سومین کنفرانس بین‌المللی مهندسی و علوم کامپیوتر
اولین کنفرانس ملی سامانه های هوشمند، کلان داده و رایانش پیشرفته

روشهای تشخیص ناهنجاری کمانرژی و حفظ حریم خصوصی در اینترنت اشیای محدودمنبع مبتنی بر Edge و Federated Learning

فائزه خبیری ، فاطمه خبیری ، محمد امینی
دانشگاه آزاد اسلامی یزد

چکیده

با گسترش سریع اینترنت اشیا (IoT) در حوزه هایی نظیر شهرهای هوشمند، صنعت و سلامت، تشخیص ناهنجاری به عنوان یکی از مؤلفه های کلیدی برای تضمین امنیت، قابلیت اطمینان و پایداری این سامانه ها مطرح شده است. با این حال، محدودیت شدید منابع محاسباتی، انرژی و حافظه در بسیاری از گرههای IoT ، به همراه نگرانی های فزاینده درباره حفظ حریم خصوصی دادهها، کارایی روشهای سنتی مبتنی بر پردازش متمرکز و انتقال دادههای خام به ابر را به شدت کاهش داده است. این چالشها ضرورت استفاده از رویکردهای غیرمتمرکز و سازگار با محیطهای محدودمنبع را برجسته میسازد. در این زمینه، رایانش لبه با انتقال پردازش به نزدیکی منبع داده و یادگیری فدرال با حذف نیاز به اشتراک گذاری داده های خام، به عنوان راهکارهایی مؤثر برای کاهش تأخیر، مصرف انرژی و ریسک نقض حریم خصوصی معرفی شده اند. پژوهشهای اخیر نشان میدهند که چارچوبهای FL-Edgeقادرند با آموزش محلی مدلها و تجمیع پارامترها در سطح فدرال، تشخیص ناهنجاری بلادرنگ را حتی در محیطهای ناهمگن و پویا فراهم کنند.این مقاله مروری نظام مند، با بررسی بیش از ۲۰ مقاله معتبر، روشهای تشخیص ناهنجاری مبتنی بر یادگیری فدرال در IoT از جمله الگوریتم های سبک وزن، یادگیری عمیق فدرال، جنگل ایزوله فدرال و خوشه بندی فدرال را طبقه بندی و تحلیل میکند. همچنین چالش های کلیدی نظیر ناهمگونی داده ها، سربار ارتباطی، امنیت مدل و توازن میان دقت و مصرف انرژی بررسی شده و مسیرهای پژوهشی آینده پیشنهاد میشود.

مقدمه

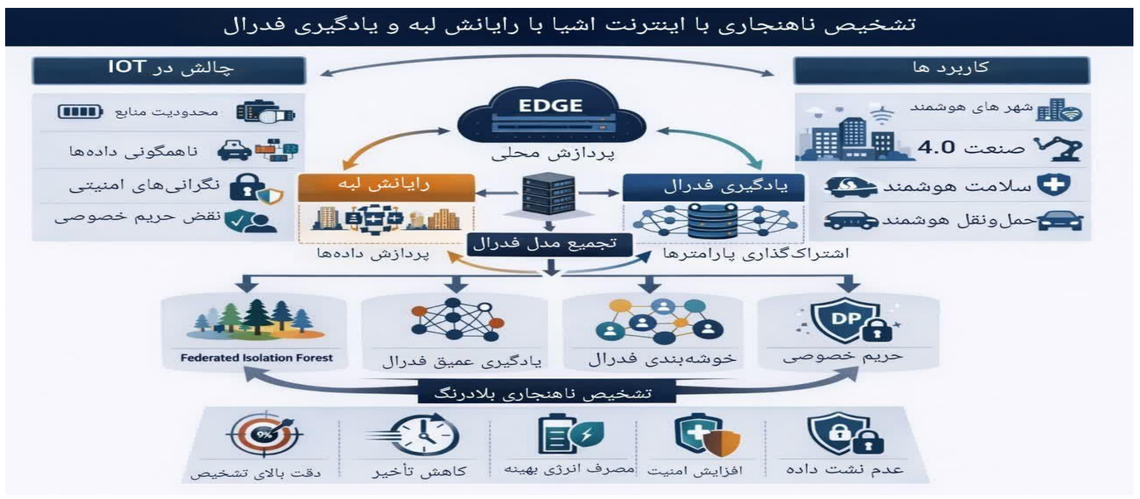
اینترنت اشیا به عنوان یکی از ارکان اصلی تحول دیجیتال، نقش محوری در حوزه هایی نظیر شهرهای هوشمند، صنعت ۴.۰، زیرساختهای حیاتی، مراقبت های سالمت و سامانه های حمل و نقل هوشمند ایفا میکند. با افزایش چشمگیر تعداد گرههای IoTو اتصال آنها به شبکه های ناهمگن، سطح حمالت سایبری، خطاهای عملیاتی و رفتارهای غیرعادی نیز به طور قابل توجهی افزایش یافته است. در این میان، تشخیص ناهنجاری به عنوان یک مکانیزم کلیدی برای شناسایی حملات، خرابیها و رفتارهای غیرمنتظره، اهمیت ویژهای در تضمین امنیت و پایداری این سامانه ها پیدا کرده است[۱_۳].

با این حال، بخش عمدهای از گرههای IoT دارای محدودیتهای شدید در منابع انرژی، توان پردازشی، حافظه و پهنای باند ارتباطی هستند. روشهای سنتی تشخیص ناهنجاری که مبتنی بر جمع آوری دادههای خام و پردازش متمرکز در سرورهای ابری میباشند، نه تنها منجر به افزایش تأخیر و مصرف انرژی میشوند، بلکه خطرات جدی در زمینه افشای دادههای حساس کاربران ایجاد میکنند. این چالشها، به ویژه در کاربردهای حساس مانند سلامت و زیرساختهای حیاتی، استفاده از رویکردهای کلاسیک را با محدودیت های اساسی مواجه ساخته اند[۱, ۲, ۴, ۵].

