پنجمین کنفرانس بین المللی مطالعات بین رشته ای در مدیریت و مهندسی
۱۴ تیر ۱۴۰۱ | محل برگزاری: دانشگاه تهران
5th International Conference on Interdisciplinary Studies in Management & Engineering (ICISME-2022)
5 July 2022 | University of Tehran
OxfordCert Universal

ارائه روشی جهت حفظ حریم خصوصی در اینترنت اشیاء مبتنی بر ماژول‌های تشخیص اثرانگشت و فرستنده-گیرنده

مهدی اکبری
کارشناسی ارشد مهندسی کامپیوتر دانشگاه آزاد اسلامی، دزفول، ایران.
mehdi1157@yahoo.com

حمید براتی
گروه مهندسی کامپیوتر، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران.
hbarati@iaud.ac.ir

چکیده

اینترنت اشیاء، فرصت‌های بزرگی را برای بهبود بخشیدن زندگی مردم ایجاد خواهد کرد. استعداد اصلی کاربردهای اینترنت اشیاء، توانایی انجام دادن کارهای مشارکتی شامل محاسبات با ورودی‌های تأمین‌شده به وسیله بخش‌های مجزا است. یکی از مشکلات اساسی اینترنت اشیاء، امنیت است. موقعیت‌یابی بر اساس اثرانگشت یکی از پرطرفدارترین فناوری‌های محلی سازی داخلی است که برای حفظ حریم خصوصی استفاده می‌شود. هدف از انجام این مقاله، تشخیص شرایط کاربر برای برقراری امنیت در اینترنت اشیاء می‌باشد. در فاز اول روش پیشنهادی، اثرانگشت دریافتی به وسیله کنترلر بررسی گردید تا تأیید یا عدم‌تأیید اثرانگشت بررسی شود. در فاز دوم روش پیشنهادی، اگر اثرانگشت دریافتی به وسیله کنترلر مورد قبول بود، سیگنال تأییدیه توسط ماژول فرستنده برای سیستم اینترنت اشیاء فرستاده شد. در فاز سوم روش پیشنهادی، سیستم گیرنده قرار دارد که می‌تواند شامل جفت گیرنده بی‌سیم و یک کنترلر مشابه باشد. جهت شبیه‌سازی و استخراج داده‌های اولیه، از شبیه‌ساز اینترنت اشیاء مبتنی بر میکروکنترلر Arduino استفاده شده است. نتایج عملی به دست آمده، استدلال روش پیشنهادی را مبنی بر این‌که فناوری شناسایی اثرانگشت یک راه‌حل بهینه در بین انواع امنیتی زیست‌سنجی است را تقویت می‌کند.

واژگان کلیدی: اینترنت اشیاء، امنیت، حریم خصوصی، اثرانگشت، میکروکنترلر Arduino

مقدمه

اینترنت اشیاء یک شبکه به سرعت در حال رشد از اشیاء به‌هم‌پیوسته است که با حسگرهایی برای جمع‌آوری و تبادل داده‌ها از طریق اینترنت بدون نیاز به دخالت انسان تعبیه شده است (Karale, 2021). اینترنت اشیاء، یک اکوسیستم در حال گسترش است که نرم‌افزار، سخت‌افزار، اشیاء فیزیکی و دستگاه‌های محاسباتی را برای برقراری ارتباط، جمع‌آوری و تبادل داده‌ها ادغام می‌کند. اینترنت اشیاء یک پلت فرم یکپارچه برای تسهیل تعاملات بین انسان‌ها و انواع اشیاء فیزیکی و مجازی، از جمله حوزه‌های مراقبت‌های بهداشتی شخصی‌سازی‌شده، فراهم می‌کند (Kashani et al, 2021). ادغام حسگرها، محاسبات سبک‌وزن و تکثیر فناوری‌های مختلف بی‌سیم در پلتفرم‌های اینترنت اشیاء، انسان‌ها را قادر می‌سازد تا به‌راحتی با دنیای فیزیکی اطراف خود تعامل داشته باشند(Babun et al, 2021). انتظار می‌رود اینترنت اشیاء فرصت‌های جدیدی را برای بهبود چندین سرویس برای جامعه به ارمغان آورد، از حمل‌ونقل گرفته تا کشاورزی، از شهرهای هوشمند تا مدیریت ناوگان

باشند(Centenaro et al, 2021). نقض حریم شخصی و امنیت، دو مشکل اصلی اینترنت اشیاء می‌باشند. این‌ها مشکلاتی هستند که زمانی که همه چیز بر عهده اینترنت گذاشته می‌شود، وجود دارند. ویژگی باز بودن محیط اینترنت اشیاء، نگرانی‌های امنیتی در مورد اشیاء مستقلی که قابلیت به اشتراک‌گذاری خدمات و سایر قابلیت‌ها به صورت فردی یا جمعی را دارند، افزایش می‌دهد. علی‌رغم داشتن مزایای اقتصادی و اجتماعی فراوان اینترنت اشیاء، اما پیاده‌سازی آن‌ها با مشکلات، ریسک‌ها و مسائل امنیتی بسیاری روبروست که باید مدنظر قرار گیرند. امروزه، معماری اینترنت باید جهت اتصال تعداد زیادی دستگاه و تضمین نمودن قابلیت تعامل بین آن‌ها، بازبینی و به‌روز شود. با این حال، موضوع اساسی در این زمینه، ملزومات امنیتی اینترنت اشیاء است که از دلایل اصلی گسترش نسبتاً آرام آن می‌باشد. هدف از انجام روش پیشنهادی، تشخیص شرایط کاربر جهت برقرار نمودن امنیت در اینترنت اشیاء می‌باشد. روش پیشنهادی در سه فاز اصلی انجام می‌گیرد. در فاز اول روش پیشنهادی، اثرانگشت دریافتی توسط کنترلر مورد بررسی قرار می‌گیرد تا تأیید یا عدم‌تأیید اثرانگشت بررسی گردد. در فاز دوم روش پیشنهادی، اگر اثرانگشت دریافتی توسط کنترلر مورد قبول باشد، سیگنال تأییدیه به وسیله ماژول فرستنده برای سیستم اینترنت اشیاء ارسال می‌گردد. در فاز سوم روش پیشنهادی، سیستم گیرنده مستقر می‌باشد که شامل جفت گیرنده بی‌سیم و یک کنترلر مشابه است. با توجه به اندازه قدرت سیگنال دریافتی، فاصله تقریبی و در نتیجه موقعیت کاربر قابل تشخیص است و امنیت برقرار می‌گردد.

در ادامه، ساختار مقاله به این شرح است که در بخش دوم، مفهوم ماژول اثر انگشت معرفی می‌شود. در بخش سوم، روش‌های پیشین در حوزه حفظ حریم خصوصی در اینترنت اشیاء بررسی می‌شوند. در بخش چهارم، روش پیشنهادی بیان خواهد شد. در بخش پنجم، نتایج حاصل از شبیه‌سازی روش پیشنهادی بیان می‌شود.

ماژول اثر انگشت

ماژول اثرانگشت می‌تواند با تجهیزات کار گذاشته شده اینترنت اشیاء متنوع همانند قفل در تجهیزات الکترونیکی متنوع و سایر وسایل امنیتی تلفیق گردد. در اجرای سیستم پیشنهادی، یک سیستم امنیتی اثرانگشت برای اینترنت اشیاء توسعه داده می‌شود. المان‌های امنیتی زیست‌سنجی متنوع تعریف شده‌اند که هریک از انواع دارای فواید و مضرات خودشان هستند. دلیل برای انتخاب کردن فنّاوری شناسایی اثرانگشت در بین فنّاوری‌های معاصر که عنبیه، اثرانگشت، صورت و صدا هستند، می‌توان مشاهده نمود که عنبیه، کم گران است و صدا نمی‌تواند در شرایط خاص قابل‌اطمینان باشد و تشخیص چهره نیازمند مقدار نور محدود متعادل است. خیلی واضح است که شناسایی اثرانگشت به عنوان سیستم پیشنهادی در سیستم امنیت اینترنت اشیاء انتخاب گردد و نمی‌توان وسایل گران را برای تمامی زمان‌ها داشت، نور نمی‌تواند در خانه در شب‌ها زیاد باشد و سرانجام نتیجه گرفته می‌شود که شناسایی اثرانگشت یک راه‌حل عملی در مقایسه با سایر سیستم‌های امنیتی است.

