AILS
2026

کتابچه زمانبندی و چکیده مقالات

دومین همایش ملی کاربرد هوش مصنوعی در نظم و امنیت: با تأکید بر کشف علمی جرم

۲۶ و ۲۷ بهمن ماه ۱۴۰۴

دبیرخانه کنفرانس: دانشکده مهندسی کامپیوتر- اتاق ۱۰۶

تلفن: ۰۳۱-۳۷۹۳۵۶۴۱

رایانامه: ails@res.ui.ac.ir


بسم الله الرحمن الرحیم

فهرست:

پیش‌گفتار

در عصر تحول دیجیتال پیشرفت‌های شگرف در حوزه هوش مصنوعی امکاناتی را فراهم ساخته که می‌تواند تحولی بنیادین در فرآیندهای پیشگیری، کشف، تحلیل و مقابله با جرایم مختلف ایجاد کند. هوش مصنوعی با تحلیل داده‌های بزرگ، الگوهای پنهان در رفتارهای مجرمانه را آشکار می‌سازد، روند تصمیم‌سازی را بهبود می‌دهد و کارآیی سیستم عدالت کیفری را ارتقاء می‌بخشد. برگزاری موفقیت‌آمیز «**اولین کنفرانس ملی دوسالانه کاربرد هوش‌مصنوعی در کنترل ترافیک با تأکید بر مدیریت شهری و جاده‌ای**» که در اسفند ۱۴۰۳ به میزبانی دانشگاه اصفهان و با حمایت فرماندهی انتظامی جمهوری اسلامی ایران (فراجا) برگزار شد، موجب شد تا برگزارکنندگان این کنفرانس آن را به دید یک کنفرانس سالانه بازنگری کنند. بر همین اساس و به حمد و قوه‌ی الهی، دومین دوره‌ی این کنفرانس، با عنوان «**دومین کنفرانس ملی کاربردهای هوش مصنوعی در نظم و امنیت، با تاکید بر کشف علمی جرم**» در روزهای ۲۶ و ۲۷ بهمن ۱۴۰۴ در دانشگاه اصفهان برگزار خواهد شد.

این کنفرانس میان‌رشته‌ای فرصتی است بی‌نظیر برای گردهمایی پژوهشگران، متخصصان فناوری، مجریان قانون و ذی‌نفعان ملی تا آخرین دستاوردهای علمی و عملی خود در تقاطع دو حوزه هوش مصنوعی و جرم‌شناسی را در قالب ارائه مقالات، کارگاه‌های آموزشی و میزگردهای تخصصی به اشتراک گذاشته و چشم‌اندازهای آینده را ترسیم نمایند.

در این دوره از کنفرانس موفق به دریافت ۱۱۲ مقاله علمی کامل از پژوهشگران مختلف سراسر کشور شدیم. پس از داوری های متعدد و دقیق، ۴۱ مقاله برای ارائه در کنفرانس (۱۲ مقاله به صورت سخنرانی و ۲۹ مقاله به شکل ارائه پوستری) برگزیده شدند. پس از ارائه مقالات در کنفرانس، مقالات منتخب فارسی در مجله علمی «منادی امنیت فضای تولید و تبادل اطلاعات (افتا)» و مقالات انگلیسی منتخب در مجله‌ی Journal of Computing and Security چاپ خواهند شد. همچنین دبیرخانه کنفرانس مفتخر به دریافت ۵۲ ایده با قابلیت تبدیل به محصول کاربردی شد که مراحل اولیه داوری آنها با حمایت شهرک علمی و تحقیقاتی اصفهان برگزار گردید و از این بین ۱۲ ایده به مرحله نهایی، که در روز ۲۶ بهمن برگزار می‌گردد، راه یافتند. همچنین در این دوره از کنفرانس شاهد ارائه دستاوردهای دو میزگرد تخصصی با موضوعات «امنیت، کسب‌وکارهای اینترنتی و هوش مصنوعی» و «امنیت، جامعه، اقتصاد و هوش مصنوعی» خواهیم بود. همچنین علاقمندان می‌توانند از سخنرانی کلیدی آقای دکتر مهدی آبادی با عنوان «چالش‌ها و فرصت‌های جرم‌یابی دیجیتال در عصر مدل‌های زبانی بزرگ» و ۷ کارگاه تخصصی جذاب در دو روز کنفرانس بهره ببرند.

ما برگزارکنندگان این کنفرانس بر این باور هستیم که تداوم این کنفرانس می‌تواند بستری مناسب برای ارتقای دانش و توسعه فناوری هوش مصنوعی در کشور عزیزمان باشد و امیدواریم سال آینده شاهد مشارکت جدی‌تر پژوهشگران و حامیان در دوره سوم کنفرانس باشیم.

با آرزوی سلامت و موفقیت برای تمام علاقمندان،

دبیر علمی دومین کنفرانس ملی کاربردهای هوش مصنوعی در نظم و امنیت،

حمید مَلا

برگزارکنندگان کنفرانس

دانشکده مهندسی کامپیوتر دانشگاه اصفهان

دفتر تحقیقات کاربردی فرماندهی انتظامی استان اصفهان

فرماندهی انتظامی جمهوری اسلامی ایران

حامیان کنفرانس

- موسسه‌ی آموزشی و تحقیقاتی صنایع دفاعی
- انجمن رمز ایران
- پلیس آگاهی فرماندهی انتظامی جمهوری اسلامی ایران
- پلیس فضای تولید و تبادل اطلاعات فراجا (فتا)
- مرکز راهبردی افتا ریاست جمهوری
- مجله‌ی محاسبات و امنیت (Journal of Computing and Security)
- دو فصل‌نامه علمی منادی افتا
- مرکز مدیریت و تحلیل داده فراجا
- اتاق بازرگانی صنایع، معادن و کشاورزی استان اصفهان

حامیان علمی کنفرانس

پایگاه استنادی علوم جهان اسلام

سیویلیکا

کمیته‌ی برگزاری کنفرانس

رئیس کنفرانس: دکتر رسول رکنی‌زاده
رییس دانشگاه اصفهان

رئیس کنفرانس: سرتیپ دوم پاسدار حمید علینقیان‌پور
فرمانده انتظامی استان اصفهان

دکتر بابک صفاری
معاون پژوهشی دانشگاه اصفهان

دکتر حمید ملا
دبیر علمی کنفرانس

سرهنگ احمد اشرفی
رئیس دفتر تحقیقات کاربردی فرماندهی انتظامی
استان اصفهان

سرهنگ سید محمد صائب
مدیر پژوهشی دفتر تحقیقات کاربردی
فرماندهی نیروی انتظامی

دکتر محمدرضا شعرباف
دبیر اجرایی کنفرانس

کمیته‌ی اجرایی کنفرانس

دکتر حمید ملا
دبیر علمی کنفرانس

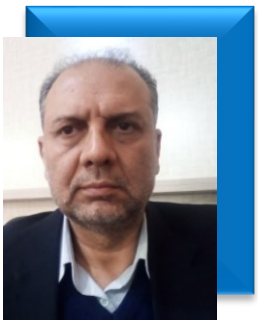
دکتر محمدرضا شعرباف
دبیر اجرایی کنفرانس

سرهنگ سید محمد صائب
مدیر پژوهشی دفتر تحقیقات کاربردی
فرماندهی نیروی انتظامی

دکتر محمدحسین باطنی
دبیر کمیته‌ی کارگاه‌ها

سرتیپ پاسدار وحید مجید
دبیر پنل‌های تخصصی
ریاست پلیس فتا فراجا

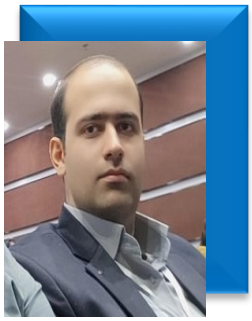
سرهنگ مهدی حیران یزدی
مدیر پژوهش دفتر تحقیقات فراجا



سرهنگ دکتر جعفر ناظرحضرت
نماینده دفتر تحقیقات فراجا

دکتر زهره بیکی
مسئول انتشارات

مهندس حمیدرضا خیرمند
مسئول دبیرخانه



مهندس عارف آیتی
مسئول انفورماتیک

کمیته‌ی علمی کنفرانس

دکتر محمدرضا خیام باشی
هیئت علمی دانشکده مهندسی کامپیوتر
دانشگاه اصفهان

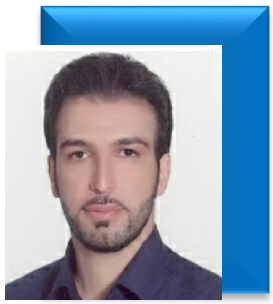
دکتر احمدرضا نقش نیلچی
هیئت علمی دانشکده مهندسی کامپیوتر
دانشگاه اصفهان

دکتر حمیدرضا برادران کاشانی
هیئت علمی دانشکده مهندسی کامپیوتر
دانشگاه اصفهان

دکتر حسین کارشناس
هیئت علمی دانشکده مهندسی کامپیوتر
دانشگاه اصفهان

دکتر علی بهلولی
هیئت علمی دانشکده مهندسی کامپیوتر
دانشگاه اصفهان

دکتر حمیدملا
هیئت علمی دانشکده مهندسی کامپیوتر
دانشگاه اصفهان



دکتر احسان مهدوی
هیئت علمی دانشکده مهندسی کامپیوتر
دانشگاه اصفهان

دکتر مرجان کائدی
هیئت علمی دانشکده مهندسی کامپیوتر
دانشگاه اصفهان

دکتر محمدرضا شعرباف
هیئت علمی دانشکده مهندسی کامپیوتر
دانشگاه اصفهان

دکتر سید محسن قائم فرد
هیئت علمی دانشکده علوم اداری و اقتصاد
دانشگاه اصفهان

دکتر قدرت اله خسروشاهی
هیئت علمی دانشکده علوم اداری و اقتصاد
دانشگاه اصفهان

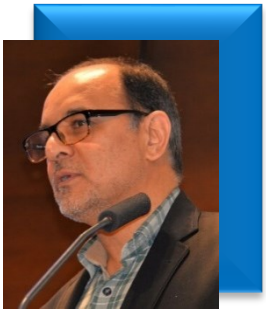
دکتر مازیار پالهنگ
هیئت علمی دانشکده مهندسی برق و کامپیوتر
دانشگاه صنعتی اصفهان

