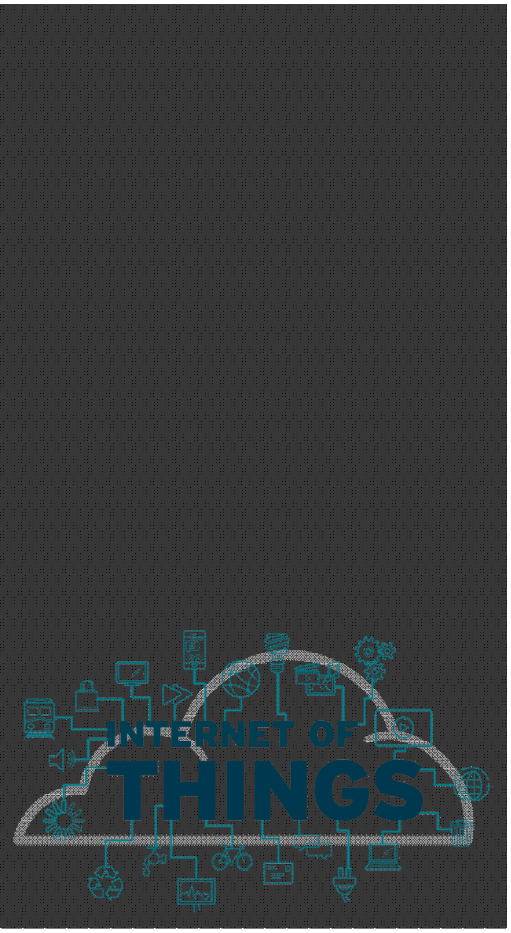


Software Defined Internet of Things Security: Properties, State of the Art, and Future Research

محمد سعید انصاری

دانشجوی دکتری معماری کامپیوتر

استاد گرامی: خانم دکتر جاسبی

تعریف مسئله

- از یک گوشی هوشمند تا شهر هوشمند، اینترنت اشیا به مرور جز لاینفکی از زندگی نوین شده است که کاربردهای آن سالانه چندین برابر می‌شود.
- منابع محدود و ماهیت ناهمگن دستگاه‌های اینترنت اشیا، کنترل امنیت را برای مدیران شبکه و امنیت کاری دشوار ساخته است.
- امروزه، شبکه‌های نرم‌افزارمحور (SDN) با ارائه روش‌های واضح و فراگیر، مورد توجه ویژه در خصوص رفع مشکلات امنیتی سنتی این حوزه قرار گرفته‌اند.
- شبکه‌های نرم‌افزارمحور با تفکیک Control plane و Data plane، مدیریت جامعی بر شبکه را ایجاد می‌کند. این تفکیک و وجود یک کنترلر مرکزی جهت مدیریت جامع شبکه، راه‌کارهایی کارا، امن و پایدار در مقابله با چالش‌های امنیتی اینترنت اشیا، ارائه می‌کند.

