



دانشکده فنی و مهندسی

کارشناسی ارشد مهندسی کامپیوتر نرم افزار

گروه مهندسی کامپیوتر و فناوری اطلاعات

گزارش سمینار

موضوع:

مدل پذیرش فناوری برای رایانش ابری، هوش مصنوعی داستان سرایی، و

برنامه مدیریت ریسک و مجوز فدرال

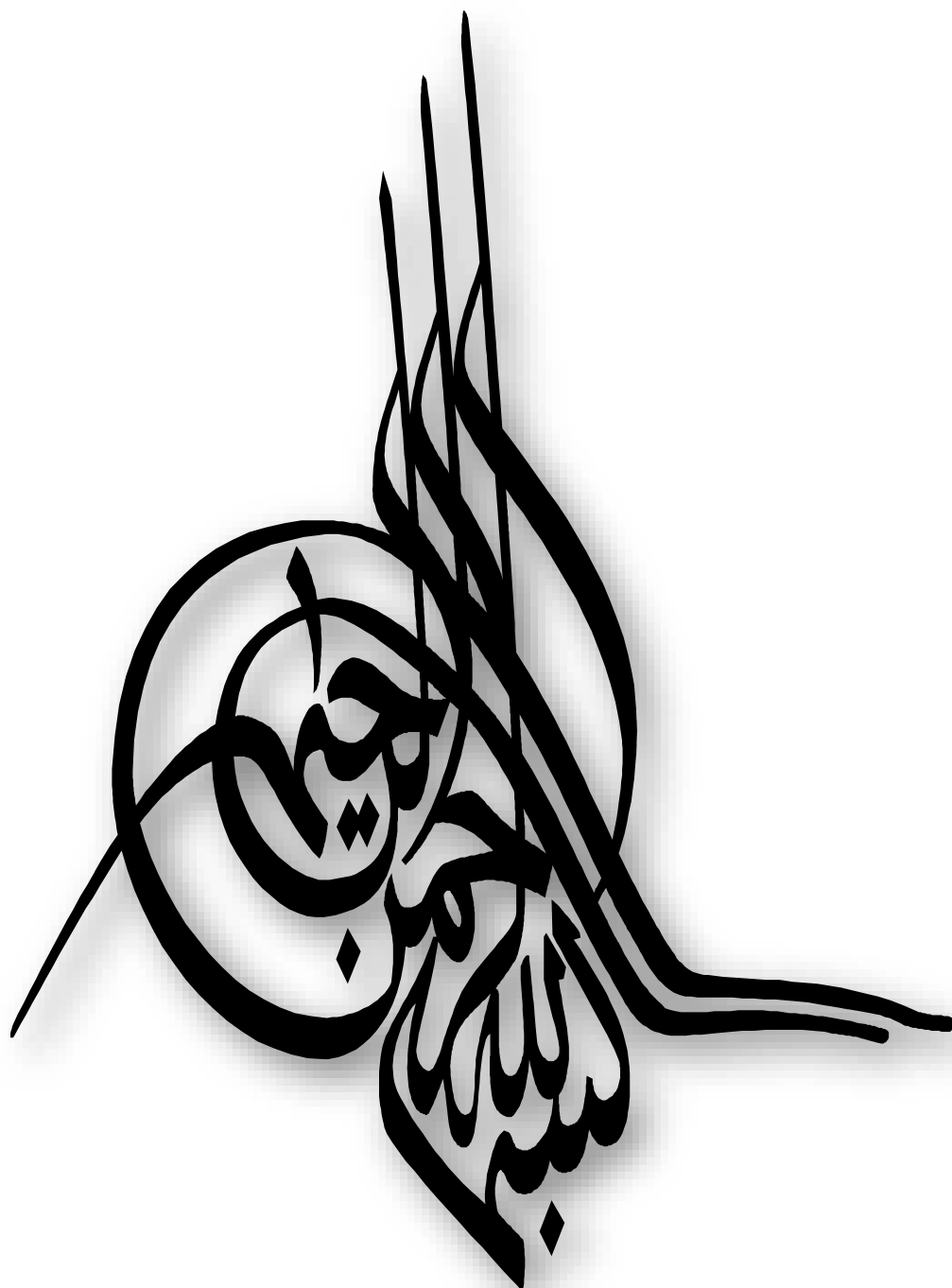
نگارش:

رضا آزاد مهر

استاد راهنما:

دکتر سید علی رضوی ابراهیمی

دی ۱۴۰۳



چکیده

این پایان‌نامه چالش‌ها و فرصت‌ها را در ادغام هوش مصنوعی مکالمه و یادگیری ماشینی (CAIML) دولت فدرال بررسی می‌کند. این بر تأثیر هوش مصنوعی مکالمه‌ای (CAI) بر تصمیم‌گیری در بخش‌ها و بهبود تعاملات انسان و فناوری، به‌ویژه در اینترنت اشیا و رایانش ابری تأکید دارد. این مطالعه داستان سرایی هوش مصنوعی، از جمله NLP، تولید شخصیت، VR/AR، یادگیری عمیق، رهبری و انطباق با FedRAMP را بررسی می‌کند. تحقیقات کیفی از PRISMA پیروی می‌کند و از NVivo برای تجزیه و تحلیل داده‌ها استفاده می‌کند. بررسی جامع ادبیات، تجزیه و تحلیل کیفی، و مصاحبه‌های متخصص چالش‌ها و فرصت‌های پذیرش CAIML را نشان می‌دهد. رهبری، عوامل اقتصادی و قانونی، حریم خصوصی، حفاظت از داده‌ها و امنیت ملی مورد مطالعه قرار می‌گیرند. پایان‌نامه با خلاصه‌ای از یافته‌ها و سؤالات تحقیقاتی خود در مورد موانع پذیرش آژانس فدرال CAI و ML، بهبودهای عملیاتی، مسائل قانونی/قانونی، حریم خصوصی، حفاظت از داده‌ها، تهدیدهای امنیتی، و استراتژی‌های رهبری مؤثر به پایان می‌رسد. ادغام CAI و ML در زیرساخت‌های فدرال و امنیت ملی و پیامدهای اطلاعاتی نیز مورد بحث قرار می‌گیرد. این پایان‌نامه به آژانس‌های فدرال توصیه می‌کند آموزش پرسنل، برنامه‌ریزی مهاجرت و پایداری راه‌حل را برای پیشبرد پذیرش CAIML در اولویت قرار دهند. این به سیاست‌گذاران و متخصصان فدرال کمک می‌کند تا فناوری‌های CAIML را با برجسته کردن پتانسیل‌ها و چالش‌های تحول‌آفرین آنها اتخاذ کنند.

کلمات کلیدی: یکپارچه‌سازی CAIML^۱، دولت فدرال^۲، رایانش ابری^۳، حریم خصوصی و حفاظت از داده‌ها^۴، شیوه‌های رهبری^۵.

^۱ CAIML integration

^۲ federal government

^۳ cloud computing

^۴ privacy and data protection

^۵ leadership practices

فهرست مطالب

عنوان صفحه

فصل اول: مقدمه

فصل اول ۱

مقدمه ۱

مقدمه ۲

۱-۱ تعریف مسئله و بیان سؤال‌های اصلی تحقیق و فرضیه ها ۳

۲-۲ سابقه و ضرورت انجام تحقیق ۵

۱-۳ هدف‌ها ۵

۴-۱ روش پژوهشی انجام شده ۶

۵-۱ مراحل انجام تحقیق ۶

۶-۱ روش انجام تحقیق ۶

۷-۱ داده های تحقیق چگونه به دست آمده اند ۷

۸-۱ چگونه نتایج را ارزیابی شده اند؟ ۷

۹-۱ ساختار گزارش تحقیق ۸

فصل دوم ۹

مفاهیم عمومی و تعاریف ۹

مقدمه ۱۰

۱-۲ مجوز فدرال (FedRAMP) ۱۰

۲-۲ هوش مصنوعی داستان‌گویی (Storytelling AI) ۱۱

۱-۲-۲ یکپارچگی هوش مصنوعی در استراتژی‌های امنیت ملی ۱۱

۲-۲-۲ چالش‌ها و فرصت‌های پذیرش هوش مصنوعی در بخش دولتی ۱۱

۲-۲-۳ ریسک‌ها و پیامدهای یکپارچگی هوش مصنوعی ۱۱

۲-۲-۴ نتیجه‌گیری ۱۱

۳-۲ مدیریت ریسک در داستان‌گویی با هوش مصنوعی (AI)	۱۲
۴-۲ مدیریت ریسک محیطی با هوش مصنوعی مکالمه‌ای (CAI)	۱۲
۵-۲ نگرانی‌های حریم خصوصی و امنیت در AI	۱۲
۱۶-۲ اخلاقی و ریسک‌های امنیتی در AI	۱۳
۷-۲ اجزای فناوری	۱۳
۱-۷-۲ جمع‌آوری و تحلیل داده‌ها	۱۳
۲-۷-۲ موتور پردازش زبان طبیعی (NLP)	۱۴
۳-۷-۲ تولید شخصیت و انیمیشن	۱۴
۴-۷-۲ تولید دیالوگ	۱۴
۵-۷-۲ فناوری‌های واقعیت مجازی	۱۵
۶-۷-۲ شناسایی و شبیه‌سازی احساسات	۱۵
۷-۷-۲ شخصی‌سازی و سازگاری	۱۶
۸-۷-۲ یادگیری عمیق با گراف	۱۶
۹-۷-۲ ترکیب یادگیری ماشین با وب معنایی	۱۷
۸-۲ نتیجه‌گیری	۱۷
فصل سوم	۱۸
مروری بر کارهای انجام‌شده	۱۸
مقدمه	۱۹
۱-۱۱-۲ ابزار و فرآیندهای جمع‌آوری داده‌ها	۱۹
۱-۱-۳ امضای‌های نیمه‌ساختاریافته	۱۹
۲-۱-۳ مشاهدات	۱۹
۳-۱-۳ تحلیل مستندات	۱۹
۴-۱-۳ نرم افزار NVivo	۱۹
۲-۲ فرآیندهای تحلیل داده‌ها	۲۰
مرحله ۱: آماده‌سازی داده‌ها	۲۰
مرحله ۲: کدگذاری اولیه	۲۰

گام ۳: توسعه تم‌ها	۲۰
گام ۴: مقایسه داده‌ها	۲۱
گام ۵: بررسی اعضا (Member Checking)	۲۱
گام ۶: بازتاب و برنامه‌ریزی اقدام	۲۱
۳-۳ بحث در مورد فرآیند تحلیل داده‌ها	۲۱
اعتمادپذیری (Trustworthiness)	۲۲
اعتبار (Credibility)	۲۲
انتقال‌پذیری (Transferability)	۲۲
قابلیت اعتماد (Dependability)	۲۲
تاییدپذیری (Confirmability)	۲۲
۳-۴ پذیرش رایانش ابری	۲۳
۳-۵ ادغام هوش مصنوعی در داستان‌گویی	۲۴
۳-۶ رعایت استانداردهای FedRAMP	۲۷
۳-۷ جمع‌بندی	۲۹
فصل چهارم	۳۰
پاسخ به سوالات تحقیق	۳۰
مقدمه	۳۱
۴-۴-۱ چالش‌های پذیرش هوش مصنوعی مکالمه‌ای و یادگیری ماشین در سازمان‌های دولتی فدرال	۳۱
۴-۴-۲ بهبود عملیات و فرآیندهای تصمیم‌گیری در سازمان‌های دولتی فدرال از طریق هوش مصنوعی و یادگیری ماشین	۳۱
۴-۴-۳ پیامدهای اقتصادی پذیرش هوش مصنوعی و یادگیری ماشین در سازمان‌های دولتی فدرال	۳۲
۴-۴-۴ پیامدهای اقتصادی پذیرش هوش مصنوعی و یادگیری ماشین در سازمان‌های دولتی فدرال	۳۲
۴-۴-۵ نگرانی‌های حریم خصوصی و حفاظت از داده‌ها در استفاده از مدل‌های زبانی بزرگ (LLMs)	۳۳
۴-۴-۶ مدیریت خطرات امنیتی در LLM‌ها برای سازمان‌های دولتی	۳۴
۴-۴-۷ ادغام هوش مصنوعی و یادگیری ماشین در زیرساخت‌های دولت فدرال	۳۶
۴-۴-۸ پیامدهای هوش مصنوعی مکالمه‌ای و یادگیری ماشین در امنیت ملی و اطلاعات	۳۷

نتیجه گیری ۳۹

فصل پنجم ۴۰

جمع بندی و پیشنهادها ۴۰

مقدمه ۴۱

۵- ۱ نتایج حاصل از تحقیق ۴۱

۵-۱-۱ شناسایی موانع اصلی پذیرش فناوری های هوشمند در سازمان های دولتی ۴۱

۵-۱-۲ مزایای پذیرش فناوری های هوشمند ۴۱

۵-۱-۳ نقش امنیت داده ها در پذیرش فناوری های هوشمند ۴۲

۵-۱-۴ ضرورت به روز رسانی قوانین و مقررات ۴۲

۵- ۲ پیشنهادها ۴۲

۵-۲-۱ بررسی تأثیرات بلند مدت پذیرش فناوری های هوشمند در سازمان های دولتی ۴۲

۵-۲-۲ توسعه مدل های پذیرش فناوری به ویژه برای بخش های دولتی ۴۲

۵-۲-۳ تحلیل چالش های مرتبط با امنیت داده ها در سطح جهانی ۴۲

۵-۲-۴ مطالعه بر روی مدل های آموزشی برای کارکنان دولتی ۴۲

۵-۲-۵ بررسی تأثیرات اجتماعی و فرهنگی پذیرش فناوری در سازمان های دولتی ۴۲

۵-۲-۶ تحلیل قوانین و مقررات برای تسهیل پذیرش فناوری های نوین ۴۳

۵- ۳ توصیه ها ۴۳

۵-۳-۱ برای آژانس های دولتی فدرال ۴۳

۵-۳-۲ برای سیاست گذاران ۴۳

۵-۳-۳ برای محققان ۴۳

۵-۳-۴ برای تمامی ذینفعان ۴۴

۵-۳-۵ توصیه های خاص ۴۴

۵- ۴ جمع بندی و نتیجه گیری ۴۴

مراجع ۴۶

مراجع ۴۷

فهرست جداول

عنوان صفحه

- جدول ۱: ماتریس کدگذاری پذیرش رایانش ابری ۲۴
- جدول ۲: موضوعات نوظهور در پذیرش رایانش ابری ۲۵
- جدول ۳: ماتریس کدگذاری هوش مصنوعی داستان گویی ۲۶
- جدول ۴: موضوعات نوظهور در هوش مصنوعی داستان گویی ۲۷
- جدول ۵: ماتریس کدگذاری برنامه مدیریت ریسک و مجوز فدرال (FedRAMP) ۲۸
- جدول ۶: موضوعات نوظهور در برنامه مدیریت ریسک و مجوز فدرال (FedRAMP) ۲۹

