**مقاله**

**: CICIoT2023 یک مجموعه‌داده بلادرنگ و یک بنچمارک برای حملاتِ در مقیاس بزرگ در محیط اینترنت اشیا**

نویسندگان:  
یوکلیدس کارلوس پینتو نتو، سجاد دادخواه\*، رافائل فریرا، علیرضا ظهورِیان، رونگشینگ لو، و علی. ا. قربانی  
دانشکده علوم کامپیوتر، دانشگاه نیوبرانزویک (UNB)، فردریکتون، نیوبرانزویک، کانادا (NB E3B 5A3)  
ایمیل‌ها:  
e.neto@unb.ca (E.C.P.N.)  
raphael.ferreira@unb.ca (R.F.)  
alireza.zohourian@unb.ca (A.Z.)  
rlu1@unb.ca (R.L.)  
ghorbani@unb.ca (A.A.G.)

* نویسنده مسئول مکاتبات: sdadkhah@unb.ca

ارجاع (Citation):  
Neto, E.C.P.; Dadkhah, S.; Ferreira, R.; Zohourian, A.; Lu, R.; Ghorbani, A.A.  
CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment.  
Sensors 2023, 23, 5941. <https://doi.org/10.3390/s23135941>

ویرایشگر علمی: آنتونیو پولیافیتو  
دریافت‌شده: ۱۴ آوریل ۲۰۲۳  
بازنگری‌شده: ۱۶ ژوئن ۲۰۲۳  
پذیرفته‌شده: ۲۰ ژوئن ۲۰۲۳  
منتشر شده: ۲۶ ژوئن ۲۰۲۳

حقوق انتشار: © ۲۰۲۳ نویسندگان.  
صاحب امتیاز انتشار: MDPI، بازل، سوئیس.  
این مقاله با مجوز Creative Commons Attribution (CC BY 4.0) منتشر شده است، که اجازهٔ استفاده و توزیع با ذکر منبع را می‌دهد.

**چکیده:**  
امروزه مفهوم اینترنت اشیا (Internet of Things یا IoT) نقشی محوری در جامعه ایفا می‌کند و قابلیت‌های جدیدی را به صنایع گوناگون ارائه می‌دهد. تعداد راهکارهای مبتنی بر اینترنت اشیا در حوزه‌هایی مانند حمل‌ونقل و سلامت رو به افزایش است و خدمات جدیدی نیز در حال توسعه‌اند. در دههٔ گذشته، جامعه شاهد افزایش شدید تعداد اتصالات مبتنی بر اینترنت اشیا بوده است؛ در واقع انتظار می‌رود در سال‌های پیش‌رو، اتصالات IoT در حوزه‌های مختلف باز هم رشد کنند.

در مقابلِ این مزایا، هنوز چالش‌های متعددی برای رسیدن به یک بهره‌برداری کارآمد و امن باقی است (برای نمونه، هم‌کنش‌پذیری/سازگاری میان‌سازمانی، امنیت، استانداردها، و فناوری‌های سمت سرور). افزون بر این، با وجود تلاش‌هایی که برای تولید مجموعه‌داده‌هایی از حمله علیه دستگاه‌های اینترنت اشیا انجام شده، هنوز انواعی از حملات بالقوه پوشش داده نشده‌اند. بیشتر تلاش‌های موجود همچنین یک توپولوژی شبکه‌ای گسترده با دستگاه‌های واقعی IoT را در نظر نمی‌گیرند. هدف اصلی این پژوهش ارائهٔ یک مجموعه‌دادهٔ جدید و گسترده از حملات علیه اینترنت اشیا است تا توسعهٔ تحلیل‌های امنیتیِ قابل‌استفاده در عملیات واقعی IoT را تسهیل کند.

برای رسیدن به این هدف، ما ۳۳ حمله را در یک توپولوژی اینترنت اشیا متشکل از ۱۰۵ دستگاه اجرا کردیم. این حملات در هفت گروه دسته‌بندی شده‌اند: حملات توزیع‌شدهٔ منع خدمت (DDoS)، منع خدمت (DoS)، شناسایی/پویش (Recon)، حملات مبتنی بر وب، حملات جست‌وجوی فراگیر (brute force)، جعل/غلط‌نما کردن (Spoofing)، و بدافزار «میرای» (Mirai). نکتهٔ مهم این است که همهٔ این حملات توسط دستگاه‌های مخربِ اینترنت اشیا علیه سایر دستگاه‌های اینترنت اشیا انجام شده‌اند (یعنی مهاجم هم یک گره IoT است، نه یک کامپیوتر عادی). این مجموعه‌داده در وب‌سایت مجموعه‌داده‌های CIC قابل دسترسی است.

**واژه‌های کلیدی:**  
اینترنت اشیا (IoT)؛ مجموعه‌داده؛ امنیت؛ یادگیری ماشین؛ یادگیری عمیق؛ DoS؛ DDoS؛ پویش/شناسایی (Reconnaissance)؛ حملات وب؛ حملهٔ brute force؛ جعل (Spoofing)؛ میرای (Mirai)

**1. مقدمه**

امروزه اینترنت اشیا (IoT) نقش محوری در جامعه دارد و قابلیت‌های تازه‌ای را به صنایع مختلف وارد کرده است [۱–۳]. پروژه‌های IoT در حوزه‌هایی مثل حمل‌ونقل و سلامت به‌طور فزاینده‌ای محبوب شده‌اند و برنامه‌های کاربردی جدیدی نیز در دست توسعه هستند [۴،۵]. این پارادایم جدید بر یک شبکهٔ بسیار متصل از حسگرها و عملگرها (actuators) تکیه دارد که در آن دستگاه‌های متعدد دائماً ترافیک شبکه تولید می‌کنند [۶–۸]. جامعهٔ پژوهشی و صنعتی سال‌هاست این مفهوم را توسعه می‌دهند و این دسته از دستگاه‌ها بیش‌ازپیش در زندگی روزمره ما حضور پیدا کرده‌اند [۹–۱۱].

این فناوری حوزه‌های متعددی را دگرگون کرده است. برای نمونه، در کاربردهای مراقبت سلامت، می‌توان بیماران را به‌طور منظم و مستمر با استفاده از فناوری اینترنت اشیا پایش کرد [۱۲–۱۴]. در حمل‌ونقل، از دستگاه‌های IoT برای تشخیص و پیشگیری از تصادفات استفاده شده است [۱۵–۱۷]. اینترنت اشیای صنعتی (Industrial IoT یا IIoT) نیز راه‌حل‌هایی مانند پایش خودکارِ با قابلیت اطمینان بالا و تأخیر کم، و کنترل مشارکتی/همکارانه ارائه کرده است [۱۸]. همچنین، کاربردهای IoT در حوزه‌هایی مانند آموزش [۱۹]، هوانوردی [۲۰]، و جنگل‌داری [۲۱] نیز توسعه یافته‌اند.

در دههٔ اخیر، جامعه افزایش چشمگیری در تعداد اتصالات IoT تجربه کرده است [۲۲]. در حقیقت انتظار می‌رود تعداد این اتصالات در چند سال آینده و در حوزه‌های گوناگون باز هم افزایش یابد [۲۳]. این روند، الهام‌بخش خلق و توسعهٔ ایده‌های تجاری و مفاهیم نوینی است که بر یک زیرساخت به‌شدت توزیع‌شده تکیه دارند. علاوه بر این، راهبردهای گوناگونی برای حل چالش‌های بالقوهٔ عملیات IoT پیشنهاد شده است؛ به این معنا که استقرار سرویس‌های جدید اکنون متکی بر یافته‌های علمی به‌دست‌آمده در سال‌های اخیر است.

با وجود این مزایا، هنوز چندین چالش کلیدی برای دستیابی به عملکرد کارآمد و امن باقی مانده است؛ از جمله هم‌کنش‌پذیری (interoperability)، امنیت، استانداردها، و فناوری‌های سمت سرور [۲۴–۲۷]. توسعهٔ برنامه‌های کاربردی جدید همچنین می‌تواند الزامات تازه‌ای به سیستم تحمیل کند [۲۸،۲۹]. برای مثال، اینترنت وسایل نقلیه (Internet of Vehicles یا IoV) ممکن است به زمان پاسخ بسیار محدودتر و سخت‌گیرانه‌تری نسبت به کاربردهای معمول IoT نیاز داشته باشد.

افزون بر آن، شناسایی و کاهش (mitigation) حملاتی که علیه دستگاه‌های اینترنت اشیا انجام می‌شوند کار دشواری است، و این دشواری دلایل مختلفی دارد. برای نمونه، وجود ارتباطات به‌شدت توزیع‌شده و استفاده از دستگاه‌های سبک (کم‌منبع) که معمولاً سازوکارهای امنیتی قدرتمند ندارند، فرآیند تشخیص و خنثی‌سازی حملات را سخت‌تر می‌کند [۳۰–۳۳].

همچنین، گرچه تلاش‌هایی برای ساخت مجموعه‌داده‌هایی شامل حملات علیه دستگاه‌های IoT انجام شده، اما هنوز مجموعهٔ کاملی از سناریوهای حمله پوشش داده نشده است. بیشتر کارهای موجود یک توپولوژی شبکه‌ای وسیع با دستگاه‌های واقعی IoT را در نظر نمی‌گیرند. در نهایت، در بسیاری از این تلاش‌ها، حملات علیه دستگاه‌های اینترنت اشیا توسط سیستم‌های کامپیوتری معمولی (غیر IoT) انجام می‌شود؛ این امر، نیاز به یک مجموعه‌داده که در آن «خودِ دستگاه‌های IoT نقش مهاجم را بازی کنند» برجسته می‌کند.

برای آن‌که توسعهٔ سامانه‌های تحلیل امنیتی (security analytics) برای تشخیص نفوذ در سناریوهای دنیای واقعی ممکن شود، داده‌های تولیدشده باید شرایط زیر را داشته باشند:  
۱. شامل انواع متنوعی از حملات باشند که می‌توانند عملیات IoT را مختل کنند؛  
۲. از یک توپولوژی گسترده با دستگاه‌های واقعی IoT از انواع و برندهای مختلف گردآوری شده باشند؛  
۳. شامل حملاتی باشند که توسط دستگاه‌های IoT مخرب، علیه دیگر دستگاه‌های IoT انجام شده‌اند.

هدف اصلی این پژوهش، ارائهٔ یک مجموعه‌دادهٔ جدید و گسترده از حملات اینترنت اشیا است تا توسعهٔ کاربردهای تحلیل امنیتی در سناریوهای واقعی IoT را تسهیل کند. برای این منظور، ما ۳۳ حمله را در یک توپولوژی اینترنت اشیا شامل ۱۰۵ دستگاه اجرا کردیم. این حملات در هفت رده طبقه‌بندی شدند:

* حملات DDoS،
* حملات DoS،
* حملات شناسایی/پویش (Recon)،
* حملات مبتنی بر وب (Web-based)،
* حملات brute force،
* حملات جعل (Spoofing)،
* و بدافزار Mirai.

همهٔ این حملات توسط دستگاه‌های اینترنت اشیا مخرب علیه دستگاه‌های اینترنت اشیا قربانی انجام شدند. این مجموعه‌داده شامل چندین نوع حمله است که در مجموعه‌داده‌های IoT دیگر موجود نیست. این موضوع به متخصصان IoT اجازه می‌دهد راهکارهای نوین تحلیل امنیتی را توسعه دهند. علاوه بر این، داده‌ها در قالب‌های مختلف در دسترس‌اند؛ بنابراین پژوهشگران می‌توانند هم از ویژگی‌هایی (featureها) که ما استخراج و ارائه کرده‌ایم استفاده کنند و هم در صورت نیاز ویژگی‌های جدید مهندسی کنند.