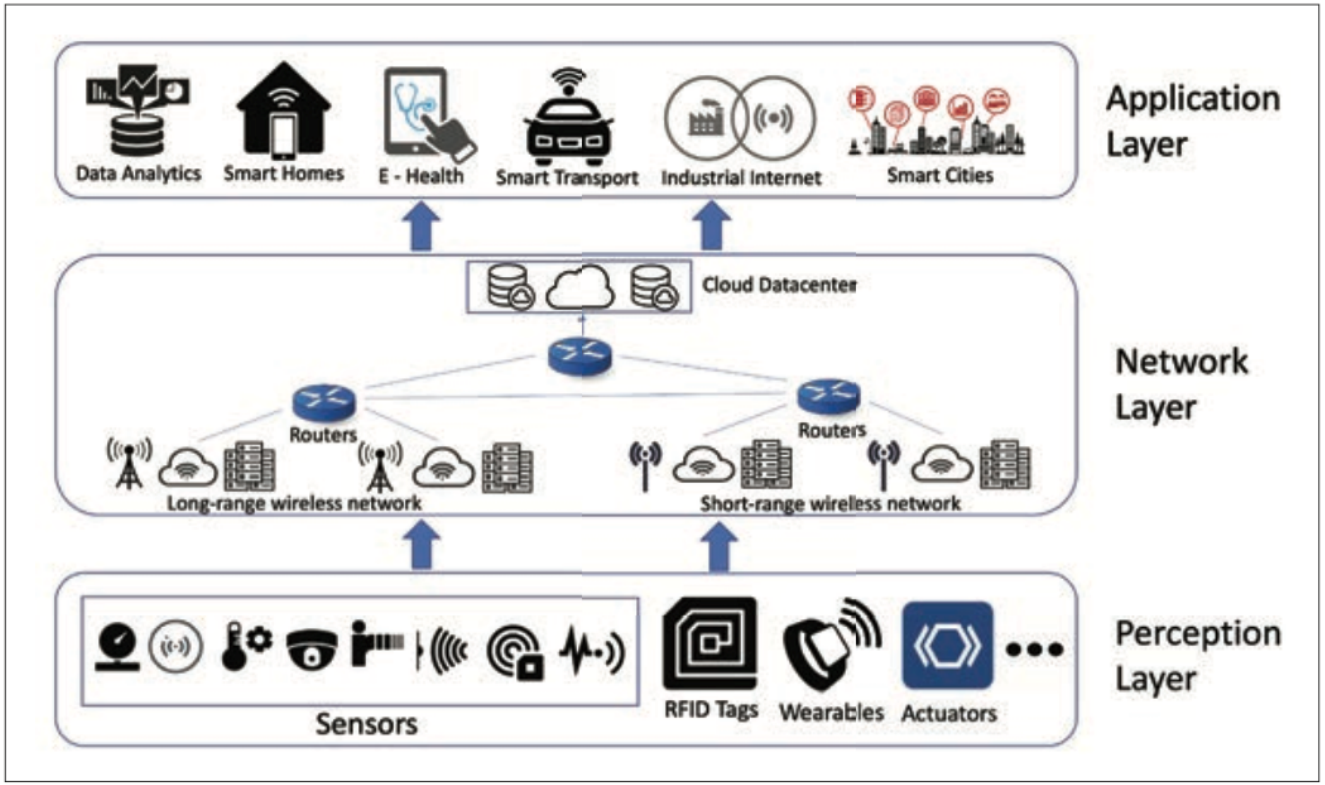
تعریف مسئله

- در این مقاله به چالش‌های موجود در این حوزه و راه‌حل‌های آن بر اساس شبکه‌های نرم‌افزارمحور پرداخته می‌شود.
- دامنه کاربردهای اینترنت اشیا، محبوبیت و استقبال زیادی پیدا کرده است.
- بنابراین ایجاد امنیت در برابر حملات و تهدیدات خصمانه، بسیار مهم است.
- در ادامه در سه بخش:
  - ساختار چارچوب اینترنت اشیا
  - دسته‌بندی تهدیدات رایج در حوزه اینترنت اشیا بر اساس لایه تحت تاثیر
  - فهم رابطه بین ذات هر لایه و تهدیدات مربوط به آن
- موضوعات بررسی می‌شوند.

