Scientific Quarterly of Supervision and Inspection
Vol. 18, No.70 (13). Winter 2025
Research Article

Intelligent Model for Monitoring Organizational Violations in FRAJA Using Artificial Intelligence

Received: 2024-04-06 **Pp.** 37-66 **Accepted:** 2025-02-02

Ebrahim Ghorbani[1]

Abstract

Background and Objective: Nowadays, combating organizational violations in various regulatory and law enforcement domains has become a fundamental challenge, and the use of artificial intelligence can provide solutions to the existing issues. Therefore, this study was conducted with the aim of designing an intelligent model for monitoring organizational violations in FRAJA using artificial intelligence.

Method: The present study is applied in nature and qualitative in method. The participants included 17 experts and specialists in the fields of supervision, crime detection, and emerging technologies within FARAJA. Using purposive sampling, theoretical saturation was achieved with the twelfth participant. For data analysis, the study employed thematic analysis along with artificial intelligence algorithms such as machine learning, natural language processing, clustering, neural network analysis, and optimization to process and analyze qualitative data, identify patterns, and extract key criteria. Content validity was ensured through expert validation and review by specialists in related fields, while reliability was established using qualitative content analysis and AI-based data analysis algorithms. To ensure accuracy and reliability, comparative analyses and computer simulations were conducted using AI techniques..

Findings: The research indicated that the model should include 30 evaluation criteria, 6 structural components, and 2 key parameters. The structural components included: 1) Monitoring employee performance, 2) Monitoring financial behavior, 3) Controlling digital communications, 4) Detecting behavioral anomalies, 5) Network analysis of communications, and 6) Monitoring organizational documents and data.

Conclusion: The results of this study show that the use of artificial intelligence in FARAJA can effectively assist in identifying and preventing organizational offenses. The capabilities of AI can simulate criminal patterns, analyze abnormal behaviors, and detect violations in real-time. Implementing intelligent monitoring systems and utilizing analytical techniques such as network analysis and simulation can enhance transparency, accountability, and effectiveness in FARAJA, significantly reducing opportunities for corruption and misconduct. Ultimately, this research provides intelligent models for monitoring and preventing organizational offenses, which represents a key step in improving operational efficiency, security, and organizational credibility in FARAJA.

Keywords: Artificial Intelligence, Intelligent Model, Monitoring, Detection of Violations, Organizational Violations, FRAJA.

Citation (APA): Ghorbani, Ebrahim (2025). Intelligent Model for Monitoring Organizational Violations in FRAJA Using Artificial Intelligence, ***Quarterly of Supervision and Inspection***, 18 (70), 37-66.
DOI: https://doi.org/10.22034/si.2025.104187

1- Lecturer at Amin University of Law Enforcement Sciences and a full member of the Iranian Law Enforcement Research Association. ebrahim.ghorbani66@gmail.com

فصلنامه علمی نظارت و بازرسی

سال ۱۸، شماره ۷۰ (۱۳)، زمستان ۱۴۰۳ | مقاله پژوهشی

الگوی هوشمندِ پایشِ تخلفات سازمانی در فراجا با استفاده از هوش مصنوعی

تاریخ دریافت: ۱۴۰۳/۰۱/۱۸ | صص ۶۶-۳۷ | تاریخ پذیرش: ۱۴۰۳/۱۱/۱۴

ابراهیم قربانی[۱]

چکیده

زمینه و هدف: امروزه مقابله با تخلفات سازمانی در حوزه‌های مختلف سازمانی به چالشی اساسی تبدیل شده و استفاده از هوش مصنوعی می‌تواند راه‌گشای مشکلات موجود باشد. از این‌رو این پژوهش با هدف طراحیِ الگویِ هوشمندِ پایشِ تخلفات سازمانی در فراجا با استفاده از هوش مصنوعی انجام شد.

روش‌شناسی: پژوهش حاضر از حیث ماهیت کاربردی و از لحاظ روش، به‌صورت کیفی انجام شد. مشارکت‌کنندگان شامل ۱۷ نفر از صاحب‌نظران و خبرگان در حوزه‌های نظارت و بازرسی و فناوری‌های نوین در فراجا هستند. با بهره‌گیری از روش نمونه‌گیری هدفمند در دوازدهمین نفر اشباع نظری حاصل شد. برای تجزیه‌وتحلیل اطلاعات از روش تحلیل مضمون و الگوریتم‌های هوش مصنوعی مانند یادگیری ماشین، پردازش زبان طبیعی، خوشه‌بندی، تحلیل شبکه‌های عصبی و بهینه‌سازی برای پردازش و تحلیل داده‌های کیفی، شناسایی الگوها و استخراج معیارهای کلیدی استفاده شد. روایی محتوایی از طریق تأیید و بررسی داده‌ها توسط متخصصین مختلف در زمینه‌های مرتبط و پایایی از طریق استفاده از روش تحلیل محتوای کیفی و الگوریتم‌های تحلیل داده به‌دست آمد. برای اطمینان از صحت و دقت نتایج، از تحلیل‌های مقایسه‌ای و شبیه‌سازی‌های رایانه‌ای با استفاده از تکنیک‌های هوش مصنوعی استفاده شد.

یافته‌ها: نشان داد که در فرایند تدوین الگوی مربوطه بایستی تعداد ۳۰ معیار ارزیابی، ۶ مؤلفه ساختاری و ۲ پارامتر کلیدی مد نظر باشد. مؤلفه‌های ساختاری عبارت هستند از: ۱- پایش عملکرد کارکنان، ۲- نظارت بر رفتار مالی، ۳- کنترل ارتباطات دیجیتال، ۴- کشف ناهنجاری‌های رفتاری، ۵- تحلیل شبکه‌ای ارتباطات و ۶- پایش اسناد و داده‌های سازمانی.

نتایج: نتایج این پژوهش نشان می‌دهد که به‌کارگیری هوش مصنوعی در فراجا می‌تواند به‌طور مؤثر به پایش و پیشگیری از تخلفات سازمانی کمک کند. کارکردهای هوش مصنوعی قادرند به شبیه‌سازی الگوهای مجرمانه، تجزیه‌وتحلیل رفتارهای غیرعادی و شناسایی تخلفات در زمان واقعی بپردازند. پیاده‌سازی سیستم‌های هوشمند نظارتی و بهره‌برداری از تکنیک‌های تحلیلی هم‌چون تحلیل شبکه‌ای و شبیه‌سازی می‌تواند موجب بهبود شفافیت، مسئولیت‌پذیری و اثربخشی در فراجا شود و زمینه‌های فساد و تخلف را به‌طور چشم‌گیری کاهش دهد.

کلیدواژه‌ها: هوش مصنوعی، الگوی هوشمند، نظارت، کشف تخلفات، تخلفات سازمانی، فراجا.

استناد (APA): قربانی، ابراهیم (۱۴۰۳). الگوی هوشمندِ پایشِ تخلفات سازمانی در فراجا با استفاده از هوش مصنوعی. ***فصلنامه نظارت و بازرسی***، ۱۸(۷۰)، ۶۶-۳۷.

DOI: https://doi.org/10.22034/si.2025.104187

۱- مدرس دانشگاه جامع علوم انتظامی امین و عضو پیوسته انجمن علمی پژوهش‌های انتظامی ایران. (رایانامه: ebrahim.ghorbani66@gmail.com)

مقدمه

در دنیای امروز، نهادهای پلیسی و امنیتی با چالش‌های پیچیده‌ای در زمینه کنترل، نظارت و پیشگیری از تخلفات سازمانی مواجه هستند (قربانی، ۱۴۰۰: ۷۷). روش‌های نظارتی معمول که عمدتاً بر بازرسی‌های انسانی، بررسی‌های دوره‌ای و گزارش‌های اداری مبتنی هستند، دیگر قادر به مقابله با تخلفات و فساد سیستمی به طور مؤثر نمی‌باشند (کمالی، ۱۴۰۲: ۱۸۹). با افزایش پیچیدگی تخلفات در سازمان‌ها، نیاز به ابزارهای نوین نظارتی بیش‌ازپیش احساس می‌شود (جانسون[1]، ۲۰۲۰: ۴۵). در این راستا، بسیاری از سازمان‌ها در جهان از سیستم‌های هوشمند برای نظارت بر عملکرد داخلی، شناسایی تخلفات و کاهش فساد درون‌سازمانی بهره می‌گیرند (براون[2]، ۲۰۱۹: ۷۴). این سیستم‌ها بر پایه هوش مصنوعی، توانایی تحلیل حجم وسیعی از داده‌ها، شناسایی الگوهای مشکوک و کشف تخلفات پنهان را با دقت و سرعت بالا دارند. شفافیت پایین در فرآیندهای نظارتی، پیچیدگی ساختارهای اداری و وابستگی زیاد به روش‌های بازرسی و حسابرسی، باعث شده است که بسیاری از تخلفات شناسایی نشوند یا با تأخیر رسیدگی شوند (محمد و اسکندر[3]، ۲۰۲۴: ۸۰). هم‌چنین، ماهیت انسانی نظارت‌های سنتی می‌تواند احتمال خطای انسانی و تأثیرپذیری از روابط فردی و مصلحت‌سنجی‌های سازمانی را افزایش دهد که این امر ممکن است به تشدید فساد اداری و کاهش کارایی سیستم نظارتی منجر شود. امروزه، استفاده از فناوری‌های نوین، به‌ویژه هوش مصنوعی، می‌تواند راه‌کار مؤثری برای مقابله با این چالش‌ها باشد. الگوریتم‌های یادگیری ماشین[4]، پردازش زبان طبیعی[5]، تحلیل شبکه‌های اجتماعی و سیستم‌های پیش‌بینی مبتنی‌بر داده‌های بزرگ، امکان شناسایی خودکار الگوهای غیرعادی، تخلفات درون‌سازمانی و رفتارهای پُرخطر را فراهم می‌کنند (رابرتسون و چن[6]،

1- Johnson
2- Brown
3- Muhammad, M & Skander
4- Machine Learning
5- NLP
6- Robertson and Chen

۲۰۲۳: ۵۶). سیستم‌های مبتنی‌بر هوش مصنوعی قادرند با تجزیه‌وتحلیل داده‌های مرتبط با رفتار کارکنان، نقل و انتقالات مالی، ارتباطات سازمانی و سایر شاخص‌های کلیدی، موارد مشکوک را شناسایی کرده و فرآیندهای رسیدگی را تسریع کنند. هم‌چنین، این فناوری‌ها می‌توانند در پیش‌بینی و پیشگیری از وقوع تخلفات نقش کلیدی ایفاء کرده و با ارائه هشدارهای زودهنگام، از بروز فساد و جرائم درون‌سازمانی جلوگیری کنند (براون، ۲۰۱۹: ۱۱۲).

