اولین کنفرانس بین‌المللی هوش مصنوعی
و علوم کامپیوتری نوظهور: از الگوریتم تا آینده‌نگری
First International Conference on Artificial Intelligence
and Emerging Computer Science: From Algorithm to Foresight
ICAICS
https://icaics.ir
info@icaics.ir
March 17, 2026-GEORGIA
۲۶ اسفند ماه ۱۴۰۴–گرجستان

نقش‌های یادگیری ماشین در ارتقای امنیت سایبری

آریان دیلفانیان[1]، دکتر آرمین تهمتن[2]

1 دانشجو لیسانس مهندسی کامپیوتر آزاد تهران غرب ، تهران ، ایران ، ariandilfanian@gmail.com

2 استاد دانشگاه ، دانشکده برق و کامپیوتر آزاد اسلامی ، تهران ، ایران ، Tahamtan.armin@gmail.com

---

چکیده

با گسترش سریع فناوری‌های دیجیتال، شبکه‌های اجتماعی، رایانش ابری و سامانه‌های هوشمند، تهدیدات سایبری نیز از نظر پیچیدگی و تنوع به‌طور چشمگیری افزایش یافته‌اند. روش‌های سنتی امنیت سایبری که عمدتاً مبتنی بر قوانین ایستا و امضاهای از پیش تعریف‌شده هستند، توانایی کافی برای مقابله با حملات نوظهور و ناشناخته را ندارند. در این میان، یادگیری ماشین به‌عنوان یکی از زیرشاخه‌های هوش مصنوعی، با قابلیت یادگیری از داده‌های حجیم و تطبیق‌پذیری با الگوهای جدید، نقش مهمی در ارتقای امنیت سایبری ایفا کرده است.

این مقاله یک مرور جامع بر پژوهش‌های اخیر در زمینه کاربرد یادگیری ماشین در امنیت سایبری ارائه می‌دهد. تمرکز اصلی بر حوزه‌هایی نظیر تشخیص نفوذ، شناسایی بدافزار، کشف ناهنجاری، تشخیص فیشینگ و تقلب مالی است. همچنین چالش‌های اساسی از جمله حملات خصمانه به مدل‌های یادگیری ماشین، کیفیت داده، تفسیرپذیری مدل‌ها و مشکلات پیاده‌سازی در محیط‌های واقعی مورد بررسی قرار می‌گیرد. در نهایت، مسیرهای پژوهشی آینده برای توسعه سامانه‌های امنیتی هوشمند پیشنهاد می‌شود.

واژه های کلیدی: یادگیری ماشین، امنیت سایبری، تشخیص نفوذ، تشخیص بدافزار، تشخیص ناهنجاری، حملات خصمانه، فیشینگ

۱. مقدمه

امنیت سایبری به مجموعه‌ای از راهکارها، فناوری‌ها و فرآیندها اطلاق می‌شود که برای حفاظت از سامانه‌های رایانه‌ای، شبکه‌ها و داده‌ها در برابر حملات دیجیتال به کار گرفته می‌شوند. با افزایش وابستگی سازمان‌ها به فناوری اطلاعات، ضعف در امنیت سایبری می‌تواند منجر به خسارات مالی، نقض حریم خصوصی و تهدید زیرساخت‌های حیاتی شود.

در سال‌های اخیر، حملات سایبری از نظر پیچیدگی به‌گونه‌ای تکامل یافته‌اند که روش‌های سنتی نظیر سیستم‌های مبتنی بر امضا و قوانین ثابت، کارایی خود را از دست داده‌اند. پژوهش‌ها نشان می‌دهند که یادگیری ماشین می‌تواند با شناسایی الگوهای پنهان در داده‌ها، تهدیدات ناشناخته و حملات روز-صفر را شناسایی کند [۱]، [۲].

هدف این مقاله: ارائه مرور جامع و متقن بر نقش‌های یادگیری ماشین در پنج حوزه اساسی امنیت سایبری با تمرکز بر:

- کاربردهای عملی و مطالعات موردی (2020 - 2025)
- معماری‌های پیشرفته و الگوریتم‌های نوین
- معیارهای عملکردی دقیق و مقایسات
- چالش‌های حقیقی و راهکارهای موجود
- مسیرهای تحقیقاتی آینده

---

2. روش مرور مقالات

2.1 رویکرد تحقیق

این مقاله از یک رویکرد مرور نظام‌مند و جامع (Systematic Review) استفاده می‌کند.