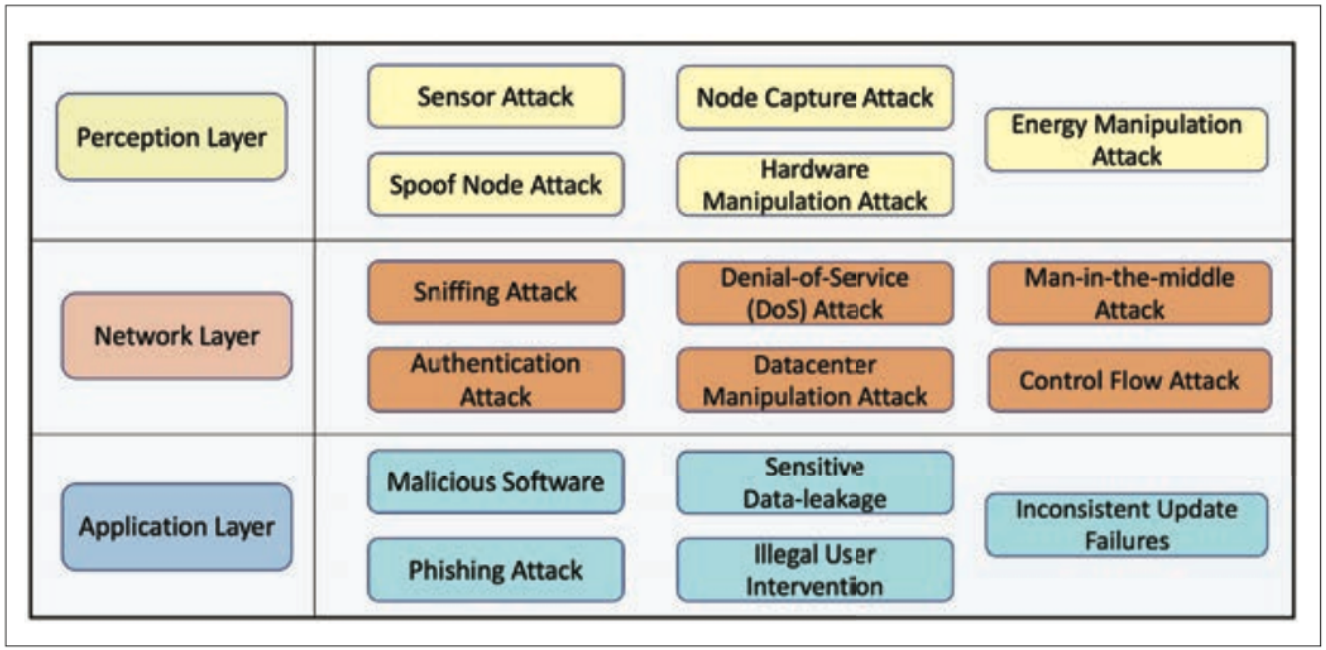
ساختار چارچوب اینترنت اشیا

- لایه Perception
- لایه ادراک، مسئول درک فیزیک طبیعی اشیا در محدوده پیاده‌سازی اینترنت اشیا و جمع‌آوری اطلاعات در مورد آن است. این لایه، سطح جمع‌آوری اطلاعات است.
  - به همین دلیل همیشه منبع جذابی برای حملات جهت دستیابی به اطلاعات حساس و ایجاد اختلال در سرویس‌های شبکه است.
- لایه Network
  - اطلاعات ارسالی از لایه Perception را به لایه Application جهت آنالیز و مصرف، می‌رساند.
  - حمله به این لایه موجب از کار افتادن کل سامانه می‌شود.
- لایه Application
- این لایه به دلیل ارتباط با مصرف‌کنندگان، محبوبیت زیادی دارد. همه برنامه‌های معروف مانند خانه هوشمند، حمل و نقل هوشمند و سلامت الکترونیکی در این لایه تعریف می‌شوند.
  - ماهیت آسیب‌پذیری‌های این لایه با دیگر لایه‌ها به دلیل حساسیت اطلاعات، متفاوت است. حملات این لایه ممکن است سامانه را از کار نیندازند ولی افشای اطلاعات عواقب ناگواری دارد.

