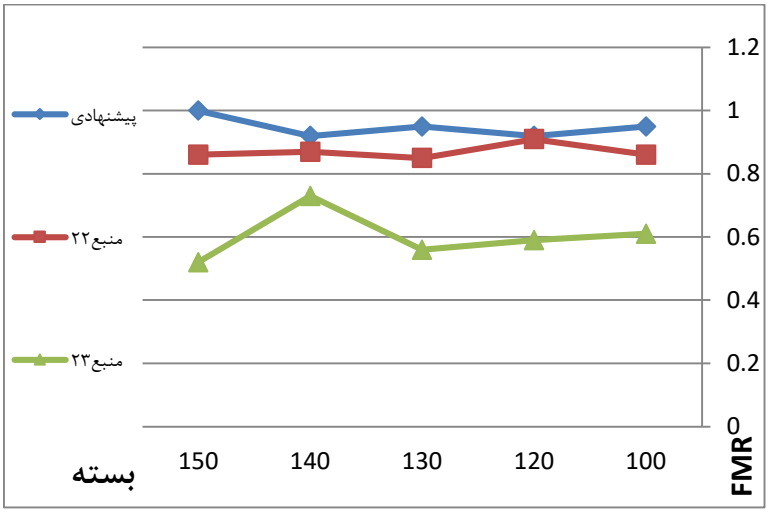
شکل ۵ . حافظه مصرفی

معیار انرژی مصرفی: در این معیار مقدار انرژی مصرفی برای انتقال اطلاعات از مبدا به مقصد تا درخواست‌های نظارت بر مدیریت دانش به‌طور کامل انجام شود، مورد مقایسه قرار گرفته‌است. در هر مرحله تعداد بسته‌های مربوط به داده‌ها بیشتر شده‌است. همان‌طورکه قابل مشاهده است روش پیشنهادی میزان انرژی مصرفی کمتری نسبت به روش‌های مشابه را به خود اختصاص داده‌است.



شکل ٦. انرژی لازم برای انتقال درخواست

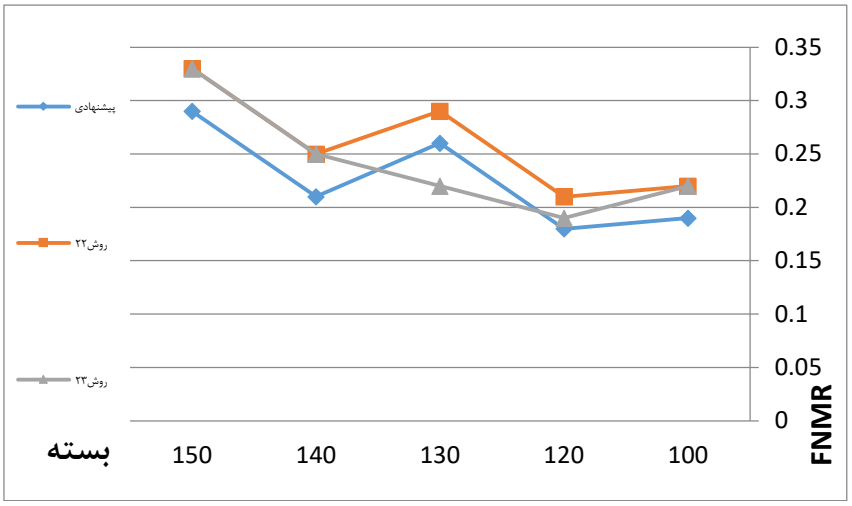
معیار FMR: نرخ تطابق جعلی یا FMR برابر است با احتمال قبول یک نمونه نادرست به‌عنوان نمونه‌ای اصلی. از این معیار به نسبت قبول نادرست یا FAR نیز یاد می‌شود. به‌بیان ساده‌تر این معیار یعنی احتمال اینکه اثر فرد B به‌اشتباه به‌عنوان اثر فرد A شناخته شده باشد. در شکل ۷ معیار FMR برای روش پیشنهادی به ازای بسته‌های مختلف مورد ارزیابی قرار گرفته‌است.



شکل ۷ . مقایسه معیار FMR

نتیجه شبیه‌سازی برای این معیار نشان می‌دهد که روش پیشنهادی از عملکرد بهتری برخوردار می‌باشد.