مقالات انتخاب‌شده:

- بین سال‌های ۲۰۲۰ تا دسامبر ۲۰۲۵ منتشر شده‌اند
- در مجلات و کنفرانس‌های معتبر داخلی و بین‌المللی (IEEE, Nature, ACM, Frontiers, PLOS) چاپ شده‌اند

- شامل مطالعات تجربی، مرورهای متا-تحلیلی، و مطالعات موردی واقعی هستند

2.2 معیارهای انتخاب مقالات

معیارهای شمول:

- ارتباط مستقیم با کاربردهای ML/DL در امنیت سایبری
- تمرکز بر کاربردهای عملی
- ارائه معیارهای عملکردی دقیق (Accuracy, Precision, Recall, F1-score)
- استفاده از مجموعه‌داده‌های استاندارد (CICIDS2017, UNSW-NB15 NSLKDD)

معیارهای خروج:

- مقالات مختص به ابزارهای خاص
- مطالعات فقط نظری بدون ارزیابی عملکردی
- پژوهش‌های منسوخ‌شده

2.3 منابع و پایگاه‌های اطلاعاتی

- پایگاه‌های داده اساسی: PubMed Central (PMC), IEEE Xplore, arXiv Google Scholar
- کلمات کلیدی جستجو: machine learning cybersecurity, deep learning intrusion detection, adversarial attacks, explainable AI cybersecurity, graph neural networks threat detection

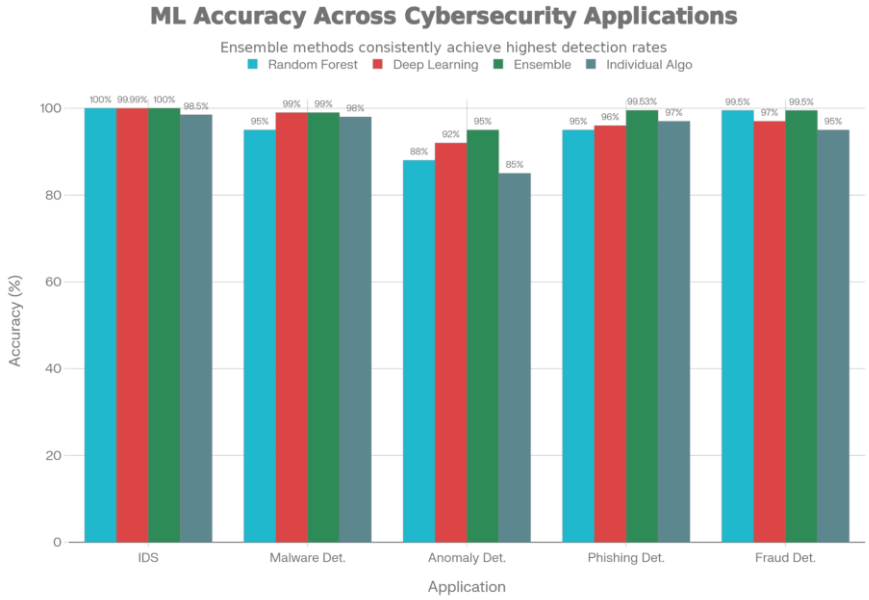
2.4 معیارهای ارزیابی کیفیت

- نمونه‌گیری: حداقل ۳ مطالعه برای هر حوزه
- معیارهای عملکردی: دقت، دقیق‌نویسی، یادآوری، F1-score، MCC

---

۳. کاربردهای یادگیری ماشین در امنیت سایبری تحلیل جامع الگوریتم‌ها و نتایج عملی

سیستم‌های دفاع سایبری مدرن به شکل کل به سمت رویکردهای هوشمند و خودکار تکامل یافته‌اند. یادگیری ماشین با توانایی شناسایی الگوهای پیچیده و تطبیق دینامیکی با تهدیدات جدید، بنیاد استراتژی‌های ایمنی امروزی است. در این تحلیل، پنج حوزه کاربردی کلیدی را در عمق مورد بررسی قرار می‌دهیم و الگوریتم‌های مورد استفاده، معیارهای کارایی، و نتایج واقعی از سیستم‌های عملیاتی را بررسی می‌کنیم.