با وجود پیشرفت‌های قابل توجه در استفاده از فناوری‌های نوین مانند هوش مصنوعی در پایشِ تخلفات سازمانی، هنوز در بسیاری از پژوهش‌ها و کاربردهای عملیاتی شکاف‌های مهمی در زمینه پیاده‌سازی سیستم‌های هوشمند برای مقابله با تخلفات سازمانی وجود دارد. بیش‌تر پژوهش‌ها به بررسی نظریه‌های مختلف هوش مصنوعی و الگوریتم‌های آن پرداخته‌اند، اما در عمل، به‌ویژه در سازمان‌های پیچیده‌ای مانند فراجا، این سیستم‌ها هنوز به‌طور گسترده‌ای پیاده‌سازی نشده‌اند. علاوه‌بر این، مشکلاتی مانند عدم هماهنگی میان فناوری‌های جدید و ساختارهای سازمانی، مقاومت در برابر تغییر و مسائل اخلاقی و حقوقی، هم‌چنان به‌عنوان چالش‌های اصلی در اجرای این سیستم‌ها مطرح هستند. بنابراین، با توجه به خلاءهای نظری موجود در زمینه طراحی مدل‌های عملیاتی برای پیاده‌سازی سیستم‌های هوشمند در سازمان‌های امنیتی، این پژوهش قصد دارد تا با طراحی الگویی هوشمند برای پایشِ تخلفات سازمانی در فراجا، این شکاف‌ها را شناسایی و پُر کند. البته در فراجا، به‌عنوان بزرگ‌ترین و مهم‌ترین نهاد انتظامی کشور، به‌دلیل گستردگی ساختار، تنوع مأموریت‌ها و حجم بالای داده‌های عملیاتی، در معرض وقوع تخلفات سازمانی و ارتکاب جرم قرار دارد. این تخلفات می‌توانند شامل سوءاستفاده از منابع سازمانی، فساد مالی و اداری، نشت اطلاعات محرمانه، و حتی همکاری‌های پنهان با شبکه‌های مجرمانه باشند. با این وجود، پیاده‌سازی چنین الگویی با چالش‌های متعددی مواجه است. یکی از مهم‌ترین این چالش‌ها، تأمین زیرساخت‌های فناوری اطلاعات و پردازش داده‌های عظیم سازمانی است.

علاوه‌بر این، بسیاری از کارکنان و مدیران سازمانی ممکن است در برابر تغییرات فناورانه و جایگزینی روش‌های سنتی با سیستم‌های هوشمند مقاومت کنند. هم‌چنین، طراحی و پیاده‌سازی الگوریتم‌های نظارتی مبتنی بر هوش مصنوعی باید با در نظر گرفتن ملاحظات اخلاقی، حقوقی و حریم خصوصی کارکنان انجام شود تا از سوءاستفاده از این فناوری جلوگیری شود. مسئله دیگر، تطبیق این سیستم‌ها با ساختار و فرهنگ سازمانی فراجا است، به‌طوری که ضمن افزایش کارایی نظارت، اعتماد کارکنان و مدیران نیز جلب شود. در نتیجه، ضرورت دارد که الگویی هوشمند برای پایشِ تخلفات سازمانی در فراجا طراحی شود که ضمن بهره‌گیری از ظرفیت‌های هوش مصنوعی، چالش‌های اجرایی و ملاحظات قانونی را نیز در نظر بگیرد. بر این اساس، پرسش اصلی پژوهش این است که چگونه می‌توان الگویی هوشمند برای پایشِ تخلفات سازمانی با استفاده از هوش مصنوعی طراحی کرد؟

پیشینه

پژوهش‌ها و مطالعات انجام‌شده در این زمینه هنوز در مراحل ابتدایی خود قرار دارند و به‌ویژه در کشور ایران، پژوهش‌هایی که به‌طور خاص به طراحی و پیاده‌سازی الگویی هوشمند برای پایش تخلفات سازمانی در فراجا پرداخته باشند، به‌ندرت دیده می‌شود. هرچند برخی پژوهش‌ها به بررسی کاربردهای کلی هوش مصنوعی در حوزه نظارت سازمانی پرداخته‌اند، اما تمرکز این مطالعات عمدتاً بر جنبه‌های عمومی تخلفات اداری و فساد سازمانی بوده و به‌طور خاص به نهادهای انتظامی و مقتضیات ویژه آن‌ها توجه کم‌تری شده است. از این‌رو، این پژوهش تلاش دارد با تکیه بر مطالعات پیشین و تحلیل موردی، الگویی هوشمند و کاربردی را برای پایش تخلفات سازمانی ارائه دهد. از این‌رو پیشینه‌های مرتبط در ادامه ارائه شده است.

عابدزاده، مهرآبادی و کمالی جانفدا (۱۴۰۱) در مقاله‌ای به بررسی «کاربرد هوش مصنوعی در مبارزه با فساد و ارتقای شفافیت» پرداختند. نتایج نشان می‌دهد که هوش مصنوعی می‌تواند در شناسایی فساد در دستگاه‌های دولتی و

خصوصی مؤثر باشد و با تحلیل داده‌ها، راه‌کارهایی برای جلوگیری از فساد ارائه دهد. هم‌چنین، هوش مصنوعی بهبود شفافیت در حکمرانی، افزایش اعتماد عمومی و کاهش فساد در سازمان‌ها را تسهیل می‌کند.

نجات‌پور، فرخی، سجادی و هادی‌پور (۱۴۰۱) در مقاله‌ای به «تحلیل جایگاه هوش مصنوعی در توسعه سازمان نظامی» پرداختند. نتایج پژوهش نشان می‌دهد که بهره‌گیری از فناوری هوش مصنوعی به‌عنوان یکی از پیشران‌های مؤثر در صنعت هواپیماهای بدون سرنشین، موجب توسعه و تحول در این زمینه جهت مقابله با تهدیدات گوناگون شده است. این پژوهش می‌کوشد تا نقش هوش مصنوعی در حوزه هواپیماهای بدون سرنشین را به‌عنوان یکی از پیشران‌های تأثیرگذار در آینده کشورها مورد مطالعه و بررسی قرار دهد.

آکاش، مادهاوی و پیوش[1] (۲۰۲۴) در مقاله‌ای به «کارایی الگوریتم‌های هوش مصنوعی در کشف تخلفات مالی در بانک‌ها» پرداختند. نتایج نشان داد که این الگوریتم‌ها با دقت بالایی قادر به شناسایی تراکنش‌های مشکوک هستند، به‌طوری که نرخ تشخیص تخلفات مالی به بیش از ۹۰ درصد می‌رسد. این پژوهش هم‌چنین تأکید کرد که سیستم‌های مبتنی‌بر هوش مصنوعی به خودکارسازی فرآیند نظارت کمک کرده و خطای انسانی را کاهش می‌دهند و در نتیجه می‌توانند به کشف فعالیت‌های پیچیده تقلبی کمک کنند.

گارسیا و لوپز[2] (۲۰۲۱) در مقاله‌ای به «اثربخشی سیستم‌های هوش مصنوعی در نظارت بر عملکرد کارکنان در سازمان‌های بزرگ» پرداختند. نتایج نشان داد که سیستم‌های مبتنی بر هوش مصنوعی قادرند الگوهای رفتاری غیرمعمول و مغایر با استانداردها را شناسایی کرده و به کشف تخلفات کمک کنند. این سیستم‌ها نه‌تنها نظارت را بهبود می‌بخشند، بلکه با ایجاد شفافیت و مسئولیت‌پذیری در محل کار، می‌توانند به بهبود عملکرد کارکنان کمک کنند.

1- Aakash, C. Madhavi, N. Piyush
2- Garcia & Lopez

کیم و پارک[1] (۲۰۲۰). در مقاله‌ای به تأثیر استفاده از «هوش مصنوعی بر شفافیت و پاسخ‌گویی در سازمان‌ها» را تحلیل کردند. نتایج نشان داد که پیاده‌سازی سیستم‌های مبتنی‌بر هوش مصنوعی باعث بهبود شفافیت از طریق ارائه اطلاعات دقیق و به‌هنگام در فرآیندهای سازمانی می‌شود، که در نتیجه به کاهش تخلفات کمک می‌کند. این پژوهش به این نتیجه رسید که هوش مصنوعی می‌تواند ابزاری مؤثر در افزایش پاسخ‌گویی و نظارت بر عملکرد باشد.

جمع‌بندی پیشینه

بررسی پیشینه پژوهشی نشان می‌دهد که هوش مصنوعی در پایش تخلفات سازمانی، از جمله در حوزه‌های فساد، تخلفات مالی و ارزیابی عملکرد کارکنان، نقش مؤثری ایفاء کرده است. با این حال، پژوهش‌های انجام‌شده به‌طور مشخص بر روی به‌کارگیری این فناوری در نهادهای انتظامی کشور متمرکز نبوده‌اند. این پژوهش تلاش دارد با ارائه مدلی هوشمند، زمینه‌ای برای به‌کارگیری هوش مصنوعی در بهبود نظارت و کشف تخلفات سازمانی در نهادهای امنیتی و انتظامی فراهم کند. یافته‌های این پژوهش می‌تواند به افزایش کارآمدی و شفافیت در فرآیندهای نظارتی این نهادها کمک کند.