پیشینه تحقیق

در (Patel et al, 2021)، روشی طراحی کرده‌اند که ابزارهای منبع باز و فناوری‌های وب شامل سرورها، حسگرها و برنامه‌های مختلف را ترکیب می‌کند. این مجموعه داده‌ها به‌عنوان مکانیسمی در نظر گرفته می‌شود که می‌تواند خلاصه‌ای از یک شهر را برای تجسم در یک نمای واحد نمایش دهد و می‌تواند به شهروندان کمک کند تا وضعیت فعلی شهر را ردیابی و تجزیه‌وتحلیل کنند. در این مقاله، چارچوب شهر هوشمند را با استفاده از معماری مبتنی بر اینترنت اشیاء ارائه کرده‌اند. راه‌حل‌های موجود نیز برای تجزیه‌وتحلیل جنبه‌های مختلف با جزئیات ارائه شده است. روش مورد بحث در این مقاله قادر به ارائه این اطلاعات است: ۱) خدمات اطلاعات اولیه و محیطی، ۲) خدمات پیشرفته مانند مراقبت‌های بهداشتی، حمل‌ونقل عمومی و خدمات سیستم پارکینگ.

در (Alzubi, 2021)، یک روش جدید احراز هویت به نام LMDS[1] را ارائه شده است که از زنجیره بلوکی برای سیستم اینترنت اشیاء پزشکی استفاده می‌کند. یک سیستم نظارت از راه دور بیمار بسیار ایمن با یک دستگاه اینترنت اشیاء در مراقبت‌های بهداشتی طراحی شده است که حرکت بدن و علائم حیاتی را برای نظارت اولیه قلب و اندازه‌گیری ECG ثبت می‌کند. این کار یک سیستم بسیار امن با کمک زنجیره بلوکی برای دستگاه‌های اینترنت اشیاء پزشکی با استفاده از امضای دیجیتالی LMDS پیشنهاد کرده است. در ابتدا، مدل LMDSG[2] وظیفه احراز هویت دستگاه‌های اینترنت اشیاء را با ساختن درختی انجام می‌دهد که در آن، برگ‌ها نماد عملکرد هش داده‌های پزشکی حساس بیمار هستند. علاوه بر این، یک کنترل‌کننده مراقبت بهداشتی متمرکز (CHC[3]) وظیفه تعیین ریشه LMDSG را با استفاده از تأیید امضای دیجیتال LMD (LMDSV[4]) انجام می‌دهد.

در (Sun et al, 2021)، مواردی مانند یک زنجیره بلوکی مجاز، یک کنترل دسترسی مبتنی بر ویژگی (ABAC[5]) و یک امضای مبتنی بر هویت (IBS[6]) را برای ایجاد یک سیستم کنترل دسترسی اینترنت اشیاء مبتنی بر زنجیره بلوکی ادغام کرده‌اند. به‌طور خاص، سیستم اینترنت اشیاء را به حوزه‌های عملکردی مختلف، به نام دامنه‌های اینترنت اشیاء، تقسیم کرده‌اند. سپس، یک دفتر کل زنجیره بلوکی محلی برای هر دامنه اینترنت اشیاء ایجاد نموده‌اند تا دستگاه‌های اینترنت اشیاء بیشتری را به‌عنوان گره‌های زنجیره بلوکی فعال کنند. دفتر کل زنجیره بلوکی محلی ویژگی‌های موجودیت‌های دامنه اینترنت اشیاء، خلاصه فایل‌های خط‌مشی و تصمیمات دسترسی را ثبت می‌کند. در همین حال، از فناوری کانال HLF برای تحقق دسترسی بین دامنه‌ای استفاده کرده‌اند و از IBS برای فیلتر کردن درخواست‌های دسترسی قانونی برای هر دامنه اینترنت اشیاء برای جلوگیری از حملات DDoS[7] استفاده نموده‌اند. همچنین یک الگوریتم انتخاب PDP[8] طراحی کرده‌اند که چندین دستگاه اینترنت اشیاء (گره‌های زنجیره بلوکی) را برای دستیابی به تصمیم‌های خط‌مشی توزیع‌شده در زمان واقعی (خارج از زنجیره) انتخاب می‌کند. در نهایت، سیستم پیشنهادی را پیاده‌سازی و ارزیابی کرده‌اند تا عملی بودن آن را نشان دهند.

در (Algarni et al, 2021) ساخت مدیران زنجیره بلوکی (BCM[9]) برای ایمن کردن کنترل دسترسی اینترنت اشیاء و همچنین امکان برقراری ارتباط امن بین دستگاه‌های اینترنت اشیاء محلی را انجام داده‌اند. علاوه بر این، این راه‌حل ارتباط امن بین دستگاه‌های اینترنت اشیاء، گره‌های مه و رایانش ابری را نیز امکان‌پذیر می‌کند. یک سیستم چندعاملی را برای ارائه مکانیسم‌های امنیتی کنترل دسترسی اینترنت اشیاء غیرمتمرکز و سبک‌وزن پیشنهاد کرده‌اند. مدیران زنجیره بلوکی، مسئول تأمین امنیت لازم برای کنترل دسترسی، ایمن‌سازی ارتباط بین دستگاه‌های محلی اینترنت اشیاء، گره‌های مه، گره‌های مه اصلی و رایانش ابری هستند. معماری پیشنهادی یک راه‌حل قابل‌تعمیم است که می‌تواند برای برنامه‌های مختلف اینترنت اشیاء اعمال شود. علاوه بر این، مسائل اینترنت اشیاء به‌طور کامل در مطالعات قبلی موردتوجه قرار نگرفته است، زیرا بیشتر مطالعات بر روی پرداختن به مسائل کنترل دسترسی در یک برنامه خاص اینترنت اشیاء مانند خانه هوشمند تمرکز دارند.

در (Pallavi & Ravi Kumar, 2021)، یک طرح احراز هویت با استفاده از گره‌های مه برای مدیریت دستگاه‌های اینترنت اشیاء با ارائه امنیت بدون در نظر گرفتن شخص ثالث قابل‌اعتماد پیشنهاد کرده‌اند. طرح احراز هویت پیشنهادی از مزایای

[1] Lamport Merkle Digital Signature
[2] Lamport Merkle Digital Signature Generation (Lmdsg)
[3] Centralized Healthcare Controller (Chc)
[4] Lamport Merkle Digital Signature Verification (Lmdsv)
[5] Atribute-Based Access Control (Abac)
[6] Identity-Based Signature (Ibs)
[7] Distributed Denial Of Service (Ddos)
[8] Policy Decision Point (Pdp)
[9] Blockchain Managers (Bcms)

استقرار گره مه استفاده می‌کند. طرح احراز هویت با استفاده از گره مه، تأیید قابل‌اعتمادی را بین صاحبان داده و درخواست‌کننده بدون وابستگی به کاربران شخص ثالث ارائه می‌دهد. طرح احراز هویت پیشنهادی با استفاده از گره‌های مه به‌طور مؤثر مشکلات یک نقطه خرابی در سیستم ذخیره‌سازی را حل کرد و با افزایش توان عملیاتی و کاهش هزینه، مزایای بسیاری را ارائه داد. طرح پیشنهادی چندین نهاد مانند کاربران نهایی، دستگاه‌های اینترنت اشیاء، گره‌های مه و قراردادهای هوشمند را در نظر می‌گیرد که به مدیریت احراز هویت با استفاده از سیاست‌های دسترسی کمک می‌کنند.

در (Guan et al, 2019)، روشی به نام APPA[1] ارائه نموده‌اند که یک برنامه جمع‌آوری داده با حفظ حریم خصوصی و ناشناختگی برای اینترنت اشیاء پیشرفته می‌باشد. مزیت روش ارائه شده، این است که در مقایسه با برنامه‌های حال حاضر از این نوع، APPA انعطاف‌پذیری، کارآمدی و مدیریت وسایل بهتری دارد. عیب روش ارائه شده، این بود که برنامه پیشنهادی را برای بعضی سناریوهای خاص به کار نبرده‌اند مثل جمع‌آوری داده در شبکه هوشمند. علاوه بر این، روی امنیت و مسائل حریم خصوصی در سیستم اینترنت اشیاء پیشرفته کار نکرده‌اند. روش ارائه شده، یک برنامه با حفظ حریم خصوصی و ناشناخته وسیله محور با احراز هویت در سیستم اینترنت اشیاء پیشرفته می‌باشد. نویسندگان این پژوهش، دریافتند که ناشناخته بودن و اعتبارسنجی چندلایه یک وسیله با گواهی مستعار انجام می‌شود. علاوه بر این، حریم خصوصی داده حس شده می‌تواند با یک روش مؤثر تضمین شود. تحلیل امنیت را برای تشریح امنیت و عناصر حفظ حریم خصوصی برنامه انجام داده‌اند. ارزیابی‌های عملکرد نشان می‌دهد که APPA انتخاب بهتری برای سیستم اینترنت اشیاء پیشرفته با وسایل محدود از نظر منابع و ارتباطات بلادرنگ است.

