دانشگاه آزاد اسلامی واحد الکترونیکی
مجله فناوری اطلاعات و امنیت شبکه

بررسی ساز وکار هوشمند دفاعی در برابر حملات سرویس انکار توزیع‌شده اینترنت اشیاء

رضا غفاری دیزجی[۱]
[۱] تهران، ایران، دانشکده فنی آزاد اسلامی واحد غرب،rezaghaffarid@gmail.com

چکیده

اینترنت اشیاء یک فناوری پیشرو است که امکان اتصال گسترده‌ای از دستگاه‌های مختلف را برای ارائه خدمات و خودکارسازی در حوزه‌های مختلف از زندگی روزمره تا سامانه‌های زیرساختی حیاتی فراهم می‌کند. بااین‌حال، این دستگاه‌ها به حملات مختلف ازجمله، حملات سرویس انکار توزیع‌شده حساس هستند. هدف، از کار انداختن یک دستگاه معتبر و جلوگیری از دسترسی کاربران معتبر به سرویس‌ها یا منابع شبکه است. این حملات می‌توانند از طریق منابع حمله توزیع‌شده، منابع حمله متنوع و تغییرات ترافیک انجام شوند؛روش دفاع هوشمندانه که بانام محافظ جریان برای مقابله با این حملات ارائه‌شده است. این روش شامل تشخیص، شناسایی، طبقه‌بندی و کاهش حملات است که دو مؤلفه اصلی به نام فیلتر جریان و راه‌انداز جریان در بر دارد و برای شناسایی، تشخیص، طبقه‌بندی و کاهش حملات استفاده می‌شود. الگوریتم تشخیص حملات بر اساس تغییرات ترافیک ارائه‌شده و دو مدل یادگیری ماشین به نام حافظه بلندمدت- کوتاه‌مدت و شبکه عصبی پیچشی یا هم‌گشتی برای شناسایی و طبقه‌بندی حملات سرویس انکار توزیع‌شده ارائه‌شده است. این مدل‌ها با تأخیر مناسبی در سرورهای لبه که قدرت محاسباتی بالاتری نسبت به یک رایانه شخصی دارند، قابلیت استفاده دارند. راهکارهایی برای رفع محدودیت‌ها و نقاط ضعف در حفاظت از سامانه‌های اینترنت اشیاء در برابر حملات امنیتی می توان استفاده کرد که از جمله آنها؛ افزایش قدرت محاسباتی و فضای ذخیره‌سازی، استفاده از شیوه‌نامه‌های امن‌تر، استفاده از فن‌های دفاعی پیشرفته، توسعه روش‌های هوش مصنوعی و یادگیری عمیق است.

کلیدواژه: امنیت اینترنت اشیاء، حملات DDoS، محاسبات لبه، هوش مصنوعی

مقدمه

اینترنت اشیا یکی از فناوری‌های نوین در زمینهٔ ارتباطات هوشمند است که مزیت‌های آن باعث می‌شود تا هرروز سازمان‌ها و مؤسسات مختلفی به این فناوری بپیوندند . بر اساس مطالعات انجام‌شده، آینده دنیای ارتباطات را می‌توان در چهارچوب[۱] IOT تصور کرد[۱]. این ویژگی باعث شده است تا محققان، علاقه‌مند به پیاده‌سازی اینترنت اشیای مبتنی بر فناوری‌های جدید (مانند شبکه 5G) باشند[۲].