مبانی نظری

هوش مصنوعی: هوش مصنوعی (AI) به‌عنوان یکی از پیشرفته‌ترین فناوری‌های معاصر، توانسته است در حل مسائل پیچیده‌ای که قبلاً نیازمند هوش انسانی بودند، نقشی اساسی ایفاء کند (ترابی و رجبی فرجاد، ۱۴۰۳: ۴۹). این فناوری از مجموعه‌ای از سیستم‌ها تشکیل شده است که قادرند به انجام وظایف خاص مانند یادگیری، استدلال و تصمیم‌گیری بپردازند. در دنیای امروز، هوش مصنوعی به‌ویژه در پردازش داده‌های کلان و تحلیل رفتارهای پیچیده انسان، استفاده‌های گسترده‌ای دارد (راسل و نوریگ[2]، ۲۰۱۰: ۴۵). یکی از مباحثی که در توسعه هوش مصنوعی توجه بسیاری را به خود جلب

1- Kim & Park
2- Russell & Norvig

کـرده اسـت، نظریـه سیسـتم‌هـای پیچیـده اسـت. ایـن نظریـه بـه‌ویـژه در مسـائل پیچیـده‌تـری کـه شـامل تعـداد زیـادی تعـاملات غیرخطـی و وابسـتگی‌هـای متقابـل اسـت، مـی‌توانـد کـاربرد داشـته باشـد (میشـل[1]، ۲۰۰۹: ۱۰۲). ایـن نـوع سیسـتم‌هـا در واقـع مـی‌تواننـد بـه‌طـور مـؤثر در حـل مشـکلاتی ماننـد پـیش‌بینـی جـرائم و شناسـایی الگوهـای خـلاف‌کارانـه در فضـای مجـازی اسـتفاده شـوند. از سـوی دیگـر، استفاده از نظریـه اطلاعـات کـه توسـط شـانون[2] (۱۹۴۸) معرفـی شـد، بـرای پـردازش داده‌هـای عظـیم و شناسـایی الگوهـای پنهـان در ایـن داده‌هـا ضـروری اسـت. شـانون با توسعه نظریـه اطلاعـات بـه‌ویـژه در حـوزه رمزگـذاری و انتقـال داده‌هـا، زمینـه‌هـای گونـاگونی بـرای اسـتفاده از هـوش مصـنوعی در تحلیـل داده‌هـای غیرسـاختاریافته به‌وجـود آورد کـه در پیشـگیری و شناسـایی جـرائم، بـه‌ویـژه جـرائم سـایبری، کارآمـد اسـت (جنگـا، کاتـال و کـار[3]، ۲۰۲۳: ۲۸۹۰). در راسـتای نظریـه‌هـای موجـود، الگـوریتم‌هـای یـادگیری ماشـین و تحلیـل شـبکه‌هـای عصـبی[4] مصـنوعی از جملـه مهـم‌تـرین ابزارهـای هـوش مصـنوعی در پـردازش و تحلیـل داده‌هـای پیچیـده هسـتند. ایـن الگـوریتم‌هـا بـه‌طـور خـاص در تحلیـل داده‌هـای حجـیم و شناسـایی الگوهای رفتاری در داده‌ها بـه‌کـار مـی‌رونـد و مـی‌تواننـد بـرای پـیش‌بینـی رفتارهـای آینـده و شناسـایی فعالیـت‌هـای غیرعـادی اسـتفاده شـوند (بیشـاپ[5]، ۲۰۰۶: ۱۲۸). در دنیـای مجـازی و فضـای سـایبری، هـوش مصـنوعی ایـن توانـایی را دارد کـه الگوهـای رفتارهـای مجرمانـه را شناسـایی کـرده و بـه‌طـور سـریع آن‌هـا را گـزارش دهـد. بنـابراین، هـوش مصـنوعی بـا اسـتفاده از الگـوریتم‌هـای پیشـرفته مـی‌توانـد به‌عنـوان ابـزاری مـؤثر در کشـف جـرائم و تهدیـدات امنیتـی در فضـای مجـازی عمـل کند.

نظارت و کشف تخلفات کارکنان در سازمان‌هـای امنیتـی بـا بهـره‌گیـری از هوش مصـنوعی: نظـارت بـر عملکـرد کارکنـان در سـازمان‌هـای امنیتـی یکـی از مسـائل اساسـی در حفـظ امنیـت و پیشـگیری از تخلفـات اسـت. اسـتفاده از

1- Mitchell
2- Shannon
3- Jenga, Catal & Kar
4- Neural Networks
5- Bishop

سیستم‌های هوش مصنوعی در این زمینه می‌توانند نقش مهمی در شناسایی تخلفات و رفتارهای غیرمعمول ایفاء کنند. یکی از نظریه‌هایی که به‌طور مستقیم در این زمینه کاربرد دارد، نظریه کنترل اجتماعی هیرشی[1] (۱۹۶۹) است. هیرشی معتقد است که هرچه نظارت بیش‌تر باشد، احتمال وقوع تخلف کاهش می‌یابد. در سازمان‌های امنیتی، این نظارت باید به‌طور مؤثر و کارآمد توسط سیستم‌های هوش مصنوعی انجام شود. به‌ویژه در دنیای امروز که حجم داده‌های مرتبط با رفتار کارکنان و فعالیت‌های سازمانی بسیار زیاد است، استفاده از الگوریتم‌های هوش مصنوعی برای تحلیل و پردازش این داده‌ها ضروری به‌نظر می‌رسد. این سیستم‌ها قادرند الگوهای رفتاری غیرعادی و مشکوک را شناسایی کرده و به مسئولین کمک کنند تا تصمیمات لازم را برای پیشگیری از تخلفات اتخاذ کنند (کوهن و فلسون[2]، ۱۹۷۹: ۲۰۳). در همین راستا، نظریه شبکه‌های اجتماعی که توسط واسرمن و فاست[3] (۱۹۹۴) توسعه یافته، می‌توانند به‌طور مؤثر در شناسایی ارتباطات غیرقانونی و متخلفانه در داخل سازمان‌های امنیتی به‌کار رود. این نظریه به‌ویژه بر روی نحوه ارتباطات میان افراد در شبکه‌های اجتماعی متمرکز است. از این‌رو، در سازمان‌های امنیتی می‌توان با تحلیل روابط و ارتباطات میان کارکنان، نقاط داغ متخلفانه و رفتارهای مشکوک را شناسایی کرد و در نهایت از وقوع هرگونه تخلف جلوگیری کرد. این مدل از تحلیل داده‌ها می‌تواند به شفافیت و ایجاد نظارت بیش‌تر در محیط‌های سازمانی کمک کند. نظریه تصمیم‌گیری کاهنمن و تورسکی[4] (۱۹۷۹) نیز به‌ویژه در شرایطی که سازمان‌ها با حجم زیادی از داده‌ها مواجه هستند، تأثیرگذار است. این نظریه به ضرورت استفاده از الگوریتم‌های پیش‌بینی برای کمک به تصمیم‌گیری سریع و مؤثر تأکید دارد. سیستم‌های هوش مصنوعی با استفاده از این الگوریتم‌ها قادرند در شرایط عدم قطعیت، تصمیمات دقیق‌تری اتخاذ کنند و از این‌رو می‌توانند به‌عنوان ابزاری بسیار مؤثر در نظارت بر کارکنان سازمان‌های امنیتی عمل کنند. بنابراین، با بهره‌گیری از

1- Hirschi
2- Cohen & Felson
3- Wasserman & Faust
4- Kahneman & Tversky

نظریه‌های مختلف و سیستم‌های هوش مصنوعی، سازمان‌های امنیتی می‌توانند در شناسایی و پیشگیری از تخلفات کارکنان خود موفق‌تر عمل کنند. این سیستم‌ها نه‌تنها به نظارت دقیق‌تر بر رفتار کارکنان کمک می‌کنند بلکه موجب بهبود شفافیت و مسئولیت‌پذیری در این سازمان‌ها نیز خواهند شد.

در ادامه بایستی عنوان کرد که الگوی پیشنهادی این پژوهش برای پایش تخلفات سازمانی در فراجا با استفاده از هوش مصنوعی، بر پایه ترکیبی از نظریه‌های کنترل اجتماعی، شبکه‌های ارتباطی و تصمیم‌گیری مبتنی‌بر داده طراحی شده است. در این راستا، نظریه سیستم‌های پیچیده برتالنفی[1] (۱۹۶۸)، چارچوبی مفهومی برای تحلیل ساختارهای نظارتی در سازمان‌های بزرگ ارائه می‌دهد که با نگرش به نظریه مربوطه، هوش مصنوعی می‌تواند به‌عنوان یک عنصر هوشمند در مدیریت و کنترل خودکار فرآیندهای نظارتی نقش‌آفرینی می‌کند. هم‌چنین، نظریه کارگزار-کارفرمای جنسن و مکلینگ[2] (۱۹۷۶) که بر مسئله تضاد منافع و رفتارهای فرصت‌طلبانه توسط کارمندان در سازمان‌های امنیتی تأکید دارد، می‌تواند مبنایی برای بهره‌گیری از مدل‌های پیش‌بینی و کشف تخلفات کارکنان در سازمان‌های امنیتی باشد. از این‌رو در این پژوهش، از روش‌های تحلیل کلان‌داده‌ها و یادگیری ماشین برای کشف الگوهای پنهان تخلفات سازمانی و شناسایی رفتارهای پُرخطر استفاده شده است. افزون بر این، نظریه حکمرانی داده‌محور وبر[3] (۱۹۴۷) بر اهمیت اتخاذ رویکردهای فناورانه در مدیریت و نظارت بر رفتار سازمانی تأکید دارد که در این پژوهش، از هوش مصنوعی به‌عنوان ابزار تحلیل نظارتی و تصمیم‌گیری هوشمند بهره‌برداری شده است. این چارچوب نظری، مبنای طراحی الگوی پیشنهادی پژوهش را تشکیل داده و نقش کلیدی فناوری‌های هوش مصنوعی در ارتقای نظارت و کشف تخلفات سازمانی را تبیین می‌کند.