در (Li et al, 2019)، جمع‌آوری اطلاعات عمومی قابل‌تأیید با حفظ حریم خصوصی و برنامه آن در اینترنت اشیاء را انجام دادند. در این پژوهش، برای داشتن یک راه‌حل برای مشکل تأیید در عملیات تجمعی امن، یک برنامه تجمعی با حفظ حریم خصوصی ارائه داده‌اند. برنامه به گره میانی امکان انجام کارهای تجمعی روی داده جمع‌آوری شده برای گره‌های منبع بدون دانستن محتوای داده را می‌دهد. در همین حین، درستی نتیجه تجمعی می‌تواند توسط تأییدکننده عمومی چک شود. تحلیل نشان می‌دهد که برنامه تحت نظریه co-CDH امن است و نتیجه آزمایشی نیز نشان می‌دهد که بهره‌وری و اثربخشی برنامه پیشنهادی تا چه میزان رضایت‌بخش است که مزیت اصلی این پژوهش است. عیب روش ارائه شده، این است که برای بهبود قدرت برنامه، یک راه مؤثر برای مالکان داده پیشنهاد نشده است. راه‌حل مشکل باید شامل روشی برای بردارهای متصل و مکانیسم تأیید برای چک کردن نتایج تجمعی باشد.

در (Liu et al, 2019)، جمع‌آوری داده خام با حفظ حریم خصوصی بدون احراز هویت معتبر برای اینترنت اشیاء را انجام داده‌اند. در این پژوهش، یک پروتکل جمع‌آوری داده حسگر اینترنت اشیاء بدون TA[2] پیشنهاد شده است که نه تنها از داده خام حفظ می‌کند، بلکه داده را از موارد همراه با آن، جدا می‌کند. با نیازهای رو به افزایش به اشتراک‌گذاری داده، پروتکل ارائه شده تضمین می‌کند که استفاده از کل داده و حریم خصوصی داده به‌طور همزمان رعایت شود. این کار نه تنها ارزش داده را بالا می‌برد بلکه نگرانی از نفوذ اطلاعات را نیز از بین می‌برد. علاوه بر این، شبیه‌سازی با ۱۰۰۰ وسیله اینترنت اشیاء نیز برای تشریح عملکرد آن، اجرا شده است و نتایج نیز نشان داده که برنامه پیشنهادی برای برنامه‌های واقعی، کاربردی است که مزیت روش ارائه شده، است.

در (Ganapathy et al, 2019)، ذخیره‌سازی امن و مدل حفظ حریم خصوصی را با استفاده از CRT[3] برای ایجاد امنیت روی ابر و برنامه‌های مبتنی بر اینترنت اشیاء انجام داده‌اند. یک مدل حفظ حریم خصوصی و ذخیره امن مبتنی بر CRT برای

[1] ADevice-Oriented Anonymous Privacy-Preserving Scheme With Authentication
[2] Trusted Authority
[3] Chinese Remainder Theorem

ذخیره امن داده ابر و دسترسی به داده کاربران ابر پیشنهاد و پیاده‌سازی شده است. در این کار، یک مکانیسم ذخیره داده مبتنی بر CRT برای ذخیره امن داده کاربر در پایگاه داده ابر پیشنهاد شده است. علاوه بر این، یک برنامه مدیریت کلید گروهی مبتنی بر CRT نیز برای دسترسی داده ابر رمزگذاری شده از سرور ابر پیشنهاد شده است که در پایگاه داده ابر ذخیره شده است. در مدل حفظ حریم خصوصی و ذخیره امن پیشنهادی، از رابطه‌های جدید برای انجام رمزگذاری و رمزگشایی استفاده می‌شود. علاوه بر این، یک برنامه رمزگذاری سزار برای رمزگذاری کلید در برنامه تولید کلید پیشنهادی استفاده شده است. آزمایش‌های مختلفی برای ارزیابی مدل امنیت داده با حفظ حریم خصوصی انجام شده است و ثابت شده است که عملکرد بهتری نسبت به دیگر مدل‌ها دارد. مزیت روش ارائه شده، این است که عملکرد بهتری از نظر سطح امنیتی نسبت به دیگر مدل‌ها دارد. عیب روش ارائه شده، این است که برنامه‌های رمزگذاری و رمزگشایی برای کاهش پیچیدگی محاسباتی ابر و برنامه‌های مبتنی بر اینترنت اشیاء را استفاده نکرده‌اند.

در (Viejo et al, 2019)، هماهنگ‌سازی حفظ حریم خصوصی و امنیت و ارائه خدمات اینترنت اشیاء مبتنی بر ابر را انجام داده‌اند. در این پژوهش، یک سیستم حریم خصوصی با طراحی برای هماهنگ‌سازی و ارائه خدمات اینترنت اشیاء مبتنی بر ابر پیشنهاد داده‌اند. این سیستم از اولین راه‌حل عملی برای هماهنگ‌سازی ابر تشکیل شده است که به دقت مسائل امنیتی و حریم خصوصی را در نظر گرفته است. علاوه بر این، این مسئله روش ارائه شده را از دیگر سیستم‌ها متمایز می‌کند که امنیت را با اعمال رمزگذاری گران در طول کل چرخه حیات مدیریت خدمات برقرار می‌کند. برخلاف این موضوع، روش ارائه شده، یک راه‌حل با بهره‌وری بالاتر است که علت آن، هماهنگ‌سازی، استفاده از استانداردها، رمزگذاری در طول ارائه خدمات است و استفاده منطقی از منابع ابر می‌کند. علاوه بر آن، یک سناریو چالشی در نظر گرفته‌اند که در آن، نهادها در سیستم محاسبات ابر داده را در شبکه‌های ناامن و باز تبادل می‌کنند و در خطر حملات فعال و غیرفعال هستند که شامل کنترل بعضی وسایل است. امنیت و مقیاس‌پذیری پروتکل‌های ارائه شده نیز به دقت تحلیل شده‌اند، نتیجه‌گیری‌ها و نتایج این تحلیل نیز نشان داده‌اند که روش ارائه شده، امن و کاربردی است که مزیت روش ارائه شده، است. عیب روش ارائه شده، این است که برای کار در یک چارچوب درخواست-پاسخ طراحی نشده است.

در (Qiu and Ma, 2018)، حفظ حریم خصوصی برای خدمات اینترنت اشیاء مبتنی بر مکان را انجام داده‌اند. در این پژوهش، الگوریتم ESPT[1] برای حفظ اطلاعات مکان کاربران برای برنامه‌های اینترنت اشیاء خدمات مبتنی بر مکان، پیشنهاد شده است. برنامه پیشنهادی، به کاربر امکان پرس‌وجو ارائه‌دهنده خدمت را می‌دهد که آیا بعضی افراد در حوزه جستجو بدون انتظار اطلاعات محرمانه هستند یا خیر. مزیت روش ارائه شده، این است که تحلیل امنیتی ثابت کرده است برنامه ESPT می‌تواند حریم خصوصی مکان را برای همه کاربران حفظ کند. عیب روش ارائه شده، سربار محاسباتی می‌باشد. ارزیابی عملکرد انجام شده توسط جاوا نیز نشان می‌دهد که برنامه پیشنهادی نه تنها برای آزمایش حفظ حریم خصوصی مناسب است، بلکه بهره‌وری را بهبود بخشیده است.

در (Simplicio et al, 2018)، قرارداد کلیدی احراز هویت سبک‌وزن و کم اعتبار برای اینترنت اشیاء بررسی شده است. نیاز به احراز هویت دستگاه سبک‌وزن در شبکه حسگر بی‌سیم به تازگی منجر به پیشنهاد بسیاری از طرح‌های کلید قرارداد شده است که بر این سناریو متمرکز شده است. با این حال، بسیاری از این طرح‌های پیشنهادی (مخصوصاً آن‌هایی که مبتنی بر شناسه هستند) از کلید بی‌اعتبار رنج می‌برند که در محدوده وسیع و محیط چند کاربره که اینترنت اشیاء را مشخص می‌کند، ناخوشایند است. تحقیقات نشان می‌دهد که متأسفانه تنها چند طرح در نوشته‌ها با چنین ویژگی‌هایی وجود دارد که بسیاری از آن‌ها در واقع از مسائل امنیتی یا عملکرد رنج می‌برند. برای رفع کمبود کاندیدهای مناسب، ترکیبی از یک نوع

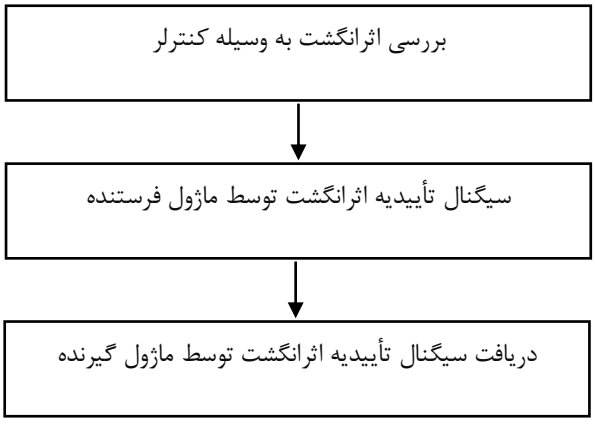
[1] Efficient And Secure Private Proximity Testing

منحنی بیضوی و کلیدهای عمومی تولید شده از گواهی‌های ضمنی که می‌تواند این الزامات را به نحوی کارآمد انجام دهد، توصیف شده‌اند. در این پژوهش، جایگزینی بی‌اعتبار رایگان را ارزیابی کرده‌اند که ممکن است برای سناریوی اینترنت اشیاء مناسب باشد. مزیت گواهی‌های ضمنی و روش ارائه شده، این است که آن‌ها می‌توانند بسیار کوتاه‌تر از گواهینامه‌های مبتنی بر کلید عمومی معمول باشند که در حافظه برای ذخیره‌سازی و پهنای باند صرفه‌جویی شود.