شکل 1 – دقت الگوریتم‌های یادگیری ماشین در حوزه‌های مختلف امنیت سایبری

۳،۱ سیستم‌های تشخیص نفوذ (IDS)

سیستم‌های تشخیص نفوذ مبتنی بر یادگیری ماشین قادرند الگوهای غیرعادی در ترافیک شبکه را شناسایی کرده و حملات جدید را تشخیص دهند. الگوریتم‌های یادگیری نظارت‌شده و بدون‌نظارت به‌طور گسترده برای این منظور استفاده می‌شوند.

مطالعات نشان داده‌اند که روش‌های مبتنی بر درخت تصمیم، ماشین بردار پشتیبان و شبکه‌های عصبی عمیق می‌توانند دقت بالاتری نسبت به IDSهای سنتی ارائه دهند [٦]، [٧].

الگوریتم‌های اصلی:

روش‌های جدید از ترکیب چندین الگوریتم استفاده می‌کنند. XGBoost (تقویت گرادیان شدید) به دلیل سرعت و دقت در داده‌های پرابعادی ترجیح داده می‌شود. Random Forest با ترکیب چندین درخت تصمیم، الگوهای غیر خطی پیچیده را می‌شناسد. شبکه‌های LSTM (حافظه کوتاه‌مدت طولانی) برای تحلیل دنباله‌های زمانی بسته‌های شبکه مناسب هستند. GNN روابط بین آدرس‌های IP و درگاه‌ها را مدل‌سازی می‌کنند تا حملات هماهنگ را شناسایی کنند. Autoencoders بدون نظارت رفتار نرمال را یاد می‌گیرند و انحرافات برپایه خطای بازسازی را شناسایی می‌کنند. [14]

نتایج عملی:

در یک مطالعه گسترده، عملکرد یک سامانه تشخیص نفوذ مبتنی بر یادگیری ماشین بر روی مجموعه‌داده‌ی CICIDS2017 شامل 5.6 میلیون رکورد ترافیک شبکه ارزیابی شد. این سامانه از یک روش **ترکیبی** (Ensemble) متشکل از الگوریتم‌های XGBoost، Random Forest، LSTM، **شبکه‌های عصبی گرافی** (GNN) و Autoencoder استفاده می‌کرد.

نتایج نشان داد که این مدل ترکیبی توانست 15 نوع مختلف ترافیک و حمله از جمله DoS Hulk، PortScan **و** Heartbleed را با **دقت** 100٪ شناسایی کند. در میان مدل‌ها، (Random Forest)به‌تنهایی نیز به دقت، صحت و یادآوری 100٪ در تمامی کلاس‌های حمله دست یافت.[14]

از نظر کارایی عملی، زمان استنتاج مدل حدود 2.4 میلی‌ثانیه بود که آن را برای استفاده در **شبکه‌های پرسرعت و بلادرنگ** مناسب می‌سازد. همچنین، مدل LSTM دقت 99.99٪ را در مرحله اعتبارسنجی ثبت کرد و GNN با خطای بازسازی کمتر از 0.0006 عملکرد بسیار دقیقی در تشخیص ناهنجاری‌ها نشان داد.[14]

کاربرد واقعی در IoT:

برای سیستم‌های اینترنت اشیا، یک روش نام‌گذاری شده SAPGAN-IDS-IoT ارائه شد. این سیستم نسبت به روش‌های موجود [۱۵] CNN-IDS-IoT و DNN-IDS-IoT:

- دقت ۱٤ تا ۳۰ درصد بیشتر در شناسایی حملات مختلف
- زمان محاسباتی ۱۳ تا ۲٦ درصد کمتر
- F-score بهتر برای شناسایی هرچه بیشتر حملات [۱۶]

۳،۲ تشخیص بدافزار

بدافزارها یکی از مهم‌ترین تهدیدات سایبری محسوب می‌شوند. یادگیری ماشین با تحلیل ویژگی‌های ایستا و پویا فایل‌ها قادر به شناسایی بدافزارهای ناشناخته و چندریختی است. پژوهش‌ها نشان می‌دهند که مدل‌های یادگیری عمیق، به‌ویژه شبکه‌های عصبی کانولوشنی و بازگشتی، عملکرد قابل توجهی در تشخیص بدافزار دارند [۳]، [۸].