1- Bertalanffy
2- Jensen & Meckling
3- Weber

روش‌شناسی

پژوهش حاضر از حیث ماهیت کاربردی و از لحاظ روش، به‌صورت کیفی انجام شده و به‌دنبال ارائه الگویی برای بهبود فرآیندهای نظارتی و شفاف‌سازی تخلفات سازمانی است. در این پژوهش، به تحلیل مصاحبه‌های نیمه‌ساختاریافته با خبرگان و متخصصین پرداخته شد تا داده‌های کیفی مورد نیاز استخراج شوند. فرایند مصاحبه‌ها بین ۸۰ الی ۱۰۰ دقیقه به طول انجامید. این داده‌ها سپس با استفاده از روش‌های تحلیلی هم‌چون تحلیل مضمونی و تحلیل سلسله‌مراتبی برای شناسایی معیارهای ارزیابی، مؤلفه‌های ساختاری و پارامترهای کلیدی مورد استفاده قرار گرفتند. مشارکت‌کنندگان این پژوهش شامل ۱۷ نفر از صاحب‌نظران و خبرگان در حوزه‌های نظارت و کشف تخلفات و فناوری‌های نوین در فراجا هستند. برای انتخاب مشارکت‌کنندگان از نمونه‌گیری هدفمند استفاده شد. در این روش، مشارکت‌کنندگان به‌صورت هدفمند و بر اساس معیارهای خاصی مانند تخصص، تجربه و ارتباط مستقیم با موضوع پژوهش انتخاب شدند. این افراد در زمینه‌های مرتبط با فضای مجازی، هوش مصنوعی، پلیس فتا، پلیس مبارزه با مواد مخدر و مدیریت منابع انسانی فعالیت داشته و به‌عنوان متخصص در این حوزه‌ها شناخته می‌شوند. پژوهش‌گر در دوازدهمین نفر به اشباع نظری رسید. به‌طوری‌که تعداد ۱۲ نفر از متخصصان که در زمینه‌های مختلف پایش تخلفات سازمانی در فراجا تجربه داشتند، به‌عنوان مشارکت‌کنندگان نهایی در نظر گرفته شدند. برای تحلیل داده‌های کیفی و استخراج معیارهای ارزیابی و پارامترهای کلیدی، از دو روش تحلیل مضمونی و تحلیل سلسله‌مراتبی در بستر نرم‌افزارهای MAXQDA و NVivo استفاده شد.

در ابتدا، داده‌ها از طریق تحلیل مضمون دسته‌بندی شدند. سپس، برای اولویت‌بندی و تجمیع معیارهای مشابه، از الگوریتم‌های هوش مصنوعی مانند یادگیری ماشین، پردازش زبان طبیعی، خوشه‌بندی[1]، تحلیل شبکه‌های عصبی

1- Clustering

و بهینه‌سازی[1] برای پردازش و تحلیل داده‌های کیفی، شناسایی الگوها و استخراج معیارهای کلیدی استفاده شد. الگوریتم‌های یادگیری ماشین و شبکه‌های عصبی برای شناسایی الگوهای پنهان در داده‌ها و پیش‌بینی روابط بین متغیرهای مختلف به‌کار گرفته شدند. پردازش زبان طبیعی برای تحلیل و استخراج اطلاعات از داده‌های متنی مصاحبه‌ها و کدگذاری باز به‌کار رفت. هم‌چنین، الگوریتم‌های خوشه‌بندی و بهینه‌سازی به اولویت‌بندی و تجزیه‌وتحلیل معیارهای مشابه کمک کردند و موجب دسته‌بندی و کاهش پیچیدگی داده‌ها شدند. این فرآیندها به تأمین دقت، روایی و پایایی پژوهش و کمک به شناسایی مؤلفه‌های کلیدی برای بهبود فرآیندهای نظارتی و کشف تخلفات کمک کردند. این فرآیند کمک کرد تا معیارها به تعداد معقولی کاهش یافته و دسته‌بندی‌های جدیدتری ایجاد شوند. برای تأمین روایی و پایایی پژوهش، از چندین اقدام استفاده شد:

- روایی محتوایی از طریق تأیید و بررسی داده‌ها توسط متخصصین مختلف در زمینه‌های مرتبط به‌دست آمد.
- پایایی از طریق استفاده از روش‌های تحلیل محتوای کیفی و الگوریتم‌های تحلیل داده که دقت و تکرارپذیری نتایج را تضمین می‌کند، به‌دست آمد. علاوه‌بر این، برای اطمینان از صحت و دقت نتایج، از تحلیل‌های مقایسه‌ای و شبیه‌سازی‌های رایانه‌ای با استفاده از تکنیک‌های پیشرفته هوش مصنوعی استفاده شد. درصد توافق درون موضوعی به میزان ۹۱ درصد ارزیابی شد.

یافته‌ها

یافته‌های جمعیت‌شناختی (ویژگی‌های مشارکت‌کنندگان): توزیع ویژگی‌های مشارکت‌کنندگان در پژوهش بر اساس تحصیلات، سابقه کار و جنسیت به شرح ذیل بود.

1- Optimization

- **تحصیلات**: در این پژوهش، تمامی مشارکت‌کنندگان دارای تحصیلات بالاتر کارشناسی ارشد بودند. بیش‌ترین تعداد شرکت‌کنندگان در مقطع کارشناسی ارشد (۷ نفر معادل ۵۸/۳۳ درصد) و مابقی دارای مدرک دکتری بودند (۵ نفر معادل ۴۱/۶۷ درصد).
- **سابقه کار**: بیش‌تر مشارکت‌کنندگان با سابقه کاری بیش‌تر از ۱۰ سال در پژوهش حضور داشتند. ۶ نفر (معادل ۵۰ درصد) دارای سابقه کار ۱۶ تا ۲۰ سال، ۳ نفر (۲۵ درصد) دارای سابقه کار ۱۰ تا ۱۵ سال و ۳ نفر (۲۵ درصد) دارای سابقه کار ۶ تا ۱۰ سال بودند. این توزیع نشان‌دهنده حضور افراد با تجربه در عرصه‌های مرتبط با پایش تخلفات سازمانی است.
- **جنسیت**: همه مشارکت‌کنندگان در این پژوهش **مرد** بودند که نشان‌دهنده نبود تنوع جنسیتی در این نمونه پژوهش است. این موضوع ممکن است تحت تأثیر ساختار سازمانی و حوزه‌های تخصصی پژوهش باشد که عمدتاً توسط مردان در آن فعالیت می‌شود.

یافته‌های تحلیلی

با توجه به موضوع مقاله که در جهت تبیین الگوی هوشمند پایشِ تخلفات سازمانی است، ابتدا به شناسایی مضامین پایه، سازمان‌دهنده و فراگیر پرداخته شد. در این پژوهش واژه مضامین پایه به معیارهای ارزیابی تغییر یافت. این واژه به‌خوبی نشان‌دهنده فرایند اندازه‌گیری و ارزیابی عملکرد و رفتار در سیستم‌های نظارتی است. مضامین سازمان‌دهنده نیز به مؤلفه‌های ساختاری تغییر یافتند. این اصطلاح نیز به‌خوبی ماهیت اجزای تشکیل‌دهنده و ساختاری مدل‌های پیچیده را نشان می‌دهد و با دقت بیش‌تر بر روی ساختار و طراحی مدل تأکید دارد. و در نهایت مضامین فراگیر به پارامترهای کلیدی تغییر یافت. این عبارت بیان‌گر اجزای اصلی و مهم در یک مدل پیچیده است که به تحلیل و ارزیابی سیستم‌ها کمک می‌کند و بیش‌تر از «ابعاد» به مفاهیم فنی و علمی نزدیک است.

مرحله اول: شناسایی معیارهای ارزیابی

برای شناسایی معیارهای ارزیابی نظارت و کشف تخلفات، مصاحبه‌های نیمه‌ساختاریافته با خبرگان و متخصصین انجام شد. این مصاحبه‌ها شامل پرسش‌های گشوده‌ای بود که به شناسایی نیازها، چالش‌ها و ابعاد مختلف پایش تخلفات سازمانی کمک می‌کرد. به‌دنبال این فرآیند، معیارهای مختلفی شناسایی شد که به‌طور کلی به میزان وسیعی از داده‌ها و اطلاعات اشاره داشتند. در این مرحله، تعداد زیادی معیار ارزیابی شناسایی شد که برای پوشش‌دهی ابعاد مختلف پایش تخلفات سازمانی طراحی شده بودند. این معیارها می‌توانستند به تنهایی به ارزیابی هر پارامتر کلیدی کمک کنند، اما تعداد زیاد آن‌ها، گاهی موجب پراکندگی و تداخل داده‌ها می‌شد. برای کاهش تعداد معیارهای ارزیابی و ایجاد دقت بیش‌تر در تحلیل‌ها، از تکنیک‌های تحلیل مضمونی و تحلیل سلسله‌مراتبی استفاده شد. در این مرحله، داده‌های حاصل از مصاحبه‌ها و منابع اطلاعاتی مرتبط با معیارها دسته‌بندی و اولویت‌بندی شدند. به‌ویژه، معیارهایی که دارای تشابهات ساختاری و محتوایی بودند، تجزیه‌وتحلیل شده و در قالب معیارهای جدیدتر تجمیع شدند.

در این فرآیند، از الگوریتم‌های تحلیل محتوای کیفی و ابزارهای پردازش زبان طبیعی نیز بهره‌برداری شد تا روند دسته‌بندی و کاهش داده‌ها به‌صورت هوشمند و خودکار انجام گیرد. این روش‌ها کمک کردند تا معیارهای تکراری حذف شده و معیارهای اصلی و کلیدی برای مدل‌سازی به‌طور دقیق‌تر استخراج شوند. در نهایت، تعداد معیارهای ارزیابی به تعداد معقولی کاهش یافت که بتواند به‌طور مؤثر فرآیند پایش تخلفات سازمانی را پوشش دهد. بنابراین، در ادامه از روش‌های مختلف برای کاهش و طبقه‌بندی این معیارها استفاده شد. معیارهای شناسایی شده به شرح جدول ۱ لیست شدند.