در (Amin et al, 2018)، یک معماری برای محیط ابری توزیع‌شده‌ای طراحی شده است که در آن، ابر خصوصی اطلاعات محرمانه را با استفاده از روش اینترنت اشیاء ذخیره می‌کند. اثبات احراز هویت دو طرفه انجام شده است و شبیه‌سازی پروتکل ارائه شده، ایمنی پروتکل را تضمین می‌کند. علاوه بر این، کشف نوشته رمزی بی‌قاعده پروتکل پیشنهادی تضمین می‌کند که پروتکل حملات امنیتی تحت نظارت سختی تابع هش است. برای تجزیه‌وتحلیل هزینه ارتباطات، فرض کرده‌اند که طول خصوصیات (کاربر، سرور)، رمز عبور، عدد تصادفی خصوصی و خلاصه پیغام هر کدام ۱۲۸ بیت را می‌گیرد. هزینه ارتباط پروتکل ارائه شده (۲۲ × ۱۲۸) = ۲۸۱۶ بیت است. پس از دستیابی به تمام الزامات امنیتی و حمایت‌های امنیتی قوی، عملکرد پروتکل پیشنهادی بسیار مناسب است. مزیت روش ارائه شده، این است که عملکرد پروتکل از سایر کارها در زمینه محاسبه، ذخیره‌سازی و هزینه ارتباطات بهتر است.

مراحل روش پیشنهادی

در شکل (۱)، مراحل روش پیشنهادی نشان داده شده است. هدف از انجام روش پیشنهادی، تشخیص شرایط کاربر برای برقراری امنیت در اینترنت اشیاء می‌باشد. روش پیشنهادی در سه فاز اصلی انجام می‌شود. در فاز اول روش پیشنهادی، اثرانگشت دریافتی به وسیله کنترلر بررسی می‌شود تا تأیید یا عدم‌تأیید اثرانگشت بررسی شود. اولین گام جهت به دست آوردن مقدار و اثرانگشت فرد، جمع‌آوری اثرانگشت‌ها است. وسایل ثبت تصویری اثرانگشت از طریق تصویر اثرانگشت به‌طور واقعی آن را به سیستم وارد می‌کند. اثرانگشت، دو حالت دارد. حالت اول، به اثرانگشتی برمی‌گردد که از طریق استفاده از یک وسیله میانجی (همچون جوهر یا کاغذ) برای به دست آوردن تصویر اثرانگشت ثبت شده است و نیز اثرانگشتی که از طریق وسایل خاص فنی تصویربرداری دیجیتال به سیستم وارد می‌شود که جمع‌آوری زمان غیرواقعی نام دارد. حالت دوم، حالتی است که سیستم از طریق حسگر پیشرفته انگشت‌نگاری همراه با وسیله خاص جمع‌آوری اثرانگشت به‌طور مستقیم به ثبت اثرانگشت از بدن واقعی فرد می‌پردازد (اثرانگشت زنده نام دارد) و آن را به صورت داده تصویری دیجیتال در زمان واقعی به سیستم می‌دهد که در روش پیشنهادی از این الگو استفاده خواهد شد. در فاز دوم روش پیشنهادی، اگر اثرانگشت دریافتی به وسیله کنترلر مورد قبول باشد، سیگنال تأییدیه توسط ماژول فرستنده برای سیستم اینترنت اشیاء فرستاده می‌شود. در فاز سوم روش پیشنهادی، سیستم گیرنده قرار دارد.



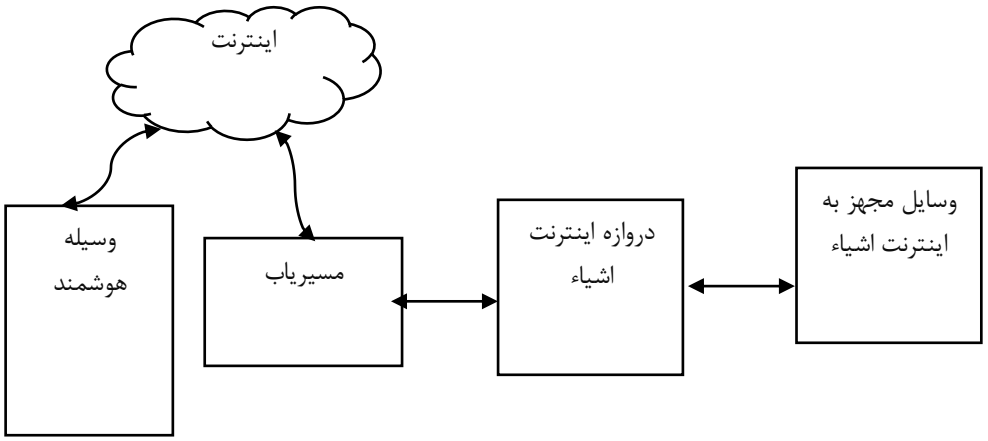
شکل (۱): مراحل روش پیشنهادی

هدف از انجام روش پیشنهادی، ارائه روشی جهت حفظ حریم خصوصی در اینترنت اشیاء مبتنی بر ماژول‌های تشخیص اثرانگشت و فرستنده-گیرنده می‌باشد. روش پیشنهادی دارای سه فاز زیر می‌باشد.

- بررسی اثرانگشت به وسیله کنترلر
- سیگنال تأییدیه اثرانگشت توسط ماژول فرستنده در روش پیشنهادی
- دریافت سیگنال تأییدیه اثرانگشت توسط ماژول گیرنده در روش پیشنهادی

بررسی اثرانگشت به وسیله کنترلر

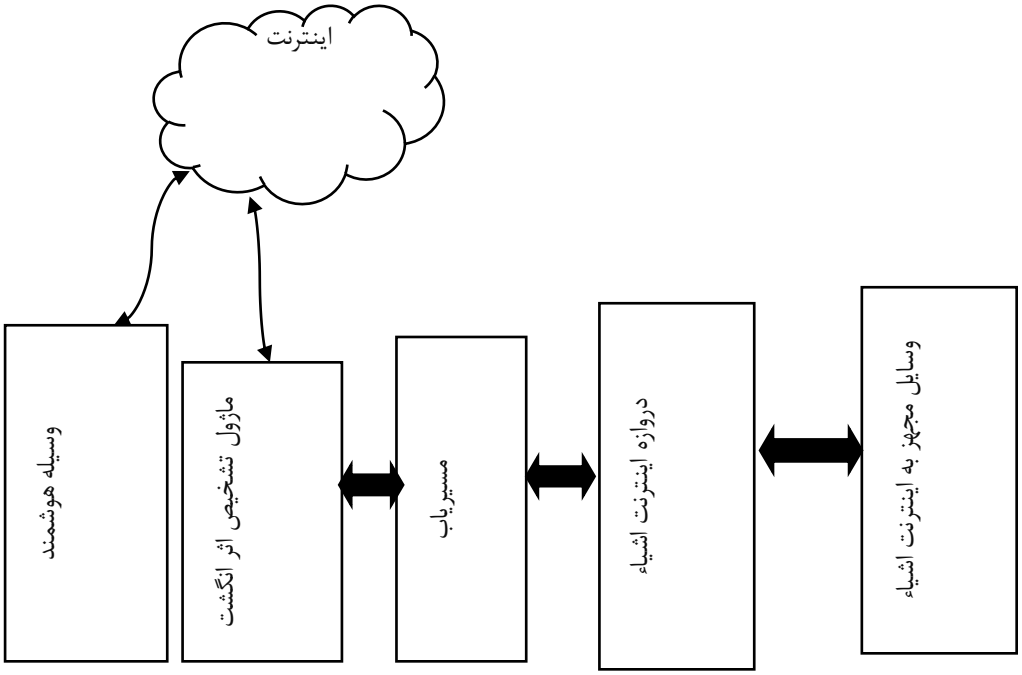
شکل (۲)، کنترل کردن سیستم امنیت موجود را از محل دور نشان می‌دهد. یک وسیله عملیاتی برای کاربر-معمولاً یک تلفن هوشمند- از جایی که دستورات کنترل/دست‌کاری به وسایل اینترنت اشیاء توسط کاربر داده می‌شوند. در بین تلفن هوشمند و وسایل اینترنت اشیاء سه جزئی که کارهای اختصاص داده شده به کاربر را فعال می‌کنند که باید انجام شوند، اینترنت، مسیریاب IP و درگاه اینترنت اشیاء هستند.