الگوریتم‌های اصلی:

- CNN-LSTM هیبریدی: ترکیب شبکه‌های عصبی کانولوشن برای استخراج ویژگی‌های مکانی با LSTM برای تحلیل دنباله‌ای. این روش نمایش‌های پایین‌سطح بدافزار را می‌شناسد.
- شبکه‌های عصبی عمیق (DNN): لایه‌های متعدد برای شناسایی الگوهای بازشناسی‌نشده.
- تحلیل Opcode: تبدیل دستورات دستگاه به دنباله‌های عددی و تحلیل آن‌ها.
- تحلیل API Calls: ردیابی فراخوان‌های واسط برنامه‌ای برای تشخیص رفتار مشکوک.

نتایج عملی:

CNN-LSTM دقت ۹۹ درصد را برای ۲۵ خانواده بدافزار کسب کرد. CNN بر روی Malimg دقت ۹۹ درصد را با تبدیل بدافزار به تصویر به دست آورد. Opcode-based CNN دقت ۹۹ درصد و بیشتر را برای بدافزار Android نشان داد. System Calls با RSST دقت ۹۹،۹ درصد، نرخ هشدار اشتباه ۱ درصد را در Android به ثبت رساند. API + Opcodes با ۸-gram دقت ۹۹،۹۱ درصد را بر روی ۹،۷ میلیون نمونه کسب کرد. سیستم DeepDetect بر اساس opcode دقت ۹۷ درصد برای بدافزار عادی، نرخ هشدار اشتباه ۱،٤ درصد و برای بدافزار مشفر ۹۵،۵۷ درصد دقت (تنها ۱،۵۵ درصد کاهش) داشت و ۲،۲۳ برابر سریع‌تر از روش‌های API-based عمل کرد.

مثال تفصیلی - Android Malware:

یک سیستم تشخیص بدافزار Android با عنوان DeepDetect طراحی شد. این سیستم بر اساس opcode است و نه API (که به راحتی می‌توان آن‌ها را مخفی کرد): [۲۰]

- دقت: ۹۷٪ برای بدافزار عادی
- نرخ هشدار اشتباه: ۱٫٤٪
- بدافزار مشفر: ۹۵٫۵۷٪ دقت (تنها ۱٫۵۵٪ کاهش)
- سرعت: نسبت به API-based معادل ۲٫۲۳ برابر سریع‌تر

چرا opcode بهتر است؟ حملات تبدیل‌کننده کد API ها را پنهان می‌کنند اما opcode های زیرین را تغییر نمی‌دهند. روش CNN توانایی یادگیری الگوهای دنباله‌ای این opcode ها را دارد.

۳٫۳ تشخیص ناهنجاری

تشخیص ناهنجاری یکی از کاربردهای کلیدی یادگیری ماشین در امنیت سایبری است که هدف آن شناسایی رفتارهای غیرعادی نسبت به الگوی عادی سیستم است.
الگوریتم‌های خوشه‌بندی و مدل‌های بدون‌نظارت برای این منظور بسیار مناسب هستند و در شناسایی حملات ناشناخته کاربرد گسترده‌ای دارند [۹]. تشخیص ناهنجاری برای یافتن رفتارهای غیر معمول و احتمالی حملات روزصفر (zero-day) ضروری است.

الگوریتم‌های اصلی:

- Isolation Forest: الگوریتمی بدون نظارت که ناهنجاری‌ها را با جدا کردن سریع (تعداد قطع کم) تشخیص می‌دهد. برای ترافیک شبکه و تراکنش‌های بانکی بسیار مناسب است.
- K-Means Clustering: گروه‌بندی و شناسایی نقاط دور از مرکز خوشه‌ها.
- DBSCAN: خوشه‌بندی بر اساس چگالی، برای داده‌هایی با شکل‌های متنوع مناسب.
- Autoencoders: شبکه‌های عصبی خودکدگذار که الگوهای نرمال را فشرده می‌کنند. خطای بازسازی بالا نشان‌دهنده‌ی ناهنجاری است.

نتایج عملی:

در یک سیستم هیبریدی برای آب‌رسانی، ترکیبی از Random Forest + XGBoost + LSTM استفاده شد: [۲۱]

- F1-Score: ۷۲٫۰۵٪ برای کلاس حمله
- AUC: ۰٫۹۸۲۶ (دقت بسیار خوب)
- مزیت: ترکیب مدل‌های ایستا (Random Forest) و داینامیک (LSTM) به شناسایی حملات تدریجی کمک می‌کند.