چارچوب پیشنهادی

یادگیری فدرال به عنوان یک چارچوب یادگیری توزیع شده، راهکاری مؤثر برای غلبه بر این چالش ارائه میدهد. در FL، مدلها به صورت محلی بر روی دستگاه ها آموزش داده شده و تنها پارامترهای مدل به اشتراک گذاشته میشوند، بدون آنکه داده های خام منتقل شوند. مطالعات اخیر نشان داده اند که ترکیب FLبا رایانش لبه میتواند ضمن حفظ حریم خصوصی، امکان تشخیص ناهنجاری دقیق و مقیاسپذیر را در محیط های محدودمنبع و ناهمگن فراهم سازد[۵, ۱۲_۱۴, ۱۶].

با وجود پیشرفتهای قابل توجه، چالشهایی نظیر ناهمگونی داده ها (IID-non)، سربار ارتباطی، امنیت مدلهای فدرال، حمالت استنتاجی، و ایجاد توازن میان دقت تشخیص و مصرف انرژی همچنان به عنوان مسائل باز پژوهشی مطرح هستند. ازاین رو، انجام یک مرور نظاممند برای تحلیل، مقایسه و طبقه بندی روش های موجود تشخیص ناهنجاری کم انرژی و حفظ حریم خصوصی مبتنی بر Edge و Learning Federated ضروری به نظر میرسد[۱۵, ۱۷_۲۴].



شکل ۱. تشخیص ناهنجاری با اینترنت اشیا با رایانش لبه و یادگیری فدرال

شبیه سازی و نتایج

این مرور نشان میدهد که ادغام رایانش لبه و یادگیری فدرال به عنوان یک پارادایم نوین، توانسته است به طور همزمان به دو چالش اساسی در اینترنت اشیای محدودمنبع پاسخ دهد: تشخیص مؤثر ناهنجاریها و حفظ حریم خصوصی داده ها. نتایج حاصل از بیش از ۲۵ مطالعه معتبر حاکی از آن است که چارچوبهای FL-Edgeبا تکیه بر آموزش محلی مدلها، تجمیع توزیع شده و حذف انتقال دادههای خام، قادر به دستیابی به دقت بالا، کاهش تأخیر و مصرف انرژی بهینه هستند؛ ویژگی هایی که برای محیطهای بلادرنگ و حساس IoTحیاتی محسوب میشوند[۱, ۵_۷, ۱۲, ۱۵].

از منظر روش شناسی، بررسی ها نشان می دهد که استفاده از الگوریتم های سبک وزن فدرال، خوشه بندی تطبیقی، و مدل های بدون نظارت نظیر Forest Isolation Federated نقش مهمی در سازگاری این چارچوب ها با محدودیت های سخت افزاری ایفا میکند. در عین حال، رویکردهای پیشرفته تری مانند یادگیری عمیق فدرال، بازی های بیزی و حتی مدل های کوانتومی فدرال، افق های جدیدی برای تشخیص ناهنجاری های پیچیده و چند بعدی گشوده اند، هرچند پیاده سازی عملی آنها هنوز با چالش هایی همراه است[۱۳, ۱۴, ۱۸, ۲۰, ۲۱].

نتیجه گیری

با وجود پیشرفت های قابل توجه، این مرور نشان میدهد که چالش هایی نظیر ناهمگونی داده ها ، سربار ارتباطی، حمالت مدل محور و نبود استاندارد های ارزیابی یکپارچه همچنان موانعی جدی برای استقرار گسترده این فناوری ها هستند. بسیاری از مطالعات بر سناریو های آزمایشگاهی متکی اند و نیاز به مجموعه داده های واقعی، بزرگ مقیاس و معیارهای ارزیابی چندبعدی (شامل دقت، انرژی، تأخیر و حریم خصوصی) بیش از پیش احساس میشود[۲, ۱۷, ۲۳, ۲۴].

در نهایت، میتوان نتیجه گرفت که آینده تشخیص ناهنجاری در IoTبه سمت چارچوبهای FL-Edgeتطبیقی، امن و کم مصرف حرکت میکند. پژوهشهای آتی باید بر بهینه سازی پروتکل های ارتباطی، طراحی مدل های فوق سبک، مدیریت هوشمند مشارکت گره ها و تقویت مکانیزم های امنیتی تمرکز کنند تا گذار از پژوهشهای آزمایشگاهی به کاربردهای صنعتی و شهری واقعی تسهیل شود[۲, ۳, ۵, ۹, ۱۰, ۱۹].

منابع

[1] Chatterjee, A. and B.S. Ahmed, IoT anomaly detection methods and applications: A survey. Internet of Things, 2022. 19: p. 100568.
[2] Narwane, V.S., et al., Quantum machine learning a new frontier in smart manufacturing: a systematic literature review from period 1995 to 2021. International Journal of Computer Integrated Manufacturing, 2025. 38(1): p. 116-135.
[3] Esmaeilzadeh, M., et al., Designing and regulating supplier development systems using ANFIS and meta-heuristic algorithms in the automotive industry. Research in Production and Operations Management, 2021. 12(3): p. 93-117.
[4] Farizi, A. and M.K. Nizam, Sistem deteksi intrusi berbasis deep learning untuk mitigasi serangan zero-day pada jaringan komputer. Karapan Network Journal: Journal Computer Technology and Mobile Ad Hoc Network, 2025. 1(01).