مقاله پژوهشی

چارچوب ترکیبی سبک‌وزن برای امنیت اینترنت اشیا با استفاده از جنگل تصادفی بهینه و انتخاب ویژگی تطبیقی در معماری لبه-ابری

محسن اشرفی

چکیده: امنیت در زیرساخت‌های اینترنت اشیا (IoT) به دلیل افزایش تهدیدات سایبری، از مهم‌ترین چالش‌های این حوزه محسوب می‌شود. اتصال پیوسته دستگاه‌های IoT به شبکه و پردازش داده‌های حساس، آنها را در معرض حملاتی نظیر انکار سرویس، نفوذ و دستکاری عملکرد قرار می‌دهد که پیامدهایی چون اختلال در سیستم و افشای اطلاعات محرمانه را به دنبال دارد. از سوی دیگر، تنوع و پیچیدگی حملات، ناهمگونی داده‌های حسگرها و تغییرپذیری رفتار نرمال سیستم‌ها، تشخیص تهدیدات را دشوار ساخته است. در این پژوهش، چارچوبی ترکیبی و سبک‌وزن مبتنی بر جنگل تصادفی بهینه (ORF) و انتخاب ویژگی تطبیقی برای بهبود امنیت IoT ارائه می‌گردد. به منظور ارزیابی، عملکرد الگوریتم‌های مختلف یادگیری ماشین شامل رگرسیون لجستیک، ماشین بردار پشتیبان، درخت تصمیم، جنگل تصادفی، شبکه عصبی مصنوعی و ORF بر روی مجموعه‌داده DS۲OS بررسی شد. نتایج نشان داد که همه مدل‌ها به دقت بالای ۰/۹۸ دست یافتند، در حالی که RF و ORF با امتیاز F1 معادل ۰/۹۹۳۷ عملکرد برتر داشتند. همچنین به‌کارگیری الگوریتم بهینه‌سازی ازدحام ذرات (PSO) موجب کاهش نرخ مثبت کاذب تا ۰/۵۷٪ شد و بهره‌گیری از معماری لبه-ابری زمان پردازش را حدود ۴۰٪ بهبود داد. روش پیشنهادی علاوه بر کاهش ۲۹٪ مصرف حافظه، یک راهکار کارآمد و مقیاس‌پذیر برای مقابله با تهدیدات امنیتی در محیط‌های IoT ارائه می‌دهد..

***کلیدواژه:* اینترنت اشیا، یادگیری ماشین، تشخیص ناهنجاری، امنیت، جنگل تصادفی بهینه (ORF)، معماری لبه ابری.**

۱- مقدمه

با رشد تصاعدی دستگاه‌ها و کاربردهای اینترنت اشیا[1] (IoT) ، تأمین امنیت این اکوسیستم گسترده به یک ضرورت حیاتی تبدیل شده است [۱]. دستگاه‌های IoT، به دلیل محدودیت منابع سخت‌افزاری و اتصال دائمی به شبکه، در برابر طیف وسیعی از حملات سایبری از جمله حملات منع سرویس[2] (DoS) ، نفوذ به داده‌ها و جاسوسی آسیب‌پذیر هستند. این حملات می‌توانند منجر به اختلال در عملکرد، افشای اطلاعات حساس و خسارات جدی شوند [۲]. با وجود توسعه سیستم‌های تشخیص نفوذ[3] (IDS)، روش‌های سنتی مبتنی بر امضا به دلیل عدم توانایی در شناسایی حملات جدید و پیچیده، کارایی لازم را ندارند. این امر نیاز به رویکردهای نوین و هوشمند برای تشخیص حمله[4] و ناهنجاری[5] را برجسته می‌سازد.

مدل‌های یادگیری ماشین ابزاری قدرتمند برای شناسایی الگوهای غیرعادی در ترافیک شبکه IoT هستند [۳] تا [۵]. با این حال، چالش‌های مهمی همچنان وجود دارد که مانع از پیاده‌سازی مؤثر این مدل‌ها می‌شود. این چالش‌ها شامل حجم و ناهمگونی داده‌های حسگرها، نیاز به پردازش در زمان واقعی و محدودیت‌های محاسباتی در دستگاه‌های لبه‌ای شبکه است. در بسیاری از مطالعات، مدل‌ها به دقت بالا دست یافته‌اند، اما غالباً پیچیدگی محاسباتی بالایی داشته یا در تشخیص انواع جدید حملات با مشکل روبرو هستند [۶] تا [۱۰]. از این رو، طراحی مدلی که ضمن حفظ دقت بالا، از نظر منابع سیستمی نیز سبک‌وزن و بهینه باشد، یک نیاز پژوهشی حیاتی است.

با وجود پیشرفت‌های قابل توجه در به‌کارگیری مدل‌های یادگیری ماشین برای تشخیص حمله و ناهنجاری در محیط‌های اینترنت اشیا، بررسی ادبیات نشان می‌دهد که همچنان چند شکاف پژوهشی اساسی پابرجاست. نخست، بخش قابل توجهی از مطالعات موجود تمرکز اصلی خود را بر بهبود دقت کلی طبقه‌بندی قرار داده‌اند، در حالی که معیارهای مهمی نظیر نرخ مثبت کاذب، هزینه محاسباتی و قابلیت اجرای بلادرنگ در محیط‌های IoT با منابع محدود، کمتر مورد توجه قرار گرفته‌اند. دوم، بسیاری از روش‌های پیشنهادی، به‌ویژه مدل‌های یادگیری عمیق و چارچوب‌های ترکیبی پیچیده، علی‌رغم دستیابی به دقت‌های بالا، از پیچیدگی محاسباتی قابل‌توجهی برخوردارند که پیاده‌سازی عملی آن‌ها را در لایه لبه و سناریوهای واقعی IoT با چالش مواجه می‌سازد. سوم، وابستگی اغلب مطالعات به یک مجموعه‌داده خاص و فقدان ارزیابی تعمیم‌پذیری بین‌داده‌ای، قابلیت اعتماد و کاربردپذیری این مدل‌ها را در محیط‌های ناهمگون اینترنت اشیا محدود می‌کند.

در پاسخ به این چالش‌ها، سهم پژوهش حاضر توسعه یک سیستم تشخیص حمله و ناهنجاری دقیق، سبک‌وزن و مقیاس‌پذیر برای اینترنت اشیا، ارائه یک چارچوب ترکیبی هوشمند مبتنی بر جنگل تصادفی بهینه‌شده[6] (ORF) و انتخاب ویژگی تطبیقی است. در این چارچوب، الگوریتم بهینه‌سازی ازدحام ذرات[7] (PSO) به‌منظور تنظیم بهینه هایپرپارامترهای جنگل تصادفی به‌کار گرفته شده است تا ضمن حفظ دقت بالا، نرخ مثبت کاذب و سربار محاسباتی به‌طور معناداری کاهش یابد.

نوآوری اصلی این پژوهش در سه محور قابل تبیین است:

این مقاله در تاریخ ۳ شهریور ماه ۱۴۰۴ دریافت و در تاریخ ۱۲ بهمن ماه ۱۴۰۴ بازنگری شد.

محسن اشرفی (نویسنده مسئول)، گروه مهندسی کامپیوتر، دانشگاه ملی مهارت، تهران، ایران، (email: m-ashrafi@tvu.ac.ir).

1. Internet of Things
2. Denial of Service
3. Intrusion Detection Systems
4. Attack Detection
5. Anomaly
6. Optimized Random Forest
7. Particle Swarm Optimization

۱. ارائه یک مدل جنگل تصادفی بهینه‌شده مبتنی بر PSO که با کاهش نرخ مثبت کاذب و مصرف حافظه، برای محیط‌های IoT با منابع محدود مناسب است؛
۲. طراحی یک معماری لبه-ابری سبک‌وزن که امکان تشخیص سریع و بلادرنگ ناهنجاری‌ها را با بهبود زمان پردازش فراهم می‌کند؛
۳. ارزیابی جامع و بین‌داده‌ای مدل پیشنهادی با استفاده از مجموعه داده DS۲OS و اعتبارسنجی خارجی روی IoTID۲۰، به‌منظور بررسی قابلیت تعمیم‌پذیری در سناریوهای واقعی و ناهمگون اینترنت اشیا.

نتایج تجربی نشان می‌دهد که چارچوب پیشنهادی، ضمن دستیابی به دقت، صحت و فراخوانی بالا، تعادل مناسبی میان کارایی تشخیصی و پیچیدگی محاسباتی برقرار کرده و می‌تواند به‌عنوان یک راهکار عملی و مقیاس‌پذیر برای ارتقای امنیت زیرساخت‌های اینترنت اشیا مورد استفاده قرار گیرد.

۲- پیشینه پژوهش

با گسترش سریع اینترنت اشیاو افزایش حملات سایبری علیه دستگاه‌ها و سرویس‌های هوشمند، تشخیص ناهنجاری و حملات به یکی از موضوعات کلیدی در حوزه امنیت IoT تبدیل شده است. در سال‌های اخیر، پژوهش‌های متعددی با بهره‌گیری از روش‌های یادگیری ماشین و یادگیری عمیق برای شناسایی رفتارهای مخرب در شبکه‌های IoT ارائه شده‌اند [۱] و [۲]. با این حال، بررسی ادبیات نشان می‌دهد که رویکردهای موجود را می‌توان در چند دسته اصلی طبقه‌بندی کرد که هر یک دارای نقاط قوت و محدودیت‌های خاص خود هستند.

بخش قابل توجهی از مطالعات از الگوریتم‌های یادگیری ماشین کلاسیک نظیر درخت تصمیم، جنگل تصادفی، ماشین بردار پشتیبان، رگرسیون لجستیک، k- نزدیک‌ترین همسایه و نایو بایز برای تشخیص حمله و ناهنجاری در محیط‌های IoT استفاده کرده‌اند [۱] تا [۱۷]. نتایج این پژوهش‌ها نشان می‌دهد که این الگوریتم‌ها، به‌ویژه جنگل تصادفی، به دلیل سادگی، تفسیرپذیری و سربار محاسباتی نسبتاً پایین، گزینه‌های مناسبی برای محیط‌های IoT با منابع محدود هستند. با این وجود، وابستگی شدید این روش‌ها به داده‌های آموزشی، حساسیت به عدم توازن کلاس‌ها و کاهش کارایی در مواجهه با حملات ناشناخته، از محدودیت‌های اصلی آن‌ها به‌شمار می‌رود [۱۰] و [۱۶].