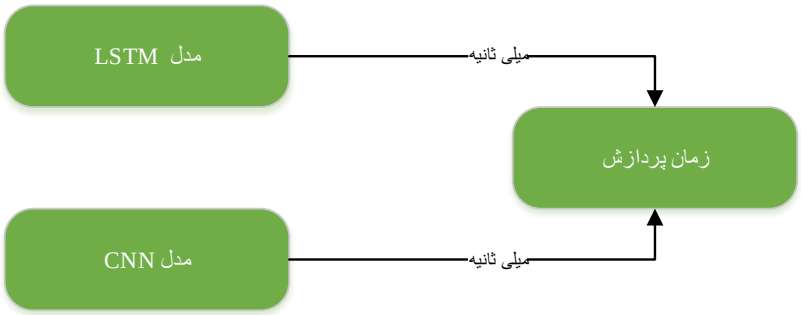
یکی از جنبه‌های کلیدی معرفی اینترنت اشیاء، توانایی پشتیبانی از بسیاری از دستگاه‌ها در مقایسه با تعداد فعلی است. مدیریت ارتباط بین میلیاردها حسگر متصل و دستگاه رادیویی یکی از برنامه‌های پیش‌بینی‌شده جدید برای اینترنت اشیاء است [۵-۳]. فراهم کردن بستر ارتباطی برای این تعداد تجهیزات باعث ایجاد مشکلات امنیتی جدید خواهد شد. برای مثال، در چنین شبکه‌ای، قربانیان حملات سایبری ممکن است دسترسی به تجهیزات خانه، اتومبیل یا تلفن‌های همراه خود را از دست بدهند.[۶] به همین دلیل در کارهای تحقیقاتی مختلف راهکارهایی برای تأمین امنیت ارتباطات در این شبکه‌ها ارائه

[۱] *Internt of thing*

شده‌است.[۷,۸] بااین‌حال، این یک مشکل حل‌نشده باقی‌مانده است و این شبکه به راه‌حل‌های امنیتی کارآمدتری نیاز دارد. با افزایش قابل‌توجه تعداد دستگاه‌ها و برنامه‌های کاربردی متصل در اینترنت اشیاء، این محیط فرصت‌های بیشتری را برای مهاجمان فراهم می‌کند تا تهدیداتی مانند حملات DoS[1] را اجرا کنند. [۹]

از سوی دیگر، بر اساس مطالعات اخیر، بیش از استفاده از راه‌حل‌های رمزگذاری برای کدگذاری، ارتباطات و داده‌های اینترنت اشیاء نیاز است، زیرا علاوه بر اینکه نمی‌تواند مهاجم را شناسایی کند، باعث هدر رفتن منابع محاسباتی شبکه می‌شود. [۱۰]

روش دفاع هوشمندانه محافظ جریان (Flow Guard) یک مکانیسم دفاعی نوآورانه IOT در برابر حملات DDoS[2]است که از مدل‌های یادگیری ماشین برای تشخیص و طبقه‌بندی حملات استفاده می‌کند. این سیستم دفاعی شامل دو جزء اصلی است: فیلتر جریان و کنترل‌کننده جریان. فیلتر جریان مسئول شناسایی و فیلترکردن جریان‌های مخرب بر اساس قوانین فیلتراسیون از پیش تعیین‌شده است، درحالی‌که کنترل‌کننده جریان بر شناسایی و طبقه‌بندی جریان‌های مخرب با استفاده از مدل‌های یادگیری ماشین تمرکز دارد. مدل LSTM[3]پیشنهادی، دقت شناسایی بالا و مدل CNN[4] دقت طبقه‌بندی بالا را که از سایر مدل‌های یادگیری ماشین بهتر عمل کرده‌اند، به دست آورده است. نتایج این مقاله همچنین نشان داد که مدل‌ها هنگام آزمایش با مجموعه داده‌های شبیه‌سازی‌شده و مجموعه داده‌های CICDDoS2019[5] توانایی تعمیم دارند و قادر به شناسایی و طبقه‌بندی مؤثر انواع حملات DDoS هستند. علاوه بر این، ارزیابی کارایی نشان داد که زمان پردازش مدل‌های LSTM و CNN در محدوده‌های قابل‌قبول است و تضمین می‌کند که عملیات عادی دستگاه‌های IOT تحت تأثیر قابل‌توجهی از مکانیسم دفاعی قرار نمی‌گیرند. (شکل ۱)