**مشارکت‌های اصلی این پژوهش عبارت‌اند از:**

• ما یک مجموعه‌دادهٔ جدید و واقع‌گرایانه از حملات IoT با نام CICIoT2023 طراحی می‌کنیم که در آن از یک توپولوژی گسترده شامل تعداد زیادی دستگاه واقعی اینترنت اشیا استفاده می‌شود؛ دستگاه‌ها هم نقش مهاجم را بازی می‌کنند و هم نقش قربانی را.

• ما ۳۳ حمله را در قالب ۷ ردهٔ مختلف علیه دستگاه‌های IoT اجرا، مستندسازی و ضبط کرده‌ایم و نشان داده‌ایم که این حملات چگونه قابل بازتولید هستند.

• ما عملکرد الگوریتم‌های یادگیری ماشین و یادگیری عمیق را با استفاده از مجموعه‌دادهٔ CICIoT2023 ارزیابی می‌کنیم تا ترافیک شبکهٔ IoT را به «مخرب» یا «سالم» طبقه‌بندی و شناسایی کنیم.

**ساختار این مقاله به صورت زیر است:**  
بخش ۲ یک مقایسهٔ گسترده بین دستاورد این پژوهش و کارهای موجود در ادبیات علمی ارائه می‌دهد.  
بخش ۳ مجموعه‌دادهٔ CICIoT2023 را معرفی می‌کند و گام‌های مربوط به فرایند جمع‌آوری داده را توضیح می‌دهد.  
بخش ۴ فرآیند استخراج ویژگی‌ و توصیف داده‌ها را ارائه می‌کند.  
بخش ۵ ارزیابی یادگیری ماشین (ML) برای طبقه‌بندی حملات مختلف با استفاده از CICIoT2023 را گزارش می‌دهد.  
در نهایت، بخش ۶ نتیجه‌گیری را ارائه می‌کند.

**2. کارهای مرتبط**

در چند سال گذشته، مقالات متعددی در زمینهٔ مجموعه‌داده‌های امنیتی برای اینترنت اشیا منتشر شده‌اند. در عمل، این داده‌ها با اهداف متفاوت و با روش‌ها و منابع متفاوت تولید شده‌اند. برای درک بهتر ویژگی‌های مجموعه‌داده‌های موجود، ما چندین ابتکار مطرح در ادبیات را مرور می‌کنیم و آن‌ها را با CICIoT2023 که در این کار پیشنهاد می‌شود مقایسه می‌کنیم.

در [34]، نویسندگان یک مجموعه‌دادهٔ جدید مبتنی بر شبکه برای تشخیص حملات بات‌نت در محیط IoT با نام N-BaIoT (۲۰۱۸) پیشنهاد می‌کنند. در این کار، از بات‌نت‌های Mirai و BASHLITE برای حمله به نه دستگاه تجاری IoT استفاده شده است. ویژگی‌های متعددی از ترافیک شبکه استخراج و سپس برای تشخیص حمله توسط یک خودرمزگذار (autoencoder) یادگیری عمیق به کار گرفته شد.

در [35]، نویسندگان یک مجموعه‌دادهٔ میزبان‌محور (host-based) برای اینترنت اشیا معرفی می‌کنند که از داده‌های واقعی دستگاه‌های IoT تشکیل شده است. این مجموعه‌داده با نام IoTHIDS (۲۰۱۸) براساس آزمایش‌هایی ساخته شده که در آن سه دستگاه، با بدافزارهای بات‌نتی مختلف آلوده شده‌اند؛ از جمله Mirai، Hajime، Adira، BASHLITE، Doflo، Tsunami و Wroba.

IoT-SH (۲۰۱۹) [36] یک مجموعه‌داده است که شامل ضبط‌های مربوط به دوازده نوع حمله (دسته‌بندی‌شده در چهار کلاس) علیه هشت دستگاه «خانهٔ هوشمند» مختلف است. برای طبقه‌بندی این حملات، یک سامانهٔ سه‌لایهٔ تشخیص نفوذ (Intrusion Detection System یا IDS) استفاده شد که در آن ترکیب‌های مختلفی از روش‌های قاعده‌محور (rule-based) و روش‌های یادگیری ماشین به کار گرفته شده‌اند.

BoT-IoT (۲۰۱۹) در [37] به عنوان یک مجموعه‌دادهٔ ترافیکی واقع‌گرایانه معرفی شده است که با در نظر گرفتن پروفایل‌های شبکه‌ای ناهمگن تولید شده. در این کار، چندین نوع حمله (از جمله DDoS، DoS، سرقت داده و اسکن/پویش) علیه پنج دستگاه اجرا شده‌اند. در مرحلهٔ ارزیابی، مجموعه‌ای از ویژگی‌های جدید بر اساس ضریب هم‌بستگی و تکنیک آنتروپی مشترک انتخاب شد و سپس برای آموزش مدل‌های مختلف یادگیری ماشین و یادگیری عمیق استفاده شد تا دقت تشخیص حمله سنجیده شود.

نویسندگان [38] مجموعه‌داده Kitsune (۲۰۱۹) را ارائه می‌دهند؛ این مجموعه‌داده شامل چهار گروه مختلف از حملات است که علیه نه دستگاه IoT اجرا شده‌اند. در آزمایش‌ها، یک دوربین امنیتی به‌طور واقعی با یک نمونهٔ واقعی از بات‌نت Mirai آلوده شد. هدف این مجموعه‌داده پشتیبانی از توسعهٔ سامانه‌های تشخیص نفوذ شبکه‌ای (NIDS) «وصل کن و استفاده کن» (plug-and-play) برای تشخیص ترافیک عادی و مخرب است.

به‌طور مشابه، IoTNIDS (۲۰۱۹) [39] تلاشی است که بر جمع‌آوری داده از یک محیط واقعی شبکهٔ IoT متمرکز است، و این داده‌ها بر مبنای تعامل بین دو دستگاه IoT (یک اسپیکر و یک دوربین) گردآوری شدند. در این تلاش چندین نوع حمله بررسی شده است، از جمله Mirai، حملهٔ مرد میانی (MITM)، DoS و اسکن.

MedBIoT (۲۰۲0) [40] یک مجموعه‌دادهٔ معماریِ شبکهٔ IoT است که بر پایهٔ ترکیبی از دستگاه‌های واقعی و شبیه‌سازی‌شده ساخته شده. در این مطالعه، نویسندگان چندین تکنیک یادگیری ماشین را با استفاده از ۱۰۰ ویژگی آماری استخراج‌شده از ترافیک شبکهٔ IoT ارزیابی کردند.

در [41]، نویسندگان مجموعه‌داده IoT-23 (۲۰۲۰) را پیشنهاد می‌کنند. این کار یک مجموعه‌دادهٔ بات‌نت است که از محیط شبکهٔ واقعی ضبط شده و شامل ترافیک سالم و مخرب است.

IoTIDs (۲۰۲۰) [42] به‌عنوان یک مجموعه‌دادهٔ متشکل از ویژگی‌های مبتنی بر جریان (flow-based) مرتبط با IoT پیشنهاد شده است. این ویژگی‌ها با استفاده از تکنیک ضریب هم‌بستگی رتبه‌بندی و با آزمون Shapiro–Wilk مرتب‌سازی شدند. در آزمایش‌ها، نویسندگان چهار نوع حملهٔ مختلف را علیه دو دستگاه IoT (یک اسپیکر و یک دوربین) اجرا و داده‌ها را ثبت کردند. سپس چندین روش یادگیری ماشین (برای مثال SVM، Gaussian Naive Bayes (G-NB)، تحلیل تفکیکی خطی (LDA)، و رگرسیون لجستیک (LR)) برای ارزیابی بر تشخیص و طبقه‌بندی حملات استفاده شد.

نویسندگان [43] مجموعه‌داده MQTT (۲۰۲۰) را ارائه می‌دهند، با هدف اصلی فراهم کردن داده‌های واقع‌گرایانه که شامل یک پروتکل سبک‌وزن اختصاصیِ سناریوهای IoT است (یعنی MQTT). در این کار، هشت دستگاه اینترنت اشیا به یک کارگزار (broker) MQTT متصل شدند و ۳۳ ویژگی متفاوت استخراج و به الگوریتم‌های مختلف یادگیری ماشین داده شد.

به‌طور مشابه، MQTT-IoT-IDS (۲۰۲۰) [44] نیز یک تلاش دیگر است که بر تولید یک مجموعه‌داده با استفاده از پروتکل سبک MQTT ــ که به‌طور گسترده در شبکه‌های IoT استفاده می‌شود ــ تمرکز دارد. نویسندگان تلاش کرده‌اند یک شبکهٔ IoT واقع‌گرایانه را بازآفرینی کنند: یک فید دوربین، دوازده حسگر MQTT، و یک کارگزار MQTT. پنج سناریو مختلف در نظر گرفته شد که تفاوت آن‌ها بر اساس نوع حمله‌ها بود. در مرحلهٔ ارزیابی، چندین نوع ویژگی مبتنی بر بسته، جریان یک‌طرفه (uni-flow) و جریان دوطرفه (bi-flow) همراه با شش الگوریتم مختلف یادگیری ماشین استفاده شد.

در [45]، نویسندگان یک مجموعه‌دادهٔ جدید تله‌متری‌محور و داده‌محور برای IoT/IIoT با نام TON-IoT (۲۰۲۰) پیشنهاد می‌کنند. این مجموعه‌دادهٔ ناهمگن شامل نمونه‌های عادی و نمونه‌های تحت حمله است که در سناریوهای گوناگون جمع‌آوری شده‌اند. در راستای ساخت یک مجموعه‌داده واقع‌گرایانه، نویسندگان زیر-دسته‌های حمله، داده‌های ثبت‌شده از لاگ‌های سیستم‌عامل، و ترافیک شبکه را لحاظ کرده‌اند. در مرحلهٔ ارزیابی، چندین الگوریتم یادگیری ماشین و یادگیری عمیق به کار گرفته شد و نتایج به‌دقت گزارش شدند.

در نهایت، مجموعه‌داده Edge-IIoTSet (۲۰۲۲) به‌عنوان یک منبع امنیت سایبری واقع‌گرایانه برای کاربردهای IoT و IIoT معرفی شده است تا توسعهٔ سامانه‌های تشخیص نفوذ (IDS) را در هر دو سناریوی متمرکز و توزیع‌شده ممکن کند [46]. در این مقاله، یک توصیف عمیق از بستری (testbed) که برای تولید داده استفاده شده ارائه می‌شود. همچنین چارچوب تولید مجموعه‌داده تشریح می‌شود. در بخش ارزیابی یادگیری ماشین، ملاحظات یادگیری متمرکز و یادگیری فدره (federated learning) نیز مطرح می‌شود.

### 3. CICIoT2023 پیشنهادی

در این بخش ابتدا زیرساخت آزمایشگاهی IoT و نحوهٔ اتصال اجزاء آن را معرفی می‌کنیم. سپس همهٔ حملاتی را که اجرا شده‌اند مرور می‌کنیم. در پایان، بینش‌هایی دربارهٔ نحوهٔ گردآوری داده برای سناریوهای سالم و مخرب ارائه می‌دهیم.

#### 3.1. آزمایشگاه IoT

تولید دادهٔ امنیتیِ قابل‌اتکا برای اینترنت اشیا که بتواند از کاربردهای واقعی پشتیبانی کند، به دلایل گوناگون چالش‌برانگیز است. یکی از مسائل اصلی، دسترسی به یک شبکهٔ وسیع متشکل از چندین دستگاه واقعی IoT است که شبیه توپولوژی‌های استقرار واقعیِ IoT باشد. بسیاری از کارهای پیشین به‌دلیل هزینه‌ها، تجهیزات موردنیاز شبکه (مانند سوئیچ‌ها، روترها و «تپِ شبکه»)، و نیروی انسانی لازم برای نگه‌داری چنین زیرساختی، یا از شبیه‌سازی استفاده کرده‌اند یا تنها تعداد اندکی دستگاه IoT را به‌کار گرفته‌اند.