شکل (۲): کنترل کردن سیستم امنیت در اینترنت اشیاء

سیستم توضیح داده در شکل (۲)، به وسیله اضافه کردن ماژول شناخت اثرانگشت مجزا اضافی توسعه داده می‌شود. هر وقت که کاربر تلاش می‌کند تا به تجهیزات اینترنت اشیاء از طریق مسیریاب IP دست پیدا کند، سیستم، کاربر را از طریق ماژول اثرانگشتی که اضافه شده است، اثبات و تأیید می‌کند؛ به عبارت دیگر اگر کاربر برای تأیید کردن خودش از طریق شناسایی اثرانگشتش شکست بخورد، نمی‌تواند به تجهیزات اینترنت اشیاء دست پیدا کند.

در روش پیشنهادی، روشی برای یک طرح امنیتی کارآمد در تجهیزات اینترنت اشیاء از طریق روش اثرانگشت ارائه می‌شود. شکل (۳) سیستم پیشنهادی را نمایش می‌دهد.

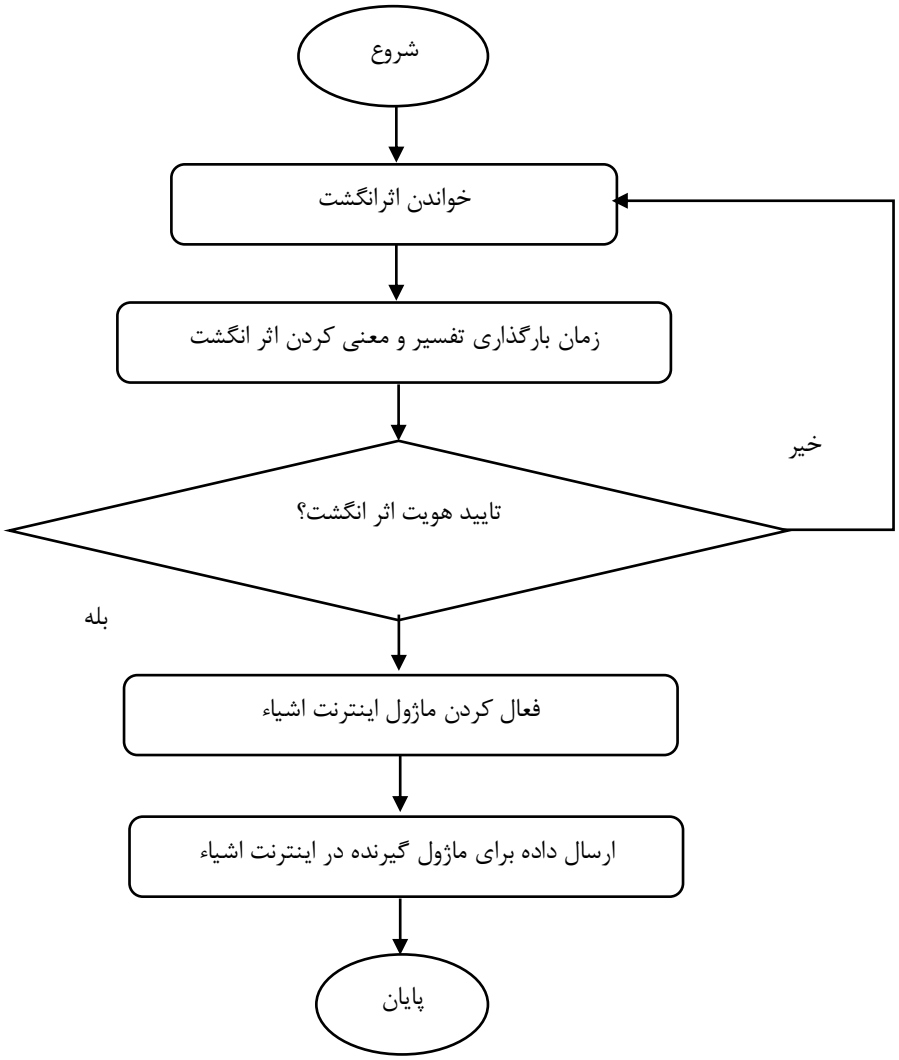


شکل (۳): طرح امنیتی در تجهیزات اینترنت اشیاء از طریق روش اثرانگشت در روش پیشنهادی

سیستم توسعه یافته می‌تواند از سه دکمه که مثلاً S1، S2 و S3 نامیده شوند، استفاده کند که S1، به پاک کردن تعلق داشته باشد و S2، به ثبت‌نام کردن و S3، مربوط به جست‌وجو کردن باشد. اگر هرکسی بخواهد به شیء در اینترنت اشیاء دسترسی پیدا کند، نیاز دارد اثرانگشتش را ثبت‌نام کند. نفر اول مدیر با یک شناسه مشخص نشان داده می‌شود و شخص باقی‌مانده که با شناسه داده شده ثبت‌نام کرده است، یک واحد اضافه می‌یابد.

سیگنال تأییدیه اثرانگشت توسط ماژول فرستنده در روش پیشنهادی

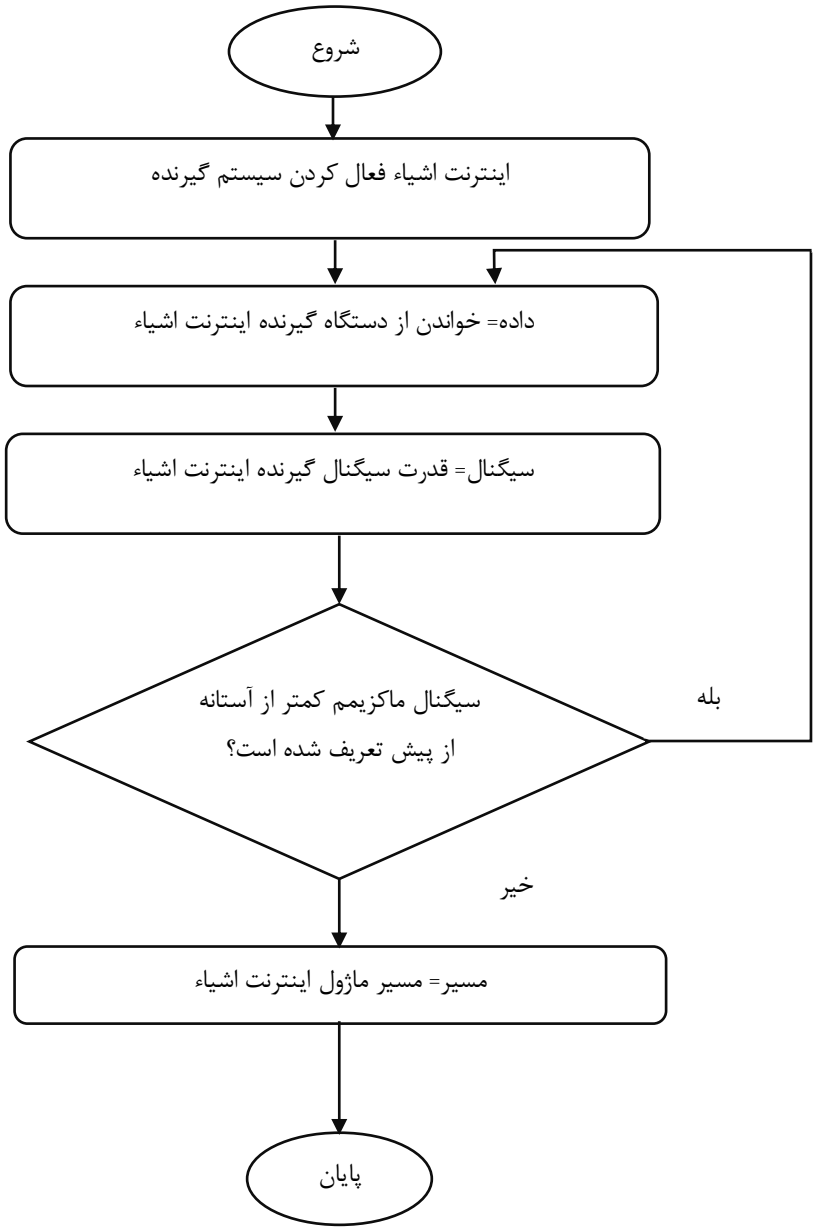
فلوچارت عملکرد ماژول فرستنده پلتفرم اینترنت اشیاء در شکل (۴) نشان داده شده است. اگر یک شخص بخواهد به شیء در اینترنت اشیاء، دسترسی پیدا کند دکمه S3 را نگه می‌دارد تا وقتی که صفحه‌نمایش نشان دهد که اثرانگشت وارد شود؛ سپس شخص نشان اثرانگشت را به ماژول می‌دهد. اگر مدیر باشد، سپس به صورت خودکار شیء می‌تواند توسط مدیر استفاده گردد. اگر به‌جز مدیر باشد، به عبارت دیگر کاربر قانونی می‌خواهد وارد اتاق شود، سپس ماژول فرستنده تأیید یا رد اثرانگشت را به گیرنده می‌دهد. ماژول شناسایی، اثرانگشت کاربر قانونی و مدیر را نگه‌داری می‌کند. محدودیت برای نگه‌داری در ماژول اثرانگشت ۲۵۶ تصویر است. ماژول اثرانگشت، تصویر را حس خواهد کرد و خروجی را وابسته به دکمه‌هایی که S1، S2 و S3 نامیده می‌شود، می‌دهد (شکل (۴)). اگر ماژول اثرانگشت را حس کند؛ سپس پایگاه داده را جست‌وجو می‌کند تا اثبات کند که آیا تصویر معتبر است یا نه که به ماژول فرستنده آن را ارسال کند. یک صفحه‌نمایش باید برای نمایش دادن وضعیت ماژول اثرانگشت به کنترل‌کننده وصل شود.