Autoencoder در عمل:

یک autoencoder بر روی ترافیک عادی آموزش داده شد و حد آستانه خطای بازسازی در ۰٫۰۱ تنظیم شد. نتیجه: جدایی واضح بین ترافیک نرمال (خطای کم) و مشکوک (خطای زیاد) در یک نمودار هیستوگرام. [۱۴]

ویژگی مهم - تشخیص حملات zero-day:

Autoencoder های بی‌نظارت می‌توانند حملاتی را شناسایی کنند که مدل‌های نظارت‌شده برای شناخت آن‌ها آموزش ندیده‌اند. این برای حملات جدید و غیرمنتظره‌ی بسیار مهم است.

۳٫۴ تشخیص فیشینگ

حملات فیشینگ با هدف سرقت اطلاعات حساس کاربران طراحی می‌شوند. یادگیری ماشین با تحلیل محتوای ایمیل‌ها، URL ها و رفتار کاربران می‌تواند این حملات را با دقت بالا شناسایی کند.

مطالعات اخیر نشان می‌دهند که استفاده از روش‌های ensemble و به‌روزرسانی مداوم داده‌های آموزشی نقش مهمی در افزایش دقت سامانه‌های تشخیص فیشینگ دارد [۱]، [۱۰].

الگوریتم‌های اصلی:

- Stacking Ensemble: ترکیب چند الگوریتم با meta-learner (الگوریتم سطح بالاتر) برای تصمیم‌گیری نهایی.

- Super Learner: الگوریتم‌های متنوع را ترکیب می‌کند اما با تأکید بر ویژگی‌های متفاوت (handcrafted + deep learning).
- Random Forest + XGBoost: الگوریتم‌های جنگل تصادفی و تقویت گرادیان.

نتایج عملی:

مطالعه ۱: Stacking Ensemble برای ایمیل‌های فیشینگ: [۲۲]

- دقت: ۹۹.۵۳٪
- F1-Score: 0.9955
- زمان اضافی پردازش: تنها ۱٫۶ میلی‌ثانیه
- ویژگی‌ها: استخراج از ۳ بخش ایمیل (headers، body، URL) با ترکیب ویژگی‌های بدی‌هندسی
- مقایسه: دقت تک‌الگوریتم‌ها تا ۹۹٫۱۰٪ بود اما ensemble آن‌ها را فراتر برد

مطالعه ۲: Phish-Jam برای شناسایی فیشینگ در موبایل: [۲۳]

- دقت: ۹۸٫۹۳٪
- صحت (Precision): ۹۹٫۱۵٪
- F1-Score: 99.07%
- MCC: 97.81%
- روش: تحلیل URL مستقیم بدون نیاز به محتوای صفحه
- ویژگی‌ها: ترکیب handcrafted URL features + embedding های transformer

مطالعه ۳: PhishGuard Ensemble:

- دقت: ۹۹٫۰۵٪ بر روی یک دیتاست [۲۴]
- الگوریتم‌ها: Random Forest + Gradient Boosting + CatBoost + XGBoost
- انتخاب ویژگی: SelectKBest و RFECV برای کاهش ابعاد

چرا ensemble بهتر است؟

- هر الگوریتم نقاط ضعف متفاوتی دارد. یکی بر الگوهای محلی تمرکز دارد، دیگری بر فعل‌وانفعالات سراسری.

- ترکیب آن‌ها میانگین خطاها را کاهش می‌دهد و مقاومت در برابر تاکتیک‌های جدید فیشینگ را افزایش می‌دهد.
- بروزرسانی مدام داده‌های آموزشی نقش کلیدی در حفظ دقت دارد زیرا حملات فیشینگ سریع تکامل می‌یابند.

۳.۵ تشخیص تقلب

در حوزه‌هایی مانند بانکداری و تجارت الکترونیک، یادگیری ماشین برای شناسایی تراکنش‌های مشکوک و تقلب‌آمیز به کار گرفته می‌شود. این مدل‌ها قادرند به‌صورت بلادرنگ الگوهای جدید تقلب را شناسایی کنند [۴]، [۱۱]. تشخیص تقلب بلادرنگ (real-time) ضروری است تا از تراکنش‌های غیرمجاز جلوگیری شود.