در این راستا، مؤسسهٔ کانادایی امنیت سایبری (CIC) جایگاهی ممتاز در زیست‌بوم امنیت سایبری دارد و سابقه‌ای از دستاوردهای اثرگذار برای صنعت و دانشگاه. نمونه‌هایی از این دست، مجموعه‌داده‌هایی است که برای توسعهٔ کاربردهای نوین امنیت سایبری به‌کار رفته‌اند و نیز همکاری‌های متعدد با صنعت برای بهبود عمل‌ورزی امنیت سایبری و توسعهٔ راه‌حل‌های جدید. این موفقیت‌ها به CIC امکان داد یک آزمایشگاه اختصاصیِ IoT با شبکه‌ای ویژه ایجاد کند تا توسعهٔ راهکارهای امنیتی IoT را تسهیل کند. در واقع، با به‌اشتراک‌گذاری داده‌های گردآوری‌شده از این توپولوژی گسترده، قصد داریم پیشرفت پژوهش در امنیت IoT را تسریع کنیم و از ابتکارهای متعدد در ابعاد مختلف امنیت IoT پشتیبانی کنیم.

(در «شکل ۱»، نمایی از آزمایشگاه IoT در CIC و دستگاه‌های آن نشان داده شده است؛ دستگاه‌های IoT در سرتاسر آزمایشگاه توزیع شده‌اند.)

#### 3.2. توپولوژی شبکهٔ IoT

توپولوژی شبکهٔ مورد استفادهٔ ما از دو بخش اصلی تشکیل شده است. در این میان، یک «تپِ شبکهٔ Gigamon» بین دو بخش قرار گرفته که ویژگی متمایز CICIoT2023 در قیاس با تلاش‌های پیشین محسوب می‌شود. سوئیچ Cisco به‌واسطهٔ همین تپ به بخش دوم متصل است. این تجهیزِ شبکه همهٔ ترافیک IoT را جمع‌آوری می‌کند و آن را به دو «مانیتورِ شبکه» می‌فرستد که مسئول ذخیره‌سازی ترافیک با استفاده از Wireshark [47] هستند.

تپِ شبکه در اصل یک سخت‌افزار است که با اتصال به کابل شبکه امکان نظارت و تحلیل ترافیک را فراهم می‌کند و یک نسخهٔ کپی از ترافیک را در اختیار ابزارهای پایش و امنیتی دیگر می‌گذارد. این تپ‌ها به گونه‌ای متصل می‌شوند که عملکرد عادی شبکه را مختل نکنند و دسترسی «تمام‌دوطرفه»، «غیرتهاجمی» و «منفعل» به ترافیک فراهم کنند، بدون آن‌که تأخیری ایجاد شود یا کارایی شبکه تحت‌تأثیر قرار گیرد. این دستگاه دو «پورت شبکه» و دو «پورت پایش» دارد و بین دستگاه‌های مهاجم و دستگاه‌های سالم قرار می‌گیرد: یک پورت به شبکهٔ مهاجمان و پورت دیگر به شبکهٔ قربانیان متصل است. از طریق پورت‌های پایش، ما قادر به ضبط ترافیکِ ورودی و خروجی شبکهٔ IoT هستیم.  
(«شکل ۲» توپولوژی شبکهٔ IoT مورد استفاده در آزمایش‌ها را نشان می‌دهد.)

در بخش دوم، یک سوئیچِ Netgear (نوع Unmanaged) به پنج «دروازه/گیت‌وی» و «ایستگاه پایه» متصل است تا ارتباط با دستگاه‌های IoT را از طریق پروتکل‌هایی مانند Zigbee و Z-Wave ممکن سازد. افزون بر این، یک کنترلر VeraPlus دیگر نیز به سوئیچ متصل است. این کنترلر به دو هاب Zigbee/Z-Wave دیگر و نیز به چندین دستگاهی که در حملات نقش «قربانی» را داشته‌اند متصل است. فهرست همهٔ دستگاه‌های IoT به‌کاررفته در این مجموعه‌داده در «جدول ۱» آمده است. توجه کنید که دستگاه‌های Zigbee و Z-Wave دارای «نشانی MAC» نیستند و برای ستون مربوطه با برچسب «N/A (ناموجود/نامرتبط)» مشخص شده‌اند.

### 3.3. جمع‌آوری داده برای سناریوهای سالم و مخرب

همان‌طور که در بخش ۳٫۲ توضیح داده شد، یک تپ شبکه و دو مانیتور ترافیک برای پایش ترافیک شبکه اختصاص داده شده‌اند. هر بسته‌ای که در شبکه ارسال می‌شود روی کامپیوترهای جداگانه ذخیره می‌گردد. در واقع، شبکه دو رابط (interface) متفاوت دارد که هر کدام به یک پورت پایش (monitoring port) متصل هستند و بسته‌های ورودی را به این کامپیوترها می‌فرستند. بنابراین، ترافیک شبکه با استفاده از Wireshark [47] مانیتور و در قالب pcap ذخیره می‌شود. از آن‌جا که دو جریان داده به‌طور هم‌زمان ذخیره می‌شوند، برای هر آزمایش از ابزار mergecap [48] استفاده می‌کنیم تا فایل‌های pcap را در هم ادغام و یکپارچه کنیم.

برای هر حمله، یک آزمایش مستقل انجام می‌شود که در آن همهٔ دستگاه‌های قابل هدف‌گیری مورد حمله قرار می‌گیرند. در تمام سناریوها، حملات توسط دستگاه‌های اینترنت اشیای مخرب علیه دستگاه‌های اینترنت اشیای آسیب‌پذیر انجام می‌شوند. برای مثال، حملات DDoS علیه همهٔ دستگاه‌ها اجرا شدند، در حالی که حملات مبتنی بر وب فقط دستگاه‌هایی را هدف گرفتند که سرویس وب ارائه می‌دادند.

**جدول ۲** ابزارهای مورد استفاده برای اجرای هر حمله و همچنین تعداد ردیف‌های دادهٔ تولید شده را نشان می‌دهد. علاوه بر آن، **شکل‌های ۳ و ۴** تعداد نمونه‌ها (instance count) را برای هر حمله و برای هر دسته (Category) تصویر می‌کنند. این مقادیر در **جدول ۳** نیز آمده‌اند.

**جدول ۲. حملات اجراشده، تعداد ردیف‌های دادهٔ ثبت‌شده، و ابزارهای مورد استفاده**

(ستون‌ها: نوع حمله / تعداد ردیف‌ها (Rows) / ابزار)

* ACK Fragmentation — تعداد ردیف: 285,104 — ابزار: hping3 [49]
* UDP Flood — 5,412,287 — ابزار: udp-flood [50]
* Slowloris — 23,426 — ابزار: slowloris [51]
* ICMP Flood — 7,200,504 — ابزار: hping3 [49]
* RSTFIN Flood — 4,045,285 — ابزار: hping3 [49]
* PSHACK Flood — 4,094,755 — ابزار: hping3 [49]
* HTTP Flood — 28,790 — ابزار: golang-httpflood [52]
* UDP Fragmentation — 286,925 — ابزار: udp-flood [50]
* ICMP Fragmentation — 452,489 — ابزار: hping3 [49]
* TCP Flood — 4,497,667 — ابزار: hping3 [49]
* SYN Flood — 4,059,190 — ابزار: hping3 [49]
* SynonymousIP Flood — 3,598,138 — ابزار: hping3 [49]

(این مجموعه، در دستهٔ DDoS قرار می‌گیرد)

* TCP Flood — 2,671,445 — ابزار: hping3 [49]
* HTTP Flood — 71,864 — ابزار: golang-httpflood [52]
* SYN Flood — 2,028,834 — ابزار: hping3 [49]
* UDP Flood — 3,318,595 — ابزارهای hping3 [49] و udp-flood [50]

(این مجموعه، در دستهٔ DoS قرار می‌گیرد)

* Ping Sweep — 2,262 — ابزارهای nmap [53] و fping [54]
* OS Scan — 98,259 — ابزار: nmap [53]
* Vulnerability Scan — 37,382 — ابزارهای nmap [53] و vulscan [55]
* Port Scan — 82,284 — ابزار: nmap [53]
* Host Discovery — 134,378 — ابزار: nmap [53]

(این مجموعه، در دستهٔ Recon (شناسایی/پویش) قرار می‌گیرد)

* SQL Injection — 5,245 — ابزار: DVWA [56]
* Command Injection — 5,409 — ابزار: DVWA [56]
* Backdoor Malware — 3,218 — ابزارهای DVWA [56] و Remot3d [57]
* Uploading Attack — 1,252 — ابزار: DVWA [56]
* XSS — 3,846 — ابزار: DVWA [56]
* Browser Hijacking — 5,859 — ابزار: Beef [58]

(این مجموعه، در دستهٔ Web-Based (مبتنی بر وب) قرار می‌گیرد)

* Dictionary Brute Force — 13,064 — ابزارهای nmap [53] و hydra [59]

(این مجموعه، در دستهٔ Brute Force قرار می‌گیرد)

* ARP Spoofing — 307,593 — ابزار: ettercap [60]
* DNS Spoofing — 178,911 — ابزار: ettercap [60]

(این مجموعه، در دستهٔ Spoofing قرار می‌گیرد)

* GREIP Flood — 751,682 — «سورس‌کد میرای» سازگار/تطبیق‌داده‌شده [61]
* Greeth Flood — 991,866 — «سورس‌کد میرای» سازگار [61]
* UDPPlain — 890,576 — «سورس‌کد میرای» سازگار [61]

(این مجموعه، در دستهٔ Mirai قرار می‌گیرد)

**جدول ۳. تعداد ردیف‌ها برای هر حمله و هر دسته**

(بخش اول جدول: هر حمله و تعداد ردیف‌های مرتبط با آن)

* DDoS-ICMP\_Flood — 7,200,504
* DDoS-UDP\_Flood — 5,412,287
* DDoS-TCP\_Flood — 4,497,667
* DDoS-PSHACK\_Flood — 4,094,755
* DDoS-SYN\_Flood — 4,059,190
* DDoS-RSTFIN\_Flood — 4,045,285
* DDoS-SynonymousIP\_Flood — 3,598,138
* DDoS-UDP\_Fragmentation — 286,925
* DDoS-ACK\_Fragmentation — 285,104
* DDoS-HTTP\_Flood — 28,790
* DDoS-SlowLoris — 23,426
* DDoS-ICMP\_Fragmentation — 452,489

(جدا از DDoS)

* DoS-UDP\_Flood — 3,318,595
* DoS-TCP\_Flood — 2,671,445
* DoS-SYN\_Flood — 2,028,834
* DoS-HTTP\_Flood — 71,864

(جدا از DoS)

* Recon-PingSweep — 2,262
* Recon-OSScan — 98,259
* Recon-VulnerabilityScan — 37,382
* Recon-PortScan — 82,284
* Recon-HostDiscovery — 134,378

(جدا از Recon)

* SqlInjection — 5,245
* CommandInjection — 5,409
* Backdoor\_Malware — 3,218
* Uploading\_Attack — 1,252
* XSS — 3,846
* Browser\_Hijacking — 5,859

(جدا از Web)

* DictionaryBruteForce — 13,064

(جدا از Brute Force)

* MITM-ArpSpoofing — 307,593
* DNS\_Spoofing — 178,911

(جدا از Spoofing)

* Mirai-greeth\_flood — 991,866
* Mirai-udpplain — 890,576
* Mirai-greip\_flood — 751,682

(دستهٔ Mirai)

* BenignTraffic — 1,098,195

(دادهٔ سالم)

(بخش دوم جدول: خلاصه‌شده بر اساس دسته‌ها / Category)

* DDoS — 33,984,560 ردیف
* DoS — 8,090,738 ردیف
* Mirai — 2,634,124 ردیف
* Benign — 1,098,195 ردیف
* Spoofing — 486,504 ردیف
* Recon — 354,565 ردیف
* Web — 24,829 ردیف
* BruteForce — 13,064 ردیف

**شکل ۳.** تعداد ردیف‌ها برای هر سناریو حمله.  
**شکل ۴.** تعداد ردیف‌ها برای هر دستهٔ حمله.

#### 3.3.1. تولید دادهٔ سالم (Benign)

دادهٔ سالم (benign) نشان‌دهندهٔ استفادهٔ عادی و مشروع از شبکهٔ اینترنت اشیاست. در این معنا، هدف اصلی فرایند گردآوری داده این است که ترافیک IoT را هم در حالت بیکار (idle) و هم در حالت تعامل انسانی جمع‌آوری کنیم (برای نمونه: دادهٔ حسگرها، درخواست‌های ارسال‌شده به Amazon Echo Dot، و دسترسی به فید ویدئویی دوربین‌های هوشمند).