به‌منظور بهبود عملکرد مدل‌های منفرد، برخی مطالعات از روش‌های ترکیبی و یادگیری گروهی مانند رأی‌گیری، بگینگ و بوستینگ استفاده کرده‌اند [۲]، [۶]، [۷]، [۱۳] و [۱۸]. این رویکردها عموماً موجب افزایش دقت تشخیص و کاهش بیش‌برازش شده‌اند و در برخی مجموعه‌داده‌های استاندارد IoT عملکرد بهتری نسبت به مدل‌های منفرد ارائه داده‌اند. با این حال، افزایش پیچیدگی محاسباتی، زمان آموزش بیشتر و دشواری پیاده‌سازی در معماری‌های مبتنی بر لبه، استفاده عملی از این روش‌ها را در محیط‌های واقعی IoT با چالش مواجه می‌سازد [۶] و [۱۳].

در برخی پژوهش‌ها، الگوریتم‌های فراابتکاری نظیر الگوریتم ژنتیک، بهینه‌سازی ازدحام ذرات و سایر روش‌های الهام‌گرفته از طبیعت برای انتخاب ویژگی یا تنظیم هایپرپارامترهای مدل‌های یادگیری ماشین به کار گرفته شده‌اند [۳]، [۴] و [۱۹]. نتایج این مطالعات نشان می‌دهد که ترکیب الگوریتم‌های یادگیری ماشین با روش‌های بهینه‌سازی می‌تواند منجر به کاهش نرخ مثبت کاذب و بهبود تعمیم‌پذیری مدل شود. با این حال، افزایش زمان آموزش و حساسیت این الگوریتم‌ها به تنظیمات اولیه، کاربرد آن‌ها را در سناریوهای بلادرنگ IoT با محدودیت منابع محدود می‌کند [۳] و [۴].

جدول ۱: مقایسه دسته‌بندی‌شده روش‌های تشخیص ناهنجاری در محیط IoT

گروه روش‌ها	منابع شاخص	مزایا	محدودیت‌ها	شکاف پژوهشی
یادگیری ماشین کلاسیک	[۱]، [۹]، [۱۰]، [۱۱]، [۱۵]، [۱۶] و [۱۷]	سبک، تفسیرپذیر، مناسب IoT کم‌منبع	وابستگی به داده، افت عملکرد در حملات جدید	نیاز به بهینه‌سازی پارامتر و کاهش FP
روش‌های Ensemble	[۲]، [۶]، [۷]، [۱۳] و [۱۸]	دقت بالا، کاهش بیش‌برازش	پیچیدگی محاسباتی، زمان آموزش بالا	طراحی مدل سبک‌وزن
بهینه‌سازی +ML	[۳]، [۴] و [۱۹]	بهبود تعمیم‌پذیری، کاهش FP	سربار آموزش، تنظیم حساس	تنظیم خودکار و کارا
یادگیری عمیق و ترکیبی	[۵]، [۲۰] تا [۲۳]	تشخیص الگوهای پیچیده	مصرف انرژی و منابع بالا	ناسازگار با Edge IoT

در سال‌های اخیر، مدل‌های یادگیری عمیق نظیر شبکه‌های عصبی کانولوشنال، شبکه‌های بازگشتی، ترنسفورمرها و معماری‌های ترکیبی به‌طور گسترده برای تشخیص حملات پیچیده در محیط‌های IoT مورد استفاده قرار گرفته‌اند [۵]، [۲۰] تا [۲۳]. این مدل‌ها توانایی بالایی در استخراج الگوهای پیچیده و غیرخطی از داده‌های حجیم دارند و در برخی مطالعات به دقت‌های بسیار بالا دست یافته‌اند. با این وجود، مصرف بالای منابع محاسباتی، نیاز به داده‌های آموزشی گسترده و سربار انرژی زیاد، کاربرد این روش‌ها را در محیط‌های واقعی IoT، به‌ویژه در لایه لبه، با محدودیت مواجه می‌سازد [۲۰] , [۲۲].

مرور ادبیات نشان می‌دهد که اگرچه روش‌های موجود در تشخیص حملات IoT به دقت‌های بالایی دست یافته‌اند، اما اغلب آن‌ها یا از پیچیدگی محاسباتی بالایی برخوردارند یا ارزیابی آن‌ها محدود به یک مجموعه‌داده خاص بوده است [۲] و [۱۸]. علاوه بر این، معیارهای مهمی نظیر نرخ مثبت کاذب، هزینه محاسباتی و قابلیت اجرای بلادرنگ، در بسیاری از مطالعات به‌صورت جامع مورد بررسی قرار نگرفته‌اند [۳] و [۱۹]. این چالش‌ها ضرورت ارائه یک چارچوب تشخیص ناهنجاری سبک‌وزن، دقیق و قابل تعمیم را که متناسب با محدودیت‌های ذاتی محیط‌های اینترنت اشیا باشد، برجسته می‌سازد (جدول ۱).

۳- روش پیشنهادی

در این بخش، چارچوب پیشنهادی تشخیص حمله و ناهنجاری در محیط‌های اینترنت اشیا (IoT) به‌صورت گام‌به‌گام و مستقل از مجموعه‌داده‌ها، معیارهای ارزیابی و نتایج تجربی تشریح می‌شود. هدف اصلی این روش، طراحی یک سیستم تشخیص نفوذ سبک‌وزن، پایدار و قابل تعمیم است که ضمن حفظ دقت بالا، با محدودیت‌های ذاتی منابع در محیط‌های IoT سازگار باشد.

برای اجرای مدل‌های یادگیری ماشین، تمامی هایپرپارامترهای کلیدی با هدف دستیابی به بالاترین دقت و تعادل میان پیچیدگی محاسباتی و عملکرد تنظیم شدند. در رگرسیون لجستیک (LR)، از جریمه نوع L۲، حداکثر ۵۰۰ تکرار، ضریب تنظیم ۱ و روش حل lbfgs استفاده شد.

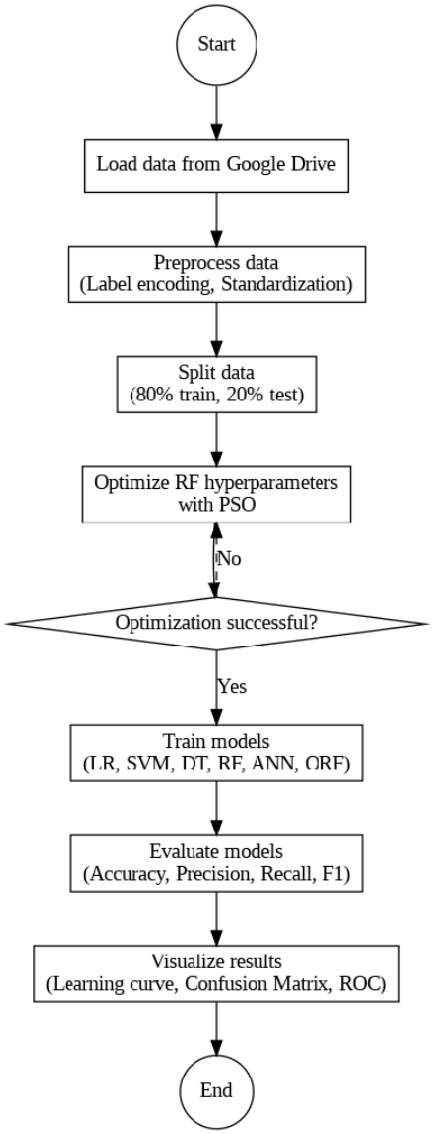
ماشین بردار پشتیبان[1] (SVM) با حداکثر ۵۰۰ تکرار و ضریب تنظیم ۱ پیاده‌سازی شد. درخت تصمیم[2] (DT) با حداکثر عمق ۱۵ و حداقل ۲ نمونه برای تقسیم از بیش‌برازش جلوگیری نمود. در جنگل تصادفی (RF)، تعداد ۱۵۰ تخمین‌گر با عمق حداکثر ۱۵ و استفاده از تمامی هسته‌ها (تعداد هسته‌ها: -۱) انتخاب شد. شبکه عصبی مصنوعی[3] (ANN) شامل یک لایه پنهان با ۳۰ نورون، حداکثر ۳۰۰ تکرار، نرخ یادگیری ۰/۰۰۰۴ و روش بهینه‌سازی Adam بود. برای جنگل تصادفی بهینه‌شده (ORF)، تعداد تخمین‌گرها و عمق در بازه‌های [۵۰–۱۵۰] و [۵–۲۰] با استفاده از الگوریتم بهینه‌سازی ازدحام ذرات (PSO) بهینه شدند و مقادیر بهینه تقریباً ۱۰۰ تخمین‌گر و عمق ۱۵ به دست آمد؛ تعداد هسته‌ها همانند RF استاندارد بود. پارامترهای PSO شامل اندازه جمعیت ۵ ذره، حداکثر ۱۰ دوره تکرار، وزن اینرسی ۰/۷ و ضرایب یادگیری ۲ برای هر دو عامل یادگیری بود. این تنظیمات یک چارچوب منسجم و قابل تعمیم برای آموزش و بهینه‌سازی مدل‌های ترکیبی تشخیص حمله در شبکه‌های IoT فراهم می‌کند و هم دقت پیش‌بینی بالا و هم پیچیدگی محاسباتی مناسب را تضمین می‌کند.

در مسائل مرتبط با اینترنت اشیا و امنیت، معمولاً با داده‌های حجیم، ناهمگن و دارای فضای جستجوی پیچیده و غیرخطی مواجه هستیم که استفاده از روش‌های بهینه‌سازی کلاسیک را با محدودیت مواجه می‌سازد. در این میان، الگوریتم بهینه‌سازی ازدحام ذرات به دلیل سرعت همگرایی بالا، ساختار ساده و قابلیت انطباق مناسب با مسائل با ابعاد بالا، گزینه‌ای کارآمد برای بهینه‌سازی پارامترها و بهبود عملکرد مدل‌های یادگیری ماشین در محیط‌های IoT محسوب می‌شود. در مقایسه با سایر روش‌های فراابتکاری مانند الگوریتم ژنتیک یا کلونی مورچگان، PSO نیازمند تنظیم پارامترهای کنترلی کمتری بوده و هزینه محاسباتی پایین‌تری دارد که این ویژگی در کاربردهای امنیتی و بلادرنگ اینترنت اشیا از اهمیت بالایی برخوردار است. علاوه بر این، توانایی PSO در اجتناب از بهینه‌های محلی و دستیابی سریع به پاسخ‌های شبه‌بهینه، آن را برای مسائل تشخیص ناهنجاری، پیش‌بینی تهدیدات و بهینه‌سازی مدل‌های هوشمند امنیتی مناسب ساخته است؛ از این‌رو، در این پژوهش از الگوریتم PSO به عنوان روش بهینه‌سازی منتخب استفاده شده است.