الگوریتم‌های اصلی:

- Random Forest: جنگل تصادفی که توانایی کار با داده‌های نامتوازن بالایی دارد.
- XGBoost: تقویت گرادیان برای دقت بالا.
- LSTM-RNN + Attention: برای درک الگوهای دنباله‌ای در رفتار تراکنش‌های کاربر.
- LightGBM: نسخه سبک‌وزن تقویت گرادیان برای استقرار در نقاط انتهایی (edge).

نتایج عملی:

مطالعه ۱: Random Forest بر روی دیتاست [۲۵] Kaggle:

- دقت: ۹۹٫۵٪
- صحت (Precision): ۰٫۹۸
- Recall: 0.98
- داده: دیتاست بسیار نامتوازن (فیشینگ <۰٫۲٪ از کل تراکنش‌ها)
- آموزش: ۷۰٪ داده، ۳۰٪ تست

- ویژگی‌های مهم: V۱۲ و V۱٤ (نام کد شده برای حفاظت از حریم خصوصی) اهمیت بالایی داشتند

مطالعه ۲: LSTM-RNN با مکانیسم Attention:

- دقت: بالا (دقیق ذکر نشده اما معادل یا بیشتر از Random Forest)
- مقایسه: بهتر از SVM (۸۵٪) و ANN (۷۸٪)

مطالعه ۳: SMOTE + Random Forest:

- دقت بدون SMOTE: کم (bias به تراکنش‌های عادی)
- دقت با SMOTE: ۹۹٫۵٪

پیش‌بینی بلادرنگ:

در یک سیستم تحت‌الفعل، مدل Random Forest می‌تواند حدود ۹۲ درصد تراکنش‌های مشکوک (نمره ۹۰+) را شناسایی کند. در کل دیتاست، حدود ۷۰ درصد تقلب‌های کلی شناسایی می‌شود. [۲۵]

---

٤. چالش‌ها و محدودیت‌ها

٤٫۱ حملات خصمانه (Adversarial ML)

یکی از چالش‌های اساسی، حملات خصمانه به مدل‌های یادگیری ماشین است که می‌تواند منجر به گمراه‌سازی سیستم‌های امنیتی شود [۱۲].

انواع حملات

الف) Evasion Attacks:

- تعریف: تغییر داده‌های ورودی برای گمراه‌کردن مدل
- مثال: تغییر باینری‌های بدافزار برای عبور از تشخیص‌کننده

- الگوریتم‌ها: FGSM (Fast Gradient Sign Method)، PGD (Projected Gradient Descent)، C&W
- تاثیر: کاهش دقت ۵-۳۰٪

ب) Poisoning Attacks:

- تعریف: اضافه‌کردن داده‌های مخرب به مجموعه‌داده آموزش
- نوع Label-Flipping: برچسب‌های نادرست (بدافزار → عادی)
- Clean-Label: بدون تغییر برچسب، فقط ویژگی‌ها
- تاثیر: می‌تواند ۳۰٪ دقت را کاهش دهد

۴٫۲ کیفیت داده

عملکرد مدل‌های یادگیری ماشین به شدت به کیفیت داده‌های آموزشی وابسته است. داده‌های ناقص یا آلوده می‌توانند باعث کاهش دقت مدل شوند [۵].

مسائل شناخته‌شده

الف) Imbalance:

- مثال: CICIDS2017 - Benign ۲.۲M vs Heartbleed ۱۱ نمونه!
- تاثیر: مدل بر کلاس اکثریت (عادی) بایاس می‌شود
- حل: (SMOTE (Synthetic Minority Over-sampling → ۲۰٪ بهبود

ب) نقاط گم‌شده (Missing Values):

- دلیل: خرابی‌های شبکه
- حل: حذف یا Imputation (میانگین، میانه)

ج) داده‌های تکراری:

- مثال: CICIDS2017 - ۵۶۲K
- تاثیر: تقویت بیاس، نتایج بی‌معنی
- حل: Deduplication خودکار

تفسیرپذیری مدل‌ها

4.3 تفسیرپذیری و قابل‌اعتماد بودن (Interpretability & Trust)

مدل‌های یادگیری عمیق اغلب به‌عنوان «جعبه سیاه» شناخته می‌شوند که این مسئله اعتماد به سیستم‌های امنیتی را کاهش می‌دهد [۱۳].