مخفف	توضیح
AI	Artificial Intelligence (هوش مصنوعی)
ML	Machine Learning (یادگیری ماشین)
CAI	Conversational Artificial Intelligence (هوش مصنوعی گفتاری)
CAIML	Conversational AI and Machine Learning (هوش مصنوعی گفتاری و یادگیری ماشین)
IoT	Internet of Things (اینترنت اشیا)
FedRAMP	Federal Risk and Authorization Management Program (برنامه مدیریت ریسک و مجوزدهی فدرال)
NLP	Natural Language Processing (پردازش زبان طبیعی)
VR	Virtual Reality (واقعیت مجازی)
AR	Augmented Reality (واقعیت افزوده)
LLM	Large Language Model (مدل زبان بزرگ)
HCI	Human-Computer Interaction (تعامل انسان و کامپیوتر)
XML	Extensible Markup Language (زبان نشانه‌گذاری توسعه‌پذیر)
DOM	Document Object Model (مدل شیء‌نگرای سند)
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses (موارد گزارش ترجیحی) (برای مرورهای سیستماتیک و متاآنالیز)
NVivo	نرم‌افزار تحلیل داده‌های کیفی
IRB	Institutional Review Board (کمیته بررسی اخلاقی)
GDPR	General Data Protection Regulation (مقررات عمومی حفاظت از داده‌ها)
HIPAA	Health Insurance Portability and Accountability Act (قانون انتقال و مسئولیت بیمه سلامت)
FISMA	Federal Information Security Management Act (قانون مدیریت امنیت اطلاعات فدرال)
FAR	Federal Acquisition Regulation (مقررات خرید فدرال)
SCCs	Standard Contractual Clauses (بندهای قرارداد استاندارد)
BCRs	Binding Corporate Rules (قوانین الزام‌آور شرکتی)

فصل اول

مقدمه

هوش مصنوعی مکالمه‌ای^۱ (CAI) در چشم‌انداز تکنولوژی کنونی، کنترل تصمیم‌گیری در بسیاری از حوزه‌های کسب‌وکار و پلتفرم‌های نوآورانه دانش‌محور را به دست گرفته است. با وجود تاریخچه طولانی CAI، این حوزه همچنان با چالش‌هایی روبرو است. این پیشرفت فناوری به طور قابل توجهی به این فناوری نوآورانه سود رسانده است. همچنین، پیشرفت‌ها در علوم و مهندسی، جایی که تأثیر این بهبودها مشاهده می‌شود، بیشتر هنگامی رخ می‌دهند که نوآوری به‌درستی مدیریت شود. روش‌ها و رویکردهای جدید در یادگیری ماشین^۲ (ML) نیز به دلایلی مشابه با CAI مورد توجه قرار گرفته‌اند. هرچند هوش مصنوعی مکالمه‌ای از مدت‌ها پیش وجود داشته است، اما اخیراً به سطحی از اطمینان دست یافته که می‌توان آن را به‌عنوان CAI با اطمینان بیشتری طبقه‌بندی کرد. پیشرفت‌های اخیر در حوزه CAI و ML به شکل قابل توجهی به توسعه سیستم‌های جدید و امن‌تر مبتنی بر اینترنت اشیا (IoT) و رایانش ابری کمک کرده‌اند (Rath et al., ۲۰۲۱). این پژوهش تحلیلی عمیق از چالش‌های مرتبط با استفاده از CAI و ML در محیط‌های اینترنت اشیا^۳ و رایانش ابری فدرال ارائه می‌دهد. همچنین فرایندی به نام CAIML را معرفی می‌کند که هوش مصنوعی مکالمه‌ای و یادگیری ماشین را با مدل‌های آسان‌های نوآوری ترکیب می‌کند. (Ferguson, n/d; ۲۰۲۰; Reunanen et al., ۲۰۲۰; Ojeda, ۲۰۲۲; Schleith, ۲۰۲۳; Ojeda, ۲۰۲۰; Hawryszkiewicz, ۲۰۲۱)

۱-۱ تعریف مسئله و بیان سوال‌های اصلی تحقیق

بیان مسئله بر این ضرورت تأکید دارد که رهبران در دولت فدرال^۴ باید به‌طور فعال روش‌های حفظ حریم خصوصی و رویکردهای نوآورانه را برای رسیدگی به نگرانی‌های امنیتی مرتبط با مدل‌های زبانی بزرگ در زمینه پذیرش رایانش ابری به‌کار گیرند. با استفاده از روش‌های دقیق PRISMA و NVivo، این پژوهش نتایج قابل اطمینان و بینش‌های ارزشمندی تولید می‌کند که به رهبران کمک می‌کند تصمیم‌های آگاهانه بگیرند، حفاظت از داده‌ها را در اولویت قرار دهند و الزامات قانونی را رعایت کنند. این پژوهش با بهره‌گیری از تحلیل‌های سیستماتیک و ابزارهای پیشرفته، ابزاری قدرتمند برای حمایت از رهبران در راستای تصمیم‌گیری بهتر و مقابله با چالش‌های امنیتی و عملیاتی فراهم می‌آورد. بیان مسئله بر چالش‌ها و فرصت‌های پذیرش رایانش ابری در دولت فدرال متمرکز است، با تأکید ویژه بر جنبه‌های اقتصادی، قانونی و دسته‌بندی (Ash & Hansen, ۲۰۲۲; Mukhamediev et al., Federal ۲۰۲۲; Park & Kim, ۲۰۲۲). زیرساخت فناوری اطلاعات دولت فدرال با مشکلات متعددی از جمله نیازهای پراکنده منابع، سیستم‌های تکراری، تنظیمات مدیریتی پیچیده، و زمان‌های طولانی فرآیند تأمین منابع روبرو است. این مشکلات منجر به ارائه ناکارآمد خدمات عمومی می‌شوند (Kundra, ۲۰۱۱). رشد نمایی رایانش ابری باعث افزایش مصرف و تولید داده شده است و شرکت‌های فعال در این حوزه را ملزم به پذیرش مالکیت فکری جدید برای پاسخگویی به تقاضاهای چشم‌انداز در حال تغییر می‌کند (Ash & Hansen, ۲۰۲۲; Mukhamediev et al., Federal ۲۰۲۲; Park & Kim, ۲۰۲۲). سادگی و قدرت آن، در سال ۲۰۰۵ Mapreduce را در Nutch ادغام کرد. در فوریه ۲۰۰۶، Cutting NDfs و Mapreduce را از Nutch استخراج نمود و پروژه جدیدی را تحت نظر Lucene آغاز کرد. وی سیستم جدید را Hadoop نامید و آن را Open Source ساخت. (Revathi, et. al., ۲۰۱۹)

این مسئله از اهمیت بالایی برخوردار است و پیامدهایی در حوزه‌های مختلف از جمله امنیت ملی، اخلاقیات، امنیت سایبری، ژئوپلیتیک و ارتباطات دارد. گنجاندن هوش مصنوعی^۵ (AI)، به‌ویژه مدل‌های زبانی بزرگ^۶ (LLMs)، در استراتژی‌های امنیت ملی و تحلیل اطلاعات، به‌عنوان یک ضرورت حیاتی شناخته می‌شود (Mikhailov, ۲۰۲۳). با این حال، استفاده از هوش مصنوعی در تحلیل اطلاعات و مقابله با تروریسم باعث ایجاد نگرانی‌های اخلاقی می‌شود (Blanchard & Taddeo, ۲۰۲۳; Esmailzadeh, ۲۰۲۳). علاوه بر این، مدل‌های زبانی بزرگ و هوش مصنوعی مولد خطرات امنیتی قابل توجهی ایجاد می‌کنند، همان‌طور که Derner و Batistič (۲۰۲۳) و Adomaitis و Grinbaum (۲۰۲۳) اشاره کرده‌اند. اجرای فناوری‌های پیشرفته مانند هوش مصنوعی نیاز به بهبود پروتکل‌های امنیت سایبری دارد (Oxford Analytica, ۲۰۲۳). از سوی دیگر، جنبه‌های ژئوپلیتیکی هوش مصنوعی، به‌ویژه در آسیای مرکزی و مقابله با تهدیدات چینی، بر اهمیت این موضوع می‌افزاید (KÜÇÜKSOLAK & FIRAT, ۲۰۲۳; Pathak & Jindal, ۲۰۲۳). استفاده از هوش مصنوعی در جنگ‌های ترکیبی و اطلاعاتی چالش‌های جدیدی را به همراه دارد که باید در تحلیل‌ها و استراتژی‌های دفاعی در نظر گرفته شوند.

^۱ Conversational Artificial Intelligence

^۴ federal government

^۲ Machine Learning

^۵ Artificial Intelligence

^۳ cloud computing

^۶ Large Language Model

سؤالات تحقیق

هدف اصلی این رساله، بررسی پذیرش هوش مصنوعی مکالمه‌ای و یادگیری ماشین (CAIML) در رایانش ابری در دولت فدرال است، با تمرکز بر چالش‌ها و فرصت‌های مرتبط با این یکپارچگی. برای رسیدن به این هدف، پرسش‌های تحقیقاتی زیر مطرح شده است:

(۱) چالش‌های اصلی که آژانس‌های دولتی فدرال در پذیرش هوش مصنوعی مکالمه‌ای و یادگیری ماشین در رایانش ابری با آن مواجه هستند، چیست؟

(۲) چگونه یکپارچگی هوش مصنوعی مکالمه‌ای و یادگیری ماشین می‌تواند کارایی و اثربخشی عملیات و فرایندهای تصمیم‌گیری آژانس‌های دولتی فدرال را بهبود بخشد؟

(۳) پیامدهای اقتصادی پذیرش هوش مصنوعی مکالمه‌ای و یادگیری ماشین در رایانش ابری برای آژانس‌های دولتی فدرال چیست؟

(۴) ملاحظات قانونی و نظارتی که باید در پذیرش هوش مصنوعی مکالمه‌ای و یادگیری ماشین در رایانش ابری در دولت فدرال مورد توجه قرار گیرد، چیست؟

(۵) نگرانی‌های حریم خصوصی و حفاظت از داده‌ها در ارتباط با استفاده از مدل‌های زبانی بزرگ (LLMs) در برنامه‌های هوش مصنوعی مکالمه‌ای و یادگیری ماشین چیست؟

(۶) چگونه آژانس‌های دولتی فدرال می‌توانند به طور مؤثر به خطرات امنیتی و آسیب‌پذیری‌های مرتبط با استفاده از مدل‌های زبانی بزرگ در هوش مصنوعی مکالمه‌ای و یادگیری ماشین رسیدگی کنند؟

(۷) چه شیوه‌های رهبری و استراتژی‌هایی برای پیاده‌سازی موفق طرح‌های هوش مصنوعی مکالمه‌ای و یادگیری ماشین در دولت فدرال لازم است؟

(۸) چگونه آژانس‌های دولتی فدرال می‌توانند اطمینان حاصل کنند که مهاجرت و یکپارچگی فناوری‌های هوش مصنوعی مکالمه‌ای و یادگیری ماشین به زیرساخت‌های موجود خود به صورت روان و مؤثر انجام می‌شود؟

(۹) پیامدهای پذیرش CAIML برای امنیت ملی و تحلیل اطلاعات در دولت فدرال چیست؟

فرضیه ۱: در دسترس بودن داده‌های کافی و مرتبط

این فرض بر این است که منابع موجود شامل ادبیات، گزارش‌ها، مطالعات موردی و دیگر منابع مرتبط در حوزه عمومی در دسترس خواهند بود که به پذیرش CAIML در رایانش ابری در دولت فدرال پرداخته‌اند. تحقیق بر اساس این منابع برای جمع‌آوری اطلاعات و بینش‌های لازم برای تحلیل استوار خواهد بود.

فرضیه ۲: دقت و قابلیت اطمینان داده‌ها

این فرض بر این است که اطلاعات به‌دست‌آمده از منابع منتخب دقیق و قابل اطمینان خواهند بود. تحقیق به طور انتقادی اعتبار و صحت منابع داده‌ها را ارزیابی خواهد کرد تا اطمینان حاصل شود که یافته‌ها و نتایج تحقیق معتبر هستند.

فرضیه ۳: رعایت اصول اخلاقی تحقیق

این تحقیق فرض می‌کند که تمام ملاحظات اخلاقی لازم در طول مطالعه رعایت خواهد شد. این شامل دریافت مجوزهای مناسب، اطمینان از حفاظت از اطلاعات شخصی، و پیروی از دستورالعمل‌های اخلاقی برای جمع‌آوری داده‌ها، تحلیل و گزارش‌دهی است.

فرضیه ۴: قابلیت تعمیم نتایج

این تحقیق فرض می‌کند که نتایج و یافته‌های به‌دست‌آمده از مطالعه، بینش‌ها و توصیه‌هایی ارائه خواهند داد که قابل تعمیم و ارزشمند برای آژانس‌های دولتی فدرال در چارچوب تعریف شده باشند. با این حال، به طور هم‌زمان پذیرفته می‌شود که زمینه‌ها، سیاست‌ها و چالش‌های خاص هر آژانس ممکن است متفاوت باشد و بنابراین قابلیت تعمیم یافته‌ها محدود باشد.

فرضیه ۵: آمادگی و همکاری شرکت‌کنندگان

این تحقیق فرض می‌کند که آژانس‌های دولتی فدرال و ذی‌نفعان آن‌ها آماده و مایل به ارائه اطلاعات و بینش‌های مرتبط با مطالعه خواهند بود. انتظار می‌رود که افراد کلیدی—شامل سیاست‌گذاران، رهبران و متخصصان—همکاری کرده و تجربیات و دیدگاه‌های خود را به طور شفاف به اشتراک بگذارند.

فرضیه ۶: پیشرفت‌های فناوری

این تحقیق فرض می‌کند که زیرساخت فناوری موجود و پیشرفت‌های مربوط به CAIML در دولت فدرال، پایه مناسبی برای تحلیل فراهم خواهند کرد. انتظار می‌رود که چشم‌انداز فناوری از یکپارچگی و پذیرش CAIML پشتیبانی کند و امکان تولید بینش‌ها و توصیه‌های معنادار را فراهم آورد.

فرضیه ۷: استمرار سیاست‌ها و مقررات

این تحقیق فرض می‌کند که سیاست‌ها، مقررات و چارچوب‌های مرتبط با پذیرش CAIML در دولت فدرال در طول دوره تحقیق نسبتاً پایدار خواهند بود. هر گونه تغییرات یا تحولات عمده در سیاست‌ها ممکن است بر نتایج و نتایج تحقیق تأثیر بگذارد.

بحث فرضیات

این فرضیات فرایند تحقیق را هدایت کرده و دیدگاه محقق را شکل می‌دهند. این فرضیات به‌عنوان بخشی ذاتی از مطالعه شناخته می‌شوند و چارچوبی برای انجام تحقیق در مرزها و انتظارات منطقی فراهم می‌آورند.