شکل ۱: فرآیند زمان پردازش

مکانیسم دفاعی FlowGuard به همراه مدل‌های LSTM و CNN، رویکردی امیدوارکننده برای مقابله با حملات سرویس انکار توزیع‌شده اینترنت اشیاء ارائه می‌دهد. (شکل۲) با شناسایی و طبقه‌بندی مؤثر جریان‌های مخرب، FlowGuard، یک استراتژی دفاعی پیشگیرانه در برابر حملات سرویس انکار توزیع‌شده (DDoS) به دستگاه‌های اینترنت اشیاء را فراهم می‌کند. ارزیابی جامع مدل‌ها، دقت و کارایی بالای آن‌ها را نشان می‌دهد، که ظرفیت آن‌ها برای کاربرد واقعی در دفاع در برابر حملات سرویس انکار توزیع‌شده اینترنت اشیاء را برجسته می‌کند. درمجموع، FlowGuard، یک مکانیسم دفاعی پیشرفته و مؤثر محوری را ارائه می‌دهد که می‌تواند امنیت شبکه‌های IoT را به‌طور قابل‌توجهی افزایش دهد.[۱۱]

[1] *Denial of Service*
[2] *Distributed Denial of Service*
[3] *Long Short-Term Memory*
[4] *Convolutional Neural Network*
[5] *Cybersecurity Intrusion Detection Dataset for Denial-of-Service Attacks in 2019*

شکل ۲: مدل دقت یادگیری ماشین

کارهای مرتبط

روش انتخاب ویژگی (FS)[1]، روشی برای تشخیص حملات DDoS در شبکه‌های اینترنت اشیاء(IOT) است که به دنبال دستیابی به اهداف اصلی بیشینه‌کردن ارتباط، دقت طبقه‌بندی، بازخوانی، دقت نمونه‌های واقعی به نمونه‌های اندازه‌گیری و کمینه کردن تکرار و تعداد بوده و شامل انتخاب ویژگی‌هایی است که برای تشخیص حملات DDoS بسیار مرتبط هستند. این اهداف به‌طورکلی به بهبود عملکرد و کارایی سیستم تشخیص نفوذ (IDS)[2] در تشخیص حملات DDoS در شبکه‌های IOT از طریق انتخاب ویژگی‌های مرتبط و مؤثر می‌پردازند، اما این روش ممکن است محدودیت‌ها و نقاط ضعف زیر را داشته باشد:

پیچیدگی محاسباتی، به علت استفاده از الگوریتم‌های بهینه‌سازی چند هدف ممکن است نیازمند محاسبات زمان‌بر یا وابستگی به داده‌های ورودی باشد که نتایج آن برای دیگر مجموعه‌های داده ممکن است قابل‌اعمال نباشد. تنظیم پارامترها نیز نیازمند تخصیص زمان و توانایی تخصصی است.

اعتبارسنجی، ارزیابی دقیق و قابل‌اعتماد نتایج به دلیل وجود چندین هدف و همچنین انتخاب ویژگی‌های مناسب و حذف ویژگی‌های غیرضروری ممکن است به دلیل پیچیدگی مسئله، چالش‌برانگیز باشند. [۱۲]

لایه‌های اصلی در معماری SDN[3] شامل لایه برنامه، لایه کنترل و لایه داده است. این لایه‌ها با هم کار می‌کنند تا انعطاف‌پذیری و قابلیت برنامه‌ریزی را که ویژگی‌های معماری SDN هستند، فراهم کنند، اما دارای محدودیت‌ها و نقاط ضعف مصرف منابع بالا، دشواری در تعریف آستانه تشخیص برای برنامه‌های مختلف، عدم شبیه‌سازی یا اجرای واقعی مرتبط با شبکه‌های تعریف‌شده، تولید تأخیر برای کاربران معتبر، دشواری محدودیت در تعریف پارامترهای کلیدی مانند زمان اوج و استفاده غیرعادی از لینک، محدودیت در تعریف معیارها و آستانه‌ها، نیاز به زمان طولانی برای اطلاع‌رسانی کنترل‌گرهای مجاور و مهار حملات و دیگر محدویت ها است. [۱۳]

استفاده از شبکه‌های تعریف‌شده توسط نرم‌افزار (SDN)، برای مدیریت تهدیدات DDoS در دستگاه‌های اینترنت اشیاء چندین مزیت شامل کنترل متمرکز، انعطاف‌پذیری و قابلیت تطبیق، قابلیت مقیاس‌پذیری، بهره‌وری منابع کارآمد، شناسایی و مهارت زودهنگام، تصمیم‌گیری تطبیقی را ارائه می‌دهد.