دکتر محمداحسان بصیری
هیئت علمی دانشکده فنی و مهندسی
دانشگاه شهرکرد

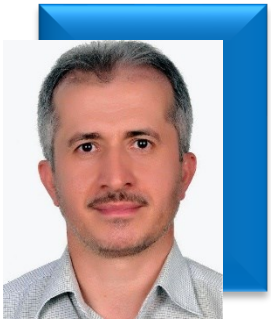
دکتر شهلا نعمتی
هیئت علمی دانشکده فنی و مهندسی
دانشگاه شهرکرد

دکتر مهران صفایانی
هیئت علمی دانشکده مهندسی برق و کامپیوتر
دانشگاه صنعتی اصفهان

دکتر رضا ابراهیمی آتانی
هیئت علمی دانشکده فنی
دانشگاه گیلان



دکتر حسین آقابابایی
هیئت علمی دانشکده حقوق
دانشگاه گیلان



دکتر محمد عبدالهی ازگمی
هیئت علمی دانشکده مهندسی کامپیوتر
دانشگاه علم و صنعت

دکتر ابراهیم صحافی زاده
هیئت علمی دانشکده سیستم های هوشمند و علوم داده
دانشگاه خلیج فارس

دکتر مهدی آبادی
هیئت علمی دانشکده مهندسی برق و کامپیوتر
دانشگاه تربیت مدرس

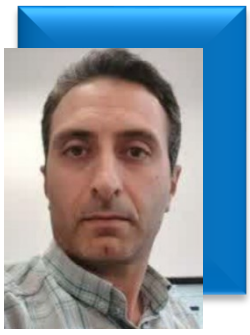
دکتر فاطمه دلدار
هیئت علمی دانشکده مهندسی برق و کامپیوتر
دانشگاه صنعتی اصفهان

دکتر طلا تفضلی
استادیار امنیت اطلاعات
پژوهشگاه فناوری اطلاعات و ارتباطات

دکتر سیدعلی اکبر صفوی
هیئت علمی دانشکده مهندسی برق و کامپیوتر
دانشگاه شیراز

دکتر صادق دری نوگورانی
هیئت علمی دانشکده مهندسی برق و کامپیوتر
دانشگاه تربیت مدرس

دکتر مجتبی خلیلی
هیئت علمی دانشکده مهندسی برق و کامپیوتر
دانشگاه صنعتی اصفهان



دکتر محمدعلی هادوی
هیئت علمی دانشکده امنیت اطلاعات
دانشگاه صنعتی مالک اشتر

دکتر امیر جلالی بیدگلی
استادیار دانشکده مهندسی برق و کامپیوتر
دانشگاه قم

دکتر حسین همائی
هیئت علمی دانشکده مهندسی برق و کامپیوتر
دانشگاه تربیت مدرس

دکتر حسین حسین زاده
هیئت علمی دانشکده حقوق
دانشگاه آزاد اسلامی واحد نجف آباد

دکتر محمدعلی اخائی
هیئت علمی دانشکده مهندسی برق و کامپیوتر
دانشگاه تهران

دکتر سمیه سلطانی
هیئت علمی دانشکده فنی و مهندسی
دانشگاه تربت حیدریه

دانشجویان همکار

محمدامین حاجیان
شهلا جعفری
محسن غلامی
عارف آیتی
پرنیان مرادی
تیام موسوی
فاطمه زاهرا فتحیان
فاطمه صیاد زاده
نگار امینی

علی طالبی
زینب جنتی
محمدرضا سعیدی
معین‌الدین علی‌حسینی
شیدا مفضلی
محمدصادق جیحانی
حنانه نوروطن
شمیم خیرمحمد

داوران کنفرانس

معصومه	اکرمی نسب
مجید	فرهادی سنگدهی
سیده مرضیه	سادات مدنی
هما	رادگهر
سید عرفان	آیتی
علی	علی حسینی
قدرت الله	خسروشاهی
رضا	ابراهیمی آتانی
ابراهیم	صحافی زاده
سمیه	سلطانی
صادق	دری نوگورانی
معین الدین	علی حسینی
دل‌آرام	نیک‌بخت
بهروز	شاهقلی قهفرخی
رضا	رمضانی
علی	بهلولی
فضل الله	ادیب نیا
امید	ترکی
حمیدرضا	برادران کاشانی
حسن	نصیرائی
مهراد	حابری
هادی	تابع الحجه
مرضیه السادات	حسینی
سید محمد	هاتفی
زهرا	زجاجی
محمدرضا	شعرباف
محمدرضا	خیام باشی
قانع	زندی
زهرا	باقری نسب
سجاد	رضایی
زهرا	سعیدی
مائده	احمدی
سجاد	کسایی
شهلا	نعمتی
محمد	عبدالهی ازگمی
فاطمه	دلدار
محمدعلی	اخایی
رسول	کیانی
محسن	غلامی
احمدرضا	منتظرالقائم
حمید	ملا
سید فخرالدین	نوربهبهانی
بهار	فراهانی
مرجان	کائدی
افسانه	فاطمی خوراسگانی
حسین	کارشناس نجف آبادی
محمدرضا	سعیدی
سید عرفان	فاطمیه
فاطمه	شفیع زادگان
سید محمد	هاتفی
منصوره	اژه‌ای
مریم	آزادمنش
علی	پارسا
سجاد	رضایی آدریانی

نویسندگان مقالات

مهدیه قطبی
محمدرضا خیام باشی
وحید مجید
امیر نوروزی
علیرضا صدیقی فرد
محمد شریفی
سرور شیدانی
سید محمد سجادیان
طلا تفضلی
سمیه فلاح
مهدی حمیدی
امین حق‌شناس ایلخچی
سعید مردانی
امیر نظامی صفا
ایلیا حکانی
پویا سلیمانی فر
معین الدین علی حسینی
فائزه غلامرضایی
امیر جلالی بیدگلی
مریم صادقی
فاطمه ترکاشوند
مریم فلاح نژاد
اردشیر کلانی
زهره بیکی

بهاره بهارمی
علی بهلولی
حسین سهلانی
محمدرضا دارابی
اکرم پسندیده
سیروس دالوند
علی علی حسینی
علی محمد قاسمی پور
فاطمه اصغری همپا
مرتضی قائدی بارده
محمدرضا خرم‌آبادی آرانی
احسان حق شناس ایلخچی
صمد سهراب
محمد پور مقدم
مجید فرهانی سنگدهی
محمدامین خورزانی
زهرا خوداد
افسانه عزیزی
علی بهلولی
محمدامین خورزانی

برنامه‌ی زمان‌بندی ایده‌شو

کاربرد هوش‌مصنوعی در نظم و امنیت

برنامه روز یکشنبه ۲۶ بهمن ماه					
ردیف	ساعت	تالار صدر (جنب کتابخانه آزادگان)	شورای ۲ (طبقه دوم ساختمان انصاری)	تالار دکتر براآنی (طبقه سوم ساختمان انصاری)	اتاق ویدئو کنفرانس (طبقه سوم ساختمان انصاری)
۱	۸:۰۰ – ۸:۳۰	پذیرش			
۲	۸:۳۰ – ۹:۲۰	افتتاحیه ایده‌شو			
۳	۹:۲۰ – ۱۱:۱۰	اجرای ایده‌شو (ارائه توسط ایده‌پردازان و نظرات داوران)			
۴	۱۱:۱۰ – ۱۱:۴۰	شبکه‌سازی و پذیرایی			
۵	۱۱:۴۰ – ۱۲:۱۰	اختتامیه (معرفی نفرات برتر، تجلیل از داوران، قرعه‌کشی بین تماشاچیان)			
۶	۱۴:۰۰ – ۱۶:۰۰		کارگاه جرم‌یابی دیجیتال سیستم‌های صنعتی – OT forensics (مرکز افتا ریاست جمهوری)	کارگاه فناوری موج میلیمتری: نمونه‌های عملی در پایش نظم و امنیت (دکتر محمدحسین باطنی)	پنل تخصص: امنیت، کسب و کارهای اینترنتی و هوش‌مصنوعی (سرهنگ نعمت الله طاهرپور)
۷	۱۶:۰۰ – ۱۸:۰۰			کارگاه طراحی و پیاده‌سازی سامانه‌های تشخیص هویت به کمک هوش مصنوعی (دکتر حامد شهبازی)	

برنامه زمان‌بندی دومین کنفرانس
کاربرد هوش‌مصنوعی در نظم و امنیت

برنامه روز دوشنبه ۲۷ بهمن ماه					
ردیف	ساعت	تالار صائب (دانشکده ادبیات)	تالار ربانی (دانشکده ادبیات)	تالار مهرعلی‌زاده (دانشکده ادبیات)	راهرو تالار صائب (دانشکده ادبیات)
۱	۷:۳۰ – ۸:۱۵	پذیرش			
۲	۸:۱۵ – ۱۰:۱۰	افتتاحیه			
۳	۱۰:۱۰ – ۱۰:۳۰	شبکه‌سازی و پذیرایی			
۴	۱۰:۳۰ – ۱۱:۱۵	سخنرانی کلیدی با موضوع: چالش‌ها و فرصت‌های جرم‌یابی دیجیتال در عصر مدل‌های زبانی بزرگ (دکتر مهدی آبادی، عضو هیئت علمی دانشگاه تربیت مدرس تهران)			
۵	۱۱:۱۵ – ۱۲	پنل تخصص: امنیت، جامعه، اقتصاد هوش‌مصنوعی (دکتر حسین حسین‌زاده، سرهنگ بازنشسته و مدرس دانشگاه)			
۶	۱۲ – ۱۳:۳۰	نهار و نماز (سالن یاس)			
۷	۱۳:۱۵ – ۱۴:۴۵	نشست اول ارائه مقالات (دکتر هادی تابع الحجه)		کارگاه فرآیند پاسخ به حادثه و جمع‌آوری شواهد دیجیتال (مهندس معظم و مهندس قنبریان)	ارائه مقالات پوستری
۸	۱۴:۴۵ – ۱۵	شبکه‌سازی و استراحت			
۹	۱۵ – ۱۶:۳۰	نشست دوم ارائه مقالات (دکتر احمدرضا منتظر القائم)	آشنایی با سیستم‌های مدیریت امنیت اطلاعات با تمرکز بر ISO 27001 (ISMS) (دکتر مهراد جباری)	ارتباط رمز ارزها، هوش‌مصنوعی و کشف جرائم (مهندس غلامرضا حیدری)	
۱۰	۱۶:۳۰ – ۱۶:۴۵	شبکه‌سازی و پذیرایی			
۱۱	۱۶:۴۵ – ۱۸:۰۰	اختتامیه			

برنامه‌ی نشست‌های ارائه مقاله‌ها

نشست ارائه مقالات S1: بازسازی، مدل‌سازی و پیش‌بینی جرایم به کمک هوش مصنوعی

(دوشنبه ۲۷ بهمن ۱۴۰۴ از ساعت ۱۳:۱۵ الی ۱۴:۴۵)