ساختار چارچوب اینترنت اشیا



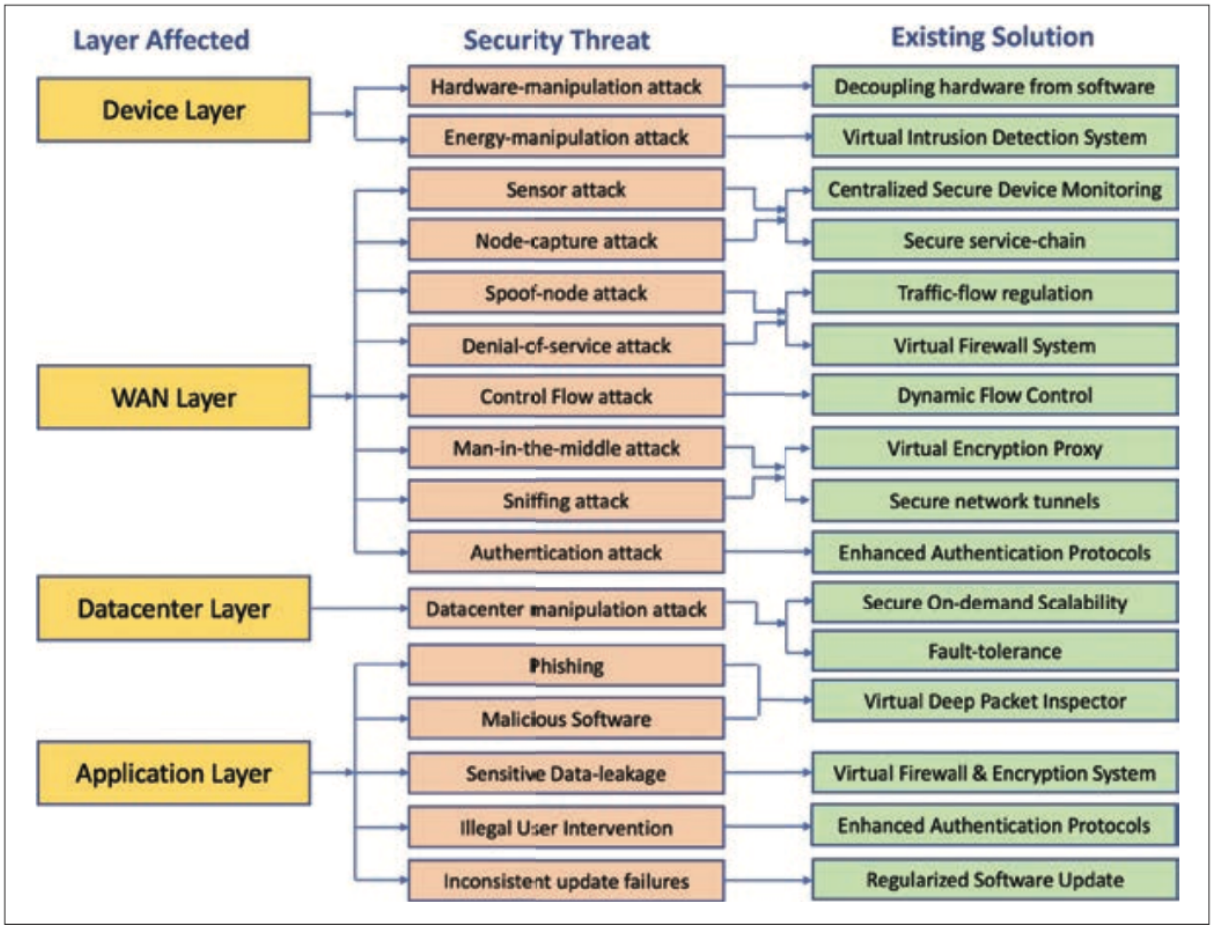
تهدیدات مربوط به چارچوب اینترنت اشیا



راه‌حل پیشنهادی

- معماری SDN-IOT از 4 لایه شکل گرفته است:
  - لایه Device
  - مشابه لایه درک معماری اینترنت اشیا
    - تفاوت اصلی در این است که هیچ جریان انفرادی یا مکانیزم نظارتی برای دستگاه وجود ندارد.
    - همه دستگاه‌ها به صورت متمرکز کنترل می‌شوند.
  - لایه WAN
  - این لایه به عنوان لایه اینترنت در ساختار در نظر گرفته می‌شود.
  - لایه Datacenter
  - لایه مرکز داده را می‌توان لایه ماندگاری خدمات کاربردی دانست.
    - ذخیره‌سازی داده‌های جمع آوری شده و پردازش شده توسط دستگاه و لایه‌های WAN
  - لایه Application
  - این لایه در دسترس کاربران قراردارد و با لایه Application در اینترنت اشیا تفاوت چندانی ندارد.

راه‌حل پیشنهادی



Critical issue	Layers affected	Existing solutions
Single point of failure	✓ Device layer ✓ WAN layer	• Multiple controllers • Replication strategies • Clean-slate recovery • Controller access restriction
Data confidentiality issues	✓ WAN layer ✓ Data center layer ✓ Application layer	• Rigid authentication mechanism • Systematic trust model • Autonomous trust management • Sandboxing techniques
Troubleshooting and speed recovery	✓ WAN layer ✓ Data center layer	• Reliable system snapshots • Immutable logs
Orchestration issues	✓ WAN layer ✓ Device layer	• FRESCO • OrchSec
Denial of service attacks	✓ WAN layer ✓ Device layer	• Rate-limiting of control channel • Event filtering • Traffic prioritization • Timeout adjustment • Localized central control
Man-in-the-middle attacks	✓ WAN layer ✓ Device layer	• Bloomfilter • Dynamic device association • Increase in data-plane programmability
Policy definition issues	✓ WAN layer	• HiPoLDS • HLP/MLP language protocols

چالش‌های موجود و کارهای آتی

مرجع

Mishra, Pritish, Ananya Biswal, Sahil Garg, Rongxing Lu, Mayank Tiwary, and Deepak Puthal, "Software Defined Internet of Things Security: Properties, State of the Art, and Future Research", IEEE Wireless Communications 27, no. 3, pp. 10-16, 2020

با تشکر از توجه شما