به‌طورکلی، استفاده از SDN برای مدیریت تهدیدات DDoS در دستگاه‌های IOT، رویکردی قوی و کارآمد را برای افزایش امنیت و انعطاف‌پذیری شبکه‌های IOT فراهم می‌کند و چالش‌های منحصربه‌فردی را که توسط دستگاه‌های IOT با منابع محدود ایجاد می‌شود، مدیریت می‌کند. برخی محدودیت‌ها و نقاط ضعف مطرح‌شده در مورد روش‌های مختلف برای مقابله با حملات DDoS شامل محدودیت‌های مرتبط با تعداد گره‌های شبکه، نیاز به بهبود در مجموعه ویژگی‌ها و نرخ یادگیری در

[1] *Feature Selection*
[2] *Intrusion Detection Seystem*
[3] *Software-Define-Network*

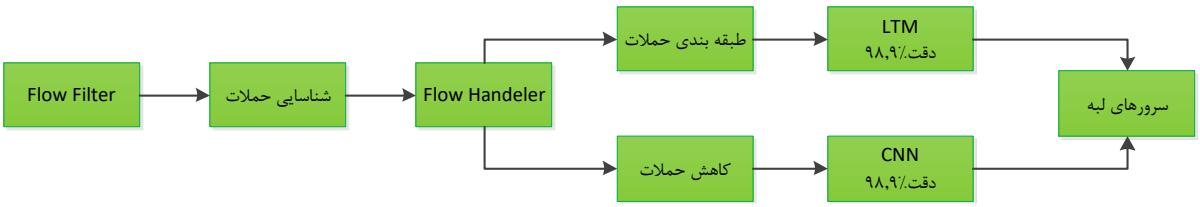
روش‌های تشخیص مبتنی بر هوش مصنوعی، ضعف در مقابله با حملات ناشناخته یا zero-day، مشکلات مربوط به حجم بزرگ ترافیک DDoS، نیاز به بهبود در مجموعه ویژگی‌ها و نرخ یادگیری در روش‌های تشخیص مبتنی بر هوش مصنوعی است.[۱۴]

نویسندگان از ResNet برای تشخیص حملات IOT استفاده کردند سپس با تبدیل داده‌های ترافیک شبکه به فرم تصویر و آموزش یک مدل CNN پیشرفته بر روی‌داده‌های تبدیل‌شده (ResNet)، مراحل جمع‌آوری داده، پیش‌پردازش داده، تشخیص حمله را بر روی تصاویر پیش‌پردازش شده آموزش دادند. این روش، علاوه بر دقت بالا، در مقایسه با روش‌های پیشین، در اصطلاحات دقت، بازخوانی برای تشخیص الگوهای حملات DoS و DDoS عملکرد بهتری داشت.
به‌طور خلاصه، نویسندگان از ResNet[1]با تبدیل داده‌های ترافیک شبکه به فرم تصویر و سپس آموزش مدل ResNet بر روی‌داده‌های تبدیل‌شده برای تشخیص بهتر حملات DoS و DDoS در شبکه‌های IOT استفاده کردند. محدودیت‌ها و نقاط ضعف بر اساس این روش شامل نیاز به داده‌های ورودی واقعی، پیچیدگی در تبدیل داده، انتخاب ویژگی‌ها، انتقال دانش به دامنهٔ جدید و محدودیت‌های مدل می‌شود.[۱۵]

روش محافظ جریان (FlowGuard)