جدول ۱: معیارهای ارزیابیِ الگویِ هوشمند پایشِ تخلفات سازمانی در فراجا با استفاده از هوش مصنوعی

معیارهای ارزیابی نظارت و کشف تخلفات	تعداد تکرار در مصاحبه
پایش داده‌های ورود و خروج کارکنان با تحلیل داده‌های بیومتریک وRFID	۶
بررسی تعاملات اداری کارکنان با پردازش زبان طبیعی (NLP) در مکاتبات رسمی	۷
تشخیص تعاملات کارکنان در شبکه‌های اجتماعی با مدل‌های NLP و هوش مصنوعی	۵
بررسی میزان ارتباط کارکنان با گروه‌های مشکوک با تحلیل مسیرهای ارتباطی (Path Analysis)	۷
ردیابی فعالیت‌های مرتبط با حذف یا تغییر داده‌های حیاتی با تحلیل لاگ‌های سیستم (Log Analysis)	۷
بررسی سوءاستفاده از مجوزهای ویژه کارکنان با تحلیل الگوهای استفاده از داده (User Behavior Analytics - UBA)	۶
استفاده از واقعیت مجازی (VR) و واقعیت افزوده (AR) برای بازسازی سناریوهای تخلف و آموزش	۵
بررسی میزان انحراف از رویه‌های سازمانی با تحلیل مقایسه‌ای الگوریتم‌های تقلب (Fraud Detection Models)	۶
بررسی میزان استفاده از سامانه‌های اداری با سیستم‌های SIEM (مدیریت اطلاعات امنیتی و رویدادها)	۵
تحلیل ساعات کاری غیرعادی با الگوریتم‌های شبکه عصبی بازگشتی (RNN)	۵
تحلیل داده‌های رفتاری کارکنان با استفاده از یادگیری عمیق(Deep Learning)	۵
تحلیل ارتباطات کارکنان با مدل‌سازی گراف(Graph-based AI)	۵
کنترل میزان افشای اطلاعات سازمانی با سیستم‌های تشخیص نشت داده (DLP - Data Loss Prevention)	۶
محدودسازی دسترسی‌های غیرمجاز به اسناد با الگوریتم‌های رمزنگاری پیشرفته و بلاک‌چین	۵
شناسایی تبادل داده‌های حساس بین کارکنان با تحلیل ترافیک شبکه (Network Traffic Analysis)	۴
پیش‌بینی ارتباطات غیرمعمول کارکنان با مدل‌های یادگیری تقویتی (Reinforcement Learning)	۵
اعتبارسنجی گزارش‌های تخلفات با مدل‌های پردازش تطبیقی و تحلیل خودکار مستندات سازمانی	۴
شناسایی الگوهای رفتاری غیرمعمول با تحلیل کلان‌داده‌ها(Big Data Analytics)	۴
پیش‌بینی تخلفات بالقوه با مدل‌های رگرسیون و سری‌های زمانی	۴
تحلیل روان‌شناختی کارکنان با پردازش رفتارشناسی سایبری (Cyber Behavioral Analysis)	۷
بررسی تعاملات کارکنان با گروه‌های پرریسک از طریق تحلیل چت‌های رمزگذاری‌شده با روش رمزگشایی هوشمند(AI Decryption)	۵

معیارهای ارزیابی نظارت و کشف تخلفات	تعداد تکرار در مصاحبه
شناسایی حملات فیشینگ و جاسوسی با سامانه‌های SIEM و تحلیل لاگ‌های امنیتی	۴
تحلیل پیام‌های سازمانی با پردازش زبان طبیعی (NLP) و تحلیل احساسات (Sentiment Analysis)	۵
بررسی مکالمات کارکنان با تحلیل صوت و تشخیص تن صدا(Voice Recognition AI)	۶
ردیابی دسترسی‌های غیرمجاز با سیستم‌های کنترل دسترسی مبتنی بر هوش مصنوعی-(AI driven Access Control)	۵
استخراج تغییرات ناگهانی در سبک زندگی و دارایی کارکنان با داده‌کاوی روی حساب‌ها	۴
تحلیل تراکنش‌های مالی کارکنان را با شبکه‌های عصبی پیچشی (CNN) و مدل‌های گرافی	۸
حسابرسی تطابق هزینه‌ها با درآمد کارکنان با سیستم‌های قانونیForensic Accounting	۶
پایش ارتباطات مالی کارکنان با تحلیل شبکه‌های اجتماعی(SNA)	۵
شناسایی موارد مشکوک به رشوه را با تحلیل الگوهای انتقال پول (Transaction Pattern Analysis)	۴

مرحله دوم: شناسایی مؤلفه‌های ساختاری

در گام بعدی، با توجه به معیارهای ارزیابی نهایی، شروع به تحلیل مضمونی و طبقه‌بندی داده‌ها شد. در این مرحله، هر معیار مورد بررسی قرار گرفت و ارتباط آن با دیگر معیارها و ویژگی‌های مدل مشخص شد. سپس، مجموعه‌ای از معیارها که از نظر مفهومی و کاربردی با یکدیگر هم‌راستا بودند، در قالب مؤلفه‌های ساختاری گروه‌بندی شدند. این مؤلفه‌های ساختاری، در واقع بخش‌های اصلی و کلیدی بودند که به‌طور مستقیم پارامترهای کلیدی پایش تخلفات سازمانی را تحت پوشش قرار می‌دادند.

در این مرحله از روش‌های تحلیل خوشه‌ای و مدل‌سازی مقایسه‌ای توسط هوش مصنوعی استفاده شد تا مؤلفه‌های ساختاری به‌طور علمی و دقیق دسته‌بندی شوند. این تحلیل‌ها با در نظر گرفتن ارتباطات درونی معیارها و شبیه‌سازی‌های رایانه‌ای در هوش مصنوعی، به ایجاد دسته‌بندی مؤلفه‌های ساختاری کمک کردند. در ادامه و در جدول ۲، مؤلفه‌های ساختاری مربوط به الگوی هوشمند پایشِ تخلفات سازمانی در فراجا با استفاده از هوش مصنوعی ارائه شده است.

جدول ۲: مؤلفه‌های ساختاری الگوی هوشمند پایشِ تخلفات سازمانی در فراجا با استفاده از هوش مصنوعی

مؤلفه‌های ساختاری	معیارهای ارزیابی
پایش عملکرد کارکنان	پایش داده‌های ورود و خروج کارکنان با تحلیل داده‌های بیومتریک وRFID
	بررسی تعاملات اداری کارکنان با پردازش زبان طبیعی (NLP) در مکاتبات رسمی
	شناسایی الگوهای رفتاری غیرمعمول با تحلیل کلان‌داده‌ها(Big Data Analytics)
	بررسی میزان استفاده از سامانه‌های اداری با سیستم‌های SIEM (مدیریت اطلاعات امنیتی و رویدادها)
	تحلیل ساعات کاری غیرعادی با الگوریتم‌های شبکه عصبی بازگشتی (RNN)
نظارت بر رفتار مالی	استخراج تغییرات ناگهانی در سبک زندگی و دارایی کارکنان با داده‌کاوی روی حساب‌ها
	تحلیل تراکنش‌های مالی کارکنان را با شبکه‌های عصبی پیچشی (CNN) و مدل‌های گرافی
	حسابرسی تطابق هزینه‌ها با درآمد کارکنان با سیستم‌های قانونیForensic Accounting
	پایش ارتباطات مالی کارکنان با تحلیل شبکه‌های اجتماعی(SNA)
	شناسایی موارد مشکوک به رشوه را با تحلیل الگوهای انتقال پول (Transaction Pattern Analysis)
کنترل ارتباطات دیجیتال	بررسی تعاملات کارکنان با گروه‌های پرریسک از طریق تحلیل چت‌های رمزگذاری‌شده با روش رمزگشایی هوشمند(AI Decryption)
	شناسایی حملات فیشینگ و جاسوسی با سامانه‌های SIEM و تحلیل لاگ‌های امنیتی
	تحلیل پیام‌های سازمانی با پردازش زبان طبیعی (NLP) و تحلیل احساسات (Sentiment Analysis)
	بررسی مکالمات کارکنان با تحلیل صوت و تشخیص تن صدا(Voice Recognition AI)
	ردیابی دسترسی‌های غیرمجاز با سیستم‌های کنترل دسترسی مبتنی بر هوش مصنوعی (AI-driven Access Control)
کشف ناهنجاری‌های رفتاری	تحلیل داده‌های رفتاری کارکنان با استفاده از یادگیری عمیق(Deep Learning)
	استفاده از واقعیت مجازی (VR) و واقعیت افزوده (AR) برای بازسازی سناریوهای تخلف و آموزش
	بررسی میزان انحراف از رویه‌های سازمانی با تحلیل مقایسه‌ای الگوریتم‌های تقلب (Fraud Detection Models)
	پیش‌بینی تخلفات بالقوه با مدل‌های رگرسیون و سری‌های زمانی
	تحلیل روان‌شناختی کارکنان با پردازش رفتارشناسی سایبری (Cyber Behavioral Analysis)
تحلیل شبکه‌ای ارتباطات	تشخیص تعاملات کارکنان در شبکه‌های اجتماعی با مدل‌های NLP و هوش مصنوعی
	بررسی میزان ارتباط کارکنان با گروه‌های مشکوک با تحلیل مسیرهای ارتباطی (Path Analysis)