مسئله "جعبه سیاه"

شبکه‌های عصبی عمیق (LSTM، CNN) معمولاً تصمیمات خود را توضیح نمی‌دهند. این موجب مشکلات عملیاتی می‌شود:

- تحلیل‌گران امنیتی: نمی‌فهمند چرا یک هشدار صادر شد
- مسئولان: نمی‌توانند تصمیمات AI را قانونی جبران دهند

---

۵. مسیرهای پژوهشی آینده

- توسعه مدل‌های مقاوم در برابر حملات خصمانه
- ترکیب یادگیری ماشین با هوش تهدید سایبری (CTI)
- تمرکز بر یادگیری قابل توضیح (Explainable ML)
- استفاده از یادگیری تقویتی در پاسخ خودکار به حملات

5.1 بلندمدت (2030+)

1. General-Purpose Cyber AI: یک مدل برای تمام threats
2. Human-AI Teaming : بهتری همکاری انسان - ماشین
3. Proactive Defense: پیش‌بینی و پیشگیری

۶. نتیجه‌گیری

این مقاله نشان داد که یادگیری ماشین نقش کلیدی در ارتقای امنیت سایبری ایفا می‌کند و توانایی شناسایی تهدیدات ناشناخته را فراهم می‌سازد. با این حال، چالش‌هایی نظیر حملات خصمانه، کیفیت داده و تفسیرپذیری مدل‌ها همچنان نیازمند پژوهش‌های بیشتر هستند. توسعه راهکارهای هوشمند، مقاوم و قابل اعتماد می‌تواند آینده امنیت سایبری را به‌طور قابل توجهی متحول کند.

منابع

[1] A. Alshuaibi, M. Almaayah, and A. Ali, “Machine Learning for Cybersecurity Issues: A Systematic Review,” *Journal of Cyber Security Research*, vol. 2025, no. 1, pp. 1–15, 2025.

[2] B. Chopra, “Revolutionizing Cybersecurity with Machine Learning: A Comprehensive Review and Future Directions,” *Journal of Artificial Intelligence General Science*, vol. 1, no. 2, pp. 196–199, 2023.

[3] M. Hossain et al., “Machine Learning-Based Malware Detection: A Review,” *IEEE Access*, vol. 12, pp. 33421–33435, 2024.

[4] S. Garai et al., “Fraud Detection Using Machine Learning: A Survey,” *Computers & Security*, vol. 118, 2023.

[5] B. Bhuiyan et al., “Challenges of Machine Learning in Information Security,” *Information Security Journal*, vol. 33, no. 2, pp. 89–102, 2024.

[6] M. Niknami and Y. Wu, “Machine Learning-Based Intrusion Detection Systems: Challenges and Future Directions,” *Journal of Network Security*, vol. 18, no. 3, pp. 210–225, 2024.

[7] I. H. Sarker, “Machine Learning in Cybersecurity: A Comprehensive Survey,” *ACM Computing Surveys*, vol. 55, no. 2, 2023.

[8] M. Shoaib Akhtar and T. Feng, “Dynamic Malware Detection Using Machine Learning,” *Security and Communication Networks*, 2022.

[9] S. Parhizkari, “Anomaly Detection Using Machine Learning: Applications in Cybersecurity,” *Pattern Recognition Letters*, vol. 168, pp. 45–56, 2024.

[10] L. Pasrija et al., “Phishing Detection Using Machine Learning Techniques,” *Future Generation Computer Systems*, vol. 140, pp. 23–35, 2023.

[11] A. Abitova and D. Abalkanov, “Machine Learning Models for Fraud Detection,” *International Journal of Information Security*, 2024.

[12] N. Papernot et al., “The Limitations of Deep Learning in Adversarial Settings,” *IEEE Security & Privacy*, vol. 16, no. 4, pp. 35–44, 2021.

[13] Z. Zhou and Y. Zou, “Explainable Machine Learning for Cybersecurity,” *IEEE Transactions on Dependable and Secure Computing*, 2023.