۲-۱ سابقه و ضرورت انجام تحقیق

در سال‌های اخیر، پذیرش فناوری‌های نوین به‌ویژه هوش مصنوعی و رایانش ابری در بسیاری از حوزه‌ها از جمله دولت‌ها و سازمان‌های دولتی موردتوجه قرار گرفته است. این فناوری‌ها به دلیل قابلیت‌هایی چون افزایش بهره‌وری، کاهش هزینه‌ها و بهبود تصمیم‌گیری، به طور گسترده‌ای در سازمان‌های مختلف مورد مطالعه قرار گرفته‌اند. اما به‌رغم این مزایا، پذیرش این فناوری‌ها در سازمان‌های دولتی با مشکلات و چالش‌هایی مواجه است. پژوهش در زمینه پذیرش فناوری‌های هوشمند، به‌ویژه در سازمان‌های دولتی، از چندین دهه پیش آغاز شده و در طول زمان بر اساس پیشرفت فناوری و تغییرات اجتماعی، گسترش یافته است. دوره زمانی تحقیق به دهه اخیر محدود است و پیشرفت‌های اخیر در زمینه پذیرش CAIML را بدون پرداختن به جزئیات فنی الگوریتم‌های خاص بررسی می‌کند. با استفاده از PRISMA و NVivo، تحقیق اطمینان حاصل می‌کند که بررسی پذیرش CAIML ۱ به صورت سیستماتیک و جامع انجام شود و هدف آن اطلاع‌رسانی و راهنمایی تصمیم‌گیرندگان و مجریان دولتی در این حوزه فناوری است.

نتیجه‌گیری: پیشینه تحقیق نشان می‌دهد که پذیرش فناوری‌های هوشمند در سازمان‌های دولتی موضوعی چندوجهی است که نیازمند توجه به ابعاد امنیتی، فرهنگی، و قانونی است. این تحقیق با تمرکز بر این چالش‌ها، تلاش می‌کند مدل‌ها و راهکارهایی برای تسهیل پذیرش این فناوری‌ها ارائه دهد.

۱ - ۳ اهداف تحقیق

این رساله قصد دارد به بررسی پیچیدگی‌های پذیرش رایانش ابری، هوش مصنوعی داستان‌گو و FedRAMP در دولت فدرال^۲ بپردازد. تمرکز اصلی این تحقیق بر ارزیابی مدل پذیرش فناوری در این زمینه است و تحلیل جامع جوانب مختلف از جمله استراتژی‌های رهبری، ملاحظات اقتصادی و قانونی، حریم خصوصی داده‌ها و حفاظت از آن‌ها را ارائه می‌دهد. این مطالعه از روش‌های تحلیل کیفی، از جمله دستورالعمل‌های PRISMA برای بررسی سیستماتیک و نرم‌افزار NVivo (نسخه ۱۴) برای تحلیل داده‌ها استفاده می‌کند تا بررسی دقیقی از چالش‌ها و فرصت‌های مرتبط با پذیرش هوش مصنوعی مکالمه‌ای و یادگیری ماشین (CAIML) انجام دهد. با بررسی یکپارچه‌سازی هوش مصنوعی مکالمه‌ای و یادگیری ماشین در زیرساخت‌های فدرال، این تحقیق هدف دارد تا به طور قابل توجهی به امنیت ملی و اطلاعاتی کشور کمک کند و اهمیت یادگیری مداوم و نوآوری در آژانس‌های دولتی را برجسته سازد. پذیرش رایانش ابری، به‌ویژه یکپارچه‌سازی CAIML، چالش‌ها و فرصت‌هایی را برای دولت فدرال به همراه دارد. پذیرش CAIML می‌تواند به بهبود کارایی عملیاتی و تصمیم‌گیری در آژانس‌های دولتی فدرال کمک کند. با این حال، جنبه‌های اقتصادی، قانونی، نظارتی، امنیتی و رهبری باید برای پذیرش موفق در نظر گرفته شوند. تحقیق در نظر دارد این مسائل را بررسی کرده و بینش‌ها و توصیه‌هایی برای آژانس‌های دولتی فدرال ارائه دهد. دامنه مطالعه به پذیرش CAIML در دولت فدرال ایالات متحده محدود است و روش‌های تحقیق کیفی برای تضمین تحلیل جامع و دقیق استفاده خواهند شد.

۱-۴ چه روش پژوهشی را استفاده کرده است؟

این تحقیق از روش کیفی بهره گرفته است که برای بررسی عمیق چالش‌ها و فرصت‌های پذیرش فناوری‌های هوش مصنوعی محاوره‌ای (CAI) و یادگیری ماشین (ML) در سازمان‌های دولتی طراحی شده است.

- از دستورالعمل‌های PRISMA برای مرور نظام‌مند ادبیات و انتخاب منابع مرتبط استفاده شده است.
- داده‌ها از طریق مرور ادبیات، مصاحبه‌های نیمه‌ساختاریافته با کارشناسان و تحلیل اسناد و مشاهدات سازمانی جمع‌آوری شده‌اند.
- تحلیل داده‌ها با استفاده از نرم‌افزار NVivo نسخه ۱۴ انجام شده است، که شامل کدگذاری، توسعه تم‌ها و شناسایی الگوها بوده است.
- از مثلث‌سازی داده‌ها (Data Triangulation) برای ترکیب و بررسی داده‌های مختلف جهت افزایش اعتبار نتایج استفاده شده است.
- رویکرد پژوهش، اکتشافی بوده و بر شناسایی چالش‌ها، فرصت‌ها و ارائه راه‌حل‌ها تمرکز داشته است.

۱-۵ مراحل انجام تحقیق

روش تحقیق این رساله بر اساس دستورالعمل‌های PRISMA و نرم‌افزار NVivo (نسخه ۱۴) طراحی شده است که امکان بررسی سیستماتیک و تحلیل کیفی ادبیات و داده‌های مرتبط را فراهم می‌آورد. با استفاده از دستورالعمل‌های PRISMA، این مطالعه اطمینان حاصل می‌کند که بررسی موجود از دانش علمی به صورت دقیق و جامع انجام می‌شود. نرم‌افزار NVivo نیز به تحلیل داده‌ها کمک خواهد کرد و امکان بررسی عمیق و تفسیر داده‌های کیفی را فراهم می‌آورد.

هدف این رساله تحلیل چالش‌ها و فرصت‌های پذیرش هوش مصنوعی مکالمه‌ای و یادگیری ماشین (CAIML) در محیط‌های ابری در دولت فدرال ایالات متحده است. این تحقیق از یک رویکرد کیفی استفاده کرده و از دستورالعمل‌های PRISMA برای بررسی سیستماتیک و نرم‌افزار NVivo (نسخه ۱۴) برای تحلیل داده‌ها بهره می‌برد. مطالعه بر آژانس‌های مختلف دولتی فدرال تمرکز خواهد کرد و دیدگاه‌های متنوعی از سیاست‌گذاران، رهبران و متخصصان جمع‌آوری خواهد کرد. این دیدگاه‌ها در چارچوب قانونی خاص دولت فدرال ایالات متحده تحلیل و تبیین می‌شوند. دوره زمانی تحقیق به دهه اخیر محدود است و پیشرفت‌های اخیر در زمینه پذیرش CAIML را بدون پرداختن به جزئیات فنی الگوریتم‌های خاص بررسی می‌کند. با استفاده از PRISMA و NVivo، تحقیق اطمینان حاصل می‌کند که بررسی پذیرش CAIML به صورت سیستماتیک و جامع انجام شود و هدف آن اطلاع‌رسانی و راهنمایی تصمیم‌گیرندگان و مجریان دولتی در این حوزه فناوری است.

۱-۶ روش انجام تحقیق

تحقیق حاضر از نوع تحقیق کیفی با استفاده از تحلیل محتوا و مطالعه موردی است. دلیل انتخاب این نوع تحقیق، تمرکز بر بررسی تجربیات و چالش‌های واقعی در پذیرش فناوری‌های نوین در سازمان‌های دولتی است. در این تحقیق از مدل‌های تحلیلی و داده‌های تجربی برای استخراج الگوها و شناسایی موانع و فرصت‌ها استفاده خواهد شد. روش تحقیق بر تحلیل کیفی مبتنی خواهد بود و از دستورالعمل‌های PRISMA برای بررسی سیستماتیک و نرم‌افزار NVivo (نسخه ۱۴) برای تحلیل داده‌ها استفاده خواهد کرد. روش‌های کمی یا رویکردهای تحقیقاتی دیگر در این مطالعه به کار نخواهند رفت. این تحقیق از یک روش شناسی تحقیق عمل‌گرا استفاده می‌کند که به طور هم‌زمان از مرور سیستماتیک ادبیات، تحلیل کیفی با استفاده از نرم‌افزار NVivo (نسخه ۱۴) و مصاحبه‌ها/مطالعات کارشناسی بهره می‌برد. این رویکرد ذاتاً کیفی است و امکان بررسی عمیق مدل پذیرش فناوری برای رایانش ابری، هوش مصنوعی داستان‌گویی و FedRAMP، از جمله نقش تأثیرگذار هوش مصنوعی داستان‌گویی در پذیرش سازمانی این فناوری‌ها را فراهم می‌کند. چارچوب تحقیق عمل‌گرا با مرور سیستماتیک ادبیات آغاز می‌شود که با راهنمایی چارچوب PRISMA برای گردآوری و ارزیابی مقالات تحقیقاتی مرتبط، به منظور ساخت یک چشم‌انداز جامع از دانش موجود در این حوزه انجام می‌گیرد. مرحله بعد شامل تحلیل کیفی با استفاده از NVivo (نسخه ۱۴) است که در آن به کدگذاری، دسته‌بندی و استخراج بینش‌ها از داده‌های به دست آمده از مصاحبه‌ها/مطالعات کارشناسی پرداخته می‌شود. این تعاملات با کارشناسان، از طریق مصاحبه‌های نیمه‌ساختاریافته، به منظور کاوش در تجربیات و دیدگاه‌های متخصصان این حوزه طراحی شده‌اند و بینش‌های کیفی غنی را ارائه می‌دهند. جمع‌آوری داده‌ها از طریق نمونه‌گیری هدفمند به طور دقیق طراحی شده و گروهی متنوع از حدود ۵۰۰ حرفه‌ای، کارشناس و متخصص هدف قرار خواهد گرفت. استخدام از شبکه‌های حرفه‌ای، رویدادهای صنعتی و پلتفرم‌های آنلاین استفاده می‌کند. ملاحظات اخلاقی در این تحقیق از اهمیت بالایی برخوردار است؛ رضایت‌نامه آگاهانه دریافت می‌شود و جمع‌آوری داده‌ها شامل مصاحبه‌ها، مشاهدات و تحلیل مستندات خواهد بود تا حقوق مشارکت‌کنندگان و یکپارچگی داده‌ها حفظ شود. چارچوب

تحلیل داده‌ها جامع است و شامل آماده‌سازی داده‌ها، کدگذاری اولیه، توسعه تم‌ها، مقایسه داده‌ها، بررسی اعضا و برنامه‌ریزی عمل انعکاسی می‌باشد. NVivo (نسخه ۱۴) نقش محوری در این فرآیند دارد و ابزار کارآمدی برای مدیریت و تحلیل داده‌های کیفی فراهم می‌آورد. طبیعت تدریجی تحقیق عمل‌گرا مزیت اصلی این تحقیق است، زیرا امکان اصلاح و بهبود مداوم تحلیل را فراهم می‌کند. اعتمادپذیری به‌عنوان یکی از ارکان این تحقیق در نظر گرفته شده است و از طریق رعایت معیارهای اعتبار، انتقال‌پذیری، قابلیت اعتماد و تأییدپذیری به آن پرداخته می‌شود. این موارد از طریق روش‌های متنوع جمع‌آوری داده‌ها، نمونه‌گیری هدفمند، بررسی اعضا و مستندسازی دقیق محقق می‌شوند. تضمینات اخلاقی نیز به‌طور دقیق رعایت شده‌اند، از جمله محافظت از حقوق مشارکت‌کنندگان، محرمانگی و امنیت داده‌ها، که پیش از استخدام مشارکت‌کنندگان تأییدیه کمیته بررسی موسسه (IRB) نیز کسب خواهد شد. در مجموع، روش‌شناسی و طراحی انتخاب شده برای این مطالعه—که شامل ملاحظات اخلاقی، استراتژی‌های جمع‌آوری و تحلیل داده‌ها و اقدامات مربوط به اعتمادپذیری است—چارچوبی جامع و دقیق برای تحقیق در مورد مدل پذیرش فناوری برای رایانش ابری، هوش مصنوعی داستان‌گویی و FedRAMP، و همچنین ارزیابی نقش هوش مصنوعی داستان‌گویی در تقویت پذیرش سازمانی این فناوری‌ها ارائه می‌دهد.

نتیجه‌گیری:

تحقیق حاضر در مورد پذیرش فناوری‌های هوشمند در سازمان‌های دولتی، با استفاده از یک رویکرد تحلیلی و کیفی، به بررسی چالش‌ها و فرصت‌ها پرداخته و یک مدل جامع برای بهبودپذیرش این فناوری‌ها ارائه می‌دهد. این تحقیق از مصاحبه‌ها، پرسش‌نامه‌ها، و مطالعه موردی استفاده می‌کند تا اطلاعات جامع و دقیقی را در زمینه پذیرش فناوری‌های نوین در بخش دولتی جمع‌آوری کند و راهکارهای عملی و علمی برای غلبه بر مشکلات موجود پیشنهاد دهد.

۷-۱ داده‌های تحقیق را چگونه به دست آورده است؟

داده‌های تحقیق از طریق چندین روش کیفی به دست آمده‌اند:

- **مرور نظام‌مند ادبیات:** بیش از ۱۳۰۰ منبع علمی شامل مقالات، گزارش‌ها و مستندات از پایگاه‌هایی مانند Google Scholar، IEEE Xplore و ACM Digital Library بررسی شده‌اند.
- **مصاحبه‌های نیمه ساختاریافته:** گفتگوهای با کارشناسان، تصمیم‌گیرندگان و متخصصان فناوری اطلاعات دولتی انجام شده است تا دیدگاه‌های عمیق درباره چالش‌ها و فرصت‌ها استخراج شود.
- **مشاهدات و تحلیل اسناد:** داده‌هایی از مشاهدات میدانی و تحلیل مستندات مرتبط با FedRAMP، سیاست‌های دولتی و اجرای فناوری‌ها جمع‌آوری شده است.
- **استفاده از نرم‌افزار NVivo:** داده‌ها برای شناسایی تم‌ها و تحلیل ارتباطات، کدگذاری و بررسی شده‌اند.
- **دستورالعمل‌های PRISMA:** فرایند انتخاب و تحلیل داده‌ها با این دستورالعمل‌ها سازمان‌دهی و شفافیت یافته است.

۸-۱ چگونه نتایج ارزیابی شده‌اند؟

نتایج تحقیق با استفاده از رویکرد کیفی و ابزارهای مشخص ارزیابی شده‌اند. ابتدا داده‌ها از طریق مرور نظام‌مند ادبیات، مصاحبه‌های نیمه‌ساختاریافته و تحلیل اسناد جمع‌آوری شدند. سپس داده‌ها در نرم‌افزار NVivo کدگذاری شده و تم‌های اصلی شناسایی شدند. برای اطمینان از اعتبار نتایج، از مثلث‌سازی داده‌ها (Data Triangulation) استفاده شد که شامل ترکیب داده‌های مختلف برای شناسایی الگوهای مشترک است. همچنین فرایند بازبینی توسط مشارکت‌کنندگان (Member Checking) انجام شد تا تفاسیر محقق تأیید شود. ارزیابی نتایج با تأکید بر اعتمادپذیری شامل بررسی اعتبار (Credibility)، انتقال‌پذیری (Transferability)، و تأییدپذیری (Confirmability) صورت گرفت. در نهایت، بازبینی نتایج توسط کارشناسان حوزه فناوری و مدیریت انجام شد تا صحت و ارتباط آن‌ها تأیید شود. این روش‌ها به دستیابی به نتایج معتبر و قابل اطمینان کمک کرده است.