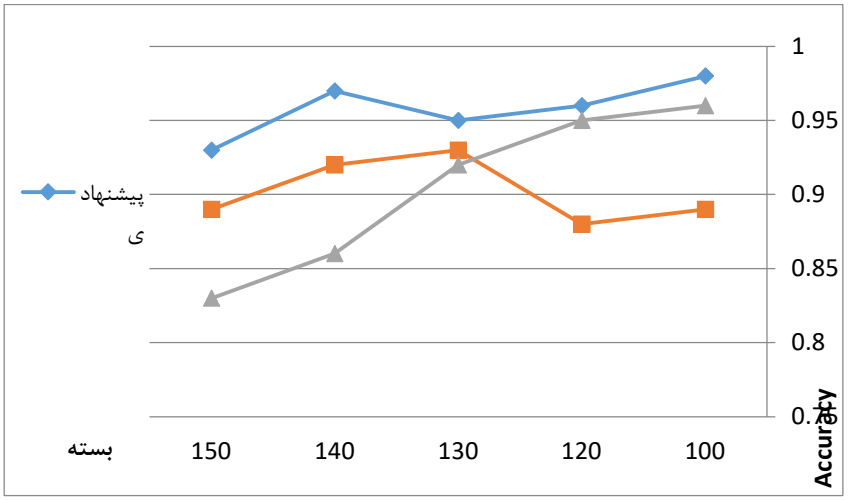
معیار FNMR : FNMR احتمال ردشدن اشتباه یک نمونه از فرد قانونی یا اصلی است. در بسیاری از موارد به FNMR به‌عنوان نسبت ردشدن نادرست یا FRR نیز اطلاق می‌شود. نتیجه شبیه‌سازی برای معیار فوق به ازای بسته‌های مختلف در شکل ۸ نمایش داده شده‌است.



شکل ۸ :مقایسه معیار FNMR

با توجه به نتیجه شبیه‌سازی روش پیشنهادی فقط در ۶ درصد مواقع دچار خطای FNMR می‌شود و نسبت به روش قبلی عملکرد بهتری دارد.

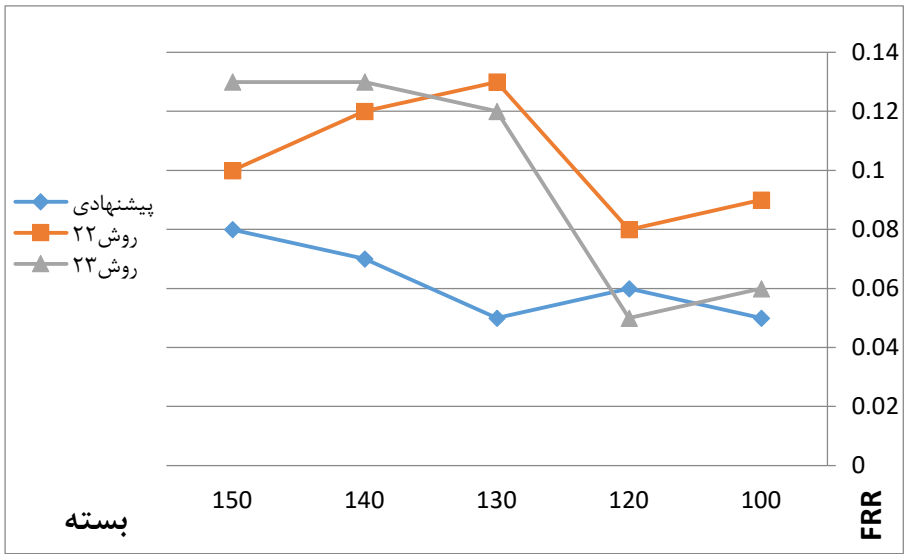
معیار دقت: این معیار نشان می‌دهد که روش پیشنهادی تا چه حد می‌تواند هویت را به‌درستی نمایش دهد. در شکل ۹ میزان دقت روش پیشنهادی برای ۱۰۰ اثر هویت متفاوت به ازای بسته‌های مختلف مورد مقایسه قرار گرفته‌است.



شکل ۹: مقایسه معیار دقت

نتیجه شبیه‌سازی نشان می‌دهد که روش پیشنهادی از دقت بالاتری نسبت به روش‌های قبلی به ازای بسته‌های مختلف برخوردار می‌باشد.

معیار عدم پذیرش اشتباه: این خطا زمانی رخ می‌دهد که یک سیستم بیومتریک، کاربر دارای مجوز را به اشتباه نپذیرد، FRRبه معنی نرخ عدم پذیرش اشتباه که خطای شماره یک هم نامیده می‌شود و درصد دفعاتی که عدم پذیرش اشتباه رخ می دهد را نشان می‌دهد.



شکل ۱۰: معیارFRR

روش پیشنهادی به‌دلیل استفاده از تحلیل رفتار کاربر باعث شده‌است که معیار عملکرد بسیار خوبی نسبت به روش‌های قبلی به ازای بسته‌های مختلف داشته باشد.