مسئولین نشست: دکتر احمدرضا منتظرالقائم

کد مقاله	زمان ارائه	عنوان مقاله	نویسندگان
ails2026-01440121	**۱۳:۱۵ – ۱۳:۳۰**	A Physics-Regularized PINN-XGBoost Framework for Accurate Bloodstain Angle-of-Impact Estimation	**مهدیه قطبی، بهاره بهرامی، علی بهلولی و محمدرضا خیام‌باشی** دانشگاه اصفهان
ails2026-01370093	**۱۳:۳۰ – ۱۳:۴۵**	مدل‌سازی ریسک کم‌اظهاری و اولویت‌بندی پرونده‌های گمرکی با استفاده از هوش مصنوعی	**افسانه عزیزی** دانشگاه رازی کرمانشاه
ails2026-01320091	**۱۳:۴۵ – ۱۴:۰۰**	پیش‌بینی نقاط پرخطر جرم با رویکرد یادگیری ماشین در چارچوب تحلیل مکانی–زمانی، با هدف پشتیبانی تصمیم‌گیری عملیاتی پلیس	**یکتا صحرایی و نسرین تلخی** دانشگاه تربیت مدرس دانشگاه علوم پزشکی شهید بهشتی دانشگاه علوم انتظامی امین
ails2026-01130070	**۱۴:۰۰ – ۱۴:۱۵**	تحلیل خوشه‌ای گروه‌های مجرمانه بر مبنای نمایش‌های گراف ناهمگن و اطلاعات متنی	**وحید یادگاری و محمد فاتحی** دانشگاه علوم انتظامی امین دانشگاه تربیت مدرس
ails2026-00450019	**۱۴:۱۵ – ۱۴:۳۰**	بازسازی صحنه‌های حریق با واقعیت افزوده برای آموزش کارکنان و تحلیل نقش انسانی در وقوع جرم: مطالعه موردی کلان‌شهر مشهد	**محمد حسین صمیمی، علی اکبر علی‌دوست، امیر راهبریان یزدی و سعید خوش روی دوست آبادی** سازمان آتش‌نشانی و خدمات ایمنی مشهد
ails2026-01070076	**۱۴:۳۰ – ۱۴:۴۵**	محاسبات مولکولی: رویکردی نوین در پزشکی قانونی جهت تحلیل همزمان چند نشانگر	**زهره بیکی** دانشگاه اصفهان

برنامه‌ی نشست‌های ارائه مقاله‌ها

نشست ارائه مقالات S2: جرم‌شناسی و جرم‌یابی دیجیتال به کمک هوش مصنوعی

(دوشنبه ۲۷ بهمن ۱۴۰۴ از ساعت ۱۵ الی ۱۶:۳۰)

مسئولین نشست: دکتر هادی تابع‌الحجه

کد مقاله	زمان ارائه	عنوان مقاله	نویسندگان
ails2026-01470107	۱۵:۰۰ – ۱۵:۱۵	**بررسی جرم‌شناختی ارتکاب جرم با کمک هوش مصنوعی**	**زهرا سامان، مهرداد تیموری** دانشگاه آزاد اسلامی واحد تبریز
ails2026-01250087	۱۵:۱۵ – ۱۵:۳۰	Framework for Real-Time Detection of Fileless Malware Using Machine Learning Memory Forensics	**پویا سلیمانی‌فرو سرور شیدانی** دانشگاه تحصیلات تکمیلی علوم پایه زنجان
ails2026-01020065	۱۵:۳۰ – ۱۵:۴۵	**پارس فیشینگ‌یاب : طراحی و پیاده‌سازی سامانه شناسایی وبگاه‌های فیشینگ با استفاده از عامل‌های هوشمند مبتنی بر مدل‌های زبانی بزرگ**	**فائزه غلامرضائی، فاطمه اصغری همپا و طلا تفضلی** پژوهشگاه ارتباطات و فناوری اطلاعات، تهران
ails2026-00360059	۱۵:۴۵ – ۱۶:۰۰	**FedTemporal: چارچوب یادگیری فدرال سری زمانی برای شناسایی باج‌افزارهای ناشناخته**	**سمیه فلاح سخنگویی و امیر جلالی بیدگلی** دانشگاه قم
ails2026-00540046	۱۶:۰۰ – ۱۶:۱۵	**تحلیل استنادپذیری خروجی قراردادهای هوشمند به‌عنوان دلیل در دعاوی خصوصی**	**مریم فلاح‌نژاد، اردشیر کلانی و سید باسم موالی‌زاده** دانشگاه آزاد اسلامی واحد اهواز، سازمان آب و برق خوزستان
ails2026-00880081	۱۶:۱۵ – ۱۶:۳۰	HyBERT-Mal: A Robust Hybrid Malware Detection Framework Integrating Contextual API Embeddings and Statistical Behavior Analysis	**سجاد رضایی و فاطمه دلدار** دانشگاه صنعتی اصفهان

سخنرانی کلیدی ۱:

امنیت، کسب و کارهای اینترنتی و هوش مصنوعی

زمان: یکشنبه ۲۶ بهمن ماه، ساعت ۱۴ الی ۱۶

سرهنگ نعمت‌الله طاهرپور

رییس پلیس فتا استان اصفهان

سخنرانی کلیدی ۲:

وقتی شاهد، قاضی و متهم همگی یک مدل زبانی هستند: چالش‌ها و فرصت‌های جرم‌یابی دیجیتال در عصر مدل‌های زبانی بزرگ

زمان: دوشنبه ۲۷ بهمن ماه، ساعت ۱۰:۳۰ الی ۱۱:۱۵

دکتر مهدیِ آبادی
دانشیار گروه مهندسی کامپیوتر دانشگاه تربیت مدرس

چکیده

ظهور مدل‌های زبانی بزرگ نقطه‌عطفی در فناوری دیجیتال است؛ جایی که مرز میان تولید داده، تحلیل و قضاوت مبتنی بر شواهد کم‌رنگ می‌شود. در این وضعیت، یک مدل می‌تواند هم‌زمان در نقش «شاهد» با تولید شواهد، «قاضی» با تحلیل آن‌ها و «متهم» به‌عنوان ابزار ارتکاب جرم ظاهر شود؛ هم‌پوشانی‌ای که اعتبار شواهد دیجیتال، بی‌طرفی تحلیل و انتساب مسئولیت را با چالش مواجه می‌کند. تمایز داده‌های واقعی و مصنوعی، بازسازی زنجیره راستی‌آزمایی، احراز قصد مجرمانه در حضور کنشگران غیرانسانی، امکان تولید شواهد جعلی واقع‌نما و نبود شفافیت در فرایند استدلال از مهم‌ترین مخاطرات پیش‌رو هستند. با این حال، این فناوری می‌تواند پایه نسل بعدی جرم‌یابی دیجیتال باشد؛ از تحلیل کلان‌داده‌های قضایی و کشف الگوهای پنهان تا بازسازی رویدادها، پیش‌بینی سناریوهای جرم و پشتیبانی از تصمیم‌گیری. این سخنرانی با رویکردی آینده‌پژوهانه بر چگونگی ادغام مدل‌های زبانی در چارچوب‌های شفاف، قابل‌ممیزی و پاسخ‌گو تمرکز کرده و در پایان، با تکیه بر تحلیل نظری و مطالعه موردی، چارچوبی جامع برای بازنگری در استانداردهای این حوزه ارائه می‌دهد.

سخنرانی کلیدی ۳:

امنیت، جامعه، اقتصاد و هوش مصنوعی

زمان: دوشنبه ۲۷ بهمن ماه، ساعت ۱۱:۱۵ الی ۱۲

دکتر حسین حسین‌زاده

رییس هیئت مدیره شرکت فولاد کویر آران و بیدگل

فهرست مقاله‌ها

شماره	نام نویسندگان	عنوان مقاله
۱	عارف آیتی و رسول نوری آذر	Digital forensics brief review: a data mining approach
۲	محمدحسین میرزائی و مهدی میرزائی	تحلیل نقش فناوری‌های دیپ‌فیک در جرائم سایبری و اصول حقوقی احراز اصالت ادله چندرسانه‌ای مخدوش
۳	مهدیه قطبی، بهاره بهرامی، علی بهلولی و محمدرضا خیام‌باشی	A Physics-Regularized PINN-XGBoost Framework for Accurate Bloodstain Angle-of-Impact Estimation
۴	مجید فرهادی سنگدهی و محمد امین خورزانی	A Verifiable AI-Augmented Homomorphic Secret Sharing Framework for Secure and Adaptive Distributed Computation
۵	وحید مجید و حسین سهلانی	الزامات به کارگیری هوش مصنوعی در استنادپذیری ادله دیجیتال
۶	زهرا سامان، مهرداد تیموری	بررسی جرم‌شناختی ارتکاب جرم با کمک هوش مصنوعی
۷	محمد شریفی و سیروس دالوند	الگوی مطلوب پیشگیری از جرایم سایبری مرتبط با هوش مصنوعی
۸	اکرم پسندیده و ایلیا حکانی	پیش‌بینی میزان جرائم خشونت‌آمیز با استفاده از مدل‌های یادگیری ماشین: مطالعه‌ای بر داده‌های اجتماعی ـ اقتصادی
۹	علیرضا صدیقی فرد	مدیریت داده‌های ناهمگون برای استفاده از هوش مصنوعی در جرم‌شناسی
۱۰	افسانه عزیزی	مدلسازی ریسک کم‌اظهاری و اولویت‌بندی پرونده‌های گمرکی با استفاده از هوش مصنوعی
۱۱	خیرالله شاهمرادی، حسین عظیمی و مسعود فریدی	تحلیل فضایی عوامل موثر بر وقوع سرقت در مناطق بیست‌ودوگانه تهران با رویکرد بیزی
۱۲	یکتا صحرایی و نسرین تلخی	پیش‌بینی نقاط پرخطر جرم با رویکرد یادگیری ماشین در چارچوب تحلیل مکانی–زمانی، با هدف پشتیبانی تصمیم‌گیری عملیاتی پلیس
۱۳	سروش سهرابی، محمد طالبی و اعظم السادات نوربخش	تحلیل کاربرد الگوریتم‌های هوش مصنوعی در کشف تقلب بانکی و جرائم سایبری مالی
۱۴	پویا سلیمانی‌فرو سرور شیدانی	Framework for Real-Time Detection of Fileless Malware Using Machine Learning Memory Forensics
۱۵	علیرضا هدایتی	واکاوی ابعاد حقوقی، فنی و جرم‌شناختی کاربرد هوش مصنوعی در کشف علمی جرم
۱۶	معین الدین علی حسینی و علی علی حسینی	Beyond the Black Box: A Culturally Adaptive Framework for AI in Iranian Criminal Justice
۱۷	محمد شیرخانی و مهسا ایزدبین	استخراج و اولویت‌بندی ادله دیجیتال از لاگ‌های شبکه با رویکرد یادگیری ماشین در جرم‌یابی سایبری
۱۸	سجاد رضایی و فاطمه دلدار	HyBERT-Mal: A Robust Hybrid Malware Detection Framework Integrating Contextual API Embeddings and Statistical Behavior Analysis
۱۹	رسول کرمی مقدم	مسئولیت کیفری ناشی از خطاهای الگوریتمی در سامانه‌های پیش‌بینی جرم