۹-۱ ساختار گزارش تحقیق

فصل اول به تعریف و مقدمه و دلایل نیاز به طرح ارائه شده پرداخته می شود.

فصل دوم مفاهیم عمومی و مفاهیم در حوزه مدل پذیرش فناوری برای رایانش ابری، هوش مصنوعی داستان سرایی، و برنامه مدیریت ریسک و مجوز فدرال پرداخته می شود.

فصل سوم به مروری بر کارهای انجام شده کار انجام شده در این تحقیق پرداخته می شود.

فصل چهارم به سؤالات اصلی این تحقیق پرداخته می شود.

فصل پنجم نیز به جمع بندی و نتیجه گیری پرداخته می شود.

فصل دوم

مفاهیم عمومی و

تعاریف حوزه پذیرش

فناوری، هوش مصنوعی

داستان‌گویی، و مدیریت

ریسک در رایانش ابری

هوش مصنوعی مکالمه‌ای (CAI) در صنایع و پلتفرم‌های مختلف رواج یافته و به پیشرفت‌های فناوری دامن زده است. (Rath et al., ۲۰۲۱) ترکیب CAI و یادگیری ماشین (ML) منجر به توسعه سیستم‌های امن‌تری در زمینه اینترنت اشیا (IoT) و رایانش ابری شده است. (Rath et al., ۲۰۲۱). این پیشرفت‌های فناورانه به کسب‌وکارها کمک کرده تا تصمیمات آگاهانه‌تری بگیرند و عملیات خود را بهبود بخشند. پذیرش CAIML در بخش دولتی فدرال به دلیل نیاز به چابکی در سیاست‌ها و جذب منابع در آژانس‌های اطلاعاتی محبوبیت یافته است (Haney, ۲۰۲۰; Schmidt et al., ۲۰۲۱). et al., ۲۰۲۱ توانایی پاسخگویی به نیازهای مشتری و هدایت فشارهای بازار برای این آژانس‌ها امری حیاتی شده است. (Haney, ۲۰۲۰) تخصیص استراتژیک منابع مالی و استفاده از فناوری‌هایی مانند CAIML می‌تواند تأثیر زیادی بر هزینه‌ها و رشد گروه‌های اطلاعاتی داشته باشد. (Novak, ۲۰۲۱) CAIML به این آژانس‌ها چابکی، تصمیم‌گیری بهبودیافته و واکنش‌پذیری بهتر در فضای اطلاعاتی ارائه می‌دهد (Allen et al., ۲۰۱۷). برای بهره‌برداری از CAIML، آژانس‌های فدرال باید آموزش کارکنان، برنامه‌ریزی برای مهاجرت، و پایداری راه‌حل‌ها را در اولویت قرار دهند و فرهنگی از بهبود مداوم ایجاد کنند (Medaglia et al., ۲۰۲۳). به‌روزرسانی‌های مداوم سیاست‌ها، راهنمایی‌های فنی و نیازهای تجاری برای پاسخگویی به الزامات جدید و دستیابی به نتایج مطلوب ضروری است (Kent, ۲۰۱۹).

۱-۲ مجوز فدرال (FedRAMP)

FedRAMP یک برنامه سراسری دولت ایالات متحده است که رویکردی استاندارد برای ارزیابی امنیتی، مجوز و نظارت مستمر بر ارائه‌دهندگان خدمات ابری (CSP) ها (ارائه می‌دهد. هدف FedRAMP اطمینان از امنیت و حریم خصوصی داده‌های فدرال ذخیره‌شده و پردازش‌شده در محیط‌های رایانش ابری است. FedRAMP مجموعه‌ای از کنترل‌های امنیتی را بر اساس استانداردهای شناخته‌شده مانند مؤسسه ملی استانداردها و فناوری (NIST) و نشر ویژه ۵۳-۸۰۰ ایجاد می‌کند. این کنترل‌ها الزامات امنیتی را که CSP ها برای محافظت از داده‌های فدرال ذخیره‌شده در فضای ابری باید رعایت کنند، مشخص می‌سازد. CSP هایی که به دنبال ارائه خدمات ابری به آژانس‌های فدرال هستند، باید ارزیابی امنیتی جامع و فرآیند مجوز را طی کنند. این شامل بررسی و ارزیابی کنترل‌های امنیتی، معماری سیستم، سیاست‌ها و رویه‌های CSP توسط یک سازمان ارزیابی شخص ثالث معتبر (۳ IPAO) است. پس از اخذ مجوز، CSP در بازار FedRAMP به‌عنوان یک ارائه‌دهنده قابل اعتماد فهرست می‌شود. FedRAMP تأکید زیادی بر نظارت مستمر دارد تا اطمینان حاصل کند که CSP ها همچنان به الزامات امنیتی پایبند هستند CSP ها باید به‌طور منظم وضعیت امنیتی خود را گزارش دهند و ارزیابی‌های دوره‌ای انجام دهند تا وضعیت مجوز خود را حفظ کنند. این رویکرد به آژانس‌ها این امکان را می‌دهد که امنیت خدمات ابری خود را مشاهده کنند. FedRAMP استفاده مجدد از مصنوعات ارزیابی امنیتی را ترویج می‌کند که به‌عنوان بسته‌های مجوز شناخته می‌شوند. این امر به کاهش ارزیابی‌های اضافی و تسریع در پذیرش خدمات ابری کمک می‌کند CSP ها. مجاز می‌توانند از وضعیت مجوز خود برای ارائه خدمات به چندین آژانس فدرال استفاده کنند و هم‌زمان در زمان و منابع برای CSP ها و آژانس‌ها صرفه‌جویی کنند. FedRAMP با ارائه یک رویکرد استاندارد شده و مبتنی بر ریسک برای امنیت خدمات ابری، نقش مهمی در پذیرش خدمات ابری توسط دولت ایالات متحده ایفا کرده است. این برنامه به آژانس‌های فدرال این امکان را می‌دهد که به راه‌حل‌های ابری ایمن و قابل اعتماد دسترسی داشته باشند و در عین حال شفافیت، همکاری و کارایی بین CSP ها و سازمان‌های دولتی را ارتقا دهند.

۲-۲ هوش مصنوعی داستان‌گویی (Storytelling AI)

حوزه هوش مصنوعی (AI) افق‌های جدیدی را برای داستان‌گویی ایجاد کرده است و پژوهشگران به بررسی کاربردها و پیامدهای مختلف این تکنولوژی در این زمینه پرداخته‌اند. مطالعات متعددی به بررسی یکپارچگی هوش مصنوعی در فرایند داستان‌گویی پرداخته‌اند و پتانسیل آن را برای انقلابی کردن در خلق و روایت داستان‌ها مورد توجه قرار داده‌اند (Fotedar et al., ۲۰۲۰; Riedl et al., ۲۰۱۱). (همچنین، استفاده از هوش مصنوعی در محیط‌های واقعیت مجازی و تأثیر آن در ایجاد احساسات از طریق شخصیت‌های هوش مصنوعی نیز بررسی شده است (Pyjas et al., ۲۰۲۲; Santiago et al., ۲۰۲۳). مدل‌های بزرگ هوش مصنوعی مولد، مانند ChatGPT از OpenAI، به طور قابل توجهی پی‌شرفت‌هایی در داستان‌گویی هوش مصنوعی ایجاد کرده‌اند (Gartner, n.d.). باین‌حال، ضروری است که محدودیت‌های این مدل‌ها شناسایی شود و راه‌حل‌های جایگزین مورد بررسی قرار گیرند، Gozalo-Brizuela & Garrido-Merchan, ۲۰۲۳. پیامدهای اخلاقی استفاده از هوش مصنوعی در داستان‌گویی نیز به‌عنوان یکی از مباحث مهم مورد توجه قرار گرفته است و تأکید بر رعایت اصول اخلاقی در این حوزه شده است (Blanchard & Taddeo, ۲۰۲۳). (علاوه بر این، همکاری میان انسان‌ها و هوش مصنوعی در داستان‌گویی داده‌ها نیز بررسی شده است (Li, Wang, Liao, & Qu, ۲۰۲۳). (این پژوهش‌ها به چالش‌ها و پیچیدگی‌های این همکاری پرداخته و دیدگاه‌هایی در مورد آن ارائه کرده‌اند.

۲-۲-۱ یکپارچگی هوش مصنوعی در استراتژی‌های امنیت ملی

در کنار تأثیر هوش مصنوعی در داستان‌گویی، یکپارچگی این فناوری در استراتژی‌های امنیت ملی نیز مورد توجه قرار گرفته است. مطالعات Mikhailov, ۲۰۲۳ بر اهمیت استراتژیک یکپارچگی هوش مصنوعی برای امنیت ملی تأکید کرده‌اند و به بهینه‌سازی استراتژی‌های امنیتی از طریق رویکردهای مبتنی بر هوش مصنوعی پرداخته‌اند. پیامدهای اخلاقی هوش مصنوعی در تحلیل‌های اطلاعاتی و مقابله با تروریسم نیز مورد بررسی قرار گرفته است (Esmailzadeh, ۲۰۲۳; Grinbaum & Adomaitis, ۲۰۲۳).

۲-۲-۲ چالش‌ها و فرصت‌های پذیرش هوش مصنوعی در بخش دولتی

پذیرش هوش مصنوعی در بخش‌های مختلف، به‌ویژه سازمان‌های دولتی، با چالش‌هایی همراه است. پذیرش رایانش ابری در بخش دولتی به یک حوزه پیچیده تبدیل شده که نیازمند توجه دقیق به عواملی مانند فرهنگ‌سازمانی، مدیریت تغییر و حمایت مدیریتی است (Carney, ۲۰۱۹; Diaz, ۲۰۲۲; Hall, ۲۰۱۹). درک موانع پذیرش رایانش ابری و بررسی استراتژی‌های مهاجرت موفق می‌تواند به پذیرش مؤثر فناوری‌های ابری در زمینه‌های دولتی کمک کند (Hall, ۲۰۲۰; Griffith, ۲۰۱۹).

۲-۲-۳ ریسک‌ها و پیامدهای یکپارچگی هوش مصنوعی

علاوه بر این، خطرات و پیامدهای یکپارچگی هوش مصنوعی در حوزه‌های مختلف مانند داستان‌گویی، امنیت ملی و دیگر زمینه‌ها نیز مورد بررسی قرار گرفته است. پژوهشگران نگرانی‌هایی در مورد حریم خصوصی، چارچوب‌های قانونی، تهدیدات امنیت سایبری و ماهیت دوگانه هوش مصنوعی مطرح کرده‌اند (Belgodere et al., ۲۰۲۳; Fotedar et al., ۲۰۲۰; Pizzo et al., n.d.). درک و رسیدگی به این خطرات و چالش‌ها برای بهره‌برداری از مزایای هوش مصنوعی در حالی که پیامدهای منفی آن کاهش یابد، ضروری است.

۲-۲-۴ نتیجه‌گیری

در نتیجه، یکپارچگی هوش مصنوعی در داستان‌گویی، امنیت ملی و بخش دولتی هم فرصت‌ها و هم چالش‌هایی را به همراه دارد. پژوهشگران جنبه‌های مختلف یکپارچگی هوش مصنوعی را از جمله مدل‌های مولد، همکاری انسان و هوش مصنوعی، ملاحظات اخلاقی، مدیریت ریسک و چارچوب‌های قانونی مورد بررسی قرار داده‌اند. تحقیقات بیشتری برای پیشبرد درک این حوزه‌ها و توسعه رویکردهای مسئولانه و عملی برای یکپارچگی هوش مصنوعی در حوزه‌های مختلف ضروری است.

۲-۳ مدیریت ریسک در داستان‌گویی با هوش مصنوعی (AI)

مدیریت ریسک در زمینه داستان‌گویی با هوش مصنوعی (AI) یکی از جنبه‌های کلیدی است که هنگام ادغام این فناوری باید مدنظر قرار گیرد. مطالعات و چارچوب‌های مختلفی برای مدیریت ریسک‌های مرتبط با AI در داستان‌گویی پیشنهاد شده‌اند. به عنوان مثال، (Tabassi ۲۰۲۳) چارچوبی برای مدیریت ریسک‌های هوش مصنوعی معرفی کرده است که دستورالعمل‌هایی برای شناسایی، ارزیابی و کاهش ریسک‌های خاص AI در داستان‌گویی فراهم می‌کند و ترویج استفاده مسئولانه و اخلاقی از سیستم‌های هوش مصنوعی را هدف قرار می‌دهد. برای عملیاتی کردن AI به شیوه‌ای مسئولانه، (Lu et al. ۲۰۲۳) (رویکرد الگوی محور معرفی کرده‌اند که بر ادغام شیوه‌های مسئولانه در طول چرخه عمر توسعه هوش مصنوعی تأکید دارد. این رویکرد، با گنجاندن اصول و الگوهای AI مسئولانه در فرآیند توسعه، به طور سیستماتیک به ملاحظات اخلاقی رسیدگی می‌کند). Xia et al. ۲۰۲۳ (یک مطالعه نقشه‌برداری سیستماتیک از ارزیابی ریسک‌های AI مسئولانه انجام داده‌اند که بر اهمیت ارزیابی ریسک‌های بالقوه و اجرای تدابیر حفاظتی برای کاهش پیامدهای منفی تأکید دارد. در ادامه، (Xia et al. ۲۰۲۳) (به بررسی چارچوب‌های ارزیابی ریسک AI پرداخته‌اند و بر لزوم استفاده از روش‌های جامع برای ارزیابی و مدیریت ریسک‌های مرتبط با AI تأکید کرده‌اند. در زمینه مدیریت ریسک سازمانی، McGrath (۲۰۲۲) چارچوبی برای مدیریت ریسک سازمانی که به طراحی راه‌حل‌های اخلاقی AI اختصاص دارد، پیشنهاد کرده است. این چارچوب، رویکردی جامع دارد و ابعاد سازمانی، قانونی و اخلاقی مدیریت ریسک AI در داستان‌گویی را در نظر می‌گیرد. Rassolov و Chubukova (۲۰۲۲) نیز چارچوب قانونی برای AI و حکمرانی مؤثر را مورد بحث قرار داده‌اند و بر اهمیت ایجاد چارچوب‌های نظارتی برای حفاظت از ذینفعان و در عین حال ترویج نوآوری در داستان‌گویی مبتنی بر AI تأکید کرده‌اند.