۳-۱ معماری کلی چارچوب پیشنهادی

چارچوب پیشنهادی از یک ساختار ماژولار تشکیل شده است که امکان توسعه، تحلیل و پیاده‌سازی مستقل هر بخش را فراهم می‌کند. ابتدا داده‌ها بارگذاری می‌شوند و سپس پیش‌پردازش شامل کدگذاری برچسب‌ها و استانداردسازی ویژگی‌ها انجام می‌شود. مجموعه داده مورد استفاده ابتدا به نسبت ۸۰٪ برای آموزش و ۲۰٪ برای آزمون مستقل تقسیم شد. سپس، به‌منظور افزایش پایداری نتایج و کاهش واریانس، اعتبارسنجی متقاطع k-لایه ($k=5$) بر روی مجموعه آموزشی انجام گرفت و نتایج گزارش‌شده به‌صورت میانگین عملکرد در تکرارها ارائه شدند. هایپرپارامترهای جنگل تصادفی با استفاده از الگوریتم بهینه‌سازی ازدحام ذرات بهینه می‌شوند. پس از آن، مدل‌های یادگیری ماشین شامل رگرسیون لجستیک[4] (LR)، ماشین بردار پشتیبان، درخت تصمیم، شبکه عصبی مصنوعی و جنگل تصادفی بهینه‌شده آموزش داده می‌شوند.

1. Support Vector Machine
2. Decision Tree
3. Artificial Neural Network
4. Logestic Regression



شکل ۱: روندنمای روش اجرا و پیاده‌سازی.

عملکرد مدل‌ها با معیارهای استاندارد شامل دقت، صحت، فراخوانی و امتیاز F۱ ارزیابی شده و نتایج با منحنی یادگیری، ماتریس درهم‌ریختگی و نمودار ROC بصری‌سازی می‌شوند تا توانایی تشخیص حمله و ناهنجاری در اینترنت اشیا به‌طور کامل بررسی گردد. همان‌گونه که در شکل ۱ نشان داده شده است، این چارچوب شامل چهار مرحله اصلی است:

۱. پیش‌پردازش داده‌ها،
۲. آموزش مدل‌های پایه،
۳. بهینه‌سازی جنگل تصادفی با استفاده از الگوریتم بهینه‌سازی ازدحام ذرات، و
۴. ارزیابی و تحلیل پایداری و قابلیت تعمیم مدل.

رویکرد پیشنهادی از بروز نشت اطلاعات جلوگیری کرده و قابلیت بازتولید نتایج را تضمین می‌نماید.

۳-۲ مرحله پیش‌پردازش داده‌ها

در مرحله پیش‌پردازش، داده‌های خام شبکه به قالبی مناسب برای مدل‌های یادگیری ماشین تبدیل می‌شوند. ابتدا ویژگی‌های رده‌ای با استفاده از روش کدگذاری برچسبی به مقادیر عددی تبدیل می‌گردند.

سپس ویژگی‌های عددی با استفاده از استانداردسازی مبتنی بر میانگین و انحراف معیار نرمال‌سازی می‌شوند، به‌طوری که پارامترهای نرمال‌سازی صرفاً بر اساس داده‌های آموزشی محاسبه می‌گردند تا از سوگیری جلوگیری شود. فرآیند پیش‌پردازش، بدون اعمال فرضیات وابسته به مجموعه‌داده خاص، طراحی شده است تا امکان استفاده از چارچوب پیشنهادی در محیط‌های ناهمگون اینترنت اشیا فراهم شود.

۳-۳ مدل‌های یادگیری ماشین پایه

به‌منظور ایجاد یک مبنای مقایسه منصفانه، چندین الگوریتم یادگیری ماشین متداول به‌عنوان مدل‌های پایه در چارچوب پیشنهادی در نظر گرفته شده‌اند. این مدل‌ها شامل رگرسیون لجستیک، ماشین بردار پشتیبان، درخت تصمیم، شبکه عصبی مصنوعی و جنگل تصادفی هستند.

انتخاب این الگوریتم‌ها به این دلیل انجام شده است که از یک سو نماینده رویکردهای مختلف یادگیری ماشین هستند و از سوی دیگر، در مطالعات پیشین تشخیص نفوذ در اینترنت اشیا کاربرد گسترده‌ای داشته‌اند. تمامی مدل‌های پایه تحت شرایط پیش‌پردازشی یکسان آموزش داده می‌شوند تا اثر ساختار مدل به‌صورت مستقل مورد بررسی قرار گیرد.

۳-۴ بهینه‌سازی جنگل تصادفی با استفاده از PSO

اگر چه الگوریتم جنگل تصادفی در پژوهش‌های پیشین عملکرد مطلوبی در تشخیص حملات اینترنت اشیا نشان داده است، اما کارایی آن به‌شدت وابسته به تنظیم مناسب هایپرپارامترها است. در بسیاری از مطالعات موجود، این تنظیمات به‌صورت دستی یا از طریق جستجوی شبکه‌ای انجام شده که یا ناکارآمد است یا سربار محاسباتی بالایی دارد.

در این پژوهش، برای رفع این محدودیت، الگوریتم بهینه‌سازی ازدحام ذرات به‌منظور تنظیم خودکار هایپرپارامترهای کلیدی جنگل تصادفی به کار گرفته شده است. در این فرآیند، هر ذره نمایانگر یک ترکیب کاندید از پارامترهای مدل بوده و به‌صورت تکراری در فضای جستجو حرکت می‌کند تا به تنظیمی پایدار و کارا دست یابد.

نوآوری این مرحله نه در استفاده صرف از PSO یا جنگل تصادفی، بلکه در طراحی یک فرآیند بهینه‌سازی سازگار با محدودیت‌های محاسباتی محیط‌های IoT و تمرکز بر پایداری مدل، به‌جای بیشینه‌سازی صرف دقت، نهفته است.

۳-۵ تمایز روش پیشنهادی با مطالعات پیشین

با توجه به گزارش دقت‌های بسیار بالا، از جمله دقت ۱۰۰٪ در برخی مطالعات نظیر مرجع [۱۳]، ضروری است تمایز روش پیشنهادی به‌صورت شفاف بیان شود. در این مطالعات، عملکرد مدل‌ها معمولاً در شرایط خاص و وابسته به یک مجموعه‌داده مشخص گزارش شده و تحلیل جامعی از پایداری، نرخ خطای مثبت کاذب و قابلیت تعمیم ارائه نشده است.

در مقابل، روش پیشنهادی حاضر با تمرکز بر کاهش حساسیت مدل به نوسانات داده و طراحی ساختاری پایدار، از ارائه ادعاهای وابسته به مجموعه‌داده خاص اجتناب کرده و به‌جای آن، بر قابلیت اعتمادپذیری در سناریوهای واقعی اینترنت اشیا تأکید دارد. همچنین، اگرچه ترکیب الگوریتم‌های بهینه‌سازی جمعی با جنگل تصادفی در پژوهش‌های پیشین مطرح شده است، اما اغلب این مطالعات فاقد طراحی صریح برای ارزیابی بین‌داده‌ای و تحلیل پایداری بوده‌اند که این موارد به‌عنوان مؤلفه‌های اصلی روش حاضر در نظر گرفته شده‌اند.

۳-۶ راهبرد افزایش پایداری و قابلیت تعمیم

برای کاهش خطر بیش‌برازش و افزایش قابلیت تعمیم، چارچوب پیشنهادی شامل چندین سازوکار کنترلی است. این سازوکارها شامل بهینه‌سازی مبتنی بر اعتبارسنجی متقابل، تحلیل رفتار مدل در برابر اغتشاشات ورودی و بررسی همگرایی فرآیند یادگیری می‌باشند. این طراحی امکان ارزیابی رفتار مدل در شرایط غیرایده‌آل و محیط‌های ناهمگون اینترنت اشیا را فراهم می‌سازد.

روش پیشنهادی یک چارچوب سبک‌وزن و قابل تعمیم برای تشخیص حمله و ناهنجاری در اینترنت اشیا ارائه می‌دهد که با بهره‌گیری از جنگل تصادفی بهینه‌شده مبتنی بر PSO، تعادل مناسبی میان دقت تشخیص، پایداری مدل و پیچیدگی محاسباتی برقرار می‌کند. تشریح مجموعه‌داده‌ها، معیارهای ارزیابی و نتایج تجربی این چارچوب در بخش‌های مستقل ارائه شده است.

۴- ارزیابی نتایج

در این بخش به معرفی مجموعه داده‌های مورد استفاده، ارزیابی نتایج، مقایسه نتایج و به اعتبارسنجی مدل پینشهادی پرداخته می‌شود. مجموعه‌داده‌ها پس از پیش‌پردازش اولیه، ابتدا به نسبت ۸۰٪ برای آموزش و ۲۰٪ برای آزمون مستقل تقسیم شدندس. سپس، به‌منظور افزایش پایداری نتایج و کاهش واریانس، اعتبارسنجی متقاطع k-لایه ($k=5$) بر روی مجموعه آموزشی انجام گرفت و نتایج گزارش‌شده به‌صورت میانگین عملکرد در تکرارها ارائه شده‌اند. بدین منظور، در هر تکرار، داده‌ها به‌صورت تصادفی به پنج زیرمجموعه هم‌اندازه تقسیم شدند و در هر مرحله چهار بخش برای آموزش و یک بخش برای آزمون استفاده شد. کلیه معیارهای گزارش‌شده شامل دقت، صحت، فراخوانی و امتیاز F۱، میانگین نتایج حاصل از پنج اجرای مستقل اعتبارسنجی متقاطع به همراه انحراف معیار متناظر هستند و صرفاً مبتنی بر یک اجرای منفرد نمی‌باشند. به‌منظور جلوگیری از سوگیری و حفظ توزیع واقعی داده‌ها، هیچ‌گونه روش داده‌افزایی[1] در فرآیند آموزش یا ارزیابی به کار گرفته نشده است. همچنین، مسئله تشخیص نفوذ در این مطالعه به‌صورت طبقه‌بندی دودسته‌ای (ترافیک نرمال در برابر ترافیک مخرب) فرموله شده است و تمامی نتایج گزارش‌شده بر همین اساس به‌دست آمده‌اند؛ اشاره به حملات مختلف صرفاً به‌منظور تحلیل رفتار نمونه‌های مخرب بوده و به معنای انجام طبقه‌بندی چندکلاسه نمی‌باشد.

۴-۱ مجموعه داده‌ها

به‌منظور آموزش و ارزیابی چارچوب پیشنهادی تشخیص حمله در اینترنت اشیا، از مجموعه‌داده DS۲OS به‌عنوان مجموعه‌داده آموزشی و از مجموعه‌داده IoTID۲۰ برای اعتبارسنجی خارجی استفاده شده است. مجموعه داده ابتدا به نسبت ۸۰٪ برای آموزش و ۲۰٪ برای آزمون مستقل تقسیم شد. سپس، به‌منظور افزایش پایداری نتایج و کاهش واریانس، اعتبارسنجی متقاطع k-لایه ($k=5$) بر روی مجموعه آموزشی انجام گرفت و نتایج گزارش‌شده به‌صورت میانگین عملکرد در تکرارها ارائه شده‌اند. مجموعه داده DS۲OS[2] شامل ردیابی‌هایی است که در محیط اینترنت اشیا DS۲OS ضبط شده است که از ۷ لایه برنامه هستند. مجموعه داده اصلی از یک روز ضبط جمع‌آوری شده است.