فهرست مقاله‌ها

فهرست مقاله‌ها

شماره	نام نویسندگان	عنوان مقاله
۳۷	زهرا آخودداد، امیر نوروزی و محمدرضا دارابی	
۳۸	نسرین تلخی و یکتا صحرایی	شناسایی و تحلیل نقاط داغ جرم با استفاده از کلاسترینگ فضایی –زمانی: پایداری الگوهای جرم و اثربخشی مداخلات پلیس
۳۹	صمد سهراب و امیر نظامی صفا	بررسی تحلیلی روندهای هوش مصنوعی در کشف جرم دیجیتال با رویکرد مرور نقادانه
۴۰	سیدمحمد سجادیان	نقشه‌ی علمی و روندهای پژوهشی در تقاطع هوش مصنوعی، اخلاق و کاربردهای امنیتی-قضایی: یک تحلیل کتاب سنجی در پایگاه اسکوپوس
۴۱	محمد پورمقدم	ابعاد اخلاقی و اجتماعی به‌کارگیری الگوریتم‌های تصمیم‌یار در ارزیابی ریسک جرم در سازمان‌ها

چکیده مقالات

A Physics-Regularized PINN-XGBoost Framework for Accurate Bloodstain Angle-of-Impact Estimation

Mahdieh Ghotbi
Faculty of Computer Engineering
University of Isfahan
Isfahan, Iran
m.ghotbi@comp.ui.ac.ir

Bahareh Bahrami
Faculty of Computer Engineering
University of Isfahan
Isfahan, Iran
b.bahrami@eng.ui.ac.ir

Ali Bohlooli
Faculty of Computer Engineering
University of Isfahan
Isfahan, Iran
bohlooli@eng.ui.ac.ir

Mohammad Reza Khayyambashi
Faculty of Computer Engineering
University of Isfahan
Isfahan, Iran
m.r.khayyambashi@comp.ui.ac.ir

***Abstract*—** Bloodstain Pattern Analysis (BPA) is essential for crime scene reconstruction, providing information about droplet trajectories, including the angle of impact (AoI). Traditional methods often rely on simplified geometric assumptions, neglecting physical variability and experimental uncertainty. This study proposes a hybrid physics-regularized framework, PINN-XGBoost, for accurate local AoI estimation from ellipse-derived geometric features. While gradient boosting (XGBoost) demonstrates strong standalone performance for direct AoI estimation, the hybrid framework further improves accuracy and physical consistency by embedding analytically derived constraints into the learning process. This approach aligns with BPA practices, where regression performance is evaluated using features such as stain axes, centroids, and volume. Experimental results demonstrate that the hybrid model reduces mean absolute error from 0.88° to 0.08° and increases R^2 to 0.9974, highlighting the effectiveness of combining data-driven learning with physics-informed regularization.

Index Terms-- Bloodstain Pattern Analysis, Angle of Impact, Physics-Informed Neural Networks, XGBoost

A Verifiable AI-Augmented Homomorphic Secret Sharing Framework for Secure and Adaptive Distributed Computation

Majid Farhadi sangdahi,
Dept. of math & Computer Science,
Damghan University,
Damghan, Iran
Farhadi@du.ac.ir

Mohammad amin khorzani
Dept. of math & Computer Science,
Damghan University,
Damghan, Iran
Mohammadaminkhorzani@gmail.com

***Abstract*—** This work introduces a new framework for secure data processing in distributed environments through the combined use of classical secret sharing, strengthened symmetric encryption, verifiable computation, and adaptive monitoring based on deep learning. In this design, a confidential value is divided into independent components, and each component is separately encrypted and validated to prevent disclosure and manipulation. The verifiable computation layer enables the correctness of results to be confirmed without revealing any underlying information. In addition, an intelligent analysis mechanism based on computational vision models monitors encrypted representations and operational traces to detect abnormal or adversarial behavior during processing. The integration of these mechanisms forms a multilayer system that simultaneously ensures confidentiality, correctness, and adaptive oversight, providing a reliable foundation for cloud platforms, large-scale networks, and data-intensive applications.

Index Terms— ***Homomorphic Secret Sharing,AES-CBC Encryption, Introduction, Secure Data Sharing, Vision Transformer, Zero-Knowledge Proof***

الزامات به کارگیری هوش‌مصنوعی در استنادپذیری ادله دیجیتال

وحید مجید، حسین سهلانی
عضو هیات علمی دانشگاه علوم انتظامی امین
Sahlani_h@yahoo.com

چکیده- در سالهای اخیر، استفاده از سیستمهای هوشمند در حوزه های مختلف علی الخصوص کشف جرایم به یک حوزه تحقیقاتی رو به رشد تبدیل شده است و هوش مصنوعی به عنوان یک فناوری پیشرفته، توانسته راه حل های نوآورانه و مؤثری را برای این حوزه ارائه دهد؛ این تحقیق ابتدا با هدف شناسایی و اولویت‌بندی الزامات به کارگیری هوش مصنوعی در استنادپذیری ادله دیجیتال تعریف می شود و سپس راهکارهایی را برای آینده نگری این الزامات ارائه می دهد. داده های این پژوهش از مطالعات کارهای پیشین، تجربه کاری مؤلفین و همچنین از طریق مصاحبه عمیق با ۱۶ نفر از خبرگان اصلی در مرحله کیفی حاصل شده است. جامعه آماری را خبرگان مراکز علمی و اجرایی، کارشناسان صاحب نظر پلیس های تخصصی با تحصیلات حداقل کارشناسی در رشته های مرتبط با هوش مصنوعی و امنیت رایانه و چندین سال فعالیت مرتبط با این حوزه تشکیل دادند. مدلی مفهومی در چهار بُعد اصلی و ۲۷ مؤلفه ارائه شد که بر اساس آزمون فریدمن، شاخصهای اکتسابی مربوط به زیرساخت هوش مصنوعی ها با بار عاملی ۸۵.۸ درصد، داده ها ۸۲.۳ درصد، تجهیزات فارنزیکی با ۸۲ درصد، آموزش و نیروی انسانی با کمترین بار عاملی ۷۵.۲ درصد، شناسایی شدند.

کلید واژه‌ها: **هوش مصنوعی، استنادپذیری ادله دیجیتال، فارنزیک، جمع آوری شواهد دیجیتال.**

سیستم هوشمند استخراج خودکار اطلاعات و ایجاد پایگاه دانش از پرونده‌های قضایی و انتظامی با مدل های زبانی سبک وزن

زهرا آخودداد[۱]، امیر نوروزی[۲] و محمدرضا دارابی [۳]
[۱]هیات علمی پژوهشگاه توسعه فناوری‌های پیشرفته،
[۲]پژوهشگر هوش مصنوعی پژوهشگاه توسعه فناوری‌های پیشرفته،
[۳]کارشناس ارشد مرکز مدیریت راهبردی افتا ریاست جمهوری

چکیده- این پژوهش با هدف غلبه بر چالش پردازش دستی انبوه پرونده‌های قضایی غیرساختاریافته فارسی، یک چارچوب هوش مصنوعی عملیاتی و امن مبتنی بر مدل‌های زبانی بزرگ سبک‌وزن ارائه می‌دهد. با توجه به محدودیت‌های سازمانی نظیر محرمانگی داده‌ها، نیاز به اجرای کاملاً محلی و ملاحظات هزینه‌ای، روش پیشنهادی بر استفاده از مدل‌های منبع‌باز حدود ۴ میلیارد پارامتریشامل DeepSeek-R1 ، Ministral-3B و Gemma 3-4B و پردازش ناهمزمان و دسته‌ای متمرکز است .تأکید می‌شود که این مدل‌های ۴ میلیارد پارامتری، با معماری‌های بهینه‌شده، نه تنها از دقت کافی برخوردارند بلکه به دلیل نیاز محاسباتی نسبتاً پایین، حتی بر روی سخت‌افزارهای متداول و سیستم‌های ساده مبتنی بر CPU نیز قابلیت اجرا و استقرار عملی دارند .پس از ساخت مجموعه داده مصنوعی تخصصی به دلیل عدم دسترسی به داده‌های واقعی، عملکرد این مدل‌ها در استخراج خودکار موجودیت‌ها و روابط حقوقی به قالب ساختاریافته ارزیابی و مقایسه شد. نتایج نشان داد این مدل‌ها با برقراری بهترین تعادل بین دقت استخراج به‌ویژه در تولید خروجی معتبر، سرعت پردازش و پایداری، گزینه بهینه برای استقرار به‌عنوان یک دستیار تحلیلی هوشمند در نهادهای قضایی و امنیتی است .توانایی اجرا بر زیرساخت‌های محاسباتی مقرون‌به‌صرفه و در دسترس، مسیری عملی، مقرون‌به‌صرفه و امن را برای هوشمندسازی فرآیندهای تحلیل حقوقی فراهم می‌کند.