۱۰) نتیجه‌گیری

در این مقاله یک روشی جهت نظارت بر مدیریت دانش و همچنین جهت ذخیره و بازیابی اطلاعات کاربران در اینترنت

اشیا ارائه گردید. با استفاده از روش پیشنهادی کاربران می‌توانند اطلاعات خود را با امنیت‌خاطر بیشتر نسبت به روش‌های مشابه و بدون اطلاع از نحوه و مکان ذخیره‌سازی، داده‌هایشان را به سرورهای ذخیره‌سازی اینترنت اشیا بسپارند. هچنین با تحلیل رفتارکاربر و امضای دیجیتال جهت احرازهویت علاوه بر دستیابی به امنیت سطح بالا، مشکل گلوگاه که اغلب روش‌های ذخیره‌سازی با آن روبرو هستند حل شود. هچنین در این مقاله دو سناریو طراحی شد یک سناریو برای زمانی که هدف ذخیره‌سازی داده‌هاست و سناریوی دیگر برای زمانی که هدف پردازش داده‌هاست. در مبحث سناریو ذخیره‌سازی داده‌ها از الگوریتم تحلیل رفتار کاربر استفاده شد. علی‌رغم اینکه ممکن است توان پردازشی و تاخیر بالایی به سیستم بدهیم بنابراین پیشنهاد می‌شود برای متونی که از نظر امنیتی نیاز به امنیت بالایی دارند استفاده از تحلیل رفتارکاربر که در سناریو اول طرح شده‌است، ایده مناسبی باشد. همچنین برای متون بزرگ پیشنهاد نمی‌کنیم از ایده طرح‌شده در سناریو اول استفاده شود چون زمان‌بر بوده و تاخیر کار بالایی دارد. در سناریو دوم نیز درمواردیکه به‌نظر می‌رسد خیلی سرعت مدنظر نباشد و بخواهیم امنیت را هم در پردازش مدنظر قرار بدهیم، استفاده از نظارت بر مدیریت دانش به‌دلیل سرعت بالا و سبک بودن، گزینه مناسبی باشد. این در حالی است که شاید برای پردازش بحث امنیت خیلی مورد توجه قرار نگرفته شده‌باشد.

منابع

Amirpor, H., Sarati, A. (2017). IoT-based knowledge management in smart city, National Congress of Modern Urban Management and Planning, Tehran, Permanent Secretariat of the Conference.(in persian). https://doi.org/10.1016/j.trb.2017.04.003

-Duc Nha Le, Loc Le Tuan, Minh Nguyen Dang Tuan,(2019), Smart-building management system: An Internet-of-Things (IoT) application business model in Vietnam, Technological Forecasting and Social Change, Vol 141, Pages 22-35. https://doi.org/1042/j.trb.2022.37.75

-Farajzad S., Mahyari M., (2019), Study of the role of IoT technology in the development of smart health, the third annual conference on business management and economics, Tehran, Institute of Management and Development Research Institute of Culture and Arts. .(in persian) https://doi.org/1029/j.trb.2010.12.17

-Farazman A., Rasoli M., (2019), Study of the role of government in implementing a smart city using the Internet of Things, the first international conference on IoT applications and infrastructure, Isfahan, Faculty of Computer Engineering, University of Isfahan .(in persian) https://doi.org/1085/j.trb.2019.36.54

-Goldozi B., Tajfar A., (2016), The Role of Knowledge Management in Internet of Things (IoT), National Conference on Electrical, Computer and Mechanical Engineering Science and Technology of Iran. .(in persian) https://doi.org/1012/j.trb.2023.24.57

-Shwartz-Asher . D, chun. S(2020), Knowledge sharing behaviors in social media, Technology in Society, Vol. 63. https://doi.org/1075/j.trb.2011.6.20

-Heinzelman, W.B., A.P. Chandrakasan, and H. Balakrishnan, (2002), An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on wireless communications, 1(4): p. 660-670. https://doi.org/1059/j.trb.2006.20.92

-Jin, Y., et al., (2014), Link quality aware and content centric data aggregation in lossy wireless networks. In IEEE Wireless Communications and Networking Conference (WCNC). https://doi.org/1026/j.trb.2021.30.128

-Kostas Kolomvatsos, (2019), Time-optimized management of mobile IoT nodes for pervasive applications, Journal of Network and Computer Applications, Vol1251, Pages 155-167. https://doi.org/1019/j.trb.2015.7.71

-Marie-Pierre Gagnon, Julie Payne-Gagnon, Jean-Paul Fortin , (2015), learning organization in the service of knowledge management among nurses: A case study, International Journal of Information Management , 693-708. https://doi.org/1062/j.trb.2005.27.8

-Suwon Kim, Seongcheol Kim, (2018), User preference for an IoT healthcare application for lifestyle disease management, Telecommunications Policy, Vol42, Issue 4, Pages 304-314. https://doi.org/1057/j.trb.2005.32.123

-Thomas. N,(2021), Towards agile knowledge management in an online organization, Procedia Computer Science, vol. 192, p4406-4415. https://doi.org/1095/j.trb.2023.32.54