۲-۴ مدیریت ریسک محیطی با هوش مصنوعی مکالمه‌ای (CAI)

هوش مصنوعی مکالمه‌ای (CAI) همچنین به بهبود مدیریت ریسک محیطی کمک می‌کند. Clímaco et al. (۲۰۲۲) کاربرد CAI را برای ارائه اطلاعات در زمان واقعی و کمک به فرآیندهای تصمیم‌گیری در مورد ریسک‌های محیطی به نمایش گذاشته‌اند. Lütge et al. (۲۰۲۲) رویکرد ارزیابی مبتنی بر ریسک را برای حکمرانی اخلاقی AI پیشنهاد کرده‌اند که یک روش شناسایی ساختاری برای شناسایی، تحلیل و کاهش ریسک‌های اخلاقی مرتبط با فناوری‌های AI ارائه می‌دهد. Barta و Görcsi (۲۰۲۱) نیز اهمیت ملاحظات مدیریت ریسک را برای کاربردهای تجاری AI برجسته کرده و بر لزوم اتخاذ رویکردی پیشگیرانه برای شناسایی و رسیدگی به ریسک‌های بالقوه در مراحل اولیه چرخه توسعه تأکید کرده‌اند.

۲-۵ نگرانی‌های حریم خصوصی و امنیت در AI

باتوجه به چالش‌های مرتبط با AI، حریم خصوصی و امنیت مسائل حیاتی هستند. مطالعات اخیر به تکنیک‌های حفظ حریم خصوصی و پیامدهای مدل‌های هوش مصنوعی پرداخته‌اند. Panda et al. (۲۰۲۳) به بررسی یادگیری خصوصی تفاضلی در زمینه‌های یادگیری درون‌متنی پرداخته‌اند و چالش‌های حریم خصوصی در کاربردهای AI را مورد توجه قرار داده‌اند. پژوهشگرانی همچون Lukas et al. (۲۰۲۳) و Huang et al. (۲۰۲۳) به بررسی نشت اطلاعات شناسایی شخصی و پیامدهای حریم خصوصی مدل‌های مبتنی بر بازیابی زبان پرداخته‌اند. این مطالعات، نیاز به رویکردهای حفظ حریم خصوصی برای حفاظت از داده‌های حساس هنگام استفاده از توانمندی‌های AI را برجسته می‌کنند.

۶-۲ ملاحظات اخلاقی و ریسک‌های امنیتی در AI

ملاحظات اخلاقی و ریسک‌های مرتبط با فناوری هوش مصنوعی همچنین در زمینه امنیت ملی و تحلیل اطلاعات مورد بررسی قرار گرفته‌اند. Mikhailov (۲۰۲۳) بر اهمیت استراتژیک یکپارچگی AI برای امنیت ملی تأکید کرده است. Blanchard و Taddeo (۲۰۲۳) اخلاق AI برای تحلیل اطلاعات را مرور کرده و توصیه‌هایی برای رسیدگی به چالش‌های کلیدی ارائه داده‌اند. Esmailzadeh (۲۰۲۳) به بررسی ریسک‌های بالقوه ChatGPT در مقابله با تروریسم و امنیت بین‌المللی پرداخته است، در حالی که Derner و Batistič (۲۰۲۳) به بررسی ریسک‌های امنیتی ChatGPT پرداخته‌اند. Grinbaum و Adomaitis (۲۰۲۳) نگرانی‌های استفاده دوگانه از AI مولد و مدل‌های زبانی بزرگ (LLMs) را مورد بحث قرار داده‌اند.

۷-۲ اجزای فناوری

حوزه هوش مصنوعی داستان‌گویی (Storytelling AI) در سال‌های اخیر به سرعت تکامل یافته است و فناوری نقش حیاتی در ایجاد تجربیات داستانی جذاب و تعاملی برای مخاطبان ایفا می‌کند. برای درک ساختار فناوری هوش مصنوعی داستان‌گویی، بررسی اجزای مختلفی که با هم همکاری می‌کنند تا تجربه داستانی یکپارچه و شخصی‌سازی شده‌ای ایجاد کنند، ضروری است. این بخش نمای کلی از اجزای مختلف ساختار فناوری هوش مصنوعی داستان‌گویی را ارائه می‌دهد.

۷-۲-۱ جمع‌آوری و تحلیل داده‌ها

جمع‌آوری و تحلیل داده‌ها اجزای اساسی هوش مصنوعی داستان‌گویی هستند، زیرا پایه‌گذار شخصی‌سازی تجربه داستانی هر کاربر هستند. سیستم‌های هوش مصنوعی داستان‌گویی می‌توانند تجربه داستانی را متناسب با نیازها و ترجیحات خاص هر کاربر از طریق جمع‌آوری داده‌هایی در مورد رفتار، ترجیحات و احساسات کاربر تنظیم کنند. این امر باعث می‌شود داستان جذاب‌تر و شخصی‌تر شود و تجربه را به یادماندنی‌تر می‌سازد. جمع‌آوری و تحلیل داده‌ها در توسعه و کاربرد هوش مصنوعی داستان‌گویی از اهمیت ویژه‌ای برخوردار است. این فرایند در بازی‌های ویدئویی برای توسعه سیستم‌های تولید داستان معلق (suspense system) استفاده شده است. (Cheong & Young, ۲۰۱۴) به طور مشابه، در زمینه فن و میکس (Phenomics)، کاربرد هوش مصنوعی بر اساس جمع‌آوری و تحلیل داده‌ها بوده است. (Nabwire et al., ۲۰۲۱) در تحلیل داده‌های کلان بیماری‌های عفونی، هوش مصنوعی برای تحلیل حجم زیادی از داده‌ها که از منابع مختلف جمع‌آوری شده‌اند، استفاده شده است (Wong et al., ۲۰۱۹). در مطالعه مدل‌های هوش مصنوعی مانند GPT-۳، جمع‌آوری و تحلیل داده‌ها برای تحلیل توانایی مدل در ارائه اطلاعات بهتر از انسان‌ها (Spitale et al., ۲۰۲۳) و پتانسیل آن به عنوان یک فناوری عمومی استفاده شده است. (Guidetti, ۲۰۲۳) قابلیت استفاده از هوش مصنوعی در سلامت عمومی نیز از طریق جمع‌آوری و تحلیل داده‌ها مورد بررسی قرار گرفته است. (Jungwirth & Haluza, ۲۰۲۳) همچنین، جمع‌آوری و تحلیل داده‌ها برای مطالعه حکمرانی هوش مصنوعی و قانون هوش مصنوعی به عنوان یک فناوری مفید برای جامعه (Lobel, ۲۰۲۳) استفاده شده است. این اجزای کلیدی در زمینه هوش مصنوعی داستان‌گویی به ایجاد تجربیات سفارشی و بهبود تعاملات کاربران با داستان‌ها کمک می‌کنند.

جمع‌آوری و تحلیل داده‌ها نقش حیاتی در توسعه و کاربرد هوش مصنوعی داستان‌گویی ایفا می‌کند. این فرایند اساس شخصی‌سازی تجربه داستانی هر کاربر را فراهم می‌کند. سیستم‌های هوش مصنوعی داستان‌گویی می‌توانند تجربه داستانی را بر اساس داده‌های جمع‌آوری شده از رفتار، ترجیحات و احساسات کاربران تنظیم کنند که موجب جذاب‌تر و به‌یادماندنی‌تر شدن داستان می‌شود. مطالعات متعددی در زمینه‌های مختلف مانند بازی‌ها، فنومیکس، تحلیل داده‌های کلان بیماری‌های عفونی، و سلامت عمومی به کاربرد جمع‌آوری و تحلیل داده‌ها پرداخته‌اند (Cheong & Young, ۲۰۱۴; Nabwire et al., ۲۰۲۱; Wong et al., ۲۰۱۹). (۲۰۲۱; Wong et al., ۲۰۱۹). جمع‌آوری و تحلیل داده‌ها همچنین در زمینه حکمرانی هوش مصنوعی و مقررات آن برای بهبود استفاده از هوش مصنوعی در حوزه‌های مختلف، از جمله داستان‌گویی، مورد استفاده قرار گرفته است. (Li et al., ۲۰۲۳)

۲-۷-۲ موتور پردازش زبان طبیعی (NLP)

موتور پردازش زبان طبیعی (NLP) اجزای اساسی هوش مصنوعی داستان‌گویی است که زبان مورد استفاده در داستان‌گویی را پردازش و درک می‌کند. این شامل تبدیل متن به گفتار، شناسایی گفتار و تحلیل احساسات است که به سیستم‌های هوش مصنوعی امکان می‌دهد گفتار، متن و احساسات را تولید و درک کنند. این اجزا به ایجاد داستان‌های تعاملی و جذاب کمک می‌کنند. بسیاری از مطالعات بر روی بهبود کارایی موتورهای NLP در هوش مصنوعی داستان‌گویی متمرکز شده‌اند، از جمله پژوهش‌هایی که برای بهبود عملکرد چت‌بات‌ها و سیستم‌های پردازش زبان طبیعی انجام شده است (Onyalo, ۲۰۲۲; Singh & Singh, ۲۰۲۲; Dale, ۲۰۲۲; Papadopoulou, ۲۰۲۲). این مطالعات نشان‌دهنده تلاش‌های مداوم برای بهبود موتورهای NLP است تا سیستم‌های هوش مصنوعی قادر به ایجاد داستان‌هایی با شباهت بیشتر به انسان و تعامل با مخاطبان شوند.

۲-۷-۳ تولید شخصیت و انیمیشن

تولید شخصیت و انیمیشن نقش حیاتی در هوش مصنوعی داستان‌گویی ایفا می‌کند، زیرا شخصیت‌های دیجیتال ایجاد شده می‌توانند با مخاطب تعامل کنند و داستان را زنده کنند. این امر واقعیت و جذابیت داستان را افزایش می‌دهد و احساس می‌کند که داستان در دنیای واقعی در حال وقوع است. با ایجاد انیمیشن برای شخصیت‌ها، سیستم‌های هوش مصنوعی داستان‌گویی می‌توانند داستان‌ها را غنی‌تر و تعاملی‌تر کنند و اجازه دهند مخاطب احساس کند که بخشی از آن است. در سال‌های اخیر، پژوهشگران به بررسی استفاده از هوش مصنوعی برای تولید شخصیت‌ها و انیمیشن‌ها پرداخته‌اند که می‌تواند در زمینه‌های مختلف داستان‌گویی استفاده شود. به عنوان مثال، برخی از مطالعات نشان داده‌اند که شخصیت‌های تولید شده توسط هوش مصنوعی می‌توانند در یادگیری شخصی‌سازی شده و بهبود رفاه تأثیرگذار باشند (Pataranutaporn et al., ۲۰۲۱). همچنین، استفاده از هوش مصنوعی برای تولید شخصیت‌های دیجیتال و انیمیشن‌ها در زمینه‌های مختلف داستان‌گویی مورد بررسی قرار گرفته است (Latif et al., ۲۰۲۲; Chen et al., ۲۰۲۲). (Amato et al., ۲۰۱۹). این مطالعات نشان می‌دهند که تولید شخصیت و انیمیشن جزو اجزای اساسی هوش مصنوعی داستان‌گویی هستند و هوش مصنوعی می‌تواند شخصیت‌ها و انیمیشن‌های منحصر به فرد و متنوعی ایجاد کند که در زمینه‌های مختلف داستان‌گویی قابل استفاده باشند.

۲-۷-۴ تولید دیالوگ

تولید دیالوگ یکی دیگر از اجزای حیاتی هوش مصنوعی داستان‌گویی است، زیرا تمرکز آن بر تولید گفتگوها و تعاملات میان شخصیت‌ها در پاسخ به ورودی‌های کاربر است. این امر باعث می‌شود داستان جذاب‌تر و تعاملی‌تر شود و به مخاطب این احساس را می‌دهد که بخشی از آن است. با تولید دیالوگ‌های پویا و شخصی‌سازی شده، سیستم‌های هوش مصنوعی داستان‌گویی می‌توانند تجربه داستانی جذاب‌تر و شخصی‌تری برای هر کاربر ایجاد کنند. در هوش مصنوعی داستان‌گویی، تولید دیالوگ بخش حیاتی از داستان‌گویی تعاملی مبتنی بر شخصیت‌ها است. تولید دیالوگ‌های باورپذیر و جذاب نیاز به در نظر گرفتن عوامل مختلفی مانند شخصیت شخصیت‌ها، سبک و زمینه دارد. Cavazza (۲۰۰۵) و Charles به بررسی تولید دیالوگ در داستان‌گویی تعاملی مبتنی بر

شخصیت‌ها پرداخته‌اند و چالش‌های تولید دیالوگ‌های معنادار و منسجم در این زمینه را مورد بررسی قرار داده‌اند (Akoury et al. ۲۰۲۳). بر تولید دیالوگ‌های مستند در محیط‌های بازی‌های ویدئویی تمرکز کرده‌اند، جایی که زمینه و محیط نقش مهمی در تعیین محتوای دیالوگ ایفا می‌کنند (Xu ۲۰۲۲). به بررسی تولید دیالوگ‌های سبک‌شناسی بر اساس شخصیت‌های داستانی در فیلم‌های روایتی پرداخته است و اهمیت در نظر گرفتن شخصیت‌ها در تولید دیالوگ را برجسته کرده است. (Biermann et al. ۲۰۲۲). به رابطه بین نویسندگان هوش مصنوعی و نویسندگان انسانی در تولید دیالوگ پرداخته و بر لزوم رعایت ارزش‌های شخصی و استراتژی‌های نوشتاری توسط نویسندگان هوش مصنوعی تأکید کرده‌اند (Lee et al. ۲۰۲۲). به بررسی همدلی در دیالوگ‌های تولید شده توسط مدل GPT-۳ پرداخته و روشی نوآورانه برای انتخاب مثال‌ها در زمینه و معیارهای ارزیابی خودکار برای تولید دیالوگ همدلانه ارائه داده‌اند. (Amjad et al. ۲۰۲۳). چارچوب EMP-EVAL را برای اندازه‌گیری همدلی در دیالوگ‌های دامن آزاد معرفی کرده‌اند که برای تولید دیالوگ‌های جذاب و احساسی ضروری است (Zhu ۲۰۲۳) و Luo (۲۰۲۳) به بررسی استفاده از ترنسفورمرهای تولیدی برای تولید مفاهیم طراحی پرداخته‌اند، که یکی دیگر از کاربردهای تولید دیالوگ در هوش مصنوعی داستان‌گویی است. در نهایت، (Safovich ۲۰۱۹) مطالعه‌ای در زمینه تولید داستان‌های انتزاعی ارائه داده است که شامل تولید یک روایت از مجموعه‌ای از داده‌های ورودی است و چالش‌ها و فرصت‌های این حوزه را مورد بررسی قرار داده است. در نتیجه، تولید دیالوگ جذاب و معنادار یکی از جنبه‌های حیاتی هوش مصنوعی داستان‌گویی است و مطالعات فراوانی برای رسیدگی به چالش‌ها و فرصت‌های موجود در این زمینه انجام شده است.