محافظ جریان برای رفع مشکلات و نقاط ضعف در زمینهٔ حملات DDoS اینترنت اشیاء، توسعه مکانیسم دفاعی هوشمند در لبه شبکه به نام FlowGuard است. این روش طراحی‌شده است تا حملات DDoS IOT را تشخیص داده، بدون اینکه فشار محاسباتی قابل‌توجهی بر روی دستگاه‌های IOT وارد کند، آنها را شناسایی، طبقه‌بندی و مقابله کند. این سیستم از دو مدل یادگیری ماشینی، LSTM و CNN، برای شناسایی و طبقه‌بندی حملات DDoS استفاده می‌کند. اجزای کلیدی FlowGuard شامل Flow Filter که وظیفه فیلتر کردن جریان‌های مخرب و تشخیص جریان‌های مخرب ناشناخته را دارد وا Flow Handler است که جریان‌های مشکوک را برای شناسایی و طبقه‌بندی حملات DDoS تجزیه و تحلیل می‌کند.

FlowGuard در سرورهای لبه‌ای که به شبکه IOT نزدیک‌تر هستند عمل و تضمین می‌کند تمام بسته‌هایی که از طریق سرورهای لبه‌ای عبور می‌کنند مورد بازرسی قرار می‌گیرند. این سیستم، دقت بالایی در شناسایی حملات(بیش از ٪۹۸,۹) و طبقه‌بندی حملات(بیش از ٪۹۹,۹) دارد بدون اینکه بر عملیات شبکه معمولی تأثیر قابل‌توجهی بگذارد. علاوه بر این، این راه‌حل به‌منظور رفع محدودیت‌های فن‌های دفاعی سنتی DDoS، یک طرح دفاعی کارآمد و قدرتمند را ارائه می‌دهد که به‌طور خاص برای محیط‌های IOT طراحی‌شده است(شکل۳).



شکل۳:مولفه های Flow Guard وعملکرد آنها

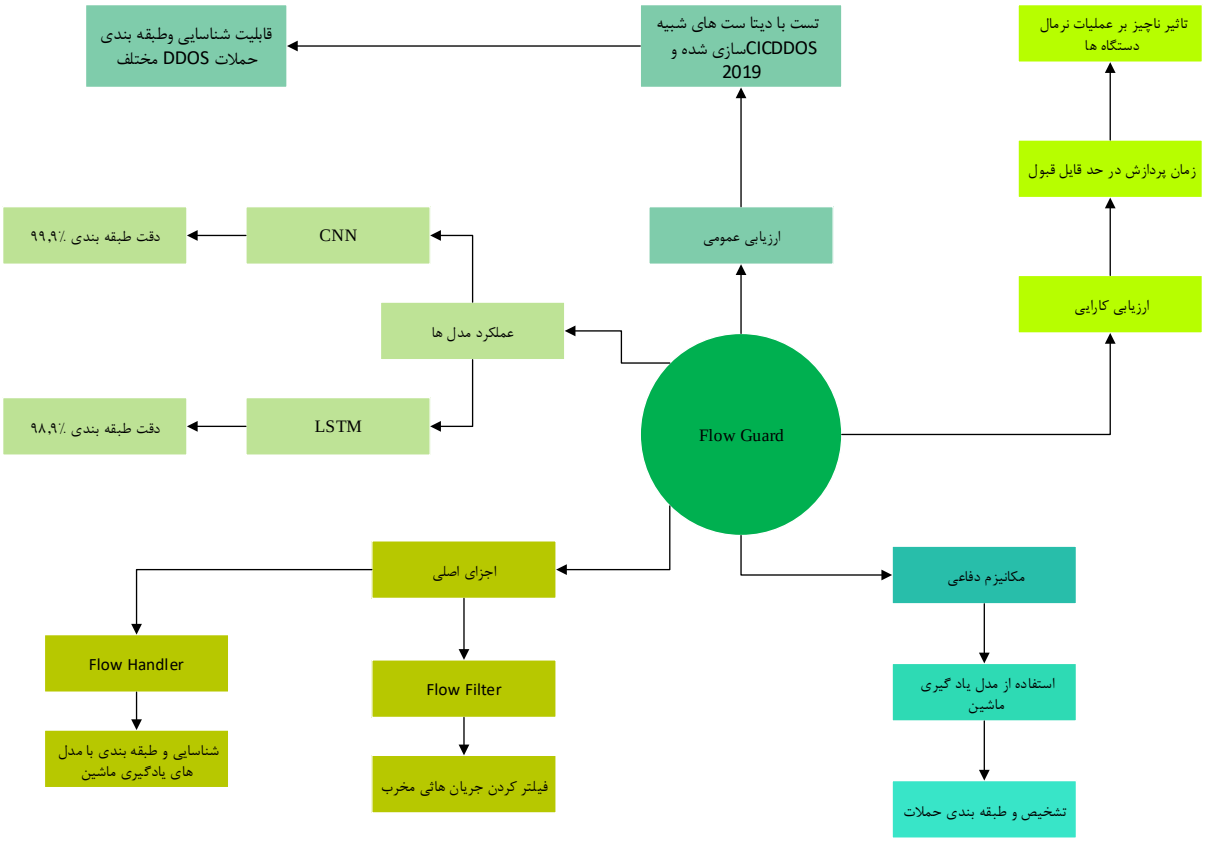
علاوه بر این، این روش بر اهمیت فن‌های بازگشت به مبدأ IP، تغییرات آنتروپی و سامانه‌های تشخیص و پیشگیری از نفوذ که در لایه‌های مختلف شبکه پشته مستقر هستند، تأکید می‌کند تا دفاع کلی را در برابر حملات DDoS IoT تقویت کند.