شکل (۴): فلوچارت ماژول فرستنده در روش پیشنهادی

دریافت سیگنال تأییدیه اثرانگشت توسط ماژول گیرنده در روش پیشنهادی

فلوچارت عملکرد ماژول گیرنده پلتفرم اینترنت اشیاء در شکل (۵) نشان داده شده است. در فاز سوم روش پیشنهادی، سیستم گیرنده قرار دارد که می‌تواند شامل جفت گیرنده بی‌سیم و یک کنترلر مشابه باشد. با توجه به میزان قدرت سیگنال دریافتی، فاصله تقریبی و در نتیجه موقعیت کاربر قابل تشخیص می‌باشد و امنیت برقرار می‌شود.



شکل (۵): فلوچارت ماژول گیرنده در روش پیشنهادی

مدل سیستم مبتنی بر سرویس برای موقعیت‌یابی کاربر در اینترنت اشیاء

اطلاعات مربوط به کاربر، ممکن است شامل احتمال سؤال از کاربر که وابسته به مکان و زمان است، باشد یا اطلاعاتی که به معناشناسی سؤالات همانند نسل یا وضعیت اجتماعی کاربر مرتبط باشد. در این پژوهش، اطلاعات جانبی در نظر گرفته شده است تا احتمال سؤال از کاربران مرتبط با مکان باشد که احتمال سؤال نامیده می‌شود؛ که مکان مربوط به کاربر وابسته به اثرانگشت در نظر گرفته شده است. به صورت خاص احتمال سؤال از کاربر در یک مکان خاص می‌تواند به وسیله یک نسبت از سؤالات مکان فعلی به تعداد کلی سؤالات از تمامی محل‌هایی که در رابطه (۱) نشان داده شد، باشد.

$$q_i = \frac{\text{mmber of queries in location i}}{\text{mmber of queries in all locations}} \quad (۱)$$

به‌طورکلی کاربران می‌توانند دو نوع اطلاعات جانبی را از یک سیستم دریافت کنند، اطلاعات جزئی و اطلاعات کلی. اطلاعات جزئی اطلاعات جمع‌آوری شده به وسیله سایر کاربران را مشخص می‌کند برای مثال، یک کاربر خاص ممکن است احتمال سؤالات مرتبط با برخی مکان‌های خاص را بداند. به دلیل این‌که سرور خدمات مبتنی بر مکان می‌تواند سؤالات خدمات مبتنی بر مکان را از تمامی کاربران دریافت کند، سرور خدمات مبتنی بر مکان می‌تواند به اطلاعات کلی دست یابد (به عبارت دیگر، احتمال سؤالات مرتبط با مکان‌ها). برای یک کاربر خاص، این مهم است که یک استراتژی بهینه برای انتخاب مکان‌های ساختگی انتخاب شود برای این‌که مکان آن شخص تحت شرایط اطلاعات جهانی محافظت گردد. در این مقاله، سرور خدمات مبتنی بر مکان مسئول مشخص کردن و به‌روزرسانی کردن اطلاعات جانبی جهانی است که کاربران می‌توانند از مکان‌هایی که به خوبی شناخته شده‌اند، دریافت کنند (برای مثال، پایگاه داده محلی از کاربرد خدمات مبتنی بر مکان).

هدف اصلی روش پیشنهادی، تولید کردن مجموعه مکان‌های جعلی برای حفظ حریم شخصی مکان کاربر است. روش پیشنهادی نیاز دارد تا k-1 مکان جعلی را از سایر مکان‌ها انتخاب کند که بر اساس اطلاعات جانبی است. در ادامه، پنج مرحله از این‌که چگونه روش پیشنهادی این مسئله را مورد توجه قرار می‌دهد، نشان داده می‌شود.

- در مرحله اول، یک کاربر خاص نیاز به مشخص کردن درجه گمنامی k دارد.
- سپس الگوریتم تمامی احتمالات سؤال به دست آمده را می‌خواند و احتمالات سؤال را از تمامی مکان‌ها به صورت کاهشی مرتب می‌کند.
- در لیست نگه‌داری شده، الگوریتم نیاز دارد تا 2k مکان نامزد را انتخاب کند که تاریخچه احتمال سؤال آن، مشابه با مکان حقیقی کاربر است. در 2k مکان نامزد، آن به صورت تصادفی k-1 مکان را انتخاب می‌کند. سپس m مجموعه را استنباط می‌کند، هر مجموعه شامل k محل است. برای هر مجموعه، یک مکان از مکان حقیقی کاربر وسایل k-1 مکان به صورت تصادفی از 2k نامزد انتخاب شده‌اند. آنتروپی برای مجموعه $j^{th}(j \in [1.m])$ می‌تواند با استفاده از رابطه (۲)، محاسبه گردد.
- سرانجام، الگوریتم باید یک مجموعه مکان بهینه را با بزرگ‌ترین آنتروپی مشخص کند تا به صورت مؤثری به گمنامی k برای کاربران دست پیدا کند.

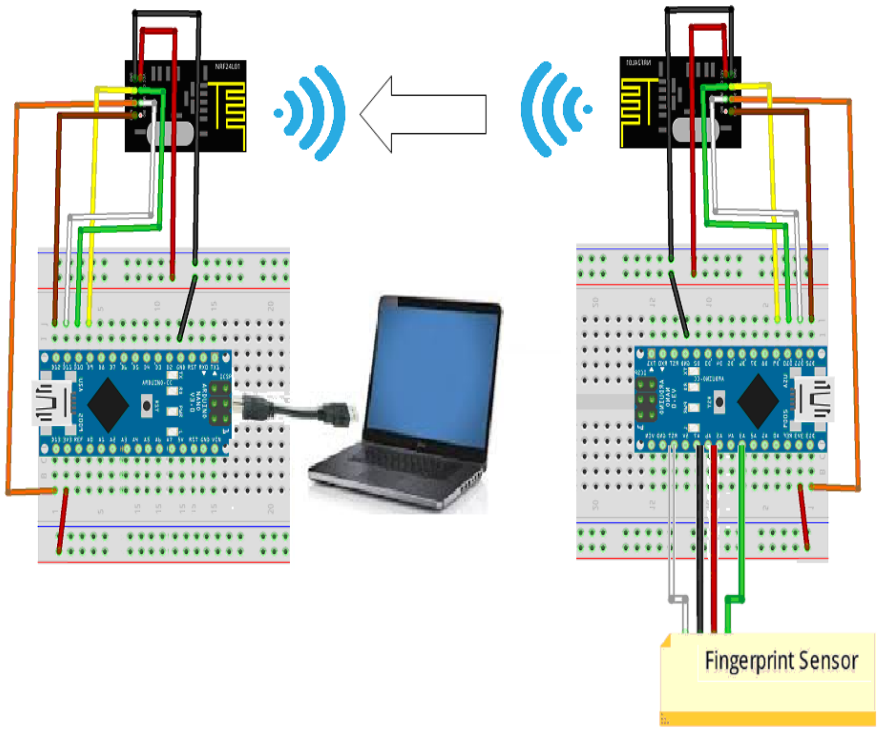
در روش پیشنهادی، درجه حریم شخصی توسط آنتروپی اندازه‌گیری می‌شود و می‌تواند به عنوان عدم قطعیت در شناسایی مکان حقیقی کاربر از محل‌های جعلی انتخاب شده باشد. روش پیشنهادی وقتی که در حال محاسبه کردن آنتروپی است، هر مکان جعلی باید یک احتمال را داشته باشد که می‌تواند تاریخچه احتمال سؤال از کاربران که مرتبط با مکان است، باشد. از p_i استفاده شود تا احتمال سؤال تاریخی از کاربران وابسته به مکان i را تعریف گردد. مطابق یک مجموعه از مکان‌های جعلی و احتمال سؤال تاریخی، می‌توان آنتروپی H از یک کاربر را در رابطه (۲) تعریف نمود.