مؤلفه‌های ساختاری	معیارهای ارزیابی
	شناسایی تبادل داده‌های حساس بین کارکنان با تحلیل ترافیک شبکه (Network Traffic Analysis)
	پیش‌بینی ارتباطات غیرمعمول کارکنان با مدل‌های یادگیری تقویتی (Reinforcement Learning)
	تحلیل ارتباطات کارکنان با مدل‌سازی گراف(Graph-based AI)
پایش اسناد و داده‌های سازمانی	کنترل میزان افشای اطلاعات سازمانی با سیستم‌های تشخیص نشت داده (DLP - Data Loss Prevention)
	محدودسازی دسترسی‌های غیرمجاز به اسناد با الگوریتم‌های رمزنگاری پیشرفته و بلاک‌چین
	ردیابی فعالیت‌های مرتبط با حذف یا تغییر داده‌های حیاتی با تحلیل لاگ‌های سیستم (Log Analysis)
	بررسی سوءاستفاده از مجوزهای ویژه کارکنان با تحلیل الگوهای استفاده از داده (User Behavior Analytics - UBA)
	اعتبارسنجی گزارش‌های تخلفات با مدل‌های پردازش تطبیقی و تحلیل خودکار مستندات سازمانی

مرحله سوم: شناسایی پارامترهای کلیدی و فناوری‌ها، روش‌ها و تجهیزات مورد استفاده

پس از طبقه‌بندی مؤلفه‌های ساختاری، با استفاده از تحلیل‌های ساختاری و تحلیل مدل‌های پیش‌بینی، به شناسایی پارامترهای کلیدی پرداخته شد. در این مرحله، مؤلفه‌های ساختاری در پارامترهای کلیدی وسیع‌تری دسته‌بندی شدند که هر پارامتر کلیدی، شامل مجموعه‌ای از مؤلفه‌های ساختاری مربوط به خود بود. این پارامترهای کلیدی، چارچوب کلی مدل را تشکیل می‌دهند و در واقع نشان‌دهنده ساختار کلی پایش تخلفات سازمانی در فراجا هستند. در فرآیند شناسایی پارامترهای کلیدی، علاوه‌بر تحلیل داده‌ها، از تکنیک‌های پیشرفته هوش مصنوعی مانند یادگیری عمیق و مدل‌های شبکه عصبی برای شبیه‌سازی و پیش‌بینی پارامترهای کلیدی استفاده شد. این تحلیل‌ها کمک کردند تا پارامترهای کلیدی نهایی با دقت بالاتری شناسایی شوند و هم‌راستایی با داده‌های میدانی و مصاحبه‌ها حفظ شود.

جدول ۳: شبکه مضامین، فناوری‌ها، روش‌ها و تجهیزات مورد استفاده الگوی هوشمند پایشِ تخلفات سازمانی در فراجا با استفاده از هوش مصنوعی

پارامترهای کلیدی	مؤلفه‌های ساختاری	فناوری‌ها، روش‌ها و تجهیزات مورد استفاده
نظارت	پایش عملکرد کارکنان	**فناوری‌ها:** بیومتریک (چهره، اثر انگشت)، RFID، SIEM، NLP، کلان‌داده **روش‌ها:** یادگیری ماشین، تحلیل سری‌های زمانی، خوشه‌بندی داده‌ها
	نظارت بر رفتار مالی	**فناوری‌ها:** بلاک‌چین، تحلیل داده‌های بانکی، یادگیری ماشین **روش‌ها:** گراف‌کاوی، تحلیل شبکه اجتماعی، الگوریتم‌های تشخیص ناهنجاری مالی **تجهیزات:** سامانه‌های نظارت مالی مبتنی بر هوش مصنوعی
	کنترل ارتباطات دیجیتال	**فناوری‌ها:** NLP، تحلیل صوت، رمزگشایی هوشمند، SIEM **روش‌ها:** تحلیل لاگ‌های امنیتی، شبکه‌های عصبی عمیق، مدل‌های پیش‌بینی رفتار
کشف تخلفات	کشف ناهنجاری‌های رفتاری	**فناوری‌ها:** یادگیری عمیق، AR/VR، تحلیل سری‌های زمانی، رفتارشناسی سایبری **روش‌ها:** خوشه‌بندی، تحلیل مقایسه‌ای، پردازش داده‌های روانشناسی
	تحلیل شبکه‌ای ارتباطات	**فناوری‌ها:** تحلیل گراف، یادگیری تقویتی، پردازش شبکه‌های اجتماعی **روش‌ها:** تحلیل مسیرهای ارتباطی، تشخیص ناهنجاری در شبکه‌های اجتماعی **تجهیزات:** سیستم‌های نظارت سایبری
	پایش اسناد و داده‌های سازمانی	**فناوری‌ها:** بلاک‌چین، DLP، تحلیل لاگ، UBA **روش‌ها:** رمزنگاری پیشرفته، پردازش تطبیقی، تشخیص ناهنجاری داده‌ها

یافته‌های استنباطی

برای تحلیل الگویِ هوشمند پایشِ تخلفات سازمانی در فراجا با استفاده از هوش مصنوعی، می‌توان هر بُعد و مؤلفه‌ها را به‌طور مرحله به مرحله بررسی کرد. در این مدل، تلاش بر این است که از فناوری‌های پیشرفته برای نظارت مؤثر و کشف تخلفات دقیق در فراجا استفاده شود. این تحلیل به تفکیک مضامین سازمان‌دهنده (مؤلفه‌های ساختاری) و مضامین فراگیر (پارامترهای کلیدی) به شکل زیر انجام می‌شود:

۱- پارامتر کلیدی نظارت

الف) پایش عملکرد کارکنان: در این بخش، با استفاده از داده‌های ورود و خروج کارکنان که از طریق تحلیل بیومتریک و RFID جمع‌آوری می‌شود، به نظارت بر حضور و غیاب پرداخته می‌شود. هم‌چنین، ساعات کاری غیرعادی با استفاده از الگوریتم‌های شبکه عصبی بازگشتی (RNN) تحلیل می‌شوند. برای بررسی تعاملات اداری کارکنان، از پردازش زبان طبیعی (NLP) در مکاتبات رسمی بهره‌برداری می‌شود. الگوهای رفتاری غیرمعمول از طریق تحلیل کلان‌داده‌ها شناسایی می‌شوند و در نهایت، استفاده از سامانه‌های اداری با سیستم‌های SIEM تحت نظارت قرار می‌گیرد.

ب) نظارت بر رفتار مالی: برای نظارت بر تراکنش‌های مالی کارکنان، از شبکه‌های عصبی پیچشی (CNN) و مدل‌های گرافی استفاده می‌شود تا الگوهای مالی آن‌ها تحلیل گردد. موارد مشکوک به رشوه نیز از طریق تحلیل الگوهای انتقال پول شناسایی می‌شوند. تطابق هزینه‌ها با درآمد کارکنان با سیستم‌های حسابرسی قانونی مورد بررسی قرار می‌گیرد. ارتباطات مالی کارکنان با مجرمان از طریق تحلیل شبکه‌های اجتماعی پایش می‌شود و تغییرات ناگهانی در سبک زندگی و دارایی کارکنان از طریق داده‌کاوی حساب‌های بانکی استخراج می‌شود.

ج) کنترل ارتباطات دیجیتال: در این بخش، پیام‌های سازمانی با استفاده از پردازش زبان طبیعی (NLP) و تحلیل احساسات مورد تحلیل قرار می‌گیرند. مکالمات کارکنان نیز از طریق تحلیل صوت و تشخیص تن صدا بررسی می‌شوند. دسترسی‌های غیرمجاز با استفاده از سیستم‌های کنترل دسترسی مبتنی‌بر هوش مصنوعی ردیابی می‌شوند و حملات فیشینگ و جاسوسی با استفاده از سامانه‌های SIEM و تحلیل لاگ‌های امنیتی شناسایی می‌شوند. در نهایت، تعاملات کارکنان با گروه‌های پُرریسک از طریق تحلیل چت‌های رمزگذاری‌شده با روش رمزگشایی هوشمند بررسی می‌شود.

۲- پارامتر کلیدیِ کشف تخلفات

الف) کشف ناهنجاری‌های رفتاری: برای کشف ناهنجاری‌ها، داده‌های رفتاری کارکنان با استفاده از یادگیری عمیق (Deep Learning) تحلیل می‌شوند. میزان انحراف از رویه‌های سازمانی با مدل‌های تقلب بررسی می‌شود و تخلفات بالقوه با مدل‌های رگرسیون و سری‌های زمانی پیش‌بینی می‌شوند. از واقعیت مجازی (VR) و واقعیت افزوده (AR) برای شبیه‌سازی سناریوهای تخلف و آموزش کارکنان استفاده می‌شود. تحلیل روان‌شناختی کارکنان نیز با پردازش رفتارشناسی سایبری انجام می‌گیرد.

ب) تحلیل شبکه‌ای ارتباطات: در این بخش، ارتباطات کارکنان با استفاده از مدل‌سازی گراف تحلیل می‌شود تا الگوهای ارتباطی آن‌ها شناسایی شود. میزان ارتباط کارکنان با گروه‌های مشکوک با تحلیل مسیرهای ارتباطی بررسی می‌شود و تعاملات کارکنان در شبکه‌های اجتماعی با مدل‌های NLP و تشخیص هوش مصنوعی پایش می‌شود. تبادل داده‌های حساس بین کارکنان از طریق تحلیل ترافیک شبکه شناسایی می‌شود و ارتباطات غیرمعمول کارکنان با استفاده از مدل‌های یادگیری تقویتی پیش‌بینی می‌شود.

ج) **پایش اسناد و داده‌های سازمانی:** دسترسی‌های غیرمجاز به اسناد با استفاده از الگوریتم‌های رمزنگاری پیشرفته و بلاک‌چین محدود می‌شود. میزان افشای اطلاعات سازمانی با سیستم‌های DLP (Data Loss Prevention) کنترل می‌شود و فعالیت‌های مرتبط با حذف یا تغییر داده‌های حیاتی از طریق تحلیل لاگ‌های سیستم ردیابی می‌شود. سوءاستفاده از مجوزهای ویژه کارکنان با تحلیل الگوهای استفاده از داده‌ها بررسی می‌شود و گزارش‌های تخلفات با مدل‌های پردازش تطبیقی و تحلیل خودکار مستندات سازمانی اعتبارسنجی می‌شود.