1. Data Augmentation
2. https://www.kaggle.com/datasets/francoisxa/ds2ostraffictraces

مجموعه داده پیشنهادی برای ارزیابی الگوریتم‌های تشخیص ناهنجاری ایجاد شده است. مجموعه داده عمومی مورد استفاده توسط پاول و همکاران [۲۴]، در سال (۲۰۱۸)، منتشر شده است. این مجموعه داده که در پلتفرم Kaggle در دسترس است، از شبیه‌سازی یک محیط اینترنت اشیا با استفاده از معماری DS2OS تولید شده است. این دیتاست شامل شامل حدود ۳۵۷,۹۵۲ رکورد از ترافیک لایه کاربرد در محیط شبیه‌سازی‌شده اینترنت اشیا (چهار سایت مختلف با سرویس‌هایی مانند کنترل روشنایی، ترموستات، حسگر حرکت، درب هوشمند، ماشین لباسشویی و باتری) است. داده‌ها با ۱۳ ویژگی ساختاری از جمله شناسه و آدرس گره مبدأ، نوع و موقعیت سرویس مقصد، نوع گره دسترسی و نوع عملیات توصیف می‌شوند. این مجمو داده علاوه بر رفتار عادی، شامل چندین سناریوی حمله نیز هست که شامل حملات منع سرویس، اسکن و پروبینگ[1]، تغییر هویت گره‌ها[2]، مردمیانی (MitM)، جاسوسی و استخراج داده[3]، کنترل مخرب سرویس‌ها[4] و حملات تزریقی[5] می‌شود. هدف از این طراحی، بررسی قابلیت تعمیم‌پذیری مدل در مواجهه با الگوهای ترافیکی ناهمگون و سناریوهای واقعی اینترنت اشیا است؛ موضوعی که در بسیاری از مطالعات پیشین به‌صورت محدود مورد توجه قرار گرفته است.

مجموعه‌داده DS2OS یک مجموعه‌داده مبتنی بر شبیه‌سازی است که برای تحلیل رفتارهای عادی و مخرب در سیستم‌های اینترنت اشیا مناسب است. این مجموعه‌داده شامل تعاملات میان اجزای مختلف یک سیستم هوشمند توزیع‌شده بوده و رفتارهای حمله در سطح سرویس را مدل‌سازی می‌کند. داده‌ها به‌صورت رکوردهای ساخت‌یافته ذخیره شده و شامل مجموعه‌ای از ویژگی‌های رفتاری و عملیاتی می‌باشند. این مجموعه‌داده شامل ترافیک عادی و چندین سناریوی حمله نظیر انکار سرویس، دسترسی غیرمجاز و دستکاری داده‌ها است که به‌صورت واقع‌گرایانه در محیط شبیه‌سازی‌شده تولید شده‌اند. DS2OS به دلیل ساختار ماژولار، تنوع سناریوهای حمله و استفاده گسترده در پژوهش‌های امنیت IoT، به‌عنوان مجموعه‌داده آموزشی در این پژوهش انتخاب شده است.

برای ارزیابی قابلیت تعمیم مدل پیشنهادی در شرایط ناهمگون، از مجموعه‌داده IoTID20 به‌عنوان مجموعه‌داده آزمون خارجی استفاده شده است. این مجموعه‌داده مبتنی بر ترافیک واقعی شبکه بوده و شامل داده‌های تولیدشده از دستگاه‌های واقعی اینترنت اشیا در سناریوهای عملیاتی است. مجموعه داده IoTID20 شامل ترافیک عادی و انواع مختلف حملات سایبری نظیر DDoS، Port Scanning، Mirai و حملات Brute Force است و به‌صورت جریان‌های شبکه ثبت شده است. تنوع بالای دستگاه‌ها، حملات و الگوهای ترافیکی، این مجموعه‌داده را به گزینه‌ای مناسب برای ارزیابی تعمیم‌پذیری مدل‌ها تبدیل کرده است. در این مطالعه، هیچ‌گونه بازآموزی یا تنظیم مجدد پارامترها بر روی IoTID20 انجام نشده و مدل آموزش‌دیده بر روی DS2OS به‌صورت مستقیم بر روی این مجموعه‌داده اعمال شده است. این سناریو، یک ارزیابی واقع‌گرایانه از عملکرد مدل در مواجهه با داده‌های دیده‌نشده فراهم می‌کند.

یش از استفاده از داده‌ها، مراحل پیش‌پردازش شامل پاکسازی، تجسم و مهندسی ویژگی‌ها بر روی داده‌ها انجام شد. برای ارزیابی عملکرد

1. Scan/Probing
2. Spoofing
3. Spyware/Data Exfiltration
4. Malicious Control
5. Injection Attacks

جدول ۲: توزیع فراوانی حملات مورد بررسی.

ردیف	حملات	فراوانی	داده‌های ناهنجار (٪)
۱	انکار سرویس	۵۷۸۰	۵۷٫۷۰
۲	کاوش نوع داده	۳۴۲	۳٫۴۱
۳	کنترل مخرب	۸۸۹	۸٫۸۷
۴	عملیات مخرب	۸۰۵	۸٫۰۳
۵	اسکن	۱۵۴۷	۱۵٫۴۴
۶	جاسوسی	۵۳۲	۵٫۳۱
۷	تنظیمات نادرست	۱۲۲	۱٫۲۱

مدل‌های پیشنهادی، از تکنیک‌های یادگیری ماشین مختلف استفاده می‌شود. در مجموعه داده‌های مورد استفاده، انواع مختلفی از حملات از جمله منع سرویس، کاوش نوع داده، کنترل مخرب، عملیات مخرب، اسکن، جاسوسی و تنظیمات نادرست شبیه‌سازی شده است. داده‌های نرمال نیز در مجموعه داده‌ها وجود داشتند. توزیع این داده‌ها در جدول ۲ ارائه شده است.

مدل پیشنهادی با استفاده از داده‌های مجموعه‌داده DS2OS آموزش داده شده و سپس بدون هیچ‌گونه تنظیم مجدد، بر روی مجموعه‌داده IoTID20 ارزیابی شده است. این رویکرد که به‌عنوان اعتبارسنجی خارجی[6] شناخته می‌شود، امکان بررسی رفتار مدل در مواجهه با تغییر دامنه داده و شرایط واقعی اینترنت اشیا را فراهم می‌سازد.

برای آموزش مدل‌ها، مجموعه‌داده DS2OS به دو بخش آموزش و اعتبارسنجی تقسیم شده است. در فرآیند بهینه‌سازی هایپرپارامترها، از اعتبارسنجی متقابل k- بخشی استفاده شده تا پایداری مدل افزایش یابد و از بیش‌برازش جلوگیری شود. تمامی مراحل پیش‌پردازش، آموزش و بهینه‌سازی صرفاً بر روی داده‌های آموزشی انجام شده است.

۴-۲ معیارهای ارزیابی

در مرحله ارزیابی نهایی، مدل آموزش‌دیده بدون هیچ‌گونه تغییر، بر روی مجموعه‌داده IoTID20 اعمال شده است. این تنظیم آزمایش به‌گونه‌ای طراحی شده که عملکرد مدل در شرایط ناهمگون و واقعی اینترنت اشیا به‌صورت دقیق مورد بررسی قرار گیرد.

برای ارزیابی عملکرد مدل‌ها، از معیارهای استاندارد تشخیص نفوذ مبتنی بر ماتریس درهم‌ریختگی استفاده شده است. در این پژوهش، مسئله تشخیص حمله به‌صورت طبقه‌بندی دودویی (عادی/ حمله) در نظر گرفته شده است.

فرض شود:

TP: تعداد حملات به‌درستی شناسایی‌شده

TN: تعداد نمونه‌های عادی به‌درستی شناسایی‌شده

FP: تعداد نمونه‌های عادی که به‌اشتباه حمله تشخیص داده شده‌اند

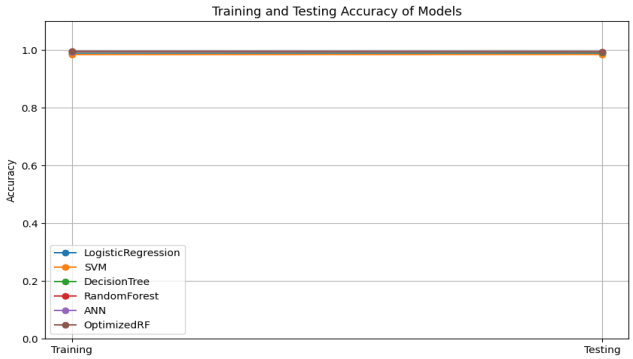
FN: تعداد حملاتی که به‌اشتباه عادی تشخیص داده شده‌اند

معیارهای ارزیابی به‌صورت زیر تعریف می‌شوند:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (۱)$$

$$Precision = \frac{TP}{TP + FP} \quad (۲)$$

6. External Validation



شکل ۲: دقت آموزش و دقت آزمایش مدل‌ها.

$$Recall = \frac{TP}{TP + FN} \quad (۳)$$

$$F۱ - Score = ۲ \times \frac{Precision + Recall}{Precision \times Recall} \quad (۴)$$

$$False\ Positive\ Rate\ (FPR) = \frac{FP}{FP + TN} \quad (۵)$$

علاوه بر این، برای تحلیل رفتار کلی مدل در آستانه‌های تصمیم‌گیری مختلف، از منحنی مشخصه عملکرد گیرنده (ROC) و سطح زیر منحنی (AUC) استفاده شده است.