۲-۷-۵ فناوری‌های واقعیت مجازی و افزوده

فناوری‌های واقعیت مجازی (VR) و واقعیت افزوده (AR) نقش حیاتی در هوش مصنوعی داستان‌گویی ایفا می‌کنند، زیرا محیط‌های تعاملی و فراگیر برای وقوع داستان‌ها ایجاد می‌کنند. این فناوری‌ها به داستان‌ها واقعیت و جذابیت می‌بخشند و باعث می‌شوند داستان به نظر برسد که در دنیای واقعی و زنده در حال رخ دادن است. با استفاده از فناوری‌های واقعیت مجازی و افزوده، سیستم‌های هوش مصنوعی داستان‌گویی می‌توانند تجربیات داستانی جذاب‌تر و تعاملی‌تری برای مخاطبان ایجاد کنند و به آن‌ها این احساس را بدهند که بخشی از داستان‌ها هستند. فناوری‌های واقعیت مجازی و افزوده در حال استفاده بیشتر در داستان‌گویی هستند و تجربه‌ای فراگیر برای کاربران فراهم می‌کنند. این فناوری‌ها به کاربران اجازه می‌دهند وارد دنیای دیجیتال شوند و با محیط‌ها و اشیاء مصنوعی تعامل کنند که آن‌ها را برای داستان‌گویی ایدئال می‌سازد. به عنوان مثال، Noh و Shin (۲۰۲۲) به بررسی استفاده از فناوری‌های واقعیت مجازی و افزوده در کتابخانه‌ها پرداخته‌اند و از این فناوری‌ها برای فعال‌سازی کتابخانه و بهبود تعامل کاربران استفاده کرده‌اند (Qian ۲۰۲۲). استفاده از فناوری واقعیت مجازی را در ایجاد هنر دیجیتال بررسی کرده است و بر کاربرد آن در روش‌های آموزشی تأکید دارد. در پژوهش‌های تجربه خدمات، (Kozinets ۲۰۲۳) از مفهوم "نتنوگرافی فراگیر" استفاده کرده که شامل استفاده از فناوری‌های واقعیت مجازی و افزوده برای مطالعه تجربیات خدمات در زمینه‌های مجازی، افزوده و متاورس است.

۲-۷-۶ شناسایی و شبیه‌سازی احساسات

شناسایی و شبیه‌سازی احساسات اجزای حیاتی هوش مصنوعی داستان‌گویی هستند، زیرا از هوش مصنوعی و یادگیری ماشین (ML) برای شناسایی و واکنش به وضعیت احساسی مخاطب و همچنین تولید و شبیه‌سازی احساسات برای شخصیت‌های داستان استفاده می‌کنند. این امر داستان را جذاب‌تر و احساسی‌تر می‌کند و باعث می‌شود مخاطب ارتباط بیشتری با شخصیت‌ها و خود داستان برقرار کند. شناسایی و شبیه‌سازی احساسات به سیستم‌های هوش مصنوعی داستان‌گویی اجازه می‌دهد تا تجربه داستانی شخصی‌سازی شده و جذاب‌تری برای هر کاربر ایجاد کنند. شناسایی احساسات بخش اساسی داستان‌گویی است، زیرا این امکان را فراهم می‌کند که روایت‌ها شخصی‌سازی و جذاب‌تر شوند (Wang et al. ۲۰۲۳). به بررسی استفاده از روایت‌های اجتماعی در داستان‌گویی شخصی‌سازی شده پرداخته‌اند، جایی که روایت‌ها از شناسایی احساسات برای تطبیق داستان با احساسات شنونده استفاده می‌کنند. De Lope و Graña (۲۰۲۳) یک بررسی مداوم از شناسایی احساسات در گفتار ارائه داده‌اند که پیشرفت‌ها و چالش‌های این حوزه را برجسته می‌کند. Jarrahi et al. (۲۰۲۳) نقش هوش مصنوعی در محیط‌های کاری را بررسی کرده‌اند، از جمله پتانسیل آن برای شناسایی احساسات و پیامدهای آن برای

کارگران (۲۰۲۳). Semeraro et al. ابزار EmoAtlas را معرفی کرده‌اند که از واژگان روانشناختی، هوش مصنوعی و علوم شبکه برای ایجاد پروفایل احساسی افراد استفاده می‌کند (۲۰۲۳). Lavi. پیامدهای اخلاقی دستکاری احساسات با استفاده از هوش مصنوعی را مورد بحث قرار داده و بر لزوم تنظیم مقررات تأکید کرده است. در نتیجه، استفاده از شناسایی احساسات در داستان‌گویی پتانسیل افزایش تجربه روایتی را دارد، اما همچنین مسائل اخلاقی مهمی را مطرح می‌کند که نیاز به رسیدگی دارند.

۷-۷-۲ شخصی سازی و سازگاری

شخصی سازی و سازگاری اجزای حیاتی هوش مصنوعی داستان‌گویی هستند، زیرا تمرکز آن‌ها بر استفاده از داده‌ها و الگوریتم‌ها برای شخصی سازی تجربه داستانی هر کاربر است و مطابق با ترجیحات، رفتار و احساسات او سازگار می‌شوند. شخصی سازی و سازگاری در هوش مصنوعی داستان‌گویی به عنوان یک حوزه تحقیقاتی روبه رشد، هدف ایجاد تجربیات داستانی جذاب تر و مؤثرتر را دنبال می‌کند. هدف از این فرایند ارائه روایت‌های شخصی شده به کاربران است که به تناسبات ترجیحات، حالات روحی و زمینه‌های آن‌ها تطبیق پیدا کند. این فرایند می‌تواند با استفاده از فناوری‌های علم داده، یادگیری ماشین (ML) و هوش مصنوعی (AI) محقق شود Göbel. و Wendel (۲۰۱۶) مفهوم شخصی سازی و سازگاری در بازی‌های جدی را مورد مطالعه قرار داده‌اند و نمای کلی از چالش‌ها و فرصت‌های مهم در این حوزه ارائه کرده‌اند. همچنین، Göbel و Mehm (۲۰۱۳) از بازی‌های دیجیتال آموزشی شخصی سازی شده و سازگار استفاده کرده‌اند که از اشیا یادگیری مبتنی بر بازی‌های روایتی برای ارتقا تجربه یادگیری استفاده می‌کنند. در سال‌های اخیر، توسعه فناوری‌های هوش مصنوعی پیشرفت‌های قابل توجهی در شخصی سازی و سازگاری در داستان‌گویی به همراه داشته است. به عنوان مثال، De Benedictis et al. (۲۰۲۳) رویکردی مبتنی بر ترنسفورمر برای انتخاب اقدامات در رباتیک اجتماعی پیشنهاد داده‌اند که می‌تواند به طور شخصی سازی شده و سازگار با کاربران عمل کند. تحقیقات دیگر نیز در زمینه شخصی سازی و سازگاری در یادگیری الکترونیکی و بهبود توانایی شناختی از طریق این فناوری‌ها پرداخته‌اند (Anoir) (۲۰۲۰). Baraka et al. (۲۰۲۱)، Wen et al. (۲۰۲۲)، et al. چارچوبی گسترده برای توصیف روبات‌های اجتماعی توسعه داده‌اند که می‌تواند در داستان‌گویی برای شخصی سازی و سازگاری استفاده شود. در نهایت، این مطالعات نشان می‌دهند که شخصی سازی و سازگاری در هوش مصنوعی داستان‌گویی یک حوزه سریعاً در حال تکامل است که فرصت‌های جدیدی برای ایجاد تجربیات داستانی جذاب تر و مؤثرتر ارائه می‌دهد.

۷-۷-۸ یادگیری عمیق با گراف‌ها

یادگیری عمیق با گراف‌ها به عنوان یک حوزه برجسته تحقیقاتی ظهور کرده است و فرصت‌های جدیدی برای مدل سازی و تحلیل داده‌های پیچیده و وابسته به هم فراهم می‌کند (Jiang ۲۰۲۲). یک بررسی جامع از کاربرد یادگیری عمیق مبتنی بر گراف‌ها در شبکه‌های ارتباطی ارائه داده است. این بررسی به معماری‌های مختلف شبکه‌های عصبی گرافی و کاربردهای آن‌ها در بهینه سازی شبکه، تشخیص ناهنجاری‌ها و پیش‌بینی ترافیک پرداخته است. همچنین، چالش‌ها و سؤالات باز تحقیقاتی در این حوزه، از جمله مقیاس پذیری، تفسیرپذیری و مدیریت شبکه‌های دینامیک، مورد بحث قرار گرفته‌اند. نمایش و طبقه‌بندی متن با استفاده از تکنیک‌های یادگیری عمیق مبتنی بر گراف‌ها توجه زیادی در پردازش زبان طبیعی (NLP) به خود جلب کرده است (Pham. et al. ۲۰۲۲). یک بررسی از استفاده رویکردهای یادگیری عمیق و مبتنی بر گراف برای نمایش و طبقه‌بندی متن ارائه داده‌اند. این بررسی به روش‌های مختلف ساخت گراف، الگوریتم‌های یادگیری نمایش مبتنی بر گراف و یکپارچگی آن‌ها با مدل‌های یادگیری عمیق پرداخته است. مزایای نمایش‌های مبتنی بر گراف برای ضبط روابط معنایی بین کلمات و اسناد، و بهبود عملکرد در وظایفی مانند تحلیل احساسات، طبقه‌بندی اسناد و خلاصه سازی متن مورد تأکید قرار گرفته است. این تحقیق همچنین چالش‌ها را شامل مقیاس پذیری مدل‌های مبتنی بر گراف و نیاز به تسهیل پذیری در طبقه‌بندی متن شناسایی کرده است. Roshanfekr et al. (۲۰۲۳) رویکردی برای یادگیری گراف‌ها از سیگنال‌های گراف با استفاده از تحلیل حساسیت در چارچوب یادگیری عمیق پیشنهاد می‌دهند. این رویکرد بر استنباط ساختار زیرین گراف بر اساس سیگنال‌های مشاهده شده تمرکز دارد. با بهره‌گیری از حساسیت گراف، این روش به دنبال ضبط روابط میان گره‌های گراف و تأثیر آن‌ها بر سیگنال‌ها است. چارچوب پیشنهادی تکنیک‌های یادگیری عمیق را با تحلیل مبتنی بر گراف ترکیب می‌کند تا یادگیری مؤثری از ساختارهای گراف از داده‌ها انجام شود. مطالعه نشان‌دهنده کارآمدی این رویکرد در بازسازی ساختارهای گراف از سیگنال‌های مختلف است. این تحقیق به کاربردهای بالقوه در زمینه‌هایی مانند تحلیل شبکه‌های اجتماعی، سیستم‌های توصیه گر و شبکه‌های زیستی اشاره می‌کند.

ترکیب یادگیری ماشین (ML) با وب معنایی در سال‌های اخیر توجه زیادی را جلب کرده است (Breit et al. ۲۰۲۳). یک مطالعه نقشه‌برداری سیستماتیک انجام دادند تا یکپارچگی تکنیک‌های یادگیری ماشین با وب معنایی را بررسی کنند. این مطالعه ادبیات موجود را مورد بررسی قرار داده و رویکردها و کاربردهای مختلفی را که در آن‌ها یادگیری ماشین و وب معنایی به هم متقاطع می‌شوند شناسایی کرده است. این مطالعه به فواید بالقوه ترکیب این دو حوزه مانند بهبود نمایندگی دانش، بهبود بازایی اطلاعات و پشتیبانی از تصمیم‌گیری هوشمند اشاره دارد. همچنین، چالش‌ها شامل ادغام داده‌ها، یادگیری انتولوژی و قابل توضیح بودن را مورد بحث قرار داده و بینش‌هایی را در مورد جهت‌گیری‌های تحقیقاتی آینده در این زمینه بین‌رشته‌ای ارائه می‌دهد.

نتیجه‌گیری

در مجموع، یادگیری عمیق با گراف‌ها در حوزه‌های مختلفی مانند شبکه‌های ارتباطی، نمایش و طبقه‌بندی متن، یادگیری ساختارهای گراف و ترکیب یادگیری ماشین با وب معنایی نویدهای زیادی نشان داده است. این مطالعات بینش‌های ارزشمندی درباره وضعیت موجود، چالش‌ها و کاربردهای بالقوه رویکردهای یادگیری عمیق مبتنی بر گراف ارائه می‌دهند. با ادامه تحقیق و نوآوری در این حوزه، انتظار می‌رود یادگیری عمیق با گراف‌ها توانایی تحلیل و درک داده‌های پیچیده وابسته به هم را گسترش دهد و راه را برای پیشرفت‌های جدید در هوش مصنوعی و تصمیم‌گیری مبتنی بر داده هموار کند.

فصل سوم

مروری بر کارهای انجام شده

فرایندهای جمع‌آوری داده‌ها شامل یک فرایند تکراری است که با طراحی تحقیق عمل‌گرا هم‌راستا است. هر چرخه/دوره، فرایند جمع‌آوری داده‌ها را با فعال‌سازی سؤالات و حوزه‌های جدید کاوش هدایت می‌کند. این پایان‌نامه دستورالعمل‌های اخلاقی تحقیق را (رنا و همکاران، ۲۰۲۱) رعایت خواهد کرد تا از حقوق و حریم خصوصی شرکت‌کنندگان حفاظت کند. در مجموع، این رویکرد جمع‌آوری داده‌ها درک جامع و چندوجهی از مدل پذیرش فناوری برای رایانش ابری، هوش مصنوعی داستان‌گویی و FedRAMP، و همچنین نقش بالقوه هوش مصنوعی داستان‌گویی در سازمان‌ها فراهم می‌آورد. ابزارها و فرایندهای جمع‌آوری داده‌های انتخابی کاملاً با طراحی مطالعه تحقیق عمل‌گرا هماهنگ هستند، به گونه‌ای که انعطاف‌پذیری، تطبیق‌پذیری و تحلیل دقیق داده‌های کیفی را امکان‌پذیر می‌سازد.

۳-۱ ابزار و فرایندهای جمع‌آوری داده‌ها

در این پایان‌نامه، ترکیبی از ابزارها و فرایندهای جمع‌آوری داده‌ها برای جمع‌آوری و تحلیل داده‌های مربوط به مدل پذیرش فناوری برای رایانش ابری، هوش مصنوعی داستان‌گویی و FedRAMP و نقش بالقوه هوش مصنوعی داستان‌گویی در ارتقای پذیرش این فناوری‌ها در سازمان‌ها به کار خواهد رفت. در بخش‌های زیر، ابزارها و فرایندهای جمع‌آوری داده‌ها شرح داده می‌شود:

۳-۱-۱ مصاحبه‌های نیمه‌ساختاریافته

مصاحبه‌های نیمه‌ساختاریافته با شرکت‌کنندگان انجام خواهد شد تا دیدگاه‌ها، تجربیات و بینش‌های آن‌ها بررسی شود. پروتکل مصاحبه بر اساس سؤالات و اهداف اولیه تحقیق توسعه خواهد یافت، به گونه‌ای که انعطاف‌پذیری لازم برای بررسی عمیق‌تر پاسخ‌های شرکت‌کنندگان و کشف موضوعات و ایده‌های نوظهور فراهم شود. آدامز (۲۰۱۵) و رام‌سدن (۲۰۱۶) راهنمایی‌هایی در مورد انجام مصاحبه‌های نیمه‌ساختاریافته و تعیین تعداد مناسب مصاحبه‌ها ارائه می‌دهند. استراتژی نمونه‌گیری هدفمند (پالینکاس و همکاران، ۲۰۱۵) برای انتخاب شرکت‌کنندگانی که دانش و تجربه مرتبط با رایانش ابری، هوش مصنوعی داستان‌گویی و FedRAMP دارند، به کار خواهد رفت.