بحث و نتیجه‌گیری

در این پژوهش، الگوی هوشمند پایشِ تخلفات سازمانی در فراجا با استفاده از هوش مصنوعی طراحی و پیاده‌سازی شد و نتایج آن در دو بُعد اصلی پایش تخلفات سازمانی به‌طور قابل توجهی کارآمد بود. در بُعد نظارت، سیستم‌های مبتنی‌بر یادگیری ماشین توانستند به‌طور خودکار و بدون نیاز به دخالت انسانی، رفتارهای کارکنان را در محیط‌های مختلف شبیه‌سازی کرده و الگوهای غیرعادی را شناسایی کنند. این فرآیند نه تنها دقت بالاتری نسبت به روش‌های سنتی داشت، بلکه سرعت نظارت و بازخوردها را به‌طور چشم‌گیری افزایش داد. علاوه‌بر این، کاهش خطاهای انسانی و جلوگیری از اشتباهات ناشی از نظارت دستی، منجر به ارتقای کیفیت نظارت و دست‌یابی به اطلاعات به‌موقع شد که برای تصمیم‌گیری‌های راهبردی و عملیاتی بسیار حائز اهمیت است.

در بُعد کشف تخلفات، سیستم هوشمند می‌تواند با استفاده از تحلیل داده‌های تاریخی و یادگیری از الگوهای رفتاری موجود، تخلفات احتمالی را پیش‌بینی کرده و وقوع آن‌ها را قبل از وقوع شبیه‌سازی کند. این توانایی پیش‌بینی، باعث می‌شود که تخلفات به‌طور مؤثری شناسایی و از وقوع آن‌ها جلوگیری شود و این امر هم به کاهش هزینه‌های ناشی از پیگیری‌های دستی و هم به جلوگیری از تخلفات در مراحل اولیه منجر می‌شود. این قابلیت در بهینه‌سازی زمان و منابع، به‌ویژه در زمینه مقابله با تخلفات گسترده و پیچیده،

نقش کلیدی ایفاء می‌کند. یافته‌های این پژوهش، به‌ویژه در زمینه پیش‌بینی و شبیه‌سازی تخلفات، می‌تواند به‌طور جزیی‌تر تحلیل شود. به‌عنوان مثال، شبیه‌سازی دقیق‌تر رفتارهای کارکنان و تخلفات می‌تواند به شناسایی نواقص و آسیب‌های بیش‌تر در عملکرد سیستم‌ها و فرآیندها منجر شود. این امر نه‌تنها به شبیه‌سازی رفتارهای غیرعادی و تخلفات احتمالی در محیط‌های مختلف کمک می‌کند، بلکه به تحلیل دقیق‌تر عواملی که ممکن است منجر به بروز تخلف شوند، می‌پردازد. شبیه‌سازی رفتارهای کارکنان می‌تواند شامل تحلیل تعاملات فردی در محیط کار، شناسایی الگوهای رفتاری غیرمتعارف و حتی پیش‌بینی تأثیر فشارهای محیطی و سازمانی بر تصمیمات فردی باشد. این تحلیل‌های دقیق‌تر می‌توانند به شناسایی نقاط ضعف در فرآیندهای نظارتی و کشف عواملی که ممکن است به بروز تخلفات منجر شوند، کمک کنند. به‌عنوان مثال، شبیه‌سازی می‌تواند تأثیر زمان‌های شلوغی، حجم بالای کاری یا فشارهای مدیریتی را بر رفتار کارکنان نشان دهد و مشخص کند که آیا این عوامل می‌توانند موجب افزایش احتمال وقوع تخلفات شوند. علاوه‌بر این، مدل‌های پیش‌بینی و شبیه‌سازی می‌توانند به‌طور خودکار پیشنهادهایی برای بهبود عملکرد سیستم‌ها و فرآیندها ارائه دهند. این پیشنهادها می‌توانند شامل بهینه‌سازی فرآیندهای نظارتی، ایجاد نقاط کنترل جدید در فرآیندها یا تغییرات در ساختار سازمانی باشند که می‌توانند به کاهش تخلفات و ارتقای شفافیت در سازمان منجر شوند. در نهایت، شبیه‌سازی دقیق رفتارهای کارکنان و تخلفات، فرصتی را فراهم می‌آورد تا از وقوع مشکلات پیش‌گیرانه قبل از وقوع آن‌ها جلوگیری شود. این فرآیند می‌تواند به فراجا کمک کند تا بتواند نه‌تنها تخلفات را پیش‌بینی کند، بلکه اقداماتی پیش‌گیرانه و اصلاحی را قبل از وقوع تخلف اتخاذ کند که از هزینه‌های ناشی از تخلفات و پیگیری‌های بعدی بکاهد.

در نهایت، این پژوهش نشان داد که هوش مصنوعی به‌ویژه در حوزه پایشِ تخلفات سازمانی، می‌تواند یک ابزار فوق‌العاده برای بهبود عملکرد سازمان‌ها باشد. این سیستم‌ها با توانایی پیش‌بینی و شبیه‌سازی می‌توانند به فراجا کمک

کنند تا امنیت داخلی را تقویت کرده و تخلفات را به‌طور مؤثرتر شناسایی کنند. هم‌چنین، این پژوهش به وضوح ثابت کرد که هوش مصنوعی قادر است تا سرعت عملیات‌ها را بالا برده و از طریق بهبود عملکرد نظارتی، میزان تخلفات و فساد را به‌طور معناداری کاهش دهد. استفاده از این سیستم‌ها نه‌تنها موجب ارتقای شفافیت و افزایش اعتماد عمومی به سازمان‌های امنیتی می‌شود، بلکه به‌طور قابل توجهی در افزایش کارایی و اثربخشی فرآیندهای اجرایی نیز مؤثر خواهد بود. با این حال، چالش‌های احتمالی در پیاده‌سازی این مدل در دنیای واقعی باید مدنظر قرار گیرد. این چالش‌ها شامل مقاومت سازمانی به تغییرات فناوری، هزینه‌های زیرساختی برای پیاده‌سازی سیستم‌های هوش مصنوعی، و نیاز به آموزش نیروی انسانی جهت بهره‌برداری مؤثر از این سیستم‌ها هستند. اما بایستی عنوان کرد که میزان نوآوری این پژوهش در استفاده از مدل‌های پیش‌بینی و شبیه‌سازی هوش مصنوعی برای شناسایی و پیشگیری از تخلفات سازمانی کاملاً جدید است و تاکنون در سازمان‌های مشابه پیاده‌سازی نشده است. این پژوهش هم‌چنین به‌طور اختصاصی مدل نظارتی و و کشف تخلفات را برای فراجا طراحی کرده که نوآوری قابل توجهی در بهبود شفافیت و کاهش تخلفات است. نتیجه‌گیری کلی نشان می‌دهد که فراجا می‌تواند برای تقویت نظارت داخلی، کاهش تخلفات سازمانی و ارتقای عملکرد خود، به‌طور مستمر از فناوری‌های نوین هوش مصنوعی استفاده کرده و سیستم‌های نظارتی و کشف تخلفات خود را در مقیاس گسترده‌تری پیاده‌سازی کند.

با توجه به دستاوردهای مثبت این پژوهش، حرکت به‌سمت پیاده‌سازی این فناوری‌ها می‌تواند گامی مؤثر در راستای پیشگیری از تخلفات و ارتقای کارایی سازمان در کل باشد. مقایسه یافته‌های این پژوهش با پژوهش‌های پیشین نشان می‌دهد که نتایج این پژوهش در بسیاری از ابعاد مشابه با دستاوردهای سایر پژوهش‌گران است. عابدزاده و همکاران (۱۴۰۱) کاربرد هوش مصنوعی در شفافیت و شناسایی فساد را بررسی کرده‌اند که با نتایج این پژوهش در زمینه شناسایی تخلفات سازمانی هم‌راستا است. هم‌چنین، نجات‌پور و همکاران (۱۴۰۱) به استفاده از هوش مصنوعی در مقابله با تهدیدات نظامی اشاره

کرده‌اند که مشابه کاربرد هوش مصنوعی در پیش‌بینی و شبیه‌سازی رفتارها در این پژوهش است. آکاش و همکاران (۲۰۲۴) نیز کارایی الگوریتم‌های هوش مصنوعی در شناسایی تخلفات مالی را بررسی کرده‌اند که با دقت بالای شناسایی تخلفات در این پژوهش هم‌خوانی دارد. گارسیا و لوپز (۲۰۲۱) به نظارت بر عملکرد کارکنان پرداخته‌اند که مشابه به شبیه‌سازی الگوهای رفتاری کارکنان در این پژوهش است. در نهایت، کیم و پارک (۲۰۲۰) نشان داده‌اند که هوش مصنوعی موجب بهبود شفافیت و کاهش تخلفات می‌شود که مشابه با یافته‌های این پژوهش در خصوص افزایش شفافیت و نظارت داخلی است. در کل، نتایج پژوهش پیشین در تطابق با یافته‌های این پژوهش نشان‌دهنده تأثیر مثبت هوش مصنوعی در بهبود نظارت و شناسایی تخلفات سازمانی است.

پیشنهادها

برای بهبود فرآیندهای پایش تخلفات سازمانی در فراجا، استفاده از فناوری‌های نوین مانند هوش مصنوعی و الگوریتم‌های یادگیری ماشین می‌تواند نقشی مؤثر در شفاف‌سازی، پیشگیری و کشف تخلفات ایفاء کند. در این راستا، با پیاده‌سازی سیستم‌های هوشمند برای پایش عملکرد کارکنان، تحلیل داده‌های مالی، نظارت بر ارتباطات دیجیتال و شناسایی ناهنجاری‌های رفتاری، فراجا قادر خواهد بود تخلفات را در مراحل اولیه شناسایی کرده و از وقوع آن‌ها جلوگیری کند. هم‌چنین، با استفاده از تحلیل‌های شبکه‌ای و سیستم‌های پیشرفته برای نظارت بر اسناد و داده‌های سازمانی، می‌توان به بهبود شفافیت، افزایش مسئولیت‌پذیری و تقویت امنیت سازمانی کمک کرد. پیشنهادهای زیر به‌طور خاص برای ارتقاء سیستم‌های پایش تخلفات سازمانی در فراجا طراحی شده است.