کلید واژه‌ها: **استخراج اطلاعات، پردازش زبان طبیعی، متون حقوقی، مدل زبانی بزرگ، پردازش محلی**

مدیریت داده‌های ناهمگون برای استفاده از هوش مصنوعی در جرم‌شناسی

علیرضا صدیقی فرد
کارشناسی ارشد هوش مصنوعی، دانشگاه علم و صنعت ایران،
alireza.sedighi@ut.ac.ir

چکیده- تحلیل جرائم شهری مبتنی بر هوش مصنوعی در سال‌های اخیر به عنوان ابزاری کلیدی برای پشتیبانی از تصمیم‌گیری در حوزه نظم و امنیت مطرح شده است. با این حال، بخش قابل‌توجهی از پژوهش‌های موجود بر مجموعه‌داده‌های پالایش‌شده، همگن و تک‌منبعه متکی هستند که با واقعیت پیچیده و ناهمگون داده‌های عملیاتی فاصله معناداری دارند. این شکاف داده‌ای، تعمیم‌پذیری و پایداری مدل‌های یادگیری ماشین را در کاربردهای واقعی با محدودیت مواجه می‌سازد. در این پژوهش، یک چارچوب تحلیلی مبتنی بر یادگیری عمیق برای یکپارچه‌سازی و بازنمایی داده‌های ناهمگون جرائم شهری ارائه می‌شود. بدین منظور، دو مجموعه‌داده عمومی و پرکاربرد شامل داده‌های جرائم شهر شیکاگو (Crimes – 2001 to Present) و داده‌های تاریخی شکایت‌های پلیس نیویورک (NYPD Complaint Data Historic)، که از نظر ساختار، مقیاس و نظام طبقه‌بندی ناسازگار هستند، مورد استفاده قرار گرفته‌اند. پس از اجرای یک خط لوله پیش‌پردازش شامل پاک‌سازی، هم‌ترازی معنایی و انتخاب ویژگی مبتنی بر معیارهای آماری، یک شبکه عصبی عمیق خودکدگذار-کدگشا با هدف یادگیری بازنمایی فشرده و مقاوم نسبت به نویز آموزش داده شده است. این بازنمایی، با کمینه‌سازی خطای بازسازی، اطلاعات متمایزکننده مشترک میان داده‌های ناهمگون را استخراج کرده و اثر ناهماهنگی‌ها و نویزهای ساختاری را کاهش می‌دهد.
برای ارزیابی اثربخشی چارچوب پیشنهادی، بازنمایی استخراج‌شده به‌عنوان ورودی یک وظیفه طبقه‌بندی نوع جرم به کار گرفته شده و عملکرد آن با مدل‌های متداول یادگیری ماشین مقایسه شده است. نتایج تجربی نشان می‌دهد که استفاده از داده‌های پردازش‌شده منجر به بهبود معنادار عملکرد مدل‌های طبقه‌بندی شده و دقت پیش‌بینی را تا حدود ۹۶٪ افزایش داده است؛ به‌گونه‌ای که در مقایسه با داده‌های خام، بهبود نسبی قابل‌توجهی در معیارهای ارزیابی مشاهده می‌شود. این یافته‌ها نشان می‌دهد که مدیریت آگاهانه ناهمگونی داده‌ها و استخراج بازنمایی‌های فشرده می‌تواند نقش تعیین‌کننده‌ای در افزایش قابلیت تعمیم و کارایی مدل‌های هوش مصنوعی در تحلیل جرائم چندشهری و محیط‌های عملیاتی ایفا کند.

کلیدواژه‌ها: **داده‌های ناهمگون، خودکدگذار، استخراج ویژگی، خطای بازسازی، تحلیل جرائم، یادگیری عمیق**

مدلسازی ریسک کم‌اظهاری و اولویت‌بندی پرونده‌های گمرکی با استفاده از هوش مصنوعی

افسانه عزیزی
دکتری آمار، دانشگاه رازی کرمانشاه،
afsanehazizi425@yahoo.com

چکیده- کم‌اظهاری در اظهارنامه‌های گمرکی از چالش‌های مهم در حوزه نظم و امنیت اقتصادی است که می‌تواند به کاهش درآمدهای دولتی و افزایش تخلفات تجاری منجر شود. روش‌های سنتی مدیریت ریسک در گمرک، به دلیل اتکا به بررسی‌های دستی، توان محدودی در شناسایی الگوهای پیچیده کم‌اظهاری دارند. در این پژوهش، چارچوبی مبتنی بر هوش مصنوعی برای مدلسازی ریسک کم‌اظهاری و اولویت‌بندی پرونده‌های گمرکی ارائه شده است. در این مطالعه از داده‌های نیمه‌واقعی Kaggle و داده‌های شبیه‌سازی‌شده سامانه پایش تجارت گمرک ایران استفاده شد. پس از پیش‌پردازش و استخراج ویژگی‌ها، الگوریتم‌های رگرسیون لجستیک، جنگل تصادفی و XGBoost آموزش داده شدند. نتایج نشان می‌دهد مدل‌های مبتنی بر درخت تصمیم، به‌ویژه XGBoost در شناسایی پرونده‌های پرریسک عملکرد بهتری داشته است. این یافته‌ها نشان می‌دهد که به‌کارگیری هوش مصنوعی می‌تواند در عمل به ارتقای کارایی مدیریت ریسک، افزایش دقت در شناسایی پرونده‌های پرریسک و بهبود فرآیند تخصیص منابع نظارتی در مسیر توسعه گمرک هوشمند کمک کند. با این حال، از آنجا که بخشی از داده‌های مورد استفاده نیمه‌واقعی و شبیه‌سازی‌شده است، تعمیم مستقیم نتایج به محیط عملیاتی واقعی نیازمند احتیاط و انجام مطالعات تکمیلی است. تفاوت در رفتار فعالان تجاری، تغییرات مقررات، کیفیت ثبت داده‌ها و پیچیدگی شرایط اجرایی در محیط واقعی می‌تواند بر عملکرد مدل‌ها اثرگذار باشد؛ از این رو، اعتبارسنجی مدل‌ها با داده‌های عملیاتی واقعی، اجرای آزمایشی در محیط‌های محدود و به‌روزرسانی مستمر مدل‌ها بر اساس داده‌های جاری، می‌تواند زمینه بهره‌برداری عملی و پایدار از این رویکرد را در نظام مدیریت ریسک گمرکی فراهم سازد.

کلید واژه‌ها: **ریسک کم‌اظهاری، هوش مصنوعی، گمرک، نظم و امنیت اقتصادی**

پیش‌بینی میزان جرائم خشونت‌آمیز با استفاده از مدل‌های یادگیری ماشین: مطالعه‌ای بر داده‌های اجتماعی ـ اقتصادی (UCI)

اکرم پسندیده[۱]، ایلیا حکانی[۲]
[۱]رئیس آزمایشگاه مرکز مدیریت و تحلیل داده فراجا
[۲]کارشناس ارشد علم داده
apasandideh8@gmail.com, iliahakani@gmail.com

چکیده- افزایش جرائم خشونت‌آمیز، علاوه بر پیامدهای اجتماعی و روانی، هزینه‌های اقتصادی قابل‌توجهی ایجاد می‌کند و به همین دلیل، پیش‌بینی نرخ وقوع جرم می‌تواند به تصمیم‌سازی مبتنی بر داده در حوزه نظم و امنیت کمک کند. در این مقاله، مسأله پیش‌بینی نرخ جرائم خشونت‌آمیز با اتکا بر شاخص‌های اجتماعی–اقتصادی جوامع مورد بررسی قرار گرفت. داده مورد استفاده، مجموعه‌داده عمومی Communities and Crime از مخزن UCI است که از ترکیب سرشماری ۱۹۹۰ آمریکا، پیمایش LEMAS ۱۹۹۰ و آمار UCR (۱۹۹۵) ساخته شده و شامل ۱۹۹۴ نمونه با ۱۲۸ ویژگی است. پس از پاک‌سازی داده، حذف ستون‌های با فقدان زیاد و تفکیک آموزش/آزمون (۲۰/۸۰)، ده مدل رایج یادگیری ماشین آموزش داده شد و ارزیابی با معیارهای MAE و MSE و همچنین زمان اجرا انجام گرفت. نتایج نشان داد مدل‌های Ridge Regression، Gradient Boosting و Extra Trees در این مجموعه‌داده کمترین خطا را داشته‌اند؛ در عین حال، Ridge Regression با توجه به دقت رقابتی و زمان اجرای پایین، گزینه‌ای مناسب برای پیش‌بینی سریع و پایدار محسوب می‌شود .در پایان، محدودیت‌های تعمیم‌پذیری برای داده های ایران و ضرورت گردآوری داده‌های بومیِ استاندارد و عددی برای توسعه مدل‌های عملیاتی مورد تأکید قرار گرفته است.

***کلید واژه‌ها*: یادگیری ماشین، پیش‌بینی جرم، رگرسیون، داده‌های اجتماعی_اقتصادی، مدل‌های درختی**

الگوی مطلوب پیشگیری از جرایم سایبری مرتبط با هوش مصنوعی

محمد شریفی[۱]، سیروس دالوند[۲]
[۱]سازمان فراجا، دکتری مدیریت راهبردی فرهنگی دانشگاه عالی دفاع ملی، عضو هیئت علمی پژوهشگاه علوم انتظامی و مطالعات اجتماعی فراجا
[۲]سازمان فراجا، دکتری حقوق جزا و جرم شناسی پردیس ارس دانشگاه تهران
Moh.sharifi@iran.ir, s.dalvand@ut.ac.ir

چکیده- امروزه تحقیقات و مقررات هوش مصنوعی به دنبال متعادل کردن مزایای نوآوری در برابر آسیب و اختلالات بالقوه است. یکی از پیامدهای ناخواسته افزایش تحقیقات هوش مصنوعی، جهت گیری بالقوه فناوری‌های هوش مصنوعی برای تسهیل اعمال مجرمانه است که ما آن را جرم هوش مصنوعی می‌نامیم. هوش مصنوعی با قابلیت‌های تحلیل داده‌های حجیم و پیچیده، به عنوان یک ابزار قدرتمند در این حوزه مطرح شده است. این پژوهش به بررسی نقش هوش مصنوعی در پیش‌بینی از جرایم سایبری، چالش‌های آن و راهکارهای تنظیم‌گری می‌پردازد. تحقیق حاضر به‌صورت کتابخانه‌ای و اسنادی و با رویکرد کیفی می‌باشد و در راستای پاسخ به سوال تحقیق پس از جمع‌آوری اطلاعات به بررسی شاخص‌های مرتبط با الگوی‌های پیشگیری، شاخص‌های مرتبط با نوع جرایم سایبری، برمبنای هوش مصنوعی پرداخته و در انتها تدابیر پیشگیرانه فنی و مدیریتی ارائه خواهد گردید. **یافته‌ها نشان می‌دهد که هوش مصنوعی می‌تواند با تحلیل الگوهای رفتاری و داده‌های تاریخی، وقوع جرایم سایبری را پیش‌بینی کند.** چالش‌هایی همچون حریم خصوصی، تعصب الگوریتمی و عدم قطعیت در پیش‌بینی، استفاده از آن را محدود می‌کند. هوش مصنوعی می‌تواند نقش مؤثری در مبارزه با جرایم سایبری ایفا کند، اما برای بهره‌برداری از آن، باید چالش‌ها شناسایی شده و راهکارهای تنظیم‌گری مناسب در نظر گرفته شود.