$$H = -\sum_{I=1}^{K} q_i \log_2 q_i \quad (۲)$$

که در آن، $q_i = p_i / \sum_{i=1}^{k} p_i$ احتمال سؤال نرمالیزه شده در مکان i است و جمع تمام p_i ها معادل با ۱ است. به دلیل این‌که آنتروپی بزرگ‌تر عدم قطعیت بیش‌تری را در شناسایی کردن مکان حقیقی کاربر از مجموعه مکان‌های جعلی باعث می‌شود، هدف به دست آوردن آنتروپی به اندازه کافی است. به صورت خاص وقتی که تمامی مکان‌های جعلی k دارای احتمال سؤال تاریخی مشابه هستند، می‌توان به آنتروپی ماکزیمم $H_{max} = \log_2 k$ دست یافت.

محیط و شرایط شبیه‌سازی

در سناریوی روش پیشنهادی، اگر اثرانگشت دریافتی به وسیله کنترلر مورد قبول باشد، سیگنال تأییدیه توسط ماژول فرستنده برای سیستم اینترنت اشیاء فرستاده می‌شود که سیستم گیرنده می‌تواند شامل جفت گیرنده بی‌سیم و یک کنترلر مشابه باشد. با توجه به میزان قدرت سیگنال دریافتی، فاصله تقریبی و در نتیجه موقعیت کاربر قابل تشخیص می‌باشد. در شکل (۶)، شماتیک سناریوی اول سیستم موقعیت‌یابی اینترنت اشیاء مشخص شده است.



شکل (۶): شماتیک سناریوی روش پیشنهادی

جهت شبیه‌سازی و استخراج داده‌های اولیه، از شبیه‌ساز اینترنت اشیاء مبتنی بر میکروکنترلر Arduino استفاده می‌شود. به‌طور خلاصه، مدل برنامه‌ریزی واسطه خدمات Arduino در روش پیشنهادی، موارد زیر را محقق می‌سازد:

- یک ساختار نرم‌افزاری جهت اجرای کد روی میکروکنترولر.
- یک پروتکل متنی برای پیام‌های مبادله شده میان مشتریان مدل برنامه‌ریزی واسطه خدمات Arduino و میکروکنترولر به‌کارگیرنده ساختار نرم‌افزار.
- یک ساختار شبکه برای ارتباط میان میکروکنترولرها و مشتری که می‌تواند با چندین زبان برنامه‌ریزی سطح بالا نوشته شود.

پارامترهای شبیه‌سازی در جدول (۱) مشخص شده‌اند.

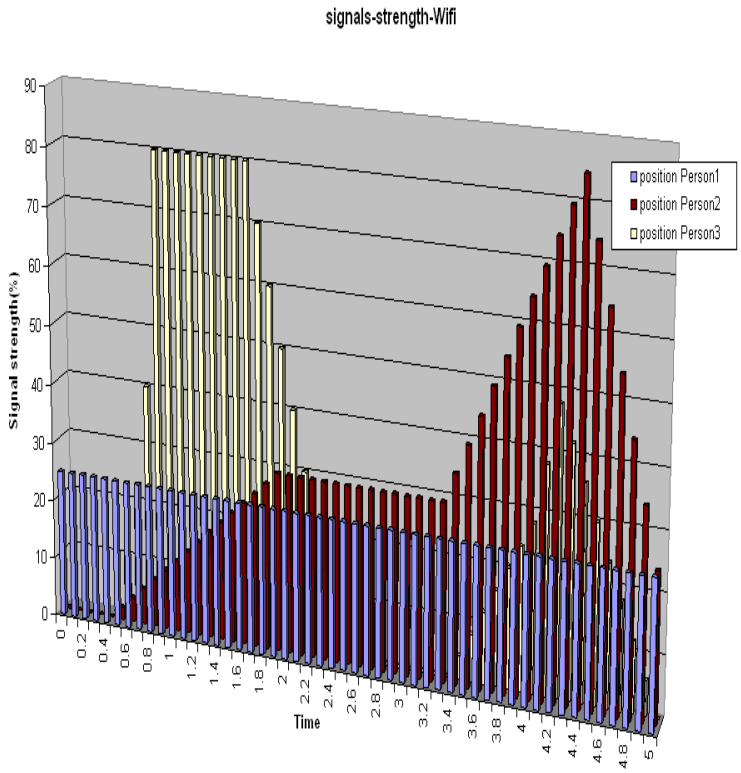
جدول (۱): پارامترهای شبیه‌سازی

پارامتر شبیه‌سازی	مقدار
مدت شبیه‌سازی جهت تحلیل نتایج به‌صورت آزمایشی	۵ ثانیه
مدت‌زمان بین نمونه‌برداری‌ها	۰,۱۰ ثانیه
تعداد نمونه در شبیه‌سازی	۵۰
تعداد فیلد نمونه‌برداری شده	۱۵۰
تعداد فیلد ارسالی جهت استخراج به پایگاه داده	۱۵۰
تعداد ماژول‌ها	۳

نتایج و مقایسه روش پیشنهادی

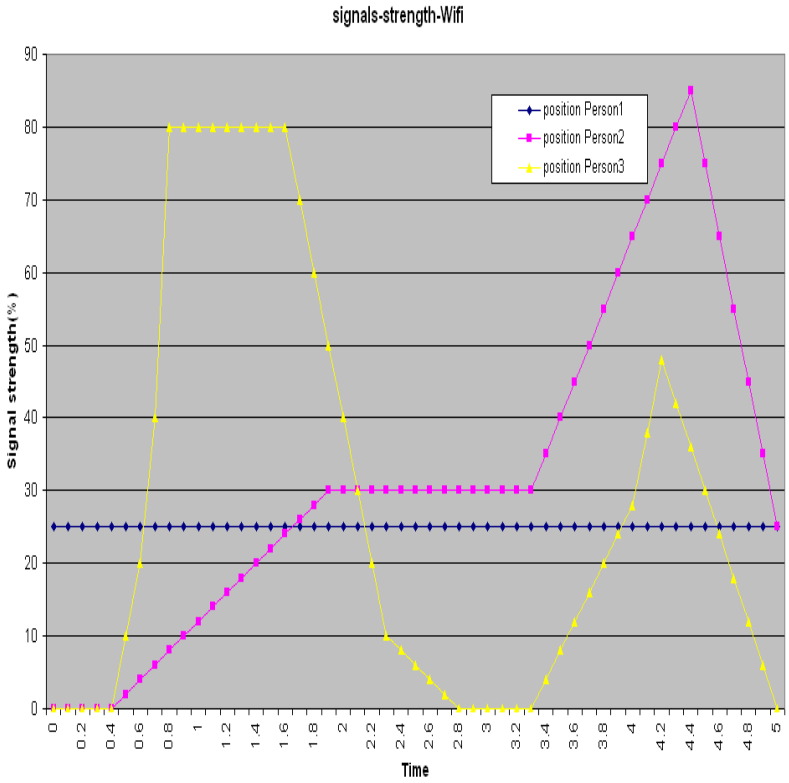
در بین تمامی شاخه‌های متفاوت تحقیقات محلی سازی داخلی، اثرانگشت توجه بیش‌تری را جلب کرده است. محل کاربر/ وسیله را از طریق مقایسه قدرت سیگنال با یک نقشه اثرانگشت مکان مشخص از پیش ایجاد شده، مشخص می‌شود. اگرچه به دلیل قدرت سیگنال بی‌سیم متغیر با زمان، نقشه اثرانگشت در این نوع از سیستم‌ها نیاز است به صورت متناوبی تنظیم گردد، مسیریاب‌های وای فای موجود می‌توانند به صورت دینامیکی قدر انتقالشان و اندازه‌گیری اثرانگشت مطلق را که در میان تجهیزات متغیر است را تغییر دهند که علاوه بر آن، تأثیر سیستم‌های مبتنی بر اثرانگشت موجود را تضعیف می‌کند. با الهام از این تغییرات، مقدار زیادی از تغییرات انجام داده است تا کارآمدی روش‌های اثرانگشت وای فای را افزایش دهد. اگرچه این کارها یک گام مهم انجام داده‌اند که در بهبود دادن پایداری سیستم محلی سازی داخلی مبتنی بر وای فای است، آن‌ها هنوز دارای پیچیدگی بالا و دقت پایین هستند. نتایج عملی به دست آمده، استدلال روش پیشنهادی را مبنی بر این‌که فناوری شناسایی اثرانگشت یک راه‌حل بهینه در بین انواع امنیتی زیست‌سنجی است را تقویت می‌کند. در شکل (۷)، نتایج شبیه‌سازی روش پیشنهادی مشخص شده است.