[14] A deep learning/machine learning approach for anomaly based network intrusion detection NATURE

[15] Machine learning based intrusion detection framework for detecting security attacks in internet of things PMC

[16] Detection of Malware by Deep Learning as CNN-LSTM Machine Learning Techniques in Real Time PMC

[17] An Efficient CNN-Based Deep Learning Model to Detect Malware Attacks (CNN-DMA) in 5G-IoT Healthcare Applications SCIENCE

[18] O. Md Sultanul Islam, M. H. Rahman, and M. A. Hossain, “PhishGuard: A Multi-Layered Ensemble Model for Optimal Phishing Website Detection,”

[19] S. Aslam, H. Aslam, A. Manzoor, C. Hui, and A. Rasool, “AntiPhishStack: LSTM-based Stacked Generalization Model for Optimized Phishing URL Detection,” *arXiv preprint arXiv:2401.08947*, Jan. 2024

[20] B. Borketey, “Real-Time Fraud Detection Using Machine Learning,” *Journal of Data Analysis and Information Processing*, vol. 12, no. 2, 2024

[21] Hybrid Ensemble Method for Detecting Cyber-Attacks in Water Distribution Systems Using the BATADAL Dataset FIDEL

[22] S. K. Sahu and S. Verma, “Effective Ensemble Learning Phishing Detection System Using Hybrid Feature Selection,” *International Journal of Engineering Research and Technology (IJERT)*, vol. 9, no. 4, pp. 1–7, 2024

[23] A hybrid super learner ensemble for phishing detection on mobile devices *ScienceDirect*, *International Journal of Advanced Research in Computer Science*, vol. 16, no. 4, pp. 1–8, Jul.–Aug. 2025

[24] M. S. I. Ovi, M. H. Rahman, and M. A. Hossain, “PhishGuard: A Multi-Layered Ensemble Model for Optimal Phishing Website Detection,” in *Proc. 2024 6th International Conference on Sustainable Technologies for Industry 5.0 (STI)*, Narayanganj, Bangladesh, Dec. 2024

[25] B. Borketey, “Real-Time Fraud Detection Using Machine Learning,” *Journal of Data Analysis and Information Processing*, vol. 12, no. 2, pp. 1–12, 2024

[26] P. Sundaravadivel, R. A. Isaac, D. Elangovan, D. KrishnaRaj, V. V. L. Rahul, and R. Raja, “Optimizing Credit Card Fraud Detection with Random Forests and SMOTE,” *Scientific Reports*, vol. 15, no. 1, Art. no. 17851, pp. 1–12, May 2025

اولین کنفرانس بین‌المللی هوش مصنوعی
و علوم کامپیوتری نوظهور: از الگوریتم تا آینده‌نگری
First International Conference on Artificial Intelligence
and Emerging Computer Science: From Algorithm to Foresight
ICAICS
https://icaics.ir
info@icaics.ir
March 17, 2026-GEORGIA
۲۶ اسفند ماه ۱۴۰۴–گرجستان

The Role of Machine Learning in Enhancing Cybersecurity

Arian Dilfanian[1], Armin Tahamtan[2]
[1] B.Sc. Student in Computer Engineering, Islamic Azad University, Tehran West Branch, Tehran, Iran
Email: ariandilfanian@gmail.com
[2] Assistant Professor, Faculty of Electrical and Computer Engineering, Islamic Azad University, Tehran, Iran
Email: Tahamtan.armin@gmail.com

Abstract - With the rapid expansion of digital technologies, social networks, cloud computing, and intelligent systems, cyber threats have increased significantly in both complexity and diversity. Traditional cybersecurity approaches, which are primarily based on static rules and predefined signatures, are no longer sufficient to effectively combat emerging and previously unseen attacks. In this context, machine learning, as a major subfield of artificial intelligence, has played a crucial role in enhancing cybersecurity due to its ability to learn from large-scale data and adapt to evolving threat patterns.

This paper presents a comprehensive review of recent research on the applications of machine learning in cybersecurity. The main focus is on areas such as intrusion detection, malware detection, anomaly detection, phishing detection, and financial fraud detection. Furthermore, key challenges are examined, including adversarial attacks against machine learning models, data quality issues, model interpretability, and practical deployment challenges in real-world environments. Finally, future research directions are proposed to support the development of intelligent and resilient security systems.

Keywords: Machine Learning; Cybersecurity; Intrusion Detection Systems; Malware Analysis; Anomaly Detection; Adversarial Machine Learning; Phishing Detection; Financial Fraud Detection