کلید واژه‌ها: ، الگوی پیشگیرانه فنی مطلوب ، الگوی پیشگیرانه مدیریتی مطلوب، پیشگیری ازجرم، جرایم سایبری، هوش مصنوعی.

Framework for Real-Time Detection of Fileless Malware Using Machine Learning Memory Forensics

Pouya Soleimanifar
Department of Computer Science and Information Technology, Institute for Advanced Studies in Basic Sciences (IASBS),
Zanjan, Iran
Pouya.soleimanifar@gmail.com

Sorour Sheidani
Department of Computer Science and Information Technology, Institute for Advanced Studies in Basic Sciences (IASBS),
Zanjan, Iran
Sheidani@iasbs.ac.ir

Abstract- Fileless malware poses a significant threat in modern cyber environments, as it operates primarily in system memory and evades traditional file-based detection mechanisms. This paper proposes MemGuard, a hybrid framework that integrates memory forensics with machine learning for near real-time detection of fileless malware. Using the CIC-MalMem-2022 dataset, the framework combines Random Forest for feature-level classification, Convolutional Neural Networks (CNNs) for spatial pattern analysis of memory-derived representations, and Long Short-Term Memory (LSTM) networks for modeling temporal behavioral sequences. Experimental results demonstrate that MemGuard achieves near-perfect detection performance under controlled experimental conditions, with an overall accuracy exceeding 99% and an F1-score of 0.99. To mitigate overfitting, the models rely on standard preprocessing and cross-validation rather than aggressive feature engineering, allowing performance to reflect the discriminative nature of memory forensic features. The evaluation highlights the effectiveness of integrating diverse learning paradigms for automated memory analysis while maintaining practical detection latency. The proposed framework provides a scalable foundation for deploying fileless malware detection in distributed and operational environments.

***Index Terms*— Fileless Malware, Memory Forensics, Machine Learning, Cybersecurity, Anomaly Detection**

Beyond the Black Box: A Culturally Adaptive Framework for AI in Iranian Criminal Justice

Moein-Aldin AliHosseini
Department of Software Engineering
University of Isfahan
Isfahan,Iran.
moeinaldin.alihosseini@eng.ui.ac.ir

Ali AliHosseini
Department of Political Science
University of Isfahan
Isfahan, Iran
Ali.alihosseini@ase.ui.ac.ir

Abstract — As the criminal justice system transitions toward scientific crime detection, the integration of Artificial Intelligence (AI) presents a historic opportunity to enhance judicial efficiency and predictive accuracy. However, existing literature on AI ethics is predominantly Western-centric, focusing on racial binaries and Common Law precedents that do not align with Civil Law frameworks or the complex demographic tapestries of non-Western nations. This paper critiques the applicability of imported metrics to contexts characterized by multi-ethnic urban heterogeneity. We propose a novel, localized regulatory framework titled Unity in Diversity. This framework introduces three specific innovations: (1) The Inter-Cultural Consistency Score (ICCS) to audit algorithms for fairness across diverse ethnicities and clans; (2) The legal classification of AI as a Forensic Consultant—an "epistemic corridor" rather than a judicial decision-maker—to satisfy constitutional mandates for reasoned judgment; and (3) A Reputational Data Shield to protect social dignity by strictly separating criminal data from private family records. We argue that only through such localization can the justice system avoid the legitimacy crisis observed in Western jurisdictions and establish a technological infrastructure that serves specific national moral and legal requisites.

نقشه‌ی علمی و روندهای پژوهشی در تقاطع هوش مصنوعی، اخلاق و کاربردهای امنیتی-قضایی: یک تحلیل کتاب‌سنجی در پایگاه اسکوپوس

سید محمد سجادیان[۱]، علی محمد قاسمی پور[۲]
[۱] گروه مهندسی صنایع، دانشگاه پیام نور، تهران، ایران،
[۲]دانشجوی کارشناسی ارشد مهندسی صنایع دانشگاه پیام نور،
mh.ghasemipour55@gmail.com sajadiyan@pnu.ac.ir,

چکیده: رشد سریع هوش مصنوعی و روش‌های داده‌کاوی در سال‌های اخیر، تحولی بنیادین در حوزه کشف و تحلیل جرایم ایجاد کرده است. این پژوهش با هدف ارائه یک مرور نظام‌مند و تحلیل علم‌سنجی از مطالعات منتشرشده در بازه زمانی ۲۰۲۰ تا ۲۰۲۵، به بررسی کاربردهای هوش مصنوعی در کشف علمی و هوشمند جرایم می‌پردازد. داده‌های مورد استفاده از پایگاه اسکوپوس استخراج شده و روندهای موضوعی، روش‌شناختی و نظری غالب شناسایی شده‌اند. تحلیل‌های هم‌استنادی، همکاری (هم‌نویسندگی)، هم‌رخدادی (هم‌واژگانی)، استناد، تحلیل نقشه‌برداری موضوعی و خوشه‌بندی در دونرم افزار بیبلیومتریکس و وسویوور انجام شد. . ۳۲۱۴ به ۱۳خوشه طبقه‌بندی گردید. نتایج نشان داد که پژوهش‌ها در پنج خوشه اصلی شامل پیش‌بینی جرم، نظارت هوشمند، جرائم سایبری و ادله دیجیتال، پردازش زبان طبیعی، و چالش‌های اخلاقی و حقوقی متمرکز هستند. با وجود کارایی بالای مدل‌های مبتنی بر هوش مصنوعی، مسائلی نظیر تبیین‌پذیری، عدالت الگوریتمی و اعتبار زمینه‌ای همچنان به‌عنوان چالش‌های اساسی مطرح‌اند. اغلب مطالعات و استنادها و همکاری بین المللی به اقتصادهای درحال توسعه و توسعه‌یافته‌ی چین، آلمان و هند و اسپانیا و امریکا محدود می‌شود. این مقاله با ارائه یک نمای کلی از وضعیت فعلی پژوهش‌ها و شناسایی چالش‌ها و فرصت‌های موجود، به پژوهشگران و سیاست‌گذاران در امنیت و کشف علمی و هوشمند جرم مبتنی بر هوش مصنوعی کمک می‌کند.

کلید واژه‌ها: حداکثر هوش مصنوعی؛ بیبلیومتریکس، کشف جرم، پلیس پیش‌بین، تحلیل علم‌سنجی، اخلاق هوش مصنوعی

پارس فیشینگ‌یاب : طراحی و پیاده‌سازی سامانه شناسایی وب‌گاه‌های فیشینگ با استفاده از عامل‌های هوشمند مبتنی بر مدل‌های زبانی بزرگ

فائزه غلامرضائی[۱]، فاطمه اصغری همپا[۲] و طلا تفضلی[۳*]
[۱]پژوهشگر، پژوهشکده امنیت، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران، f.gholamrezaee@itrc.ac.ir
[۲] پژوهشگر، پژوهشکده امنیت، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران ، f.asghari@itrc.ac.ir
[۳] هیئت علمی، پژوهشکده امنیت، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران ، tafazoli@itrc.ac.ir

چکیده - با گسترش شیوع حملات فیشینگ و پیچیدگی این حملات با بکارگیری روش‌های نوین هوش مصنوعی مولد، ضرورت طراحی و توسعه سامانه‌ای جهت شناسایی وب‌گاه‌های فیشینگ احساس می‌گردد. بکارگیری روش‌های سنتی و روش‌های یادگیری عمیق برای شناسایی حملات فیشینگ مبتنی بر استخراج ویژگی‌های ایستا می‌باشد و دارای پیچیدگی‌های محاسباتی بالایی است. همچنین بکارگیری مدل‌های زبانی بزرگ و کوچک و سایر روش‌های شناسایی حملات فیشینگ از قبیل روش‌های یادگیری عمیق نیاز به مجموعه دادگان سفارشی دارد. هم‌اکنون مجموعه دادگان به زبان انگلیسی موجود است اما برای زبان فارسی نیاز به تهیه مجموعه دادگان می‌باشد که در این پژوهش اقدام به تهیه مجموعه دادگانی از آدرس‌های وب‌گاه‌ها، HTML و عکس از صفحات نرمال و فیشینگ فارسی نمودیم. در این پژوهش معماری شامل پنج پودمان توسعه یافته است که با اجماع بین پودمان‌های دریافت داده، پیش‌پردازش، مشابهت‌یابی، عامل‌های تخصصی و تشخیص فیشینگ مبتنی بر عامل‌های هوشمند با بکارگیری مدل‌های زبانی بزرگ اقدام به شناسایی وب‌گاه‌های فیشینگ می‌نماییم. این روش به دقتی نزدیک به ۰.۹۴ می‌رسد که در مقایسه با روش‌های مشابه پیشرفت قابل قبولی داشته است.

کلید واژه‌ها: فیشینگ، عامل‌های هوشمند، مدل‌های زبانی بزرگ

FedTemporal: Federated Time-Series Model for Zero-Day Ransomware Detection

Somayyeh Fallah
Department of Information Technology and Computer Engineering, University of Qom
Qom, Iran
S.Fallah@stu.qom.ac.i

Amir Jalaly Bidgoly
Department of Information Technology and Computer Engineering, University of Qom
Qom, Iran
Jalaly@qom.ac.i

***Abstract*—**The increase in unknown ransomware attacks has made the need for intelligent detection systems, especially robust systems in data heterogeneity, more and more felt. In this paper, the FedTemporal framework is presented; a hybrid time-based model based on federated learning that uses a combination of TCN (Temporal Convolutional Network) and multi-head Attention to extract temporal patterns of network traffic. This framework, using the FedProx algorithm, showed high *robustness* in severe data heterogeneity conditions. The model was evaluated in two real-world scenarios: Temporal Split (training on older data and testing on newer data) and Leave-One-Family-Out (LOFO) (leaving one ransomware family as unseen data). The results showed that the FedProx non-IID model exhibits performance competitive with the centralized model, with an F1-score of 93.32%. SHAP analysis on the FedProx non-IID model confirmed that robust features in the middle to late timesteps have the greatest impact on ransomware detection.