همچنین در شکل (۸)، مقایسه چالش‌های مختلف در روش پیشنهادی، نشان داده شده است. حالت‌های متفاوتی برای موقعیت شخص نسبت به ماژول‌های دریافت سیگنال‌های اینترنت اشیاء در نظر گرفته می‌شود که شامل ثابت بودن موقعیت شخص، نزدیک شدن شخص متصل به اینترنت اشیاء و دور شدن شخص متصل به اینترنت اشیاء می‌باشد. فراهم‌سازی مکان دقیق، یک کار مهم در کاربردهای اینترنت اشیاء و سناریوها است. این مسئله نیاز تحقیق و توسعه مبتنی بر اثرانگشت سیستم‌های محلی سازی داخلی را بالا برده است، به دلیل این‌که اطلاعات دستگاه موقعیت‌یاب جهانی در محیط‌های داخلی در دسترس نیست. در این بخش، ارزیابی عملکرد این سیستم‌ها و الگوریتم‌های محلی سازی مرتبط بر اساس مجموعه نمونه از پیش مشخص شده در محیط‌های آزمایش، انجام شده است. تعیین اندازه نمونه و روش نمونه‌برداری می‌تواند به صورت قابل‌توجهی بر روی قابلیت اطمینان خروجی تأثیر بگذارد.



شکل (۷): نتایج قدرت سیگنال دریافتی، فاصله تقریبی و در نتیجه تشخیص موقعیت کاربر

مشخص شده است که وقتی مقدار زیادی داده از منابع مختلف جمع و پردازش می‌شوند، عملکرد اینترنت اشیاء ممکن است دارای تأثیر قابل‌توجهی بر روی امنیت کاربرانش باشد. علاوه بر این، با در نظر گرفتن افزایش تمایل برای جمع‌آوری داده مجزا و حریم شخصی در اینترنت اشیاء، تعداد زیادی از مشکلات برخلاف تأثیر حریم شخصی از منظر قانونی وجود دارند. داده مدیریت یا پردازش شده در اینترنت اشیاء به صورت زیاد به وسیله اطلاعات محل تحت تأثیر است و به نوبت به امنیت مکانش تأثیر می‌گذارد. وقتی که اطلاعات مکان یک مؤلفه اصلی در زنجیره تأمین و ساخت مؤثر است، سیستم انتقال کارآمد کاربردهای موبایل آگاه به محتوا و بی‌شمار سیستم اینترنت اشیاء است، حملات حریم خصوصی و عواقب زیان‌بار آن می‌تواند وقتی که اطلاعات مکان حساس بدون موافقت کاربر آشکار می‌شود، اتفاق بیفتد. این‌ها چالش‌هایی را در امنیت اینترنت اشیاء و حریم شخصی نشان می‌دهند که ماژول‌های تشخیص اثرانگشت و فرستنده-گیرنده توانسته است باعث افزایش امنیت در اینترنت اشیاء شود.



شکل (۸): مقایسه چالش‌های مختلف در شبیه‌سازی

نتیجه‌گیری

در این مقاله، تشخیص شرایط کاربر برای برقراری امنیت در اینترنت اشیاء انجام شده است. روش پیشنهادی در سه فاز اصلی انجام شد. در فاز اول روش پیشنهادی، اثرانگشت دریافتی به وسیله کنترلر بررسی گردید تا تأیید یا عدم‌تأیید اثرانگشت بررسی شود. در فاز دوم روش پیشنهادی، اگر اثرانگشت دریافتی به وسیله کنترلر مورد قبول بود، سیگنال تأییدیه توسط ماژول فرستنده برای سیستم اینترنت اشیاء فرستاده شد. در فاز سوم روش پیشنهادی، سیستم گیرنده قرار دارد که می‌تواند شامل جفت گیرنده بی‌سیم و یک کنترلر مشابه باشد. با توجه به میزان قدرت سیگنال دریافتی، فاصله تقریبی و در نتیجه موقعیت کاربر قابل تشخیص می‌باشد و امنیت برقرار می‌شود. جهت شبیه‌سازی و استخراج داده‌های اولیه، از شبیه‌ساز اینترنت اشیاء مبتنی بر میکروکنترلر آردینو استفاده شده است.

مراجع

Algarni, S., Eassa, F., Almarhabi, K., Almalaise, A., Albassam, E., Alsubhi, K., & Yamin, M. (2021). **Blockchain-based secured access control in an IoT system**. Applied Sciences, 11(4), 1772.

Alzubi, J. A. (2021). **Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare**. Computer Communications, 170, 200-208.

Amin, R., Kumar, N., Biswas, G. P., Iqbal, R., & Chang, V. (2018). **A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment**. Future Generation Computer Systems, 78, 1005-1019.

Babun, L., Denney, K., Celik, Z. B., McDaniel, P., & Uluagac, A. S. (2021). **A survey on IoT platforms: Communication, security, and privacy perspectives**. Computer Networks, 192, 108040.

Centenaro, M., Costa, C. E., Granelli, F., Sacchi, C., & Vangelista, L. (2021). **A survey on technologies, standards and open challenges in satellite Iot**. IEEE Communications Surveys & Tutorials, 23(3), 1693-1720.

Ganapathy, S. (2019). **A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications**. Computer Networks, 151, 181-190.

Guan, Z., Zhang, Y., Wu, L., Wu, J., Li, J., Ma, Y., & Hu, J. (2019). **APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT**. Journal of Network and Computer Applications, 125, 82-92.

Karale, A. (2021). **The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws**. Internet of Things, 15, 100420.

Kashani, M. H., Madanipour, M., Nikravan, M., Asghari, P., & Mahdipour, E. (2021). **A systematic review of IoT in healthcare: Applications, techniques, and trends**. Journal of Network and Computer Applications, 192, 103164.

Kaur, R., Verma, K., Jain, S. K., & Kesswani, N. (2019). **Efficient Routing Protocol for Location Privacy Preserving in Internet of Things**. International Journal of Information Security and Privacy (IJISP), 13(1), 70-85.

Li, T., Gao, C., Jiang, L., Pedrycz, W., & Shen, J. (2019). **Publicly verifiable privacy-preserving aggregation and its application in IoT**. Journal of Network and Computer Applications, 126, 39-44.

Liu, Y. N., Wang, Y. P., Wang, X. F., Xia, Z., & Xu, J. F. (2019). **Privacy-preserving raw data collection without a trusted authority for IoT**. Computer Networks, 148, 340-348.

Pallavi, K. N., & Ravi Kumar, V. (2021). **Authentication-based access control and data exchanging mechanism of iot devices in fog computing environment**. Wireless Personal Communications, 116(4), 3039-3060.

Patel, M., Mehta, A., & Chauhan, N. C. (2021). **Design of Smart Dashboard based on IoT & Fog Computing for Smart Cities**. In 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 458-462). IEEE.

Qiu, Y., & Ma, M. (2018, July). **Privacy Preserving for Location-Based IoT Services**. In International Conference on Smart Grid and Internet of Things (pp. 36-45). Springer, Cham.

Simplicio Jr, M. A., Silva, M. V., Alves, R. C., & Shibata, T. K. (2017). **Lightweight and escrow-less authenticated key agreement for the internet of things**. Computer Communications, 98, 43-51.

Sun, S., Du, R., Chen, S., & Li, W. (2021). **Blockchain-based IoT access control system: towards security, lightweight, and cross-domain**. IEEE Access, 9, 36868-36878.

Viejo, A., & Sánchez, D. (2019). Sec**ure and privacy-preserving orchestration and delivery of fog-enabled IoT services**. Ad Hoc Networks, 82, 113-125.