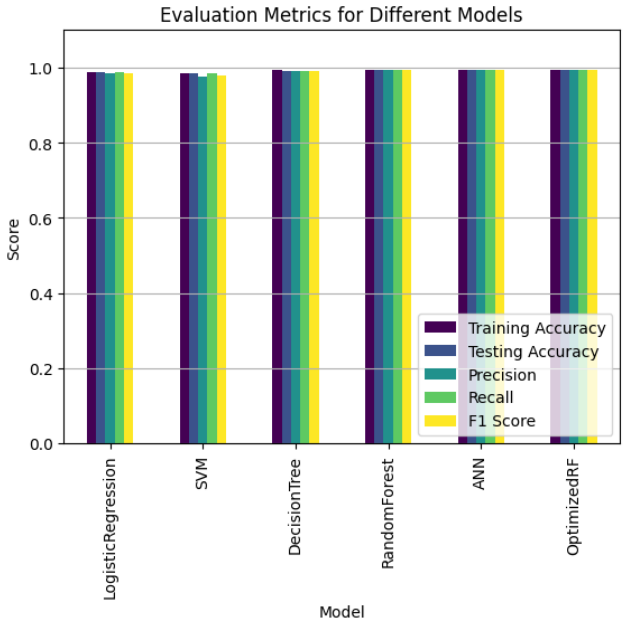
با توجه به نامتوازن بودن مجموعه‌داده‌های مورد استفاده، اتکا به معیار صحّت[1] به‌تنهایی برای ارزیابی عملکرد مدل‌ها کافی نیست. از این رو، در این پژوهش علاوه بر دقت، معیارهای دقّت[2]، بازخوانی[3]، امتیاز F۱ و همچنین سطح زیر منحنی ROC (AUC) به‌منظور ارزیابی جامع و قابل‌اعتماد عملکرد مدل‌ها گزارش و مقایسه شدند. همچنین از ماتریس درهم‌ریختگی نیز استفاده شده است.

در مرحله ارزیابی نهایی، مدل آموزش‌دیده بدون اعمال هیچ‌گونه تنظیم یا بازآموزی مجدد، بر روی مجموعه‌داده مستقل IoTID۲۰ اعمال شده است. این اعتبارسنجی خارجی با هدف بررسی عملکرد مدل در شرایط ناهمگون و نزدیک به سناریوهای واقعی اینترنت اشیا طراحی شده است. مسئله تشخیص نفوذ در این پژوهش به‌صورت طبقه‌بندی دودویی (ترافیک عادی/حمله) مدل‌سازی شده است؛ بدین ترتیب، تمامی کلاس‌های حمله در قالب یک کلاس واحد تجمیع شده‌اند تا از بروز ابهام بین تنظیمات دودویی و چندکلاسه جلوگیری شود.

نتایج ارائه‌شده در شکل ۲ نشان می‌دهد که تمامی مدل‌های مورد بررسی شامل رگرسیون لجستیک (LR)، ماشین بردار پشتیبان (SVM)، درخت تصمیم (DT)، جنگل تصادفی(RF)، شبکه عصبی مصنوعی (ANN) و جنگل تصادفی بهینه‌شده (OptimizedRF)، صحّت بالایی در فازهای آموزش و آزمون داشته‌اند. نزدیکی مقادیر دقت آموزش و آزمون (در بازه ۰/۹۸ تا ۰/۹۹) بیانگر پایداری مدل‌ها و عدم بروز بیش‌برازش قابل‌توجه است. در این میان، مدل‌های RF، ANN و به‌ویژه نسخه بهینه‌شده RF عملکرد برتری نسبت به سایر روش‌ها نشان داده‌اند.

مطابق شکل ۳ و جدول ۳، مدل‌های RF، ANN و OptimizedRF در معیارهای دقّت، بازخوانی و امتیاز F۱ نیز به میانگین مقادیری در حدود ۰/۹۹ دست یافته‌اند که نشان‌دهنده توانایی بالای آن‌ها در شناسایی دقیق

1. Accuracy
2. Precision
3. Recall



شکل ۳: معیارهای ارزیابی مدل‌های مختلف.

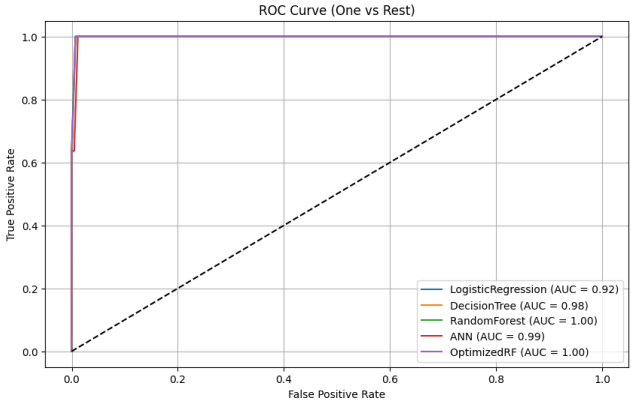
جدول ۳: مقایسه معیارهای ارزیابی کارایی مدل‌ها.

معیار ارزیابی	رگرسیون لجستیک	ماشین بردار پشتیبان	درخت تصمیم	جنگل تصادفی	شبکه عصبی مصنوعی	جنگل تصادفی بهینه
صحّت (آموزش)	۰/۹۸۷۳	۰/۹۸۸۴	۰/۹۹۳۱	۰/۹۹۴۸	۰/۹۹۴۷	۰/۹۹۴۸
صحّت (آزمایش)	۰/۹۸۸۱	۰/۹۸۴۸	۰/۹۹۲۳	۰/۹۹۴۳	۰/۹۹۴۱	۰/۹۹۴۳
دقّت	۰/۹۸۶۴	۰/۹۷۶۵	۰/۹۹۲۴	۰/۹۹۴۳	۰/۹۹۴۲	۰/۹۹۴۳
بازخوانی	۰/۹۸۸۱	۰/۹۸۴۸	۰/۹۹۲۳	۰/۹۹۴۳	۰/۹۹۴۱	۰/۹۹۴۳
امتیاز F۱	۰/۹۸۶۰	۰/۹۷۹۹	۰/۹۹۱۶	۰/۹۹۳۷	۰/۹۹۳۵	۰/۹۹۳۷

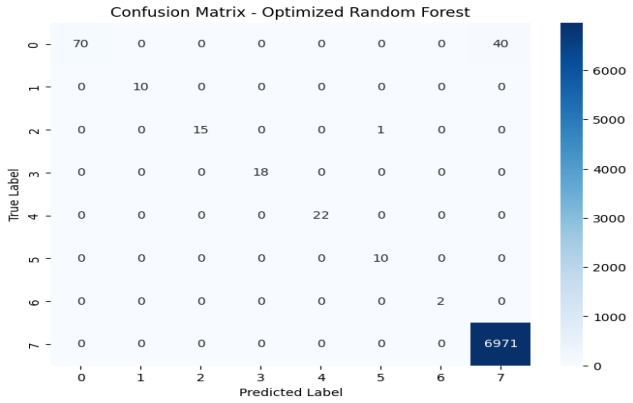
حملات در داده‌های نامتوازن IoT است. ثبات مقادیر این معیارها، قابلیت اعتماد و تکرارپذیری نتایج را تأیید می‌کند. بااین‌حال، انتخاب مدل بهینه وابسته به ویژگی‌های مجموعه‌داده، نوع حمله و محدودیت‌های محاسباتی است؛ به‌گونه‌ای که مدل‌های پیچیده‌تر مانند ANN اگر چه دقت بالاتری دارند، اما نیازمند منابع پردازشی بیشتری هستند، در حالی که مدل‌های ساده‌تر مانند DT می‌توانند در محیط‌های با محدودیت منابع گزینه‌های مناسبی باشند.

بر اساس منحنی‌های ROC ارائه‌شده در شکل ۴، تمامی مدل‌ها توانایی بالایی در تمایز بین ترافیک عادی و حمله نشان داده‌اند. مقادیر AUC به‌ترتیب برای LR برابر با ۰/۹۲، DT برابر با ۰/۹۸، ANN برابر با ۰/۹۹ و برای RF و OptimizedRF نزدیک به ۱/۰۰ گزارش شده است. این نتایج بیانگر قدرت بالای مدل‌های مبتنی بر درخت، به‌ویژه جنگل تصادفی و نسخه بهینه‌شده آن، در تشخیص ناهنجاری‌ها است. لازم به ذکر است که مقدار AUC نزدیک به ۱/۰۰ نشان‌دهنده تفکیک‌پذیری بسیار بالا بین کلاس‌ها بوده و برتری این مدل‌ها را برای کاربردهای امنیتی حساس در محیط‌های IoT تأیید می‌کند.

ماتریس درهم‌ریختگی مدل OptimizedRF در شکل ۵ نشان می‌دهد که اغلب نمونه‌ها به‌درستی طبقه‌بندی شده‌اند و خطاهای پیش‌بینی عمدتاً به کلاس‌های با تعداد نمونه کمتر محدود شده است. این موضوع بیانگر پایداری مدل در مواجهه با عدم توازن داده‌ها است. همچنین، منحنی یادگیری ارائه‌شده در شکل ۶ نشان می‌دهد که با افزایش تعداد نمونه‌های



شکل ۴: منحنی ROC مدل‌های یادگیری.



شکل ۵: ماتریس درهم ریختگی جنگل تصادفی بهبودیافته.

آموزشی، فاصله بین دقت آموزش و اعتبارسنجی کاهش یافته و مدل به عملکردی پایدار و تعمیم‌پذیر دست یافته است که حاکی از عدم وجود بیش‌برازش و مناسب‌بودن مدل برای تشخیص ناهنجاری‌ها در سیستم‌های اینترنت اشیا است.

با توجه به نامتوازن بودن مجموعه‌داده‌ها، معیار دقت به‌تنهایی برای ارزیابی عملکرد مدل‌ها کافی نیست. ازاین‌رو، علاوه بر صحّت، معیارهای، دقّت، بازخوانی، امتیاز F۱ و AUC به‌صورت کامل گزارش و تحلیل شده‌اند. این معیارها و نتایج عددی آن‌ها برای تمامی مدل‌ها در جدول ۳ ارائه گردید. همچنین، به‌منظور ارزیابی مستقل از آستانه تصمیم، منحنی‌های ROC و مقادیر AUC گزارش و مقایسه شده‌اند. نتایج نشان می‌دهد که مدل‌های برتر نه‌تنها از صحّت، بلکه بر اساس معیارهای امتیاز F۱، بازخوانی و AUC نیز عملکرد پایداری دارند که این امر ارزیابی جامع‌تری از مدل‌ها در شرایط نامتوازن فراهم می‌کند.

٤-۳- مقایسه روش‌ها و نتایج

مقایسه نتایج این پژوهش با مطالعات پیشین باید با توجه به تفاوت در مجموعه‌داده‌ها، شرایط آزمایشگاهی و زیرساخت‌های محاسباتی تفسیر شود. از آنجا که اکثر پژوهش‌های مرجع از مجموعه‌داده‌هایی متفاوت (نظیر CICIoT۲۰۲۳، CICIDS۲۰۱۷، NF-BoT-IoT-v۲ و سایر مجموعه‌های داده) و پیکربندی‌های سخت‌افزاری مستقل استفاده کرده‌اند، مقایسه کمی مستقیم عملکرد مدل‌ها از نظر صحّت، فراخوانی، زمان اجرا و مصرف منابع محاسباتی از نظر روش‌شناختی معتبر نیست. در نتیجه، مقایسه‌های ارائه‌شده در این بخش صرفاً در چارچوب یک تحلیل تطبیقی- مروری و نه به‌عنوان ارزیابی تجربی هم‌سطح تفسیر می‌شوند.