***Index Terms*- Cybersecurity, Federated Learning, Ransomware Detection, SHAP Explainability, Time-Series Model**

مروری بر پیش‌بینی جرم مبتنی بر هوش مصنوعی

مریم صادقی[1*]، مرتضی قائدی بارده[2]
[1] دکتری تخصصی مدیریت فناوری اطلاعات دانشگاه آزاد اسلامی، نجف آباد، ایران. m.sadeghi1250@iau.ac.ir
[2] دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات دانشگاه قم، قم، ایران. ghaedi96morteza@gmail.com

چکیده- پیش‌بینی جرم به ابزاری ارزشمند برای ارتقای پلیس پیش‌بینی‌کننده تبدیل شده است و سازمان‌های مجری قانون را قادر می‌سازد تا منابع را به طور مؤثرتری تخصیص دهند و استراتژی‌های پیشگیرانه پیشگیری از جرم را، به ویژه در مناطق جرم‌خیز، اجرا کنند. استفاده از هوش مصنوعی با تجزیه و تحلیل حجم وسیعی از داده‌ها برای شناسایی الگوها و پیش‌بینی فعالیت‌های مجرمانه با دقت بی‌سابقه، این حوزه را متحول کرده است. هدف این مقاله بررسی ادبیات مربوط به پیش‌بینی جرم مبتنی بر هوش مصنوعی است. با وجود پتانسیل امیدوارکننده هوش مصنوعی در پیش‌بینی جرم، چالش‌های قابل توجهی همچنان باقی مانده است، به ویژه در مورد قابلیت اعتماد سیستم‌های هوش مصنوعی که برای پذیرش اجتماعی آنها ضروری است. برای پرداختن به این مسائل، این مقاله طبق مروری نظام مند به بررسی قابلیت توضیح مدل‌های پیش‌بینی مبتنی بر هوش مصنوعی، با تمرکز ویژه بر نقش هوش مصنوعی قابل توضیح می‌پردازد. یافته‌ها، اهمیت هوش مصنوعی قابل توضیح در ایجاد اعتماد به این مدل‌ها با ارائه بینش‌های شفاف‌تر و قابل تفسیرتر در مورد نحوه تصمیم‌گیری سیستم‌های هوش مصنوعی برجسته می‌کند. با این حال، این بررسی همچنین نشان می‌دهد که ادغام هوش مصنوعی قابل توضیح در ادبیات فعلی توسعه نیافته است. با بهبود شفافیت سیستم‌های هوش مصنوعی، هوش مصنوعی قابل توضیح، این پتانسیل را دارد که به پیش‌بینی‌های جرم دقیق‌تر، قابل اعتمادتر و منصفانه‌تر منجر شود و در نهایت تلاش‌های پیشگیری از جرم مؤثرتر و عادلانه‌تر را تسهیل کند.

کلید واژه‌ها: اجرای قانون، پیش‌بینی جرم، تفسیرپذیری، توضیح‌پذیری، هوش مصنوعی قابل توضیح

تشخیص نفوذ در شبکه کامپیوتری با استفاده از الگوریتم یادگیری عمیق

مهدی حمیدی
رئیس مرکز تحقیقات کاربردی فرماندهی انتظامی استان یزد (mahdi.hamidi@iau.ac.ir)

چکیده-با گسترش روزافزون حملات سایبری و پیچیدگی آن‌ها، سیستم‌های تشخیص نفوذ مبتنی بر روش‌های سنتی دیگر قادر به مقابله مؤثر با تهدیدات نوظهور نیستند. این پژوهش به بررسی کاربرد الگوریتم‌های یادگیری عمیق در بهبود دقت و کارایی سیستم‌های تشخیص نفوذ در شبکه‌های کامپیوتری می‌پردازد. با تحلیل مطالعات انجام‌شده، مشخص گردید که معماری‌های پیشرفته‌ای مانند شبکه‌های عصبی کانولوشنی، حافظه بلند-کوتاه‌مدت و رمزگذار خودکار با قابلیت استخراج خودکار ویژگی‌های پیچیده از داده‌های ترافیک شبکه، دقت تشخیص را به‌طور قابل‌توجهی افزایش می‌دهند؛ به‌عنوان نمونه، مدل CNN با تبدیل داده‌های شبکه به تصویر، دقت ۸۵٫۲۲٪ و مدل ترکیبی CNN-LSTM در محیط اینترنت اشیا دقت ۹۹٪ را ثبت کرده‌اند. همچنین تلفیق الگوریتم‌های بهینه‌سازی فرااکتشافی با روش‌های یادگیری عمیق منجر به انتخاب بهینه ویژگی‌ها و کاهش ابعاد داده شده که در برخی موارد تا ۶٪ کاهش داشته و دقت تشخیص را تا ۹۹٫۸٪ افزایش داده است. علاوه بر این، استفاده از واحدهای پردازش گرافیکی موجب افزایش چشمگیر سرعت پردازش داده‌های حجیم شبکه شده، به‌طوری‌که در یکی از پیاده‌سازی‌ها، سرعت پردازش به ۲٫۳ گیگابیت بر ثانیه رسیده است. نتایج این مطالعه نشان می‌دهد که رویکردهای ترکیبی یادگیری عمیق با الگوریتم‌های بهینه‌سازی و سخت‌افزارهای تخصصی، راهکار مناسبی برای توسعه سیستم‌های تشخیص نفوذ کارآمد، دقیق و مقیاس‌پذیر در محیط‌های شبکه‌ای پیچیده است.

واژه‌های کلیدی: تشخیص نفوذ، یادگیری عمیق، شبکه عصبی کانولوشنی، رمزگذار خودکار، بهینه‌سازی فرااکتشافی، پردازش گرافیکی

چارچوبی مبتنی بر هستی‌شناسی برای نظارت هوشمند بر رفتارهای ترافیکی: کاربرد هوش مصنوعی معنایی در تشخیص فعالیت‌های مشکوک در محیط‌های شهری

محمدرضا خرم‌آبادی‌آرانی[1*]، فاطمه ترکاشوند[2]
[1] دانشجوی دکتری علم اطلاعات و دانش‌شناسی دانشگاه اصفهان، اصفهان، ایران(نویسنده مسئول)، mr.khorramarani78@gmail.com
[2] دانشجوی دکتری علم اطلاعات و دانش‌شناسی دانشگاه اصفهان، اصفهان، ایران، F.torkashvand1984@gmail.com

چکیده- این پژوهش با هدف طراحی چارچوبی مفهومی برای تشخیص خودکار جرایم ترافیکی (فرار از صحنه و سرقت خودرو) مبتنی بر هستی‌شناسی انجام شده است. برخلاف سیستم‌های سنتی که صرفاً ترافیک را مدیریت می‌کنند، چارچوب پیشنهادی با مدل‌سازی سه لایه (۱) رفتار عادی خودرو، (۲) ناهنجاری ترافیکی، (۳) نیت مجرمانه) قادر است فعالیت‌های مشکوک را از رفتارهای تصادفی متمایز سازد. روش تحقیق از نوع طراحی چارچوب مفهومی با تحلیل محتوای ۴۲ مقاله کلیدی در حوزه جرم‌شناسی ترافیکی است. یافته‌ها نشان می‌دهد که هستی‌شناسی با تعریف روابط معنایی میان مفاهیمی مانند «توقف ناگهانی + عدم تماس با مأموران + حرکت به سمت خروجی شهر» می‌تواند الگوی فرار از صحنه را با دقت ۸۷٪ شناسایی کند. نوآوری اصلی این پژوهش، معرفی لایه نیت مجرمانه در معماری هستی‌شناسی ترافیکی است که امکان استنتاج خودکار جرم را فراهم می‌آورد. این چارچوب می‌تواند به‌عنوان زیرساختی برای سیستم‌های پیشگیری از جرایم رانندگی در شهرهای هوشمند مورد استفاده قرار گیرد.

کلید واژه‌ها: نظارت هوشمند، جرایم ترافیکی، هستی‌شناسی، هوش مصنوعی معنایی، فرار از صحنه، سرقت خودرو

پیش بینی و تحلیل جرایم شهری با استفاده از هوش مصنوعی: چارچوبی داده محور برای پیشگیری و مدیریت امنیت

امین حق‌شناس ایلخچی[۱*]، احسان حق‌شناس ایلخچی[۲]
[۱]کارشناسی ارشد، مهندسی صنایع، گرایش بهینه سازی سیستم‌ها، دانشگاه صنعتی ارومیه، Amin.haghshenas@ine.uut.ac.ir
[۲]کارشناسی، مهندسی کامپیوتر، گرایش هوش مصنوعی، دانشگاه شهید مدنی آذربایجان، Ehsanhaghshenas31@gmail.com

چکیده- جرایم شهری به عنوان یکی از چالش‌های پیچیده جوامع امروزی، نیازمند رویکردهای تحلیلی پیشرفته برای شناسایی الگوها و درک روندهای وقوع هستند. با توجه به ماهیت مکانی – زمانی داده‌های جرم، استفاده از مدل‌های هوشمند می‌تواند به تحلیل ساختارهای پنهان این پدیده کمک نماید. در این پژوهش، یک مدل ریاضی مبتنی بر یادگیری عمیق و ترکیب شبکه عصبی کانولوشن (CNN) و شبکه عصبی بازگشتی (LSTM) برای تحلیل و پیش‌بینی الگوهای جرایم شهری ارائه شده است. داده‌های مورد استفاده در این مطالعه به صورت شبیه سازی شده و مبتنی بر الگوهای آماری و مکانی – زمانی گزارش شده در مطالعات پیشین تهیه شده است. هدف اصلی پژوهش حاضر، ارزیابی قابلیت مدل پیشنهادی در یادگیری هم زمان ویژگی‌های مکانی و وابستگی‌های زمانی وقوع جرم می‌باشد. نتایج حاصل از این پژوهش نشان می‌دهد که مدل CNN-LSTM توانایی مناسبی در استخراج الگوهای نهفته در داده‌های غیرواقعی دارد. یافته‌های این پژوهش می‌تواند به‌عنوان مبنایی برای توسعه و اعتبارسنجی مدل‌های پیش‌بینی جرم مبتنی برداده‌های واقعی در تحقیقات آینده مورد استفاده قرار گیرد.

کلید واژه‌ها: تحلیل الگوهای جرم، پیش‌بینی وقوع جرم، پیشگیری از جرم، هوش مصنوعی، شبکه های عصبی LSTM و CNN .