[1] *Residual Network*

نقاط قوت استفاده از LSTM و CNN را می‌توان توانایی در تشخیص الگوها و امکان استفاده از داده‌های ساختاریافته بیان کرد؛ LSTM و CNN قادرند الگوهای پیچیده و تغییرات زمانی را تشخیص دهند که می‌تواند برای تشخیص حملات DDoS مفید باشد. این شبکه‌ها می‌توانند الگوهای مشخصی را که به‌صورت متناوب و پیچیده در حملات DDoS ظاهر می‌شوند تشخیص دهند و اقدامات دفاعی مناسب را انجام دهند. همچنین LSTM و CNN قادر به کار با داده‌های ساختاریافته مانند ترافیک شبکه هستند. این امکان به آن‌ها کمک می‌کند تا الگوهای مختلف ترافیک شبکه را تشخیص داده و از حملات DDoS دفاع کنند.

نقاط ضعف استفاده از LSTM و CNN را نیز می‌توان نیاز به داده‌های بزرگ و پیچیدگی آموزش برشمرد. استفاده از LSTM و CNN نیازمند داده‌های بزرگ و متنوع است که ممکن است در برخی از موارد، دسترسی به چنین داده‌هایی دشوار باشد. برای آموزش مؤثر این شبکه‌ها نیازمند داده‌های بزرگ و گوناگون هستیم تا بتوانند الگوهای مختلف را تشخیص دهند. همچنین آموزش و تنظیم مدل‌های LSTM و CNN نیازمند تخصص و زمان زیادی است. این فرآیند، نیازمند دانش تخصصی و تجربه در زمینهٔ شبکه‌های عصبی است و ممکن است زمان‌بر باشد.[۱۱]