از نظر سخت‌افزار، ما از یک تپ شبکه به‌همراه دو مانیتور شبکه استفاده کردیم. از نظر نرم‌افزار، برای گرفتن کل ترافیک از Wireshark استفاده شد. افزون بر این، تمام دستگاه‌های IoT با پارامترهای پیش‌فرض پیکربندی شده‌اند و هیچ اسکریپت مخرب یا کد حمله روی آن‌ها فعال نبوده است. به این ترتیب، گردآوری ترافیک سالم در زمانی انجام شده که هیچ حمله‌ای در حال اجرا نبوده است.

این فرایند طی یک دورهٔ ۱۶ ساعته انجام شد.

#### 3.3.2. اجرای حملات DoS و DDoS

این حملات به تهدیدهای «سیل‌آسا» (flooding) اشاره دارند که هدفشان مختل کردن دسترس‌پذیری عملیات IoT است.

در حملهٔ منع خدمت (DoS)، یک Raspberry Pi منفرد وظیفهٔ سرازیر کردن (فlood کردن) دستگاه‌های IoT را بر عهده دارد. در حملهٔ منع خدمت توزیع‌شده (DDoS)، چندین Raspberry Pi برای اجرای حمله به‌صورت هماهنگ به کار گرفته می‌شوند؛ این هماهنگی از طریق پیکربندی master–client مبتنی بر SSH انجام می‌شود.

حملاتی که در این بخش اجرا شدند عبارت‌اند از:

* **ACK Fragmentation:** در این حمله از تعداد نسبتاً کمی بستهٔ با اندازهٔ حداکثری استفاده می‌شود تا عملکرد شبکه را مختل کند. در بسیاری از موارد، این بسته‌های قطعه‌قطعه‌شده (fragmented) با موفقیت ارسال می‌شوند و روترها، فایروال‌ها و سامانه‌های پیشگیری از نفوذ آن‌ها را قبول می‌کنند، زیرا بازسازی (reassembly) بسته‌های تکه‌تکه‌شده انجام نمی‌شود [62].
* **Slowloris:** این حمله مبتنی بر ارسال درخواست‌های ناقص HTTP از طریق اتصالات باز به سمت یک وب‌سرور هدف است و روی لایهٔ کاربرد (application layer) متمرکز است [63].
* **ICMP / HTTP / UDP / TCP Flood:** در این نوع حملات، دستگاه هدف با هجوم انواع مختلف بسته‌ها (ICMP، HTTP، UDP، TCP) تحت‌فشار قرار می‌گیرد تا از کار بیفتد [64–66].
* **RSTFIN Flood:** این حمله مبتنی بر ارسال حجم زیادی از بسته‌های TCP با فلگ‌های RST و FIN به‌سمت یک هدف مشخص است [67].
* **PSH-ACK Flood:** در این حمله، سرور هدف با حجم زیادی از درخواست‌های PUSH و ACK تحت بار قرار می‌گیرد و کارایی آن کاهش می‌یابد [68].
* **UDP Fragmentation:** گونه‌ای خاص از UDP Flood است که پهنای‌باند بیشتری مصرف می‌کند، در حالی که تعداد بسته‌های ارسالی را کاهش می‌دهد [69].
* **ICMP Fragmentation:** در این حمله مجموعه‌ای از بسته‌های IP تکه‌تکه‌شده که حاوی بخش‌هایی از پیام‌های ICMP هستند ارسال می‌شود [70].
* **SYN Flood:** زیرنوعی از سیل TCP است که مرحلهٔ دست‌دهی اولیهٔ TCP را هدف قرار می‌دهد. در SYN Flood تعداد زیادی بستهٔ SYN (synchronize) به سرور هدف فرستاده می‌شود، اما مرحلهٔ دست‌دهی هرگز با ارسال بستهٔ ACK نهایی تکمیل نمی‌شود [71].
* **Synonymous IP Flood:** در این حمله تعداد بسیار زیادی بستهٔ دست‌کاری‌شدهٔ TCP-SYN ارسال می‌شود که آدرس مبدأ و مقصد هر دو روی آدرس هدف تنظیم شده‌اند؛ این باعث می‌شود سرور منابع خود را برای پردازش این ترافیک تقلبی مصرف کند [72].

#### 3.3.3. گردآوری اطلاعات از توپولوژی IoT (Reconnaissance)

این دسته از حملات با هدف جمع‌آوری حداکثر اطلاعات ممکن دربارهٔ هدف انجام می‌شوند. یک مهاجم می‌تواند از یک حملهٔ شناسایی (Recon یا Scan) به‌عنوان مرحلهٔ آماده‌سازی برای حملات بعدی استفاده کند.

روش‌های متنوعی برای انجام این نوع حملات وجود دارد. برخی از محبوب‌ترین و تهدیدکننده‌ترین انواع آن عبارت‌اند از:

* **Ping Sweep (یا Ping Scan):** این نوع حملهٔ شناسایی برای تشخیص میزبان‌های فعال در یک شبکه استفاده می‌شود. مهاجم مجموعه‌ای از بسته‌های ICMP Echo Request (ping) را به یک محدوده از آدرس‌های IP روی یک شبکه ارسال می‌کند و سپس ICMP Echo Reply (pong) برگشتی را تحلیل می‌کند تا تشخیص دهد کدام میزبان‌ها فعال و پاسخ‌گو هستند [73].
* **OS Scan (اسکن سیستم‌عامل):** این حمله که با نام «تشخیص اثرانگشت سیستم‌عامل» (OS fingerprinting) نیز شناخته می‌شود، برای شناسایی نوع و نسخهٔ سیستم‌عامل در حال اجرای روی میزبان هدف به‌کار می‌رود. مهاجم پاسخ دستگاه هدف به بسته‌های مختلف شبکه، یا رفتار پورت‌ها و سرویس‌های باز را تحلیل می‌کند تا نوع و نسخهٔ سیستم‌عامل را حدس بزند [74].
* **Vulnerability Scan (اسکن آسیب‌پذیری):** این نوع ارزیابی امنیت شبکه مبتنی بر ابزارهای خودکار است که تلاش می‌کنند آسیب‌پذیری‌های بالقوه را در یک سامانه یا شبکهٔ کامپیوتری شناسایی کنند. هدف اسکن آسیب‌پذیری، پیدا کردن ضعف‌هایی است که می‌تواند به مهاجم اجازه دهد دسترسی غیرمجاز بگیرد یا اطلاعات حساس را سرقت کند [75].
* **Port Scan (اسکن پورت):** این حمله با هدف شناسایی پورت‌های باز و فعال روی میزبان هدف انجام می‌شود. مهاجم بسته‌هایی را به پورت‌های مختلف میزبان هدف می‌فرستد و تلاش می‌کند اتصال برقرار کند. سپس پاسخ‌ها تحلیل می‌شوند تا مشخص شود کدام پورت‌ها باز، بسته، یا فیلتر شده‌اند [76].
* **Host Discovery (کشف میزبان):** که با نام Host Identification یا Host Enumeration هم شناخته می‌شود، برای شناسایی میزبان‌های فعال در یک شبکه به‌کار می‌رود. در این روش از تکنیک‌های مختلفی برای تشخیص آدرس‌های IP دستگاه‌های متصل به شبکه استفاده می‌شود. این مرحله در بسیاری از حملات سایبری قدم اول است [77].

#### 3.3.4. بهره‌برداری از آسیب‌پذیری‌های وب (Web-Based Exploits)

در این سناریو، سرویس‌های وبی که روی دستگاه‌های IoT اجرا می‌شدند هدف قرار گرفتند. حملات مبتنی بر وب (Web-based attacks) بر سوءاستفاده از سرویس‌های وب تمرکز دارند و می‌توانند شامل تزریق (injection)، ربایش (hijacking)، مسموم‌سازی (poisoning)، جعل (spoofing)، و DoS باشند [78].

حملات وبی اجراشده در این پژوهش عبارت‌اند از:

* **SQL Injection:** حمله‌ای علیه برنامه‌های وب که با تزریق کد SQL مخرب در فیلدهای ورودی برنامه انجام می‌شود. هدف این حمله، دسترسی غیرمجاز به پایگاه‌داده، سرقت اطلاعات حساس، یا اجرای دستورات دلخواه روی سرور پایگاه‌داده است [79].
* **Command Injection:** حمله‌ای که در آن مهاجم دستورات مخرب را در یک فیلد ورودی تزریق می‌کند تا نهایتاً به سیستم هدف دسترسی غیرمجاز بگیرد، اطلاعات حساس را بدزدد، یا دستورات دلخواه را روی سامانهٔ هدف اجرا کند [80].
* **Backdoor Malware:** در این حالت، بدافزاری روی سیستم هدف نصب می‌شود که به مهاجم اجازه می‌دهد در آینده دسترسی غیرمجاز بگیرد. این بدافزار (Backdoor) یک درب پنهانی روی سیستم ایجاد می‌کند که می‌تواند برای دور زدن سازوکارهای امنیتی و دسترسی به اطلاعات حساس یا انجام اعمال مخرب استفاده شود [81].
* **Uploading Attack:** در این حمله، مهاجم از آسیب‌پذیری‌های مربوط به قابلیت «آپلود فایل» در یک برنامهٔ وب سوءاستفاده می‌کند. هدف این است که فایل‌های مخرب (مانند بدافزار) روی سیستم قربانی آپلود شود و سپس از آن فایل‌ها برای دسترسی غیرمجاز یا اجرای کد دلخواه روی سیستم هدف استفاده شود.
* **Cross-Site Scripting (XSS):** حمله‌ای که در آن مهاجم کد مخرب (مثلاً جاوااسکریپت) را در یک صفحهٔ وب تزریق می‌کند. این کد سپس در مرورگر هر کاربری که به آن صفحه دسترسی دارد اجرا می‌شود و می‌تواند اطلاعات حساس (نظیر کوکی‌ها، توکن‌های نشست، و داده‌های شخصی) را سرقت کند یا فعالیت‌های مخرب دیگری مثل هدایت ترافیک انجام دهد [82].
* **Browser Hijacking:** در این نوع حمله، مهاجم تنظیمات مرورگر قربانی را تغییر می‌دهد (مثلاً صفحهٔ خانه، موتور جستجوی پیش‌فرض، یا بوکمارک‌ها) تا کاربر را به وب‌سایت‌های دیگر هدایت کند یا تبلیغات ناخواسته نشان بدهد. هدف این حمله معمولاً ایجاد درآمد از طریق تبلیغات یا سرقت اطلاعات شخصی است [83].