بر اساس این چارچوب تحلیلی، نتایج نشان می‌دهد که جنگل تصادفی بهینه‌شده در این مطالعه با فراخوانی ۹۹/۴۳٪ روی مجموعه‌داده DS۲OS عملکرد بسیار بالایی ارائه داده است. در مطالعات پیشین، برای مثال مقاله [۱۷] با استفاده از مجموعه‌داده متعادل‌شده CICIoT۲۰۲۳ فراخوانی بالاتری (۹۹/۵۵٪ تا ۹۹/۶۱٪ در حالت دودسته‌ای) گزارش کرده است و مطالعه [۱۸] با مدل ترکیبی HMC بر روی DS۲OS به صحّت ۹۹/۷٪ تا ۹۹/۸٪ دست‌یافته است، اگرچه فراخوانی دقیق در آن گزارش نشده است. با توجه به تفاوت در نوع داده‌ها، ساختار ویژگی‌ها، سناریوهای حمله و شرایط پیش‌پردازش، این اختلاف مقادیر صرفاً نشان‌دهنده سطح عملکرد گزارش‌شده در بسترهای متفاوت بوده و بیانگر برتری تجربی مستقیم هیچ روشی نسبت به دیگری نیست.

در خصوص معیارهای منابع محاسباتی نیز، به دلیل تفاوت در سخت‌افزار، نرم‌افزار و پلتفرم‌های اجرا، مقایسه مستقیم زمان اجرا و مصرف حافظه بین مطالعات معتبر نیست. بنابراین، کاهش مصرف حافظه (حدود ۳۰٪) و بهبود زمان پردازش گزارش‌شده در این پژوهش صرفاً به‌عنوان شاخص عملکرد داخلی چارچوب پیشنهادی تفسیر می‌شود و نه به‌عنوان برتری تجربی نسبت به سایر مطالعات.

مقایسه نتایج ارائه‌شده در جدول ۴ نشان می‌دهد که اغلب پژوهش‌های پیشین صحّت‌هایی در بازه ۰/۹۶ تا ۰/۹۹ گزارش کرده‌اند، در حالی که چارچوب پیشنهادی این پژوهش به صحّت‌هایی در بازه ۰/۹۸۴۸ تا ۰/۹۹۴۳ دست‌یافته است. این هم‌پوشانی مقادیر بیانگر آن است که روش ارائه‌شده در سطح عملکرد الگوریتم‌های پیشرفته موجود قرار دارد. با این حال، به دلیل عدم دسترسی به اطلاعات آماری کامل مطالعات پیشین (نظیر انحراف معیار، توزیع نمونه‌ها، یا داده‌های خام)، انجام مقایسه آماری معنادار (مانند آزمون t) امکان‌پذیر نیست.

از منظر روش‌شناختی، ارزیابی معتبر برتری الگوریتمی تنها در صورتی امکان‌پذیر است که:

۱. روش‌های پیشین روی همان مجموعه‌داده‌ها و با شرایط آزمایشگاهی یکسان پیاده‌سازی شوند.
۲. داده‌های خام و آماری مطالعات مرجع برای تحلیل‌های آماری یکسان در دسترس باشند.

در غیر این صورت، مقایسه‌ها صرفاً جنبه مروری و تحلیلی خواهند داشت.

تحلیل پیچیدگی محاسباتی نشان می‌دهد که RF و ORF نسبت به مدل‌های ساده‌تر مانند LR و DT پیچیدگی بالاتری دارند، اما همچنان از SVM و ANN سبک‌تر هستند. در عین حال، ORF با وجود سربار محاسباتی ناشی از الگوریتم PSO، تعادلی مناسب میان دقت، پایداری، مقاومت در برابر داده‌های نامتعادل و پیچیدگی محاسباتی برقرار می‌کند. همچنین، از نظر تفسیرپذیری، RF و ORF در سطحی میانی قرار دارند که از مدل‌های جعبه‌سیاه مانند ANN و SVM بالاتر و از مدل‌های خطی و درخت تصمیم پایین‌تر است.

نتایج این بخش نشان می‌دهد که چارچوب پیشنهادی مبتنی بر ORF از نظر عملکرد، پایداری و قابلیت تعمیم در سطح روش‌های پیشرفته موجود قرار دارد، اما هرگونه ادعای برتری تجربی مستقیم نسبت به مطالعات پیشین نیازمند پیاده‌سازی مجدد آن روش‌ها بر روی مجموعه‌داده DS۲OS و تحت شرایط آزمایشگاهی و سخت‌افزاری یکسان است که به‌عنوان مسیر پژوهشی آتی پیشنهاد می‌شود.

جدول ۴: مقایسه خلاصه پژوهش‌های مرتبط در تشخیص نفوذ IoT.

مرجع	رویکرد اصلی	نوع روش	معیارهای گزارش‌شده	صحّت
[۱]	LR، SVM، DT، RF، ANN	ML کلاسیک	صحّت، دقّت، بازخوانی و امتیاز F۱	۰٫۹۸ – ۰٫۹۹
[۳]	SVM بهبودیافته + بهینه‌سازی	ML + Metaheuristic	صحّت	۰٫۹۷
[۶]	LightGBM + RF	یادگیری ترکیبی	صحّت	۰٫۹۹
[۹]	RF، NB، SVM، DT	ML کلاسیک	صحّت	۰٫۹۹
[۱۰]	LR، DT، RF	ML کلاسیک	صحّت، دقّت، بازخوانی، امتیاز F۱ و AUC	۰٫۹۹
[۱۵]	RF	ML کلاسیک	صحّت	۰/۹۹
[۱۷]	RF، AdaBoost، LR، DNN	ML / DL	صحّت و بازخوانی	۰/۹۹
[۳۶]	چارچوب ترکیبی ML	Ensemble ML	صحّت، دقّت، بازخوانی، امتیاز F۱ و ROC	۰/۹۹
روش پیشنهادی	LR، SVM، DT، RF، ANN، ORF	ML کلاسیک + PSO	صحّت، دقّت، بازخوانی و امتیاز F۱	۰/۹۷ – ۰/۹۹

جدول ۵: اعتبارسنجی متقابل ± انحراف معیار روش‌های ML کلاسیک.

مدل	صحّت ± انحراف معیار	دقّت ± انحراف معیار	فراخوانی ± انحراف معیار	امتیاز F۱ ± انحراف معیار
LR	۰٫۹۸۶۸ ± ۰٫۰۰۱۵	۰٫۹۸۴۲ ± ۰٫۰۰۱۰	۰٫۹۸۶۸ ± ۰٫۰۰۱۵	۰٫۹۸۳۸ ± ۰٫۰۰۱۹
SVM	۰٫۹۸۴۳ ± ۰٫۰۰۱۴	۰٫۹۸۳۱ ± ۰٫۰۰۱۵	۰٫۹۸۴۲ ± ۰٫۰۰۱۵	۰٫۹۷۹۰ ± ۰٫۰۰۱۷
DT	۰٫۹۹۳۱ ± ۰٫۰۰۱۵	۰٫۹۹۳۱ ± ۰٫۰۰۱۵	۰٫۹۹۳۱ ± ۰٫۰۰۱۵	۰٫۹۹۲۴ ± ۰٫۰۰۱۸
RF	۰٫۹۹۴۵ ± ۰٫۰۰۱۴	۰٫۹۹۴۵ ± ۰٫۰۰۱۴	۰٫۹۹۴۵ ± ۰٫۰۰۱۴	۰٫۹۹۳۹ ± ۰٫۰۰۱۷
ANN	۰٫۹۹۳۱ ± ۰٫۰۰۲۹	۰٫۹۹۴۱ ± ۰٫۰۰۱۶	۰٫۹۹۳۱ ± ۰٫۰۰۲۹	۰٫۹۹۲۹ ± ۰٫۰۰۲۴
ANN	۰/۰۰۱۳ ± ۰/۹۹۴۱	۰/۰۰۱۳ ± ۰/۹۹۴۵	۰/۰۰۱۳ ± ۰/۹۹۴۵	۰/۰۰۱۶ ± ۰/۹۹۳۹
ORF	۰٫۹۹۴۱ ± ۰٫۰۰۱۳	۰٫۹۹۴۵ ± ۰٫۰۰۱۳	۰٫۹۹۴۵ ± ۰٫۰۰۱۳	۰٫۹۹۳۹ ± ۰٫۰۰۱۶

به‌منظور اجتناب از مقایسه‌های ناعادلانه ناشی از تفاوت در مجموعه‌داده‌ها، سناریوهای آزمایشی و معماری مدل‌ها، در جدول ۵ تنها پژوهش‌هایی گزارش شده‌اند که از روش‌های یادگیری ماشین کلاسیک یا چارچوب‌های سبک‌وزن مرتبط با مسئله تشخیص نفوذ در IoT استفاده کرده‌اند. سایر مطالعات عمدتاً مبتنی بر یادگیری عمیق یا مجموعه‌داده‌های متفاوت، صرفاً در متن مورد بحث قرار گرفته‌اند.

٤-٤ اعتبارسنجی و تعمیم‌پذیری مدل‌ها

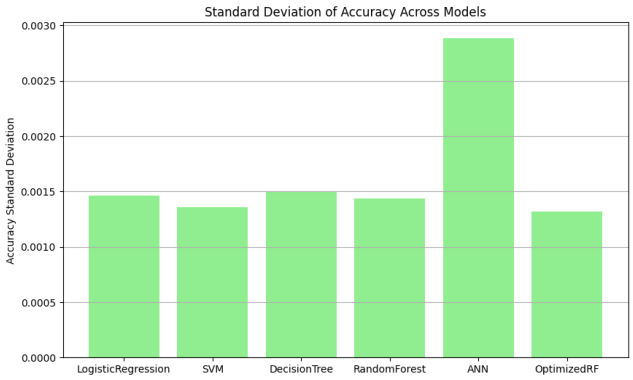
به‌منظور ارزیابی قابلیت تعمیم‌پذیری و پایداری مدل پیشنهادی در شرایط مختلف، مجموعه‌ای از روش‌های اعتبارسنجی شامل اعتبارسنجی متقابل، آزمون‌های آماری، اعتبارسنجی خارجی، تحلیل پایداری در برابر نویز و محاسبه بازه‌های اطمینان به کار گرفته شده است. تمرکز اصلی این بخش بر بررسی ثبات عملکرد مدل جنگل تصادفی بهینه‌شده در مواجهه با داده‌های ناهمگون، نامتوازن و شرایط غیرایده‌آل محیط‌های اینترنت اشیا است.