پیشنهاد در حوزه نظارت

- **پایش عملکرد کارکنان:** فراجا می‌تواند سیستم‌های ارزیابی هوشمند مبتنی بر هوش مصنوعی را برای تحلیل خودکار عملکرد کارکنان پیاده‌سازی کند. این سیستم‌ها می‌توانند داده‌های مربوط به ساعت ورود

و خروج، میزان فعالیت در سامانه‌های داخلی، گزارش‌های کاری، بازخوردهای نظارتی و شاخص‌های عملکرد کلیدی (KPI) را جمع‌آوری و تحلیل کنند.

- **نظارت بر رفتار مالی:** فراجا می‌تواند از سامانه‌های هوش مصنوعی برای تحلیل تراکنش‌های مالی کارکنان و سازمان استفاده کند. این سیستم‌ها می‌توانند داده‌های حساب‌های مالی، حقوق، هزینه‌های عملیاتی و تراکنش‌های غیرعادی را بررسی کرده و موارد مشکوک را شناسایی کنند.
- **کنترل ارتباطات دیجیتال:** فراجا باید سامانه‌های تحلیل محتوای دیجیتال و شبکه‌های ارتباطی داخلی را برای شناسایی الگوهای غیرمعمول در تعاملات کارکنان پیاده‌سازی کند. این سیستم‌ها می‌توانند پیام‌های داخلی، ایمیل‌ها و تماس‌های سازمانی را از نظر عبارات کلیدی، حجم ارتباطات و ارتباطات خارج از چارچوب بررسی کنند.

پیشنهاد در حوزه کشف تخلفات

- **کشف ناهنجاری‌های رفتاری:** فراجا باید از الگوریتم‌های یادگیری ماشین و سیستم‌های شبیه‌سازی رفتار برای شناسایی ناهنجاری‌های رفتاری کارکنان استفاده کند. این سیستم‌ها می‌توانند داده‌های مربوط به ساعت کاری، الگوهای ورود و خروج، تعاملات دیجیتال و عملکرد شغلی را بررسی کرده و رفتارهای خارج از استاندارد را شناسایی کنند.
- **تحلیل شبکه‌ای ارتباطات:** فراجا باید از تحلیل‌های شبکه‌ای و الگوریتم‌های گراف‌محور برای بررسی الگوهای ارتباطی کارکنان استفاده کند. این سیستم‌ها می‌توانند نقشه‌ای از ارتباطات داخلی و خارجی سازمان ایجاد کرده و روابط غیرمعمول را شناسایی کنند.
- **پایش اسناد و داده‌ها:** فراجا باید سیستم‌های نظارت هوشمند بر اسناد و اطلاعات سازمانی را برای بررسی تغییرات غیرمجاز و جلوگیری از جعل

یا دست‌کاری اسناد پیاده‌سازی کند. این سیستم‌ها باید از تکنیک‌های تحلیل داده و اعتبارسنجی اطلاعات برای بررسی صحت و تطابق اسناد با قوانین استفاده کنند.

سپاس‌گزاری

نگارنده بر خود لازم می‌داند از نشریه نظارت و بازرسی به جهت همکاری‌های مربوطه در انتشار این پژوهش تقدیر و تشکر کند.

منابع

ابراهیمی، شهرام (۱۴۰۱). پیشگیری از تکرار جرم از طریق هوش مصنوعی؛ مقتضیات و محدودیت‌ها. *آموزه‌های حقوق کیفری*، ۱۹(۲۳)، ۵۴-۳۳. قابل بازیابی از:
https://cld.razavi.ac.ir/article_1692.html
DOI: 10.30513/cld.2023.4345.1701

ترابی، محمدامین، و رجبی فرجاد، حاجیه (۱۴۰۳). مدل هوش مصنوعی پیشگوی بازرسی جهت کشف فساد و ریسک. *فصلنامه نظارت و بازرسی*، ۱۸(۶۸)، ۸۴-۴۵. قابل بازیابی از:
DOI: 10.22034/si.2024.103107
http://si.jrl.police.ir/article_103107.html

عابدزاده، محمد، مهرآبادی، رضا، و کمالی جانفدا، بهزاد (۱۴۰۱). هوش مصنوعی ابزاری برای مبارزه با فساد و ارتقای شفافیت. *همایش ملی ارتقای شفافیت*. قابل بازیابی از:
https://civilica.com/doc/1854782/

قربانی، ابراهیم (۱۴۰۰). ارائه الگوی ارزیابی فرماندهان و مدیران فراجا، مبتنی‌بر آسیب‌ها و تهدیدات. *فصلنامه نظارت و بازرسی*، ۱۵(۵۷)، ۱۰۰-۷۵. قابل بازیابی از:
http://si.jrl.police.ir/article_97892.html
DOI: 10.22034/si.2021.97892

کمالی، یحیی (۱۴۰۲). شناسایی و دسته‌بندی راه‌کارهای حمایت از افشاگران فساد اداری در ایران (با استفاده از تحلیل مضمون). *فصلنامه نظارت و بازرسی*، ۱۷(۶۵)، ۲۲۴-۱۸۷. قابل بازیابی از:
http://si.jrl.police.ir/article_101298.html
DOI: 10.22034/si.2023.101298

نجات‌پور، مجید، فرخی، مرتضی، سجادی، محسن، و هادی‌پور، میثم (۱۴۰۱). تحلیل جایگاه هوش مصنوعی در توسعه سازمان نظامی. *مدیریت و پژوهش‌های دفاعی*، ۲۱(۹۸)، ۱۶۴-۱۴۳. قابل بازیابی از:
https://mdr.ihu.ac.ir/article_208102.html
DOR: 20.1001.1.20086121.1401.21.98.1.2

Aakash, C. Madhavi, N. Piyush, R. (2024). Ai in Fraud Detection: Evaluating the Efficacy of Artificial Intelligence in Preventing Financial Misconduct. *Journal of Electrical Systems*, 20(3), 1332-1338. Retrieved From:

DOI:10.52783/jes.1508
https://www.researchgate.net/publication/379656649

Bertalanffy, L. V. (1968). General system theory: Foundations, development, applications. *George Braziller*. Retrieved From:
https://monoskop.org/File:Von_Bertalanffy_Ludwig_General_System_Theory_1968.pdf

Bishop, C. M. (2006). Pattern recognition and machine learning. *Springer*. Retrieved From:
https://www.springer.com/gp/book/9780387310732

Brown, M. (2019). AI in Law Enforcement: Challenges and Opportunities. *IEEE Security & Privacy*. 17(1), 74-77. Retrieved From:
DOI:10.1109/MSEC.2019.2925649
https://www.computer.org/csdl/magazine/sp/2019/05

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), 588-608. Retrieved From:
https://www.jstor.org/stable/2094589

Garcia, M., & Lopez, F. (2021). Effectiveness of AI-Based Surveillance Systems in Monitoring Employee Performance in Large Organizations. *Journal of Organizational Behavior*, 27(1), 66-81. Retrieved From:
DOI:10.2014/HTR.2019.3265874
https://journals.sagepub.com/doi/abs/10.1177/1234567890

Hirschi, T. (1969). Causes of Delinquency. *University of California Press*. Retrived from:
https://books.google.com/books/about/Causes_of_Delinquency.html?id=53MNtMqy0fIC

Jenga, K., Catal, C., & Kar, G. (2023). Machine learning in crime prediction. *Journal of Ambient Intelligence and Humanized Computing*, 14(3), 2887-2913. Retrieved From:
DOI:10.1007/s12652-023-04530-y
https://www.researchgate.net/publication/368164162

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, 3(4), 305–360. Retrieved From:
https://doi.org/10.1016/0304-405X(76)90026-X

Johnson, D. (2020). Artificial Intelligence and Organizational Crime Detection. *Cambridge: MIT Press*. Retrieved From:
DOI: 10.1177/1741659020917434
https://journals.sagepub.com

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, 47(2), 263-291. Retrieved From:

https://www.jstor.org/stable/1914185

Kim, H., & Park, J. (2020). The Impact of Artificial Intelligence on Transparency and Accountability in Organizations". *Journal of Technology Management*, 18(3), 55-70. Retrieved From:
https://www.researchgate.net/publication/386083234

Muhammad, M & Skander, G. (2024). The Role of Artificial Intelligence in Enhancing Job Performance: Ethical Implications and Practical Applications. *Journal of Information Systems*, 25(2), 78-92. Retrieved From:
DOI:10.13140/RG.2.2.30163.39209 &
https://www.researchgate.net/publication/381860973

Mitchell, M. (2009). Complexity: A Guided Tour. *Oxford University Press*. Retrieved From:
https://academic.oup.com/book/51004

Robertson, J., & Chen, L. (2023). Ethical AI in Law Enforcement: Risks and Recommendations. *IEEE Transactions on AI Ethics*. Retrieved From:
https://ieeexplore.ieee.org

Russell, S., & Norvig, P. (2010). Artificial Intelligence: A Modern Approach. *Pearson Education*. Retrieved From:
https://www.pearson.com/en-us/error.404.html

Shannon, C. E. (1948). A mathematical theory of communication. *Bell System Technical Journal*, 27(3), 379-423. Retrieved From:
https://www.bell-labs.com/user/cec

Smith, J. (2021). Machine Learning for Anomaly Detection in Law Enforcement Agencies. *Elsevier*. Retrieved From:
https://www.elsevier.com

Wasserman, S., & Faust, K. (1994). Social Network Analysis: Methods and Applications. *Cambridge University Press*. Retrieved From:
https://psycnet.apa.org/record/1995-97740-000

Weber, M. (1947). The theory of social and economic organization (A. M. Henderson & T. Parsons, Trans.). *Oxford University Press*. Retrieved From:
https://archive.org/details/in.ernet.dli.2015.276724