#### 3.3.5. جعل در ارتباطات (Spoofing Communication)

حملات جعل (Spoofing) به مهاجم اجازه می‌دهد با هویت یک سیستم قربانی ظاهر شود و به‌طور غیرقانونی به ترافیک شبکه دسترسی پیدا کند. هدف اصلی این روش‌ها معمولاً شامل گرفتن دسترسی به سامانه‌ها، سرقت داده و انتشار بدافزار است [84].

دو نمونهٔ رایج و مهم از حملات جعل:

* **ARP Spoofing:** در این حمله، مهاجم پیام‌های دست‌کاری‌شدهٔ ARP (Address Resolution Protocol) را در شبکه ارسال می‌کند تا آدرس MAC دستگاه مخرب را با آدرس IP یک دستگاه مشروع در شبکه مرتبط نشان بدهد. این کار به مهاجم اجازه می‌دهد ترافیک شبکه را شنود کند، تغییر بدهد یا مسدود کند [85].
* **DNS Spoofing:** در این حمله، مهاجم ورودی‌های DNS را (مثلاً در کش DNS) تغییر می‌دهد تا کاربران به وب‌سایت‌های جعلی یا مخرب هدایت شوند. این امر می‌تواند به سرقت اطلاعات حساس، پخش بدافزار و دیگر فعالیت‌های مخرب منجر شود [86].

#### 3.3.6. تهدیدهای brute-force

حملات brute-force شامل ارسال مکرر داده (مثلاً گذرواژه‌ها یا عبارت‌های عبور) است تا در نهایت دسترسی به سیستم به‌دست آید [87].

یکی از روش‌های رایج در این دسته، «حملهٔ brute-force واژه‌نامه‌ای» (dictionary brute-force attack) است. در این روش مهاجم تلاش می‌کند گذرواژه یا عبارت عبور درست را حدس بزند، با این کار که بارها و بارها کلمات موجود در یک فهرست از پیش تعریف‌شدهٔ کلمات (که از منابع مختلف جمع‌آوری شده) را امتحان می‌کند. هدف این حمله یافتن رمز درست از طریق امتحان کردن همهٔ کلمات موجود در واژه‌نامه است [88].

#### 3.3.7. میرای (Mirai) به‌عنوان یک تهدید برای IoT

میرای (Mirai) یک حملهٔ DDoS در مقیاس بزرگ است که می‌تواند دستگاه‌های IoT را هدف بگیرد. در این پژوهش، ما گونه‌های مختلفی از حملات میرای را با استفاده از پنج Raspberry Pi اجرا کرده‌ایم (همان‌طور که در **شکل ۵** نشان داده شده است)، همراه با اتصال‌هایی که در لایه‌های مختلف شبکهٔ IoT در نظر گرفته شده‌اند.

برای اتصال به اینترنت، یک گیت‌وی (gateway) از یک نمونهٔ ویندوز ۱۰ استفاده می‌کند تا دسترسی به اینترنت را فراهم و پایش کند. این دسترسی از طریق یک سوئیچ unmanaged از نوع Netgear ممکن می‌شود که هم دستگاه‌های مهاجم و هم دستگاه‌های IoT عادی را به هم متصل می‌کند. چندین ابزار مختلف برای انجام این حملات استفاده شد و یک پیکربندی ویژهٔ میرای نیز به‌کار رفت. یک «ناظر اینترنت اشیا» (online IoT supervisor) عملیات چندین دستگاه IoT در توپولوژی را هماهنگ می‌کند (برای نمونه حسگرها، دوربین‌ها و اسپیکرهای هوشمند).

در نهایت، برخی از کارهای موجود در ادبیات، میرای را در مجموعهٔ حملات خود لحاظ نکرده‌اند. در مقابل، ما بر چندین حمله تمرکز کرده‌ایم که می‌توانند علیه دستگاه‌های IoT اجرا شوند و تحلیل و اجرای حملات جدید IoT (برای نمونه، حملاتی مبتنی بر پروتکل‌های آینده) را به‌عنوان مسیر آیندهٔ این پژوهش در نظر می‌گیریم.

**شکل ۵.** چارچوب پایهٔ حمله برای این مجموعه‌داده.

حملهٔ Mirai دستگاه‌ها را آلوده می‌کند تا یک بات‌نت تشکیل شود که می‌تواند قربانیان مشخص را با سیل ترافیک بمباران کند. این تهدید می‌تواند در زمینه‌های مختلف اختلال ایجاد کند. برخی از گونه‌های رایج آن:

* **GREIP Flood:** در این نوع، مهاجم داخل بسته‌های GRE یک لایهٔ درهم‌کپسوله‌شده از بسته‌ها قرار می‌دهد و سیستم قربانی با حجم زیادی از بسته‌های تونل‌شدهٔ GRE بمباران می‌شود. در لایهٔ داخلی، IP و پورت‌ها تصادفی هستند، اما لایهٔ بیرونی از IPهای واقعی استفاده می‌کند [89].
* **GREETH Flood:** این حمله از نظر منطق شبیه GREIP است، اما تمرکز اصلی آن بر نوع کپسوله‌سازی است که در آن سربرگ اترنت (ethernet header) برای تونل‌سازی استفاده می‌شود [89].
* **UDP Plain:** در این تهدید، قربانی با بسته‌های UDP بمباران می‌شود که بخش داده (payload) تکرارشونده دارد، ولی محتوای بار هر بسته با بستهٔ قبلی تفاوت دارد. این کار بار شدیدی روی پهنای‌باند قربانی وارد می‌کند [89].

### 4. استخراج ویژگی و توصیف داده

مجموعه‌دادهٔ CICIoT2023 در دو قالب در دسترس است: **pcap** و **csv**.

* فایل‌های pcap شامل دادهٔ اصلی‌ای هستند که در شبکهٔ IoT مرکز CIC و در سناریوهای مختلف جمع‌آوری شده‌اند. این فایل‌ها همهٔ بسته‌های ارسالی را شامل می‌شوند و می‌توان از آن‌ها برای استخراج و مهندسی ویژگی‌های جدید استفاده کرد.
* فایل‌های csv روشی ساده‌تر برای بارگذاری و استفاده از داده ارائه می‌دهند. این فایل‌ها شامل مجموعه‌ای از ویژگی‌هایی هستند که از فایل‌های pcap اصلی استخراج شده‌اند و بر اساس یک «پنجرهٔ با اندازهٔ ثابت از بسته‌ها» (window of packets) خلاصه شده‌اند. یعنی ویژگی‌ها از یک دنبالهٔ بسته‌ها که بین دو میزبان تبادل شده‌اند استخراج می‌شوند.

روشی که برای تولید این مجموعه‌داده استفاده شده در **شکل ۶** نشان داده شده است. ابتدا داده تولید (و ضبط) و سپس برچسب‌گذاری می‌شود. این مرحلهٔ اولیه شامل اجرای واقعی حملات علیه دستگاه‌های IoT است. سپس داده‌ها به‌گونه‌ای پردازش می‌شوند که پژوهشگران بتوانند به‌سادگی به آن‌ها دسترسی یابند. در نهایت، یک ارزیابی یادگیری ماشین (ML) انجام می‌دهیم تا نشان دهیم این مجموعه‌داده چگونه می‌تواند برای طبقه‌بندی حملات استفاده شود.

**شکل ۶.** روش به‌کاررفته برای تولید مجموعه‌داده.

**شکل ۷** نشان می‌دهد که تولید داده، استخراج و برچسب‌گذاری برای هر سناریوی حمله (و همچنین سناریوی سالم) چگونه انجام شده است. فاز اول بر استفاده از ابزارهای مختلف (فهرست‌شده در جدول ۲) برای اجرای حملات علیه دستگاه‌های IoT در شبکه متکی است. پس از آن، ترافیک شبکه با استفاده از Wireshark در قالب pcap ضبط می‌شود. در نهایت، برای هر حمله‌ای که اجرا شده، کل ترافیک ضبط‌شده با همان برچسب آن حمله علامت‌گذاری می‌شود.

**شکل ۷.** روش به‌کاررفته برای تولید مجموعه‌داده برای هر سناریو.

در مرحلهٔ **پردازش داده** (که در **شکل ۸** نشان داده شده)، ترافیک شبکه شامل همهٔ حملات و همچنین ترافیک سالم جمع‌آوری می‌شود. از آن‌جا که این داده‌ها در مجموع حدود 548 گیگابایت حجم دارند، ابتدا آن‌ها را به قطعات کوچک‌تر 10 مگابایتی تقسیم می‌کنیم تا بتوانیم تبدیل‌ها را به‌شکل موازی انجام دهیم. این کار با استفاده از TCPDUMP [90] انجام می‌شود.

پس از آن، یک روند موازی برای استخراج مجموعه‌ای از ویژگی‌ها با استفاده از بستهٔ DPKT [91] اجرا می‌شود و این ویژگی‌ها در فایل‌های csv جداگانه ذخیره می‌شوند. این ویژگی‌ها در **جدول ۴** توضیح داده شده‌اند.

در این فرایند، از DPKT برای استخراج ویژگی‌ها به‌صورت انعطاف‌پذیر استفاده شد، با توجه به ویژگی‌های مهم در رفتار شبکهٔ IoT که در کارهای پیشین برجسته شده‌اند. در عین حال، ابزارهای دیگری مثل CICFlowMeter [92] و Nfstream [93] نیز می‌توانند برای استخراج ویژگی‌ها به کار روند.

در این مرحله ما پاک‌سازی داده (data cleaning) را هم انجام می‌دهیم و بسته‌های ناقص (یعنی بسته‌هایی که برخی ویژگی‌ها در آن‌ها تهی/null هستند) حذف می‌شوند. در آزمایش‌های ما، تنها «timestamp» از فهرست نهایی حذف شده است، چون مهر زمانی (timestamp) رفتار شبکه را توصیف نمی‌کند و بیشتر برای مرتب‌سازی استفاده می‌شود. همهٔ ویژگی‌های دیگر بدون تغییر باقی می‌مانند تا عملکرد مدل‌های یادگیری ماشین در این شرایط سنجیده شود.

**شکل ۸.** پردازش داده: تبدیل فایل‌های pcap به csv.

این ویژگی‌ها با تکیه بر پیشنهادهای موجود در ادبیات امنیت IoT [8,46] استخراج شده‌اند. هرچند این ویژگی‌ها پیش‌تر استفاده و ارزیابی شده‌اند، هدف ما ارائهٔ روشی انعطاف‌پذیر برای آموزش مدل‌های ML با چندین ویژگی است. بنابراین پژوهشگر می‌تواند ویژگی‌های بیشتری را، چه با استفاده از اسکریپت‌های ما و چه مستقیماً از ترافیک خام شبکه (pcap)، استخراج یا مهندسی کند.

پس از استخراج ویژگی‌ها، مقادیر ثبت‌شده را در پنجره‌هایی با اندازهٔ ۱۰ بسته و ۱۰۰ بسته گروه‌بندی می‌کنیم تا اختلاف اندازهٔ داده‌ها بین سناریوها را کاهش دهیم.