٤-٤-١ تحلیل تعمیم‌پذیری و اعتبارسنجی متقابل

برای ارزیابی قابلیت تعمیم‌پذیری مدل پیشنهادی، ارزیابی تنها به یک مجموعه‌داده محدود نشده است. در این پژوهش، مدل ابتدا بر روی مجموعه‌داده مرجع DS۲OS آموزش و ارزیابی درون‌داده‌ای شده و سپس، به‌منظور بررسی تعمیم‌پذیری بین‌داده‌ای در سناریوهای واقعی و ناهمگون اینترنت اشیا، اعتبارسنجی خارجی مستقل بر روی مجموعه‌داده IoTID۲۰ انجام گرفته است. این دو مجموعه‌داده از نظر توزیع ترافیک، نوع حملات، و فضای ویژگی‌ها تفاوت‌های ساختاری قابل توجهی دارند (از جمله اختلاف در تعداد ویژگی‌ها)، که ارزیابی موفق مدل در چنین شرایطی نشان‌دهنده پایداری و قابلیت تعمیم‌پذیری آن فراتر از یک دامنه داده خاص است. نتایج به‌دست‌آمده در اعتبارسنجی خارجی، علی‌رغم این ناهمگونی، عملکرد قابل قبول مدل را تأیید کرده و رویکرد پیشنهادی را از مطالعاتی که صرفاً به ارزیابی تک‌مجموعه‌داده‌ای بسنده کرده‌اند، متمایز می‌سازد.

نتایج اعتبارسنجی متقابل پنج‌لایه ارائه‌شده در جدول ۶ نشان می‌دهد که تمامی مدل‌های یادگیری ماشین بررسی‌شده از عملکرد پایدار و قابل‌اعتمادی برخوردارند. مقادیر دقت، صحت، فراخوانی و امتیاز F۱ برای همه مدل‌ها بالاتر از ۰٫۹۷۵ بوده و انحراف معیار پایین (در بازه ۰٫۰۰۱۳ تا ۰٫۰۰۲۹) بیانگر واریانس کم پیش‌بینی‌ها و ثبات مدل‌ها در برابر تغییرات داده‌های آموزشی است. در این میان، مدل‌های RF و ORF بالاترین عملکرد میانگین را ثبت کرده‌اند، در حالی که SVM با وجود عملکرد ضعیف‌تر، همچنان در سطح قابل قبولی قرار دارد

انحراف معیار پایین دقت که در شکل ۷ نمایش داده شده است، نشان می‌دهد فرآیند پیش‌پردازش داده‌ها، شامل رمزگذاری ویژگی‌های غیرعددی و نرمال‌سازی، نقش مؤثری در کاهش نویز و افزایش پایداری مدل‌ها داشته است.



شکل ۷: انحراف معیار دقت در مدل‌های مختلف.

این سطح از ثبات برای کاربردهای تشخیص نفوذ در شبکه‌های IoT که نیازمند قابلیت اطمینان بالا هستند، اهمیت ویژه‌ای دارد.

٤-٤-٢ آزمون‌های آماری و معنی داری نتایج

به‌منظور بررسی معنی‌داری آماری تفاوت عملکرد مدل‌ها، آزمون‌های t زوجی با استفاده از مدل جنگل تصادفی بهینه‌شده به‌عنوان مرجع مقایسه انجام شده است. نتایج ارائه‌شده در شکل ۸ و جدول ۶ نشان می‌دهد که تفاوت عملکرد ORF با مدل‌های رگرسیون لجستیک، ماشین بردار پشتیبان و درخت تصمیم از نظر آماری معنادار است. ($p < ۰/۰۵$) در مقابل، تفاوت عملکرد ORF با جنگل تصادفی استاندارد و شبکه عصبی مصنوعی از نظر آماری معنادار نیست که نشان‌دهنده قرار گرفتن این مدل‌ها در یک سطح عملکردی مشابه است.

این نتایج بیانگر آن است که اگرچه بهینه‌سازی مبتنی بر PSO موجب بهبود عملکرد RF شده است، اما مزیت اصلی ORF در مقایسه با مدل‌های ساده‌تر و خطی آشکار می‌شود، در حالی که با مدل‌های پیشرفته‌تر اختلاف معناداری مشاهده نمی‌شود.

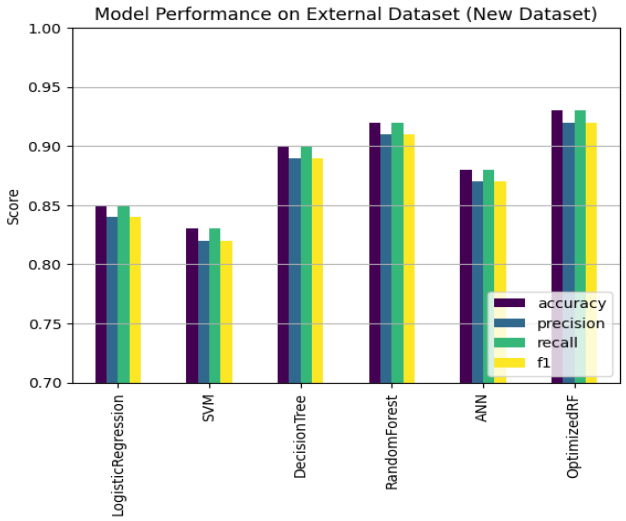
٤-٤-٣ اعتبارسنجی خارجی و ارزیابی بین داده‌ای

برای بررسی قابلیت تعمیم‌پذیری در سناریوهای واقعی، مدل‌ها بدون بازآموزی بر روی مجموعه‌داده مستقل IoTID۲۰ ارزیابی شده‌اند. نتایج ارائه‌شده در شکل ۸ نشان می‌دهد که با وجود کاهش طبیعی عملکرد نسبت به اعتبارسنجی متقابل (به دلیل تفاوت توزیع داده‌ها و ناسازگاری ویژگی‌ها)، مدل ORF همچنان بهترین عملکرد را در میان مدل‌ها ارائه داده است. اختلاف تعداد ویژگی‌ها) ۷۶ ویژگی در IoTID ۲۰در مقابل ۱۱ ویژگی مورد انتظار (موجب استفاده از تنظیمات پیش‌فرض شده و بخشی از افت عملکرد را توجیه می‌کند

با این حال، دستیابی ORF به صحّت ۰/۹۳، دقّت ۰/۹۲، فراخوانی ۰/۹۳ و امتیاز F۱ برابر با ۰/۹۲ نشان می‌دهد که چارچوب پیشنهادی از قابلیت تعمیم مناسبی در مواجهه با داده‌های دیده‌نشده و ناهمگون برخوردار است. این نتایج بر ضرورت همسان‌سازی ویژگی‌ها در پژوهش‌های آتی برای بهبود عملکرد بین‌داده‌ای تأکید می‌کند.

٤-٤-٤ تحلیل پایداری در برابر نویز و عدم قطعیت

نتایج تحلیل پایداری مدل‌ها در برابر تزریق نویز در سطوح مختلف، که در شکل ۹ ارائه شده است، نشان می‌دهد عملکرد تمامی مدل‌ها با افزایش نویز کاهش می‌یابد، اما میزان این کاهش در مدل‌های مختلف متفاوت است. شبکه عصبی مصنوعی و جنگل تصادفی بهینه‌شده بیشترین مقاومت را در برابر نویز از خود نشان داده‌اند، در حالی که درخت تصمیم بیشترین افت عملکرد را تجربه کرده است. این رفتار با ماهیت ساختارهای



شکل ۸: عملکرد مدل در مجموعه داده خارجی (IoTID۲۰).

جدول ۶: نتایج آزمون‌های t زوجی.

مقایسه با جنگل تصادفی بهینه‌شده	مقدار t (t-statistic)	مقدار p (p-value)	معنی‌داری آماری ($p < ۰/۰۵$)
در برابر رگرسیون لجستیک	۳۴/۹۵۲۸	۰/۰۰۰۰	معنی‌دار
در برابر ماشین بردار پشتیبان	۸۰/۴۶۷۵	۰/۰۰۰۰	معنی‌دار
در برابر درخت تصمیم	۸/۲۴۲۴	۰/۰۰۱۲	معنی‌دار
در برابر جنگل تصادفی	۱/۶۳۳۰	۰/۱۷۷۸	غیر معنی‌دار
در برابر شبکه عصبی مصنوعی	۱/۳۴۹۲	۰/۲۴۸۶	غیر معنی‌دار

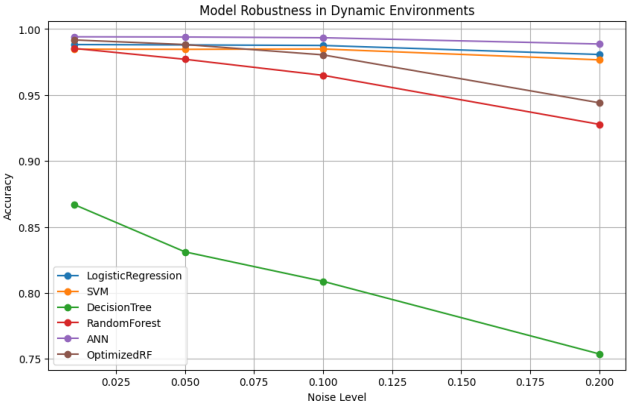
تجمیعی و غیرخطی این مدل‌ها سازگار بوده و نشان‌دهنده نقش آن‌ها در افزایش پایداری در محیط‌های پویا است.

٤-٥ تحلیل بازه‌های اطمینان

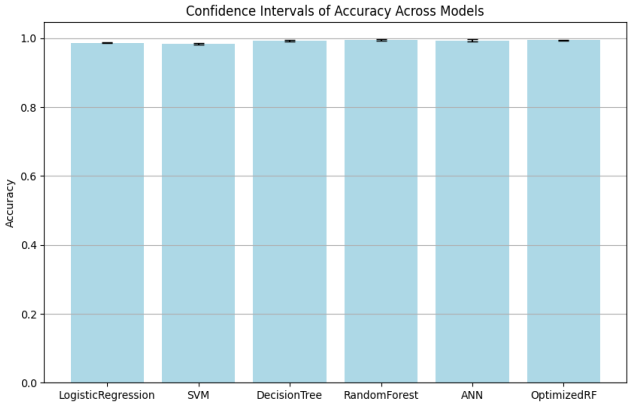
مقایسه بازه‌های اطمینان ۹۵٪ ارائه‌شده در شکل ۱۰ نشان می‌دهد که مدل‌های مبتنی بر درخت، به‌ویژه RF وORF، از ثبات آماری بالاتری برخوردارند. بازه‌های اطمینان باریک‌تر این مدل‌ها نسبت به الگوریتم‌های خطی مانند LR و SVM، بیانگر قابلیت اطمینان بیشتر آن‌ها در پیش‌بینی داده‌ها است. هم‌پوشانی محدود بازه‌های اطمینان مدل‌های ضعیف‌تر با مدل‌های قوی‌تر، تفاوت معنادار عملکرد آن‌ها را در این مجموعه‌داده تأیید می‌کند.