۳-۱-۲ مشاهدات

مشاهدات میدانی برای به‌دست‌آوردن بینش‌های دست‌اول در مورد استفاده از فناوری‌های رایانش ابری، هوش مصنوعی داستان‌گویی و FedRAMP در سازمان‌ها انجام خواهد شد. یادداشت‌های میدانی برای ثبت مشاهدات تهیه می‌شود تا اطلاعات زمینه‌ای مربوطه و الگوها یا موضوعات نوظهور ثبت شوند. داده‌های جمع‌آوری‌شده از طریق مشاهدات، داده‌های مصاحبه‌ها را تکمیل کرده و درک عمیق‌تری از رفتارها و اقدامات شرکت‌کنندگان فراهم می‌آورد (لاوسون، ۲۰۱۶).

۳-۱-۳ تحلیل مستندات

مستندات مختلف مانند سیاست‌های سازمانی، گزارش‌ها، دستورالعمل‌ها و ادبیات مرتبط برای به‌دست‌آوردن بینش‌های اضافی در مورد مدل پذیرش فناوری و نقش هوش مصنوعی داستان‌گویی مورد تحلیل قرار خواهند گرفت. روش تحلیل محتوا که توسط سال‌دانا (۲۰۲۱) بیان شده، به‌عنوان راهنمایی برای تحلیل سیستماتیک مستندات استفاده خواهد شد که این امکان را فراهم می‌آورد تا موضوعات و الگوهای کلیدی شناسایی شوند.

۳-۱-۴ نرم‌افزار NVivo

برای پشتیبانی از سازمان‌دهی و تحلیل داده‌های جمع‌آوری‌شده، از نرم‌افزار تحلیل داده‌های کیفی مانند NVivo (نسخه ۱۴) استفاده خواهد شد (پاولوس، ۲۰۲۳). NVivo یک پلتفرم کارآمد برای کدگذاری، طبقه‌بندی و شناسایی روابط بین داده‌ها فراهم می‌آورد. این نرم‌افزار به شناسایی الگوها و موضوعات نوظهور در منابع مختلف داده کمک خواهد کرد و فرایند تحلیل و تفسیر یافته‌ها را تسهیل می‌کند (تنگ، ۲۰۲۳).

بحث در مورد فرایندها

فرایندهای جمع‌آوری داده‌ها شامل یک فرایند تکراری است که با طراحی تحقیق عمل‌گرا هم‌راستا است. هر چرخه/دوره، فرایند جمع‌آوری داده‌ها را با فعال‌سازی سؤالات و حوزه‌های جدید کاوش هدایت می‌کند. این پایان‌نامه دستورالعمل‌های اخلاقی تحقیق را (رنا و همکاران، ۲۰۲۱) رعایت خواهد کرد تا از حقوق و حریم خصوصی شرکت‌کنندگان حفاظت کند.

در مجموع، این رویکرد جمع‌آوری داده‌ها درک جامع و چندوجهی از مدل پذیرش فناوری برای رایانش ابری، هوش مصنوعی داستان‌گویی و FedRAMP، و همچنین نقش بالقوه هوش مصنوعی داستان‌گویی در سازمان‌ها فراهم می‌آورد. ابزارها و فرایندهای جمع‌آوری داده‌های انتخابی کاملاً با طراحی مطالعه تحقیق عمل‌گرا هماهنگ هستند، به گونه‌ای که انعطاف‌پذیری، تطبیق‌پذیری و تحلیل دقیق داده‌های کیفی را امکان‌پذیر می‌سازد.

۲-۳ فرآیندهای تحلیل داده‌ها

در این پایان‌نامه، فرایندهای تحلیل داده‌ها برای استخراج بینش‌های معنادار از داده‌های جمع‌آوری‌شده بسیار مهم خواهند بود. روش تحلیل داده‌های انتخاب‌شده با طراحی تحقیق عمل‌گرا هم‌راستا است که خود در سنت تحقیق کیفی قرار دارد. مراحل تحلیل داده‌ها برای هر چرخه/دوره به طور دقیق توضیح داده خواهد شد تا امکان تکثیر آن توسط دیگر پژوهشگران فراهم شود. لازم به ذکر است که ترجیحات و همکاری شرکت‌کنندگان در سایت تحقیق هنگام تعیین روش تحلیل داده‌ها در نظر گرفته خواهد شد، زیرا این فرایند ممکن است شامل استفاده از نرم‌افزار تحلیل داده‌های کیفی و روش‌های سنتی تحلیلی دستی باشد.

مرحله ۱: آماده‌سازی داده‌ها

قبل از تحلیل، داده‌های جمع‌آوری‌شده که شامل مصاحبه‌ها، مشاهدات، مستندات و احتمالاً ضبط‌های صوتی یا تصویری هستند، به‌دقت تبدیل به نسخه‌های متنی خواهند شد. این فرایند ترانویسی برای تبدیل گفتار یا پدیده‌های مشاهده‌شده به فرمت نوشتاری که قابل تحلیل سیستماتیک باشد، ضروری است. پس از ترانویسی، داده‌ها به طور دقیق سازمان‌دهی خواهند شد و طبق انواع و منابع مختلف دسته‌بندی خواهند شد. سپس هر بخش از داده‌ها کدگذاری خواهد شد و برچسب‌هایی به آن‌ها اختصاص داده می‌شود که به شناسایی مفاهیم و الگوهای کلیدی کمک می‌کند. این سازمان‌دهی اولیه و کدگذاری، طبق روش‌های رنا و همکاران (۲۰۲۱)، گام‌های ضروری برای آماده‌سازی داده‌ها جهت تحلیل عمیق هستند.

مرحله ۲: کدگذاری اولیه

در مرحله کدگذاری اولیه، هر بخش از داده‌ها به طور دقیق مورد بررسی قرار خواهد گرفت. کدگذاری باز برای بخش‌های مختلف اعمال خواهد شد، جایی که کدهای خاصی که مفاهیم، موضوعات یا الگوهای مشاهده‌شده در داده‌ها را نشان می‌دهند، به آن‌ها اختصاص داده می‌شود. این فرایند که تحت راهنمایی سال دانا (۲۰۲۱) انجام می‌شود، یک رویکرد اکتشافی است که در آن داده‌ها بدون دسته‌بندی‌های از پیش تعیین‌شده تفسیر می‌شوند. هدف این مرحله این است که تا حد ممکن بی‌طرف و باز بمانیم تا داده‌ها بتوانند معانی و روابط ذاتی خود را نشان دهند.

این مراحل تحلیل داده‌ها به محقق این امکان را می‌دهند که به طور عمیق و سیستماتیک به بررسی اطلاعات بپردازد و به شناسایی الگوها و موضوعات اصلی در ارتباط با پذیرش فناوری رایانش ابری، هوش مصنوعی داستان‌گویی و FedRAMP و نقش این فناوری‌ها در سازمان‌ها بپردازد.

گام ۳: توسعه تم‌ها

پس از کدگذاری اولیه، گام بعدی شامل گروه‌بندی کدهای باز برای توسعه تم‌های گسترده‌تر و فراگیرتر است. این مرحله برای شناسایی ارتباطات و روابط بین کدهای مختلف حیاتی است که منجر به شکل‌گیری تم‌های کلیدی می‌شود. در این فرایند، با ظهور بینش‌های جدید در تحلیل، تم‌ها به طور مداوم اصلاح و بازنگری خواهند شد، روشی که توسط سالدانا (۲۰۲۱) تأکید شده است. این رویکرد تکراری اطمینان می‌دهد که تم‌ها به‌درستی پیچیدگی‌ها و ظرافت‌های داده‌ها را نمایان می‌سازند.

گام ۴: مقایسه داده‌ها

در این گام، با جمع‌آوری داده‌های بیشتر از طریق چرخه‌ها یا دوره‌های مختلف، مقایسه‌هایی بین داده‌های مختلف انجام خواهد شد. هدف از این مقایسه شناسایی شباهت‌ها، تفاوت‌ها و الگوهای نوظهور است که در مجموعه‌های مختلف داده‌ها ظاهر می‌شوند. این فرایند تکراری، همان‌طور که توسط پالینکاس و همکاران (۲۰۱۵) اشاره شده، برای اصلاح تم‌های نوظهور و عمیق‌تر کردن تحلیل کلی ضروری است. این مقایسه‌ها به تحلیلگر کمک می‌کند تا درک جامع‌تری از داده‌ها به دست آورد و اطمینان حاصل کند که تحلیل تمام ابعاد و جنبه‌های مرتبط با موضوع تحقیق را دربر می‌گیرد.

گام ۵: بررسی اعضا (Member Checking)

برای تقویت اعتبار و تأییدپذیری یافته‌ها، بررسی اعضا به‌عنوان بخشی از فرایند تحقیق انجام خواهد شد (سالدانیا، ۲۰۲۱). این مرحله شامل به‌اشتراک‌گذاری داده‌های تحلیل شده و تم‌های توسعه‌یافته با شرکت‌کنندگان برای بازبینی و تأیید است. هدف از این گام اعتبار سنجی دقت و ارتباط‌پذیری تفسیرهایی است که محققین از داده‌ها انجام داده‌اند. شرکت‌کنندگان فرصتی خواهند داشت تا یافته‌ها را تأیید، اصلاح یا گسترش دهند و این اطمینان را ایجاد کنند که نتایج به‌طور واقعی و صحیح نمایانگر تجربیات و دیدگاه‌های آنان است.

گام ۶: بازتاب و برنامه‌ریزی اقدام

در طول فرایند تحلیل داده‌ها، بازتاب و بحث مستمر با شرکت‌کنندگان و همکاران تحقیقاتی انجام خواهد شد. این بحث‌های بازتابی، همان‌طور که توسط لائوسون (۲۰۱۶) اشاره شده، به‌منظور به‌دست آوردن بینش‌های بیشتر در مورد داده‌ها خواهند بود. این بازتاب‌ها برای تصحیح و بهینه‌سازی طرح اقدام برای مطالعه بسیار حیاتی هستند تا اطمینان حاصل شود که اهداف کلی تحقیق به‌خوبی دنبال می‌شود. این مرحله بازتابی تنها به تحلیل داده‌ها محدود نمی‌شود، بلکه در نظر گرفتن پیامدهای یافته‌ها و برنامه‌ریزی گام‌های بعدی در فرایند تحقیق نیز بخش مهمی از آن است.

۳-۳ بحث در مورد فرایند تحلیل داده‌ها

در فرایند تحلیل داده‌ها، ممکن است از نرم‌افزار تحلیل داده‌های کیفی مانند NVivo برای مدیریت، سازمان‌دهی و تحلیل داده‌ها استفاده شود (پاولوس، ۲۰۲۳). با این حال، ترجیحات شرکت‌کنندگان و همکاران تحقیقاتی در نظر گرفته خواهد شد و در صورتی که روش سنتی‌تر ترجیح داده شود، از کدگذاری دستی و روش‌های تحلیلی سنتی استفاده خواهد شد.

این روش‌های تحلیل داده‌ها اجازه می‌دهند تا یافته‌های تحقیق به‌طور کامل بررسی، تفسیر و تأیید شوند، به‌گونه‌ای که اعتمادپذیری و دقت مطالعه را تقویت می‌کند. ماهیت تکراری طراحی تحقیق عمل‌گرا نیز به اصلاح و غنی‌سازی مستمر تحلیل‌ها کمک کرده و درک جامع‌تری از مدل پذیرش فناوری برای رایانش ابری، هوش مصنوعی داستان‌گویی و FedRAMP به دست می‌دهد.

اعتمادپذیری (Trustworthiness)

در سنت کیفی، به‌ویژه در طراحی تحقیق عمل‌گرا که در این مطالعه مورد استفاده قرار گرفته است، اعتمادپذیری تحقیق عاملی حیاتی است. برای تضمین اعتمادپذیری قوی، این تحقیق به چهار معیار اصلی: اعتبار، انتقال‌پذیری، قابلیت اعتماد، و تأییدپذیری پایبند خواهد بود. در زیر، به تفصیل شرح داده می‌شود که چگونه هر یک از این معیارها در زمینه این پایان‌نامه رعایت خواهند شد.

اعتبار (Credibility)

اعتبار به میزان قابل اعتماد بودن یافته‌های تحقیق اشاره دارد. در این مطالعه، اعتبار از طریق استفاده از روش‌های متنوع جمع‌آوری داده‌ها، از جمله مصاحبه‌ها، مشاهدات و تحلیل مستندات تقویت خواهد شد، همان‌طور که آدامز (۲۰۱۵) توصیه کرده است. این روش‌ها دیدگاه‌ها و تجربیات مختلفی از شرکت‌کنندگان جمع‌آوری کرده و غنای یافته‌های تحقیق را افزایش می‌دهند. همچنین، برای تقویت اعتبار، بررسی اعضا به‌عنوان بخشی از فرآیند تحقیق گنجانده شده است تا شرکت‌کنندگان صحت و ارتباطیابی یافته‌ها را تایید کنند (سالدانیا، ۲۰۲۱).

انتقال‌پذیری (Transferability)

انتقال‌پذیری به میزان قابلیت کاربرد یافته‌های تحقیق در زمینه‌ها یا موقعیت‌های دیگر اشاره دارد. این پایان‌نامه با ارائه توضیحات جامع در مورد زمینه تحقیق، ویژگی‌های شرکت‌کنندگان و روش‌شناسی‌های به‌کارگرفته‌شده، به‌گونه‌ای مستند شده که خوانندگان قادر باشند ارزیابی کنند که یافته‌ها در زمینه‌های مختلف قابل اعمال هستند یا خیر (آنت و آنت، ۲۰۱۶). همچنین، استفاده از تکنیک‌های نمونه‌گیری هدفمند برای انتخاب شرکت‌کنندگانی که تجربیات و دیدگاه‌های آن‌ها نمایانگر گروهی وسیع‌تر از افراد است، قابلیت انتقال‌پذیری یافته‌ها را تقویت می‌کند (پالینکاس و همکاران، ۲۰۱۵).

قابلیت اعتماد (Dependability)

قابلیت اعتماد به ثبات و یکپارچگی فرایند تحقیق و نتایج آن اشاره دارد. برای تضمین قابلیت اعتماد، یک مسیر حسابرسی جامع که فرایندها، تصمیمات و اصلاحات تحقیقاتی را ثبت می‌کند، حفظ خواهد شد (رنا و همکاران، ۲۰۲۱). این مستندسازی دقیق امکان تکثیر فرآیند تحقیق و ارزیابی قابلیت اعتماد آن را فراهم می‌آورد. علاوه بر این، مشاوره و بررسی همتایان و کارشناسان میدانی نیز در نظر گرفته شده است تا لایه اضافی از دقت و صحت در تحقیق لحاظ شود (لکسیس و ژولیان، ۲۰۲۲).