* اندازهٔ پنجرهٔ **۱۰ بسته** برای این سناریوها استفاده شد: Backdoor Malware، Benign Traffic، Browser Hijacking، Command Injection، Dictionary Brute Force، DNS Spoofing، MITM ARP Spoofing، Host Discovery، OS Scan، Ping Sweep، Port Scan، SQL Injection، Uploading Attack، Vulnerability Scan، و XSS.
* اندازهٔ پنجرهٔ **۱۰۰ بسته** برای این سناریوها استفاده شد:  
  DDoS ACK Fragmentation، DDoS HTTP Flood، DDoS ICMP Flood، DDoS ICMP Fragmentation، DDoS PSHACK Flood، DDoS RSTFIN Flood، DDoS SlowLoris، DDoS SYN Flood، DDoS SynonymousIP Flood، DDoS TCP Flood، DDoS UDP Flood، DDoS UDP Fragmentation، DoS HTTP Flood، DoS SYN Flood، DoS TCP Flood، DoS UDP Flood، Mirai GREIP Flood، Mirai Greeth Flood، و Mirai UDPPlain.

برای هر پنجره، میانگین ویژگی‌ها با استفاده از Pandas [94] و NumPy [95] محاسبه می‌شود. در پایان، همهٔ خرده‌فایل‌ها با Pandas به یک فایل csv پردازش‌شده ترکیب می‌شوند. بنابراین، مجموعه‌دادهٔ csv نهایی، ترکیبی از ویژگی‌های هر تکه از داده است.

افزون بر این، هر حمله در این پژوهش ویژگی‌های خاص خودش را دارد. برای مثال، ترافیک شبکهٔ تولیدشده توسط یک حملهٔ DDoS معمولاً بسیار بزرگ‌تر از ترافیک ایجادشده توسط یک حملهٔ Spoofing است. این تفاوت در ویژگی‌های دیگر مجموعه‌داده نیز مشهود است.

**جدول ۴** همهٔ ویژگی‌های ارائه‌شده در مجموعه‌داده را فهرست می‌کند و **جدول ۵** مشخصات آماری این ویژگی‌ها را نشان می‌دهد. برای هر ویژگی در کل مجموعه‌داده، میانگین (mean)، انحراف معیار (std)، کمینه (min)، چارک ۲۵٪، میانه (۵۰٪)، چارک ۷۵٪، و بیشینه (max) گزارش شده است.

**جدول ۴. ویژگی‌های استخراج‌شده از ترافیک شبکه**

(ستون‌ها: شماره / نام ویژگی / توضیح)

1. ts — مُهر زمانی (Timestamp)
2. flow\_duration — مدت‌زمان جریان بسته
3. Header\_Length — طول هدر
4. Protocol Type — نوع پروتکل (IP، UDP، TCP، IGMP، ICMP، یا Unknown) به‌صورت عددی
5. Duration — زمان زنده‌بودن (TTL) بسته
6. Rate — نرخ ارسال بسته در یک جریان
7. Srate — نرخ ارسال بسته‌های خروجی در یک جریان
8. Drate — نرخ دریافت بسته‌های ورودی در یک جریان
9. fin\_flag\_number — مقدار فلگ FIN
10. syn\_flag\_number — مقدار فلگ SYN
11. rst\_flag\_number — مقدار فلگ RST
12. psh\_flag\_number — مقدار فلگ PSH
13. ack\_flag\_number — مقدار فلگ ACK
14. ece\_flag\_number — مقدار فلگ ECE
15. cwr\_flag\_number — مقدار فلگ CWR
16. ack\_count — شمارش بسته‌های ACK
17. syn\_count — شمارش بسته‌های SYN
18. fin\_count — شمارش بسته‌های FIN
19. urg\_count — شمارش بسته‌های URG
20. rst\_count — شمارش بسته‌های RST
21. HTTP — آیا پروتکل لایهٔ کاربرد HTTP است؟ (بله/خیر به‌صورت باینری)
22. HTTPS — آیا پروتکل لایهٔ کاربرد HTTPS است؟
23. DNS — آیا پروتکل لایهٔ کاربرد DNS است؟
24. Telnet — آیا پروتکل لایهٔ کاربرد Telnet است؟
25. SMTP — آیا پروتکل لایهٔ کاربرد SMTP است؟
26. SSH — آیا پروتکل لایهٔ کاربرد SSH است؟
27. IRC — آیا پروتکل لایهٔ کاربرد IRC است؟
28. TCP — آیا پروتکل لایهٔ انتقال TCP است؟
29. UDP — آیا پروتکل لایهٔ انتقال UDP است؟
30. DHCP — آیا پروتکل لایهٔ کاربرد DHCP است؟
31. ARP — آیا پروتکل لایهٔ پیوند داده ARP است؟
32. ICMP — آیا پروتکل لایهٔ شبکه ICMP است؟
33. IPv — آیا پروتکل لایهٔ شبکه IP است؟
34. LLC — آیا پروتکل لایهٔ پیوند داده LLC است؟
35. Tot\_sum — جمع طول همهٔ بسته‌ها در یک جریان
36. Min — کمینهٔ طول بسته در جریان
37. Max — بیشینهٔ طول بسته در جریان
38. AVG — میانگین طول بسته در جریان
39. Std — انحراف معیار طول بسته در جریان
40. Tot\_size — طول بسته‌ها
41. IAT — فاصلهٔ زمانی میان این بسته و بستهٔ قبلی (Inter-Arrival Time)
42. Number — تعداد بسته‌ها در جریان
43. Magnitude — ریشهٔ دومِ (میانگین طول بسته‌های ورودی + میانگین طول بسته‌های خروجی)
44. Radius — ریشهٔ دومِ (واریانس طول بسته‌های ورودی + واریانس طول بسته‌های خروجی)
45. Covariance — کوواریانس طول بسته‌های ورودی و خروجی
46. Variance — نسبت واریانس طول بسته‌های ورودی به واریانس طول بسته‌های خروجی
47. Weight — تعداد بسته‌های ورودی ÷ تعداد بسته‌های خروجی

(یادآوری: به‌دلیل استخراج متن از PDF، برخی نویسه‌های خاص مثل ligature در کلماتی مانند flow / flag ممکن است در نسخه اصلی به‌شکل «ﬂow» یا «ﬂag» آمده باشند. در این ترجمه، صورت عادی آن‌ها استفاده شده است.)

**جدول ۵. توصیف آماری مجموعه‌داده**

(ستون‌ها: نام ویژگی / میانگین (Mean) / انحراف معیار (Std) / کمینه (Min) / چارک ۲۵٪ / میانه (۵۰٪) / چارک ۷۵٪ / بیشینه (Max))

نمونه‌هایی از مقادیر گزارش‌شده در جدول (برای کل مجموعه‌داده):

* flow\_duration
  + میانگین: 5.76544939
  + Std: 285.034171
  + Min: 0
  + 25٪: 0
  + 50٪: 0
  + 75٪: 0.10513809
  + Max: 394,357.207
* Header\_Length
  + میانگین: ‎76,705.9637
  + Std: ‎461,331.747
  + Min: 0
  + 25٪: 54
  + 50٪ (میانه): 54
  + 75٪: ‎280.555
  + Max: ‎9,907,147.75
* Protocol Type
  + میانگین: ‎9.06568989
  + Std: ‎8.94553292
  + Min: 0
  + 25٪: 6
  + 50٪: 6
  + 75٪: ‎14.33
  + Max: 47
* Duration
  + میانگین: ‎66.3507169
  + Std: ‎14.0191881
  + Min: 0
  + 25٪: 64
  + 50٪: 64
  + 75٪: 64
  + Max: 255
* Rate و Srate
  + میانگین: ‎9064.05724
  + Std: ‎99,562.4906
  + Min: 0
  + 25٪: ‎2.09185589
  + 50٪: ‎15.7542308
  + 75٪: ‎117.384754
  + Max: ‎8,388,608
* Drate
  + میانگین: ‎5.46×10^-6
  + Std: ‎0.00725077
  + مقادیر چارکی پایین عمدتاً صفر هستند.
  + Max: ‎29.7152249
* فلگ‌ها (مانند fin\_flag\_number، syn\_flag\_number، ...)
  + این مقادیر معمولاً بین 0 و 1 هستند و میانگین‌های پایین دارند (مثلاً syn\_flag\_number حدود 0.2073 با Std حدود 0.4054 و Max برابر 1).
* ویژگی‌های لایهٔ کاربرد و انتقال (HTTP، HTTPS، DNS، Telnet، SMTP، SSH، IRC، TCP، UDP و …)
  + این‌ها به‌صورت باینری (۰ یا ۱) ثبت شده‌اند و در جدول میانگین و انحراف معیار آن‌ها (نشان‌دهندهٔ نرخ حضور آن پروتکل در داده) گزارش شده است.
  + برای نمونه:
    - TCP: میانگین ≈ 0.5738 ، Std ≈ 0.4945 ، Max = 1
    - UDP: میانگین ≈ 0.2119 ، Std ≈ 0.4087 ، Max = 1
    - DHCP، ARP، ICMP، IPv، LLC نیز با همین الگو گزارش شده‌اند. برای IPv و LLC، مقدار Max برابر 1 و میانگین خیلی نزدیک به 1 گزارش شده است (حدود 0.9998+).
* Tot\_sum (جمع طول بسته‌ها در جریان)
  + میانگین: ‎1308.32257
  + Std: ‎2613.30273
  + Min: 42
  + 25٪: 525
  + 50٪: 567
  + 75٪: ‎567.54
  + Max: ‎127,335.8
* Min و Max و AVG (طول بسته)
  + Min: کمینهٔ طول بسته در جریان، با میانگین ≈ ‎91.6073 و بیشینه تا ‎13,583
  + Max: بیشینهٔ طول بسته در جریان، با میانگین ≈ ‎181.9634 و بیشینه تا ‎49,014
  + AVG: میانگین طول بسته در جریان، با میانگین ≈ ‎124.6688
* Std (انحراف معیار طول بسته در جریان)
  + میانگین ≈ ‎33.3248
  + Std (برای Std!) ≈ ‎160.3357
  + Max تا ‎12,385.2391 گزارش شده است.
* Tot\_size (اندازهٔ بسته‌ها)
  + میانگین ≈ ‎124.691567
  + و مقادیر چارکی نزدیک به حدود 50–54 بایت هستند.  
    (در متن استخراج‌شده از PDF برخی ارقام ممکن است دچار چسبیدگی ظاهری شده باشند، اما در اصل جدول اعداد به‌صورت با دقت بالا گزارش شده‌اند.)
* IAT (فاصلهٔ بین‌رسیدن بسته‌ها)
  + میانگین: ‎83,182,525.9
  + Std: ‎17,047,351.7
  + Min: 0
  + 25٪: ‎83,071,566
  + 50٪: ‎83,124,522.4
  + 75٪: ‎83,343,908
  + Max: ‎167,639,436
* Number (تعداد بسته‌ها در جریان)
  + میانگین ≈ ‎9.4985
  + 25٪، 50٪، و 75٪ همگی حدود ‎9.5 گزارش شده‌اند
  + Max برابر 15
* Magnitude
  + میانگین ≈ ‎13.12182
  + Std ≈ ‎8.6286
  + Min ≈ ‎9.1651
  + Max ≈ ‎164.821115
* Radius
  + میانگین ≈ ‎47.0949848
  + Std ≈ ‎226.769647
  + Max تا ‎17,551.2708 گزارش شده است.
* Covariance
  + میانگین ≈ ‎30,724.3565
  + Std ≈ ‎323,710.68
  + Max تا ‎154,902,159 گزارش شده است.
* Variance
  + میانگین ≈ ‎0.0964376
  + Std ≈ ‎0.233001
  + Max = 1
* Weight
  + میانگین ≈ ‎141.51237
  + Std ≈ ‎21.0683
  + 25٪، 50٪، و 75٪ تقریباً ‎141.55
  + Max ≈ ‎244.6

(تا اینجا جدول ۵.)