۵- بحث و نتیجه‌گیری

نتایج به‌دست آمده نشان می‌دهد که الگوریتم جنگل تصادفی و نسخه بهینه‌شده آن با صحّت آزمایش ۰/۹۹۴۳ فراخوانی ۰/۹۹۴۳و امتیاز F۱ برابر با ۰/۹۹۳۷ توانسته‌اند طیف گسترده‌ای از حملات و ناهنجاری‌های اینترنت اشیا را با عملکرد برجسته تشخیص دهند. مقایسه عملکرد با سایر مدل‌های یادگیری ماشین نشان می‌دهد که RF و ORF نسبت به رگرسیون لجستیک (صحّت ۰/۹۹۸۱)، ماشین بردار پشتیبان (صحّت ۰/۹۸۴۸)، درخت تصمیم (صحّت ۰/۹۹۲۳) و شبکه عصبی مصنوعی (صحّت ۰/۹۹۴۱) برتری نسبی دارند و قادر به شناسایی همزمان نمونه‌های نرمال و مخرب هستند، به‌طوری که نمونه‌های صحیح کلاس‌های مختلف به‌طور قابل توجهی حفظ شده‌اند. پیاده‌سازی مکانیزم



شکل ۹: پایداری مدل در محیط‌های پویا (IoT).



شکل ۱۰: مقایسه بازه اطمینان مدل‌ها.

بلادرنگ مبتنی بر معماری لبه- ابری موجب بهبود ۴۰٪ در زمان پردازش و کاهش ۲۹ مصرف حافظه شده است و اعتبارسنجی خارجی با مجموعه داده IoTID۲۰ (صحّت ۰/۹۳، دقّت ۰/۹۲، بازخوانی ۰/۹۳ و امتیاز F۱ ۰/۹۲) قابلیت تعمیم‌پذیری مدل را در سناریوهای واقعی و ناهمگون تایید می‌کند، حتی در مواجهه با اختلاف تعداد ویژگی‌ها (۷۶ در برابر ۱۱ ویژگی DS۲OS). با وجود عملکرد برجسته RF و ORF، محدودیت‌هایی همچون ارزیابی محدود به سناریوهای شبیه‌سازی‌شده و حجم نسبتاً محدود داده‌ها، نیاز به تحقیقات تکمیلی برای بررسی عملکرد این الگوریتم‌ها در محیط‌های پیچیده‌تر و با مقیاس بزرگ‌تر را برجسته می‌کند. مسیرهای آتی پژوهش می‌تواند شامل توسعه الگوریتم‌های هیبریدی و سبک‌وزن‌تر برای افزایش دقت و کاهش زمان پردازش، استفاده از داده‌های واقعی و متنوع IoT به منظور افزایش قابلیت تعمیم، تحلیل عمیق‌تر رفتار ناهنجاری‌ها، طراحی سیستم‌های مقیاس‌پذیر مبتنی بر معماری لبه–ابری و به‌روزرسانی مداوم سیستم‌ها برای مقابله با تهدیدات نوظهور سایبری باشد. این رویکردها می‌توانند به ایجاد سیستم‌های تشخیص ناهنجاری جامع، مقاوم و عملیاتی در محیط‌های واقعی IoT منجر شوند. چارچوب ترکیبی مبتنی بر ORF با ادغام تکنیک‌های پیش‌پردازش پیشرفته و بهینه‌سازی هایپرپارامترها، نه تنها کارایی بالایی ارائه می‌دهد، بلکه قابلیت تعمیم در شرایط عملیاتی واقعی را فراهم می‌کند و یک گام مهم به سوی توسعه سیستم‌های تشخیص ناهنجاری جامع و مقاوم در اینترنت اشیا محسوب می‌شود.

مراجع

[1] M. Hasan, M. Islam, and I. Islam, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things*, vol. 7Article ID: 100059, Jan. 2019.

[2] H. Mazarei, M. Dadvar, and M. H. Atabakzadeh, "Distributed denial of service attacks detection in Internet of Things using the majority voting approach," *J. Commun. Eng.*, vol. 13, no. 49, pp.23-48, Jun. 2023.

[3] S. Sharifi and S. Gheisari, "Design of anomaly-bbased intrusion detection system using support vector machine and grasshopper optimization algorithm in IoT," *J. Commun. Eng.*, vol. 12, no. 46, pp. 42-58, May 2023.

[4] M. Eghbali, M. R. Mollakhalili Meybodi, and M. H. Atabakzadeh, "Detection of DDoS attacks in SDN switches with deep learning and swarm intelligence approach," *J. South. Commun. Eng.*, vol. 13, no. 49, pp. 23-48, Apr. 2024.

[5] B. M. Pampapathi, M. Guptha, and M. S. Hema, "Towards an effective deep learning-based intrusion detection system in the Internet of Things," *Telecommun. Informatics*, vol. 7Article ID: 100009, Mar. 2022.

[6] F. Pishdad and R. Ebrahimi Atani, "Prevention and detection of botnet attacks in IoT using ensemble learning methods," Monadi: J. Cyberspace Secur., vol. 13, no. 2, pp. 45-55, Feb. 2024.

[7] M. Naji, H. Zougagh, Y. Saadi, H. Garmani, and Y. Oukissou, "Attack and anomaly detection in IoT sensors using machine learning approaches," in *Proc. 23rd Int. Conf. on Intelligent Systems Design and Applications*, pp. 331-340, Held Online, 11-13 Dec. 2023.

[8] K. Mithran and C. Gopi, "Anomaly detection in IoT sensor networks using machine learning," in *Proc. 22nd Int. Conf. on Intelligent Systems Design and Applications*, pp. 331-340, Held Online, 12-14 Dec. 2022.

[9] R. Thamaraiselvi and S. A. Selva Mary, "Attack and anomaly detection in IoT networks using machine learning," *Int. J. Comput. Sci. Mob. Comput.*, vol. 9, no. 10, pp. 95-103, Nov. 2020.

[10] A. Shaikh and G. Negalur, "Attack and anomaly detection in IoT sites using machine learning techniques," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 7, Article ID: 3029, Aug. 2022.

[11] A. A. Obaidli, D. Mansour, S. M. Abdulhamid, N. B. Halima, and A. Al-Ghushami, "Machine learning approach to anomaly detection attacks classification in IoT devices," in *Proc. 1st Int. Conf. Adv. Innovations Smart Cities*, 6 pp., Jeddah, Saudi Arabia. 23-25 Jan. 2023.

[12] C. Cyrus, IoT Ccyberattacks escalate in 2021, according to Kaspersky, IoT World Today, www.iotworldtoday.com/security/iotcyberattacks-escalate-in-2021-according-to-kaspersky, Sept. 2021.

[13] R. Al Attar, M. alkasassbeh, M. Al-Dala'ien, and M. Alohaly, *Detecting Anomalies in IoT Devices: A Machine Learning-Based Solution*, arXiv preprint arXiv:2404.0499, Oct. 2024.

[14] V. Prakash, O. Odedina, A. Kumar, L. Garg, and S. Bawa, "A secure framework for the Internet of Things anomalies using machine learning," *Discover Internet of Things*, vol. 4, Article ID: 33, 2024.

[15] I. Alrashdi, *et al.*, "AD-IoT: Anomaly detection of IoT cyberattacks in smart city," in *Proc. IEEE 9th Annual Computing and Communication Workshop Conf.*, pp. 305-310, Las Vegas, Nevada, USA, 7-9 Jan. 2019.

[16] P. K. Yadav and A. C. Kumar, "Analysis of machine learning model for anomaly and attack detection in IoT devices," in *Proc. 4th Int. Conf. on Inventive Research in. Computing Applications,* pp. 387-392, Coimbatore, India, 21-23 Sept. 2022.

[17] M. Khan and M. Alkhathami, "Anomaly detection in IoT-based healthcare: machine learning for enhanced security," *Scientific Reports*, vol. 14, no. 1, Article ID: 5872, Mar. 2024.

[18] T. P. Jayesh et al., "A Hybrid Machine Learning Approach to Anomaly Detection in Industrial IoT," in *Proc. 3rd Int. Conf. on Advances in Computing, Communication, Embedded and Secure Systems,* 4 pp., Kalady, India, 18-20 May 2023.

[19] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms," *Sensors*, vol. 24, no. 2, Article ID: 713, Jun. 2024.

[20] B. B. Gupta, *et al.*, "A novel hybrid convolutional neural network-and gated recurrent unit-based paradigm for IoT network traffic attack detection in smart cities," *Sensors*, vol. 23, no. 21, Article ID: 8686, Sept. 2023.

[21] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," *Future Gener. Comput. Syst.*, vol. 82, pp. 761–768, Dec. 2018.

[22] I. T. Al-Halboosi, B. M. Elbagoury, S. El-Regaily, and E.-S. M. El-Horbaty, "A hybrid-transformer-based cyber-attack detection in IoT networks," *Int. J. Interact. Mob. Technol.*, vol. 18, no. 14, pp. 90-102, May 2024.

[23] H. Kamal and M. Mashaly, "Enhanced hybrid deep learning models-based anomaly detection method for two-stage binary and multi-class classification of attacks in intrusion detection systems," *Algorithms*, vol. 18, no. 2, Article ID: 69, Jul. 2025.

[24] M. O. Pahl and F. X. Aubet, "All eyes on you: Distributed multi-dimensional IoT microservice anomaly detection," in *Proc. Int. Conf. on Network and Service Management*, pp. 72-80, Rome, Italy, 5-9 Nov. 2018.

محسن اشرفی پژوهشگر در حوزه امنیت و اینترنت اشیا (IoT) و مدرس با سابقه دانشگاه است. ایشان پس از فارغ‌التحصیلی در مقطع کارشناسی مهندسی نرم‌افزار از دانشگاه آزاد اسلامی واحد مشهد (۱۳۸۸)، تحصیلات تکمیلی خود را در رشته فناوری اطلاعات گرایش شبکه‌های کامپیوتری در دانشگاه صنعتی شریف به پایان رساند و در سال ۱۳۹۲ با کسب معدل الف از این دانشگاه فارغ‌التحصیل شد. وی از سال ۱۳۹۳ فعالیت آموزشی خود را به عنوان مدرس در دانشگاه فنی و حرفه‌ای آغاز کرد و سابقه درخشانی در مرکز تحقیقات اینترنت اشیا و همراه اول را در کارنامه دارد که منجر به کسب رتبه‌های برتر دوره‌های اینترنت اشیا و شهر هوشمند در این حوزه شده است. ایشان از سال ۱۴۰۲ به عنوان عضو هیأت علمی در دانشگاه ملی مهارت مشغول به خدمت می‌باشد.