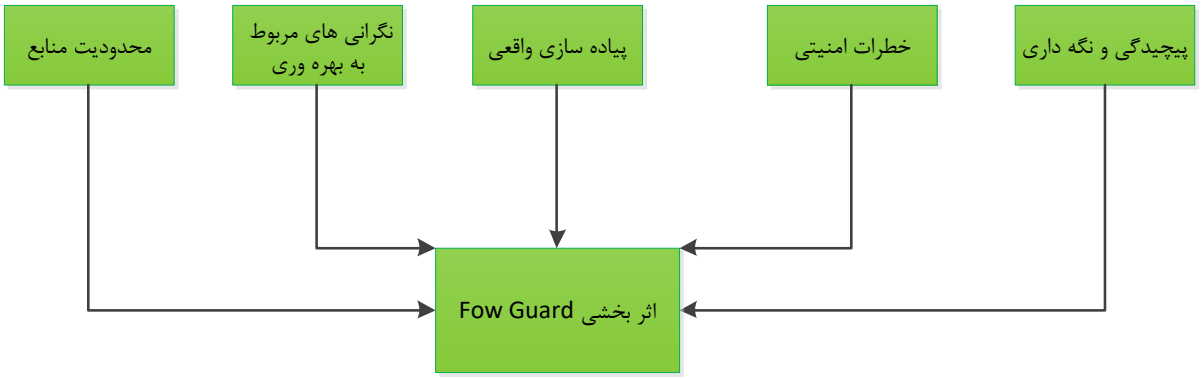
نقاط ضعف پیشنهادی راه‌حل FlowGuard به‌طور بالقوه می‌توانند شامل محدودیت‌های منابع دستگاه‌های اینترنت اشیاء که دارای قدرت محاسباتی و ذخیره‌سازی محدودی هستند، نگرانی‌های مربوط به کارایی، استقرار در دنیای واقعی، خطرات امنیتی مرتبط با پیاده‌سازی مکانیسم‌های دفاعی مبتنی بر یادگیری ماشینی، پیچیدگی و نگهداری باشند. به‌طور کلی می‌توان برای این روش نقشه مفهومی ذیل را ترسیم کرد. (شکل۴)



شکل ۴: نقشه مفهومی روش Flow Guard

نتایج

درحالی‌که روش FlowGuard قابلیت‌های امیدوارکننده‌ای را در تشخیص، شناسایی و طبقه‌بندی حملات DDoS در محیط‌های IOT نشان می‌دهد، مهم است که نقاط ضعف بالقوه مربوط به محدودیت‌های منابع، کارایی، چالش‌های استقرار در دنیای واقعی، خطرات امنیتی و پیچیدگی را در نظر بگیریم. رفع این نقاط ضعف برای تضمین کارایی و عملی بودن راه‌حل در سناریوهای امنیتی واقعی IOT حیاتی است(شکل۵).



شکل۵:اثر بخشی روش Flow Guard

روش FlowGuard، یک رویکرد مؤثر و عملی برای رفع نقاط ضعف و چالش‌های مرتبط با حملات DDoS IOT ارائه می‌دهد و یک مکانیسم دفاعی قوی را فراهم می‌کند که از مدل‌های یادگیری ماشینی و معماری متمرکز بر لبه‌ای برای تأمین امنیت شبکه‌های IOT بهره می‌برد.

به‌طورکلی، استفاده از LSTM و CNN می‌تواند برای تشخیص حملات DDoS مفید باشد اما نیاز به‌دقت و توجه به محدودیت‌ها و مشکلات مربوطه دارد. این روش‌ها نیازمند منابع و دانش تخصصی برای پیاده‌سازی مؤثر هستند.

نتیجه‌گیری

مطابق با روش‌های بررسی‌شده در مقالات، می‌توان از راهکارهای زیر برای رفع محدودیت‌ها و نقاط ضعف در حفاظت از سامانه‌های IOT در برابر حملات امنیتی استفاده کرد:

افزایش قدرت محاسباتی و فضای ذخیره‌سازی: با افزایش قدرت محاسباتی و فضای ذخیره‌سازی دستگاه‌های IOT، می‌توان از روش‌های پیشرفته‌تری برای تشخیص و پیشگیری از حملات استفاده کرد. این امر می‌تواند باعث افزایش امکانات امنیتی دستگاه‌ها و کاهش آسیب‌پذیری‌ها شود.

استفاده از شیوه‌نامه‌های امن‌تر: انتخاب شیوه‌نامه‌های ارتباطی امن‌تر و پیچیده‌تر برای دستگاه‌های IoT می‌تواند به کاهش آسیب‌پذیری‌ها و افزایش امنیت این دستگاه‌ها کمک کند.

پیاده‌سازی سامانه‌های تشخیص حملات پیشرفته: استفاده از سامانه‌های تشخیص حملات هوشمند و پیشرفته برای تشخیص حملات Slow Request/Response و دیگر حملات DDoS می‌تواند به موفقیت‌آمیز بودن در پیشگیری از حملات کمک کند.