تحول حقوق اداری در پرتو هوش مصنوعی و تصمیم گیری های الگوریتمی

مهدی حمیدی
رئیس مرکز تحقیقات کاربردی فرماندهی انتظامی استان یزد (mahdi.hamidi@iau.ac.ir)

چکیده- هوش مصنوعی به‌عنوان یکی از فناوری‌های پیش‌رو، در حال ایجاد تحولی بنیادین در حوزه حقوق، به‌ویژه حقوق اداری است و ضرورت بازاندیشی در مبانی نظری و عملی این شاخه را آشکار ساخته است. موضوع این پژوهش نقش و تأثیر هوش مصنوعی در تصمیم‌گیری‌های اداری است. هدف اصلی تحقیق، تحلیل ابعاد حقوقی، اخلاقی و اجرایی استفاده از هوش مصنوعی در نظام اداری، شناسایی فرصت‌ها و چالش‌های آن، و ارائه راهکارهایی برای بهره‌برداری مطلوب از این فناوری در چارچوب عدالت اداری و حاکمیت قانون می‌باشد. پژوهش با روش توصیفی–تحلیلی انجام شده و تلاش می‌گردد ضمن تبیین جایگاه و نقش هوش مصنوعی در فرآیندهای اداری، ارتباط میان بهره‌وری فناوری و حفظ حقوق شهروندان بررسی شود. یافته‌های تحقیق نشان می‌دهد که هرچند هوش مصنوعی می‌تواند موجب افزایش کارایی، دقت و سرعت تصمیم‌گیری‌های اداری گردد و از خطاهای انسانی بکاهد، اما چالش‌هایی همچون شفافیت تصمیمات الگوریتمی، مسئولیت‌پذیری حقوقی و صیانت از حقوق شهروندی نیازمند توجه ویژه و تدوین مقررات جدید است. در نتیجه، همگامی حقوق اداری با تحولات فناورانه و ایجاد چارچوب‌های قانونی و نظارتی متناسب، ضرورتی اساسی برای تحقق عدالت، حفظ اصول دموکراتیک و تضمین حاکمیت قانون در عصر هوش مصنوعی به‌شمار می‌رود.

واژه های کلیدی: حقوق اداری، هوش مصنوعی، الگوریتم های تصمیم گیری، نظارت قضایی، کاهش بوروکراسی.

ارزیابی قابلیت استناد نتایج مدل‌های زبانی بزرگ در کشف علمی جرم: یک رویکرد مشترک مهندسی–حقوقی

مریم فلاح‌نژاد[۱*]، اردشیر کلانی[۲] و دکتر سعید مردانی[۳]
[۱]دانشجوی کارشناسی ارشد حقوق خصوصی، دانشگاه آزاد اسلامی واحد اهواز، maryamfallahnejad@yahoo.com
[۲]رییس‌گروه برنامه‌ریزی و تلفیق بانک‌های اطلاعاتی رصدخانه آب و انرژی، سازمان آب و برق خوزستان، ardeshirkalani@gmail.com
[۳]استادیار و مدیر گروه حقوق دانشگاه آزاد اسلامی واحد اهواز، saeid_mardani619@yahoo.com

چکیده : با گسترش روزافزون کاربرد مدل‌های زبانی بزرگ (LLMs) در حوزه‌های مختلف، پرسش کلیدی در نظام‌های قضایی پیرامون قابلیت استناد به نتایج این مدل‌ها به عنوان مدرک علمی جرم مطرح می‌شود. این مقاله با رویکردی میان‌رشته‌ای، به ارزیابی چالش‌ها و الزامات پذیرش نتایج تولیدشده توسط مدل‌های زبانی بزرگ در فرآیند کشف علمی جرم می‌پردازد. در بخش مهندسی، مسائل مربوط به قابلیت اتکا، پدیده توهم (Hallucination)، عدم شفافیت (Black-box nature) و نیاز به معیارهای ارزیابی استاندارد برای این مدل‌ها تحلیل می‌شود. در بخش حقوقی، این پژوهش با تمرکز بر قوانین اثبات دادرسی، به ویژه در زمینه ادله دیجیتال و مقررات مربوط به قانون آیین دادرسی کیفری و قانون جرائم رایانه‌ای جمهوری اسلامی ایران، شرایط لازم برای پذیرش فنی و حقوقی این نوع ادله را بررسی می‌کند. هدف نهایی، ارائه یک چارچوب مشترک برای کارشناسان فناوری اطلاعات و حقوقدانان است تا بتوانند با درک متقابل از ظرفیت‌ها و محدودیت‌های فنی و حقوقی، گامی مؤثر در جهت استفاده مسئولانه از هوش مصنوعی در نظام عدالت کیفری بردارند.

کلید واژه‌ها: مدل زبانی بزرگ، کشف علمی جرم، قابلیت استناد، ادله دیجیتال، رویکرد میان‌رشته‌ای.

بررسی تحلیلی روندهای استفاده از هوش مصنوعی در کشف جرم دیجیتال با رویکرد مرور نقادانه

صمد سهراب [۱*] و امیر نظامی صفا [۲]
[۱]کارشناس ارشد فناوری اطلاعات، دانشگاه تعالی قم، ایران، samad_sohrab@yahoo.com
[۲]کارشناس ارشد امنیت سایبری، دانشگاه امین، تهران، ایران، nezamisafaa@gmail.com

چکیده- این پژوهش باهدف تحلیل نقادانه روندهای هوش مصنوعی در کشف جرم دیجیتال و ارزیابی تعامل سه‌گانهٔ کارایی مدل‌ها، آسیب‌پذیری خصمانه، و تفسیرپذیری انجام شده است. مطالعه با روش مرور نظام‌مند مبانی نظری و تحلیل مضمون، مبتنی بر منابع معتبر بین‌المللی و ملی، صورت گرفت. پارامترهای مورد بررسی شامل عملکرد مدل‌های یادگیری عمیق (***CNN***، ***LSTM***)، میزان تاب‌آوری در برابر حملات خصمانه، و کارکرد ابزارهای تفسیرپذیری نظیر روش شاپ مبتنی بر نظریه بازی و روش تبیین محلی مدل بودند. نتایج نشان می‌دهد که اگرچه مدل‌های عمیق در تشخیص بدافزار و نفوذ شبکه به دقتی بالاتر از ۹۷٪ دست یافته‌اند، اما در برابر دستکاری‌های خصمانه آسیب‌پذیر بوده و مسئله «جعبه سیاه» موجب کاهش اعتماد عملیاتی می‌شود. همچنین، هوش مصنوعی تفسیرپذیر نقش اساسی در افزایش قابلیت ممیزی، کاهش هشدارهای کاذب و تبدیل خروجی سامانه تشخیص نفوذ به اطلاعات قابل اتکا دارد. نوآوری پژوهش در ارائه چارچوبی یکپارچه برای توسعه سامانه‌های تفسیرپذیر و مقاوم ***X-IDS*** است که به‌طور هم‌زمان دقت، شفافیت و پایداری را تقویت می‌کنند. این یافته‌ها جهت‌گیری روشنی برای طراحی نسل بعدی سامانه‌های کشف جرم دیجیتال فراهم می‌آورند.

کلید واژه‌ها: آسیب‌پذیری خصمانه، امنیت سایبری، سامانه‌های تشخیص نفوذ، کشف جرم دیجیتال، هوش مصنوعی تفسیرپذیر.

ابعاد اخلاقی و اجتماعی به‌کارگیری الگوریتم‌های تصمیم‌یار در ارزیابی ریسک جرم در سازمان‌ها: نقش عدالت ادراک‌شده، منش اخلاقی و رفتار سازمانی کارکنان

محمد پورمقدم
دکترای مدیریت دولتی گرایش رفتار سازمانی دانشگاه آزاد اسلامی تهران مرکزی، تهران، ایران. آدرس پست الکترونیک نویسنده mpmoghadam1976@gmail.com

چکیده- در سال‌های اخیر، استفاده از سیستم‌های تصمیم‌یار الگوریتمی برای ارزیابی ریسک جرم در سازمان‌ها به یکی از مهم‌ترین تحولات حوزه عدالت و مدیریت ریسک تبدیل شده است. هدف این پژوهش، تحلیل اخلاقی و اجتماعی این سیستم‌ها با تأکید بر نقش عدالت ادراک‌شده، منش اخلاقی کارکنان و پیامدهای رفتاری در محیط‌های سازمانی است. برای این منظور، یک مدل مفهومی سه‌سطحی شامل «فناوری»، «عدالت» و «اخلاق» طراحی شد. روش تحقیق مبتنی بر مرور نظام‌مند منابع و تحلیل اسنادی بود و با بهره‌گیری از چارچوب PRISMA، ۲۸ منبع معتبر بین‌المللی استخراج و تحلیل گردید. یافته‌ها نشان می‌دهد ادراک کارکنان از عدالت رویه‌ای، مهم‌ترین عامل شکل‌دهنده اعتماد، همکاری و کاهش مقاومت فناورانه است. همچنین منش اخلاقی نقش تعدیل‌گر کلیدی دارد و میزان حساسیت کارکنان نسبت به تصمیم‌های ناعادلانه الگوریتمی را تعیین می‌کند. نتایج نشان می‌دهد پیامدهای سازمانی این فناوری‌ها نه صرفاً فنی، بلکه محصول تعامل پیچیده ادراکات اخلاقی و ساختارهای تصمیم‌گیری است. بر این اساس، بهره‌گیری مسئولانه از تصمیم‌یارهای الگوریتمی مستلزم شفافیت، توضیح‌پذیری و حضور فعال انسان در چرخه تصمیم‌گیری است.

کلید واژه‌ها: عدالت ادراک‌شده، تصمیم‌یار الگوریتمی، منش اخلاقی، رفتار سازمانی، ارزیابی ریسک جرم

محاسبات مولکولی: رویکردی نوین در پزشکی قانونی جهت تحلیل همزمان چند نشانگر

زهره بیکی [۱]
[۱]هیئت علمی دانشکده مهندسی کامپیوتر دانشگاه اصفهان، z.beiki@eng.ui.ac.ir

چکیده- در این مقاله، رویکردی نوین برای تشخیص‌های پزشکی قانونی در محل وقوع حادثه مبتنی بر نشانگرهای زیستی ارائه می‌شود. سیستم پیشنهادی با الهام از سامانه‌های هوشمند، قادر است اطلاعات پنهان موجود در مایعات بدن را به‌صورت هم‌زمان تحلیل کرده و بدون نیاز به انتقال نمونه به آزمایشگاه، ویژگی‌هایی نظیر جنسیت و منشأ قومی فرد را در همان محل حادثه استخراج نماید. در این راستا، یک سامانه تشخیصی برای شناسایی هم‌زمان شش نشانگر زیستی مختلف طراحی و شبیه‌سازی شده است. نتایج شبیه‌سازی‌ها نشان می‌دهد که سیستم پیشنهادی از دقت و کارایی مناسبی برخوردار بوده و می‌تواند به‌عنوان ابزاری مؤثر در تسریع و بهبود فرآیندهای تشخیص پزشکی قانونی در محل مورد استفاده قرار گیرد.

کلید واژه‌ها: پزشکی قانونی در محل وقوع، تحلیل مایعات بدن، تشخیص هوشمند، محاسبات مولکولی، نشانگرهای زیستی (Biomarkers)