### 5. ارزیابی یادگیری ماشین (ML)

برای نشان دادن این‌که چگونه می‌توان از مجموعه‌دادهٔ CICIoT2023 برای آموزش روش‌های تشخیص و طبقه‌بندی حملات مبتنی بر یادگیری ماشین (ML) استفاده کرد، روند ارزیابی ML در **شکل ۹** نمایش داده شده است.

در گام نخست، همهٔ مجموعه‌داده‌هایی که مطابق فرایند نشان‌داده‌شده در شکل ۸ تولید شده‌اند با هم ترکیب می‌شوند. یعنی ترافیک مخرب و ترافیک سالم با هم ادغام شده و به یک «مجموعهٔ ادغامی» (blended dataset) تبدیل می‌شوند. این ادغام و درهم‌زدن (shuffle) داده با استفاده از PySpark [96] انجام شده است.

پس از یکپارچه‌سازی داده، ما عملکرد ML را از سه منظر بررسی می‌کنیم:

1. **طبقه‌بندی چندکلاسه (Multiclass Classification):** هدف در این حالت، طبقه‌بندی ۳۳ حملهٔ مجزا است.
2. **طبقه‌بندی گروهی (Grouped Classification):** در این حالت، حملات در ۷ گروه (برای مثال DDoS و DoS و …) دسته‌بندی می‌شوند و مدل باید گروه را تشخیص دهد.
3. **طبقه‌بندی دودویی (Binary Classification):** در این حالت، مدل باید بین «مخرب» و «سالم» تمایز قائل شود.

در هر حالت، مجموعه‌داده به دو بخش آموزش (۸۰٪) و آزمون (۲۰٪) تقسیم می‌شود. پیش از آموزش مدل‌ها، داده‌ها با روش StandardScaler [97] نرمال‌سازی می‌شوند. در پایان، نتایج به‌صورت یک خروجی تلفیقی گزارش می‌شوند.

**شکل ۹.** جریان ارزیابی یادگیری ماشین (ML) که در این پژوهش استفاده شده است.

#### 5.1. معیارها (Metrics)

ارزیابی مدل‌ها و پیکربندی‌های مختلف ML بر اساس معیارهای استاندارد انجام می‌شود. اگر  
TP نشان‌دهندهٔ «تشخیص درست مورد مثبت» (True Positive)،  
TN «تشخیص درست مورد منفی» (True Negative)،  
FP «تشخیص اشتباه یک مورد منفی به‌عنوان مثبت» (False Positive)،  
و FN «تشخیص اشتباه یک مورد مثبت به‌عنوان منفی» (False Negative) باشد، معیارهای زیر استفاده شده‌اند [98]:

* **دقت (Accuracy):** نسبت کل پیش‌بینی‌های درست (مثبت درست و منفی درست) به کل پیش‌بینی‌ها. این معیار نشان می‌دهد مدل تا چه حد به‌طور کلی درست پیش‌بینی می‌کند.
* **بازخوانی / یادآوری (Recall یا Sensitivity):**

Rec=TPTP+FNRec=TP+FNTP​

این معیار نشان می‌دهد چه سهمی از نمونه‌های «واقعاً مثبت» توسط مدل درست به‌عنوان مثبت شناسایی شده‌اند.

* **دقت مثبت (Precision):**

Pre=TPTP+FPPre=TP+FPTP​

این معیار نسبتِ «مثبت‌های درست» را به «همهٔ مواردی که مدل مثبت اعلام کرده» اندازه می‌گیرد. یعنی از مواردی که مدل می‌گوید حمله هستند، چند تا واقعاً حمله بوده‌اند.

* **امتیاز F1 (F1-Score):**

F1=2×Pre×RecPre+RecF1=Pre+Rec2×Pre×Rec​

F1 میانگین هارمونیک Precision و Recall است و تعادلی بین این دو معیار فراهم می‌کند.

#### 5.2. ارزیابی (Evaluation)

در فاز ارزیابی، ما پنج روش یادگیری ماشین را که در حوزه‌های مختلف ــ از جمله امنیت سایبری ــ با موفقیت به‌کار رفته‌اند استفاده کردیم:

* **رگرسیون لجستیک (Logistic Regression) [99]**
* **پرسپترون (Perceptron) [100]**
* **AdaBoost [101–103]**
* **جنگل تصادفی (Random Forest) [104]**
* **شبکهٔ عصبی عمیق (Deep Neural Network) [105]**

**شکل ۱۰** عملکرد همهٔ این روش‌ها را در سناریوهای مختلف نشان می‌دهد، وقتی که مسئلهٔ طبقه‌بندی را در سه حالت فرموله می‌کنیم:

* حالت دودویی (یعنی فقط «مخرب» در برابر «سالم»)،
* حالت چندکلاسه (یعنی تمایز بین ۳۳ نوع حمله)،
* و حالت گروهی (یعنی ۷ گروه حمله).

(ادامهٔ نتایج عددی عملکرد مدل‌ها و تحلیل مقایسه‌ای در بخش‌های بعدی مقاله آورده می‌شود.)

**5.3. بحث**

برای این‌که نشان دهیم هر مدل روی هر کلاس (ردهٔ ترافیک) چطور عمل می‌کند، جدول‌های ۷ و ۸ ماتریس سردرگمی (confusion matrix) را برای جنگل تصادفی (Random Forest) و شبکهٔ عصبی عمیق (Deep Neural Network) در سناریوی طبقه‌بندی چندکلاسه با هشت کلاس نشان می‌دهند.

**جدول ۷. ماتریس سردرگمی برای شبکهٔ عصبی عمیق در حالت طبقه‌بندی چندکلاسه (۸ کلاس).**

ستون‌ها = برچسبِ پیش‌بینی‌شده توسط مدل  
سطرها = برچسبِ واقعی در داده

| **واقعی \ پیش‌بینی‌شده** | **Benign (سالم)** | **Brute Force** | **DDoS** | **DoS** | **Mirai** | **Recon (پویش/شناسایی)** | **Spoofing (جعل)** | **Web (وب‌محور)** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Benign | 230,229 | 1 | 7 | 2 | 0 | 9,270 | 3,812 | 1 |
| Brute Force | 1,054 | 438 | 3 | 0 | 0 | 1,216 | 271 | 1 |
| DDoS | 23 | 0 | 7,523,853 | 1,012 | 545 | 653 | 65 | 0 |
| DoS | 15 | 0 | 4,933 | 1,787,065 | 60 | 61 | 33 | 0 |
| Mirai | 10 | 0 | 258 | 41 | 583,283 | 64 | 21 | 0 |
| Recon | 18,517 | 2 | 968 | 30 | 1 | 55,656 | 3,455 | 1 |
| Spoofing | 30,485 | 0 | 17 | 0 | 15 | 10,021 | 67,257 | 3 |
| Web | 1,976 | 0 | 1 | 0 | 0 | 2,028 | 1,221 | 207 |

توضیح:

* «Benign» = ترافیک سالم
* «Brute Force» = حمله جست‌وجوی فراگیر/پسورد حدس‌زدنی
* «DDoS» = منع خدمت توزیع‌شده
* «DoS» = منع خدمت
* «Mirai» = زیرخانوادهٔ حملات میرای
* «Recon» = شناسایی/پویش
* «Spoofing» = جعل (مثل ARP spoofing و DNS spoofing)
* «Web» = حملات مبتنی بر وب (تزریق، XSS، ربایش مرورگر و …)

**جدول ۸. ماتریس سردرگمی برای جنگل تصادفی در حالت طبقه‌بندی چندکلاسه (۸ کلاس).**

| **واقعی \ پیش‌بینی‌شده** | **Benign** | **Brute Force** | **DDoS** | **DoS** | **Mirai** | **Recon** | **Spoofing** | **Web** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Benign | 234,929 | 4 | 24 | 2 | 4 | 3,192 | 5,159 | 8 |
| Brute Force | 1,342 | 169 | 1 | 0 | 0 | 844 | 626 | 1 |
| DDoS | 15 | 0 | 7,525,049 | 557 | 18 | 339 | 173 | 0 |
| DoS | 7 | 0 | 1,088 | 1,790,979 | 34 | 12 | 47 | 0 |
| Mirai | 5 | 0 | 603 | 18 | 582,921 | 100 | 30 | 0 |
| Recon | 11,565 | 6 | 1,418 | 11 | 16 | 60,006 | 5,591 | 17 |
| Spoofing | 14,618 | 1 | 18 | 6 | 11 | 4,743 | 88,371 | 30 |
| Web | 1,140 | 1 | 3 | 1 | 1 | 1,265 | 2,792 | 230 |

برداشت از این دو ماتریس:

* در هر دو مدل، بعضی کلاس‌ها تقریباً «بی‌نقص» تشخیص داده می‌شوند، مخصوصاً آن‌هایی که تعداد نمونه‌های خیلی زیادی در مجموعه‌داده دارند.
  + برای مثال، خطای مدل برای DDoS، DoS و Mirai خیلی کم است.
  + بعد از آن‌ها، Recon (شناسایی/پویش) و Spoofing (جعل) هم نسبتاً خوب تشخیص داده می‌شوند.
* در مقابل، مدل‌ها در بعضی کلاس‌ها مشکل دارند:
  + حملات وب‌محور (Web-based attacks) اغلب به‌اشتباه به‌صورت «Benign» (سالم)، یا «Recon»، یا «Spoofing» برچسب می‌خورند.
  + حملات Brute Force هم همین الگو را دارند: معمولاً یا سالم تشخیص داده می‌شوند یا به یکی از کلاس‌های مشابه انداخته می‌شوند.

این خطاها نشان می‌دهد که الگوهای ترافیکی بعضی دسته‌ها شبیه هم هستند و مدل در جدا کردنشان از هم دچار تداخل می‌شود. با این حال، در بیشتر موارد تشخیص موفق است و همین باعث نتایج کلیِ نشان‌داده‌شده در شکل ۱۰ می‌شود.

در واقع، نتایج نشان می‌دهند که عملکرد طبقه‌بندی چندکلاسه وقتی بدتر می‌شود که سر و کار ما با سه کلاس خاص باشد:

* Benign (ترافیک سالم)،
* Recon (شناسایی/پویش)،
* Spoofing (جعل).

ترافیک این سناریوها می‌تواند از نظر الگوهای آماری تا حدی شبیه باشد، و ما قصد داریم این پدیده را در کارهای آینده دقیق‌تر بررسی کنیم.

در نهایت، جدول‌های ۹ و ۱۰ مجموعه‌دادهٔ پیشنهادی CICIoT2023 را با مجموعه‌داده‌های امنیتی اینترنت اشیای شناخته‌شدهٔ موجود مقایسه می‌کنند.