استفاده از فن‌های دفاعی پیشرفته: پیاده‌سازی فن‌های دفاعی پیشرفته مانند شبکه‌های تشخیص نفوذ و سامانه‌های پیشگیری از نفوذ می‌تواند به تشخیص و پیشگیری از حملات DDoS کمک کند.

توسعه روش‌های هوش مصنوعی و یادگیری عمیق: استفاده از روش‌های هوش مصنوعی و یادگیری عمیق برای تشخیص حملات ناشناخته و غیر قابل پیش‌بینی می‌تواند به افزایش دقت در تشخیص حملات و کاهش تأثیر آن‌ها کمک کند.

این راهکارها می‌توانند به بهبود امنیت سامانه‌های IOT و کاهش تأثیر حملات امنیتی بر روی آن‌ها کمک کنند.

استفاده از شبکه‌های عصبی مانند LSTM و CNN به‌عنوان روش هوش مصنوعی برای دفاع در برابر حملات DDoS مزایا و محدودیت‌های خود را دارد.

منابع

1. Ahmed Raoof, Ashraf Matrawy, Chung-Horng Lung,Secure Routing in IoT: Evaluation of RPL's Secure Mode under Attacks. Computer science cryptography and security Carleton (University Canada, 2019)

2. Cao, K., et al., Enhancing physical-layer security for IoT with nonorthogonal multiple access assisted semi-grant-free transmission. IEEE Internet of Things Journal, 2022. 9(24): p. 24669-24681.

3. Chen, P., et al., Effectively detecting operational anomalies in large-scale iot data infrastructures by using a gan-based predictive model. The Computer Journal, 2022. 65(11): p. 2909-2925.

4. El-Hajj, M., et al., A survey of internet of things (IoT) authentication schemes. Sensors, 2019. 19(5): p. 1141.

5. Glissa, G., A. Rachedi, and A. Meddeb. A secure routing protocol based on RPL for Internet of Things. in 2016 IEEE Global Communications Conference (GLOBECOM). 2016. IEEE.

6. Gupta, B., et al., Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers. Computers & Electrical Engineering, 2022. 98: p. 107726.

7. Khanna, A. and S. Kaur, Internet of things (IoT), applications and challenges: a comprehensive review. Wireless Personal Communications, 2020. 114: p. 1687-1762.

8. Kore, A. and S. Patil, Cross layered cryptography based secure routing for IoT-enabled smart healthcare system. Wireless Networks, 2022: p. 1-15.

9. Li, B., et al., Dynamic event-triggered security control for networked control systems with cyber-attacks: A model predictive control approach. Information Sciences, 2022. 612: p. 384-398.

10. Stoyanova, M. Nikoloudakis, Y. Panagiotakis, S. Pallis, E. & Markakis, E. K. A survey on the internet of things (IoT) forensics: Challenges, approaches, and open issues. IEEE Commun. Surv. Tutor. 22(2), 1191–1221 (2020).

11. Hussain, F., Abbas, S. G., Husnain, M., Fayyaz, U. U., Shahzad, F., & Shah, G. A. (2020, November). IoT DoS and DDoS attack detection using ResNet. In 2020 IEEE 23rd International Multitopic Conference (INMIC) (pp. 1-6). IEEE.

12. Roopak, M., Tian, G. Y., & Chambers, J. (2020). Multi-objective-based feature selection for DDoS attack detection in IoT networks. IET Networks, 9(3), 120-127.

13. R., Russello, G., & Zanna, P. (2021). Mitigating ddos attacks in sdn-based iot networks leveraging secure control and data plane algorithm. Applied Sciences, 11(3), 929

14. .Bhayo, J., Jafaq, R., Ahmed, A., Hameed, S., & Shah, S. A. (2021). A time-efficient approach toward DDoS attack detection in IoT network using SDN. IEEE Internet of Things Journal, 9(5), 3612-3630.

15. Jia, Y., Zhong, F., Alrawais, A., Gong, B., & Cheng, X. (2020). Flowguard: An intelligent edge defense mechanism against IoT DDoS attacks. IEEE Internet of Things Journal, 7(10), 9552-9562.