* جدول ۹ روی نوع حمله‌ها تمرکز دارد: کدام مجموعه‌داده‌ها شامل چه نوع حملاتی هستند (مانند DDoS، DoS، اسکن/Recon، جعل، تزریق وب، brute force، Mirai و غیره).
* جدول ۱۰ روی مشارکت‌ها/ویژگی‌های کلی تمرکز دارد: آیا آن مجموعه‌داده توپولوژی بزرگ دارد؟ آیا حملات متنوع و زیاد دارد؟ آیا دسته‌بندی آن ساختارمند است؟ آیا ارزیابی یادگیری ماشین/یادگیری عمیق همراهش ارائه شده است؟

به‌طور خلاصه از جدول ۹ (مقایسهٔ نوع حملات در مجموعه‌داده‌ها):

* بسیاری از مجموعه‌داده‌های پیشین فقط زیرمجموعهٔ کوچکی از سناریوهای حمله را پوشش می‌دهند.
  + بعضی‌ها تمرکزشان روی Mirai است،
  + بعضی روی DoS / DDoS کلاسیک،
  + بعضی روی اسکن و پویش پورت،
  + بعضی روی ترافیک MQTT،
  + و بعضی بر محیط‌های صنعتی (IIoT).
* CICIoT2023 برخلاف خیلی از مجموعه‌داده‌های قبلی، مجموعهٔ بزرگی از حملات مختلف را یک‌جا دارد، از جمله:
  + حملات DDoS متنوع (SYN Flood، UDP Flood، ICMP Flood، تکه‌تکه‌سازی/Fragmentation، Slowloris، HTTP Flood و …)،
  + حملات DoS محلی،
  + حملات Recon (پویش پورت، کشف میزبان، اسکن سیستم‌عامل، اسکن آسیب‌پذیری و …)،
  + حملات وب (تزریق SQL، تزریق فرمان/Command Injection، آپلود مخرب، XSS، ربایش مرورگر و …)،
  + brute force از نوع دیکشنری،
  + حملات جعل (ARP Spoofing، DNS Spoofing)،
  + و سناریوهای خاص مبتنی بر Mirai (مثل GREIP Flood، Greeth Flood، UDPPlain).

چنین گستره‌ای در یک مجموعه‌دادهٔ واحد در کارهای قبلی دیده نشده بود.

به‌طور خلاصه از جدول ۱۰ (مقایسهٔ مشارکت‌های سطح‌بالا بین مجموعه‌داده‌ها):

این جدول مجموعه‌داده‌ها را از نظر ویژگی‌های کلیدی زیر مقایسه می‌کند:

* آیا توپولوژی گسترده و واقعی با بیش از ۱۰۰ دستگاه IoT دارد؟
* آیا ۳۳ حمله اجرا شده و در ۷ دسته گروه‌بندی شده‌اند؟
* آیا برای این مجموعه‌داده واقعاً ارزیابی یادگیری ماشین و یادگیری عمیق (ML و DL) انجام و گزارش شده است؟

خلاصهٔ ادعای نویسندگان در جدول ۱۰:

* CICIoT2023 تنها مجموعه‌داده‌ای است که هم یک توپولوژی گسترده با بیش از ۱۰۰ دستگاه واقعی IoT دارد،
* و هم ۳۳ حمله اجراشده را در قالب ۷ دسته ارائه می‌کند،
* و هم ارزیابی ML و DL روی همین داده‌ها گزارش شده است.

**6. نتیجه‌گیری**

امروزه اینترنت اشیا (IoT) به‌طور فزاینده‌ای در جامعه اهمیت پیدا می‌کند. در چنین فضایی، توسعهٔ راهکارهای امنیتی نقش اساسی دارد، چون این راهکارها شرط لازم برای داشتن عملیات اینترنت اشیای کارآمد، امن و قابل اتکا هستند.

این پژوهش یک مجموعه‌دادهٔ جدید و بزرگ از حملات IoT معرفی کرد تا توسعهٔ برنامه‌های تحلیل امنیتی (security analytics) برای سناریوهای واقعی اینترنت اشیا را تسهیل کند. در این فرایند:

* ۳۳ حمله در یک توپولوژی اینترنت اشیا با ۱۰۵ دستگاه اجرا شد.
* این حملات در هفت دسته قرار گرفتند:
  + DDoS،
  + DoS،
  + Recon (شناسایی/پویش)،
  + Web-based (مبتنی بر وب)،
  + brute force،
  + Spoofing (جعل)،
  + و Mirai.
* همهٔ حملات توسط دستگاه‌های اینترنت اشیای مخرب انجام شد که سایر دستگاه‌های اینترنت اشیا را هدف می‌گرفتند (یعنی مهاجم هم خودش یک گره IoT بود، نه یک لپ‌تاپ یا سرور سنتی).

این مجموعه‌داده همچنین شامل چندین نوع حمله است که در هیچ‌یک از مجموعه‌داده‌های IoT قبلی کنار هم وجود نداشتند. این مسئله به متخصصان IoT اجازه می‌دهد روی توسعهٔ راه‌حل‌های جدید تحلیل امنیتی کار کنند و از داده‌ها در قالب‌های مختلف استفاده کنند. مجموعه‌داده از طریق وب‌سایت مجموعه‌داده‌های CIC در دسترس است (آدرس داده شده در مقاله؛ دسترسی ذکر شده برای تاریخ ۱۹ ژوئن ۲۰۲۳).

در مقایسه با کارهای روز (state of the art)، CICIoT2023 چند امتیاز دارد:

* استفاده از یک توپولوژی بزرگ و واقعی با تنوع بالای دستگاه‌های IoT؛
* اجرای تعداد زیادی حمله که پیش از این هرگز در یک مجموعه‌دادهٔ امنیت IoT به‌صورت یکجا دیده نشده بود؛
* و ارزیابی اینکه روش‌های متداول یادگیری ماشین و یادگیری عمیق در سناریوهای مختلف طبقه‌بندی (دودویی، چندکلاسهٔ ۸‌دسته‌ای، و چندکلاسهٔ ۳۴‌کلاسه) چگونه عمل می‌کنند.

در نهایت، این کار مسیر چند خط پژوهشی آینده را باز می‌کند، از جمله:

* بهینه‌سازی مدل‌های ML،
* بررسی ویژگی‌ها (featureها) و این‌که هرکدام چطور روی رفتار مدل‌ها اثر می‌گذارند،
* تفسیر تصمیم‌های طبقه‌بندی (قابلیت توضیح‌پذیری)،
* و بررسی قابلیت انتقال‌پذیری (transferability) از این مجموعه‌داده به مجموعه‌داده‌های دیگر.

**مشارکت نویسندگان (Author Contributions)**

* مفهوم‌پردازی (Conceptualization):  
  E.C.P.N.، S.D.، R.F.، A.Z.، R.L. و A.A.G.
* روش‌شناسی (Methodology):  
  E.C.P.N.، S.D.، R.F.، A.Z.، R.L. و A.A.G.
* پیاده‌سازی نرم‌افزار (Software):  
  E.C.P.N.، S.D.، R.F. و A.Z.
* اعتبارسنجی (Validation):  
  E.C.P.N.، S.D.، R.F.، A.Z.، R.L. و A.A.G.
* تحلیل رسمی (Formal Analysis):  
  E.C.P.N.، S.D.، R.F. و A.Z.
* بررسی/کاوش (Investigation):  
  E.C.P.N.، S.D.، R.F.، A.Z.، R.L. و A.A.G.
* تدارک منابع (Resources):  
  E.C.P.N.، S.D.، R.F. و A.Z.
* گردآوری داده (Data Curation):  
  E.C.P.N.، S.D.، R.F. و A.Z.
* نگارش پیش‌نویس اولیه (Writing—Original Draft Preparation):  
  E.C.P.N.، S.D.، R.F. و A.Z.
* نگارش—مرور و ویرایش (Writing—Review and Editing):  
  E.C.P.N.، S.D.، R.F.، A.Z.، R.L. و A.A.G.
* مصورسازی/بصری‌سازی (Visualization):  
  E.C.P.N.، S.D.، R.F. و A.Z.
* سرپرستی/نظارت (Supervision):  
  R.L. و A.A.G.
* مدیریت پروژه (Project Administration):  
  S.D.، R.L. و A.A.G.
* تأمین مالی (Funding Acquisition):  
  R.L. و A.A.G.

همهٔ نویسندگان نسخهٔ منتشرشدهٔ نهایی مقاله را خوانده و تأیید کرده‌اند.

**تأمین مالی (Funding)**

این پژوهش هیچ بودجهٔ بیرونی/خارجی دریافت نکرده است.

**بیانیهٔ کمیتهٔ اخلاق (Institutional Review Board Statement)**

لازم نیست / کاربرد ندارد.  
(Not applicable)

**رضایت آگاهانه (Informed Consent Statement)**

لازم نیست / کاربرد ندارد.  
(Not applicable)

**بیانیهٔ دسترسی به داده (Data Availability Statement)**

آدرس دسترسی به داده‌ها:  
https://www.unb.ca/cic/datasets/iotdataset-2023.html  
(دسترسی در تاریخ ۱۹ ژوئن ۲۰۲۳ گزارش شده است.)

(در این صفحه مجموعه‌دادهٔ CICIoT2023 برای دانلود / استفاده پژوهشی در دسترس قرار داده شده است.)

**قدردانی (Acknowledgments)**

نویسندگان با قدردانی اعلام می‌کنند که این کار با پشتیبانی «مؤسسهٔ کانادایی امنیت سایبری» (Canadian Institute for Cybersecurity - CIC)، همچنین حمایت مالی «Canada Research Chair» و «Mastercard» انجام شد.

**تضاد منافع (Conflicts of Interest)**

نویسندگان اعلام می‌کنند که تضاد منافع ندارند.

**منابع (References)**

در این بخش، فهرست مراجع مقاله آمده است. چون مراجع شامل عنوان‌ مقاله‌ها، نام نویسندگان و جزئیات انتشار هستند و باید دقیق باقی بمانند، عموماً در متون پژوهشی به همان زبان اصلی (انگلیسی) نقل می‌شوند. ساختار کلی ورودی‌های ارجاعی این مقاله شامل موارد زیر است (نمونه‌ها):

1. Da Xu, L.; He, W.; Li, S. “Internet of things in industries: A survey.” IEEE Transactions on Industrial Informatics, 2014, 10, 2233–2243.  
   (این مرجع یک مرور (survey) دربارهٔ اینترنت اشیا در صنعت است.)
2. Nauman, A.; Qadri, Y.A.; Amjad, M.; Zikria, Y.B.; Afzal, M.K.; … Kim, S.W. “Multimedia Internet of Things: A comprehensive survey.” IEEE Access, 2020, 8, 8202–8250. [CrossRef]
3. Habibzadeh, H.; Dinesh, K.; Shishvan, O.R.; Boggio-Dandry, A.; … Soyata, T. “A survey of healthcare Internet of Things (HIoT): A clinical perspective.” IEEE Internet of Things Journal, 2019, 7, 53–71. [CrossRef]
4. Lee, S.K.; Bae, M.; Kim, H. “Future of IoT networks: A survey.” Applied Sciences, 2017, 7, 1072. [CrossRef]
5. Afrifa, S.; Varadarajan, V.; Appiahene, P.; Zhang, T.; Domfeh, E.A. “Ensemble Machine Learning Techniques for Accurate and Efficient Detection of Botnet Attacks in Connected Computers.” Eng, 2023, 4, 650–664. [CrossRef]

[...]

تا

1. Danso, P.K.; Neto, E.C.P.; Dadkhah, S.; Zohourian, A.; … Ghorbani, A.A. “Ensemble-based Intrusion Detection for Internet of Things Devices.” Proceedings of the 2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET), Marietta, GA, USA, 19–21 December 2022; pp. 34–39.
2. Bapat, [ادامهٔ مرجع ۹۹ و بعدی‌ها در نسخهٔ PDF آمده‌اند، شامل مراجع فنی مانند PySpark، StandardScaler، DPKT، CICFlowMeter، NFStream، Pandas، NumPy، و غیره. این مراجع ابزارها و منابع نرم‌افزاری و همچنین متون روش‌شناسی را پوشش می‌دهند و برای بازتولید کار لازم هستند.]

(کل فهرست منابع در نسخهٔ PDF تا مرجع ۹۹ ادامه دارد و همگی در متن مقاله با شماره ارجاع داده شده‌اند. محتوای کتابخانه‌ها و آدرس‌های وب مثل اسناد DPKT، Pandas، NumPy، PySpark، و Scikit-learn نیز در این بخش آمده‌اند و برای شفافیت علمی و تکرارپذیری کار نقل شده‌اند.)