تأییدپذیری (Confirmability)

تأییدپذیری به بی‌طرفی و عینیت یافته‌های تحقیق اشاره دارد. برای پشتیبانی از تأییدپذیری، از نرم‌افزار تحلیل داده‌های کیفی NVivo (نسخه ۱۴) استفاده خواهد شد (پاولوس و همکاران، ۲۰۲۳). این نرم‌افزار امکان تحلیل سیستماتیک و شفاف داده‌ها را فراهم می‌آورد و به شناسایی الگوها، تم‌ها و روابط در داده‌ها کمک می‌کند، در نتیجه تفسیرهای شخصی و مغرضانه را کاهش می‌دهد. علاوه بر این، در طول فرآیند تحقیق، شیوه‌های انعکاسی به‌کار گرفته می‌شود تا محقق بتواند هرگونه تعصب شخصی خود را شناسایی و برطرف کند و اطمینان حاصل کند که یافته‌ها منعطف به داده‌ها و نه به پیش‌فرض‌ها و تمایلات شخصی محقق هستند (سالدانیا، ۲۰۲۱).

۳-۴ پذیرش رایانش ابری

از طریق تحلیل گسترده پذیرش رایانش ابری، چندین یافته کلیدی به دست آمده است که با چالش‌ها و ملاحظات مطرح شده در جدول ۱ هم‌خوانی دارد. به‌طور مشابه با نگرانی‌ها و مسائل مربوط به امنیت و تطابق در رایانش ابری که اهمیت این دو عامل را در پذیرش رایانش ابری نشان می‌دهند، یافته‌های کلیدی بر چالش‌های چندوجهی که سازمان‌ها با آن مواجه هستند، از جمله پیچیدگی‌های مهاجرت داده‌ها و نیاز به رهبری visionary و مدیریت تغییر تأکید دارند. علاوه بر این، خطرات حریم خصوصی داده‌ها در رایانش ابری و استفاده اخلاقی از داده‌ها به‌طور موازی با اهمیت حفظ تعادل میان حریم خصوصی داده‌ها و استفاده اخلاقی از داده‌ها در رایانش ابری، که بخش جدایی‌ناپذیر از پذیرش رایانش ابری است، به‌طور قابل توجهی برجسته شده است. علاوه بر این، پیامدهای عمیق پذیرش رایانش ابری برای امنیت ملی و تحلیل‌های اطلاعاتی، با پیامدهایی که در جدول ۱ ذکر شده‌اند، هم‌راستا است. این یافته‌ها نشان می‌دهند که پذیرش رایانش ابری تنها یک پروژه فناوری اطلاعاتی نیست، بلکه یک ضرورت استراتژیک است که بر اهمیت استراتژی‌های جامع، رهبری visionary و یادگیری و نوآوری مستمر تأکید دارد، موضوعاتی که در جدول ۱ نیز به‌وضوح برجسته شده‌اند. این یافته‌ها نه تنها به چالش‌های فنی، بلکه به ابعاد استراتژیک و مدیریتی پذیرش رایانش ابری پرداخته‌اند، و به این نتیجه می‌رسند که برای موفقیت در این فرآیند، سازمان‌ها باید نه تنها بر فناوری‌ها، بلکه بر فرهنگ سازمانی، رهبری مناسب، و پیاده‌سازی استراتژی‌های مستمر نوآوری و یادگیری تمرکز کنند.

جدول ۱

ماتریس کدگذاری پذیرش رایانش ابری

توضیح/گزیده	f	کد
چالش‌های مرتبط با مهاجرت داده‌ها به ابر	۱،۳۴۲	چالش‌های مهاجرت داده‌ها در ابر
خطرات مرتبط با حریم خصوصی داده‌ها در ابر	۱،۳۴۲	خطرات حریم خصوصی داده‌ها در ابر
ملاحظات اخلاقی در استفاده از داده‌ها در ابر	۱،۳۴۲	استفاده اخلاقی از داده‌ها در ابر
تأکید بر یادگیری مداوم در فناوری‌های ابری	۱،۳۵۱	یادگیری مداوم در رایانش ابری
چالش‌های مرتبط با یکپارچه‌سازی در محیط‌های ابری	۹۱۲	چالش‌های یکپارچه‌سازی در ابر

توضیح/گزیده	f	کد
مدیریت تغییر در پذیرش رایانش ابری	۸۹۷	مدیریت تغییر در پذیرش ابر
ارتقای خدمات مشتری از طریق فناوری‌های ابری	۹۲۶	بهبود خدمات مشتری در ابر
اجرای اقدامات امنیت سایبری در رایانش ابری	۸۲۷	اقدامات امنیت سایبری در ابر
رهبری با رویکرد دوراندیشانه برای پذیرش ابر	۶۷۶	رهبری دوراندیش در پذیرش ابر
مسائل مرتبط با انطباق در رایانش ابری	۸۰۴	مسائل انطباق در رایانش ابری

توجه: این جدول نمایی کلی از ۱۰ کد برتر و میزان شیوع آن‌ها در داده‌ها ارائه می‌دهد.

۳-۱۵ ادغام هوش مصنوعی در داستان‌گویی

یافته‌های مربوط به ادغام هوش مصنوعی در داستان‌گویی، الگوهای مشترکی با چالش‌ها و ملاحظات موجود در جدول ۳ دارند. همان‌طور که نگرانی‌های مربوط به امنیت داده‌های هوش مصنوعی و خطرات حریم خصوصی داده‌ها اهمیت حفاظت از داده‌ها در کاربردهای هوش مصنوعی را نشان می‌دهند، ادغام هوش مصنوعی نیز نیاز به ادغام یکپارچه فناوری‌های هوش مصنوعی را برجسته می‌کند، در حالی که خطرات امنیتی و حریم خصوصی بالقوه را نیز باید مد نظر قرار داد. به‌طور مشابه، استفاده اخلاقی از داده‌های هوش مصنوعی با ملاحظات اخلاقی استفاده از داده‌های هوش مصنوعی هم‌راستا است و بر اهمیت ادغام مسئولانه هوش مصنوعی در فرآیندهای داستان‌گویی تأکید دارد.

علاوه بر این، یادگیری مداوم هوش مصنوعی با ضرورت یادگیری و سازگاری مستمر در زمان ادغام هوش مصنوعی در شیوه‌های داستان‌گویی همخوانی دارد. باتوجه‌به اینکه هوش مصنوعی نقش حیاتی در تحلیل اطلاعات ایفا می‌کند، چالش‌های ادغام که در جدول ۳ ذکر شده است، با پیچیدگی‌های تلفیق بینش‌های مبتنی بر هوش مصنوعی در تجربه‌های داستانی مطابقت دارد.

این یافته‌ها بر این نکته تأکید دارند که ادغام هوش مصنوعی در فرایندهای داستان‌گویی نه‌تنها نیازمند توجه به چالش‌های تکنولوژیکی است، بلکه باید ملاحظات اخلاقی، امنیتی، و حریم خصوصی به‌طور هم‌زمان موردتوجه قرار گیرد. به‌ویژه، باید از یادگیری مستمر و تطابق فناوری هوش مصنوعی با نیازهای پیچیده و رو به تغییر داستان‌گویی حمایت شود.

موضوع	زیر موضوعات کلیدی و دیدگاه‌ها
چالش‌های پذیرش ابر	چالش‌های مهاجرت داده‌ها، مسائل انطباق، کمبود تخصص، نگرانی‌های هزینه
امنیت و انطباق	نگرانی‌های امنیتی، قوانین حریم خصوصی داده‌ها، مقررات فدرال، اقدامات امنیت سایبری
پیامدهای اقتصادی	صرفه‌جویی در هزینه‌ها، بازگشت سرمایه، تخصیص بودجه
حریم خصوصی و اخلاق داده	ریسک‌های حریم خصوصی داده، استفاده اخلاقی از داده، تعارض بین انطباق و حریم خصوصی، سیاست‌های مدیریت داده
موضوع	زیر موضوعات کلیدی و دیدگاه‌ها
کارایی و خودکارسازی	خودکارسازی فرآیندهای ابری، تصمیم‌گیری مبتنی بر داده، تحلیل پیش‌بینی
رهبری و تغییر	رهبری چشم‌انداز، مدیریت تغییر، فرهنگ نوآوری، یادگیری مستمر
یکپارچگی و مهاجرت	استراتژی‌های مهاجرت، چالش‌های یکپارچگی، تأثیر سیستم‌های قدیمی
تأثیر بر امنیت ملی	پیامدهای امنیت ملی، تحلیل اطلاعات، نگرانی‌های انتقال‌گذاری داده
خدمات مشترک	بهبود خدمات مشتری، ایجاد مدل رقابتی
همکاری و نوآوری	همکاری، فناوری‌های پیشرفته

توضیح: این جدول، موضوعات کلیدی که از تحلیل داده‌ها به دست آمده را خلاصه می‌کند.

بنابراین، این یافته‌های کلیدی نشان‌دهنده تعادل حیاتی میان بهره‌برداری از پتانسیل داستان سرایی هوش مصنوعی و پرداختن به جنبه‌های اخلاقی، امنیتی و یکپارچه سازی در پذیرش هوش مصنوعی هستند. این تعادل نه تنها برای بهبود تجربیات روایتی ضروری است، بلکه برای اطمینان از کاربرد مسئولانه و امن هوش مصنوعی در زمینه‌های گسترده‌تر مانند امنیت ملی و رعایت مقررات نیز اهمیت دارد. این یافته‌ها نیاز به توجه دقیق به این عوامل را برجسته می‌کنند تا از پتانسیل هوش مصنوعی به حداکثر برسیم، درحالی که حریم خصوصی، امنیت داده‌ها و استانداردهای اخلاقی نیز حفظ شود؛ مسئله‌ای که به‌ویژه در بخش‌های حساس مانند دفاع ملی و صنایع تحت نظارت مقررات اهمیت دارد.

جدول ۳

ماتریس کدگذاری هوش مصنوعی داستان‌گویی

توضیحات /گزیده	f	کد
نگرانی‌ها درباره امنیت داده در باره برنامه‌های هوش مصنوعی	۱،۳۴۲	نگرانی‌ها درباره امنیت داده در AI
ریسک‌های مرتبط با حریم خصوصی داده در هوش مصنوعی	۱،۳۴۲	ریسک‌های حریم خصوصی داده در AI
ملاحظات اخلاقی در استفاده از داده‌ها در هوش مصنوعی	۱،۳۴۲	ملاحظات اخلاقی از داده در AI
توضیحات /گزیده	f	کد
اقداماتی برای تضمین امنیت داده در هوش مصنوعی	۱،۳۴۲	اقدامات امنیت داده بر AI
تأثیر هوش مصنوعی بر امنیت ملی	۳۵۱	تأثیر هوش مصنوعی بر امنیت ملی
تأکید بر یادگیری مداوم در حوزه هوش مصنوعی	۳۴۲	یادگیری مستمر در هوش مصنوعی
تأثیر هوش مصنوعی بر سیستم‌های قدیمی در فرایندپذیرش	۳۱۱	تأثیر بر سیستم‌های قدیمی
استفاده از هوش مصنوعی برای تحلیل اطلاعات	۳۱۷	تحلیل اطلاعات با استفاده از AI
چالش‌های مرتبط با یکپارچه‌سازی هوش مصنوعی	۲۶۷	چالش‌های یکپارچه‌سازی AI
چالش‌ها در رعایت مقررات مربوط به هوش مصنوعی	۲۶۴	چالش‌های انطباق با AI

توضیح: این جدول مروری بر ۱۰ کد برتر و فراوانی آن‌ها در داده‌های مرتبط با هوش مصنوعی داستان‌گویی ارائه می‌دهد.

جدول ۳ به‌عنوان یک ابزار تحلیلی حیاتی عمل می‌کند و چشم‌انداز پیچیده هوش مصنوعی داستان‌گویی را به اجزای اساسی آن تقلیل می‌دهد. از طریق بررسی دقیق داده‌ها، جدول ۳ جوهره هوش مصنوعی داستان‌گویی را با شناسایی موضوعات و نگرانی‌های پرتکراری که در مباحث و ابتکارات این حوزه غالب هستند، به تصویر می‌کشد. این کدها تنها بازنمایی‌های آماری نیستند، بلکه نشانگرهای کلیدی از روایت‌هایی هستند که هوش مصنوعی داستان‌گویی در چشم‌انداز فناوری امروز می‌بافد. این جدول بازتابی از ترکیب خلاقیت روایی و نوآوری فناورانه است و بر ملاحظات همیشگی امنیت داده‌ها، رفتار اخلاقی، پیامدهای امنیت ملی، یادگیری مستمر، و چالش‌های مرتبط با ادغام و انطباق هوش مصنوعی تأکید دارد. در حالی که سازمان‌ها و داستان‌گویان هوش مصنوعی را به‌عنوان یک همراه در داستان‌گویی می‌پذیرند، جدول ۳ مسیر آینده را روشن می‌کند و به ما یادآوری می‌کند که هنر داستان‌گویی همگام با توانایی‌ها و مسئولیت‌های روایت‌های مبتنی بر هوش مصنوعی در حال تحول است.

جدول ۴ به طور خلاصه عناصر اصلی سیستماتیک استخراج شده از تحلیل داده‌های هوش مصنوعی داستان‌گویی را جمع‌بندی می‌کند. این موضوعات به صورت سیستماتیک در دسته‌بندی‌های کلیدی سازمان‌دهی شده‌اند و نمایی واضح و مختصر از بینش‌های اساسی در حوزه هوش مصنوعی داستان‌گویی ارائه می‌دهند.

جدول ۴

موضوعات نوظهور در هوش مصنوعی داستان‌گویی

موضوع	زیرموضوعات کلیدی و دیدگاه‌ها
امنیت و حریم خصوصی	نگرانی‌های امنیت داده‌های هوش مصنوعی خطرات مربوط به جرایم خصوصی داده‌ها استفاده اخلاقی از داده‌ها اقدامات امنیتی داده‌ها تأثیر بر امنیت ملی
انطباق و مقررات	چالش‌های انطباق هوش مصنوعی مقررات فدرال مرتبط با داده‌ها تأثیر بر سیستم‌های قانونی
هوش و تحلیل	تحلیل هوش یادگیری مداوم
چالش‌های ادغام	چالش‌های مرتبط با ادغام هوش مصنوعی

توضیح: این جدول موضوعات کلیدی استخراج شده از تحلیل داده‌ها را خلاصه می‌کند.

۳- رعایت استانداردهای FedRAMP

یافته‌های کلیدی در مورد رعایت استانداردهای FedRAMP بر ماهیت چندوجهی این چارچوب حیاتی در زمینه سازمان‌های دولتی فدرال تأکید دارند. در حالی که FedRAMP رویکرد استاندارد برای امنیت ابری فراهم می‌آورد، با چالش‌هایی روبه‌رو است. این چالش‌ها شامل محدودیت‌های منابع و الزامات در حال تغییر هستند که نیاز به مدیریت دقیق دارند. اقدامات امنیتی تقویت شده امری ضروری هستند؛ اما باید با نگرانی‌ها در مورد هزینه‌های انطباق نیز تعادل برقرار کنند. این مطالعه بر لزوم رهبری بصیرتمند و استراتژی‌های مدیریت تغییر تأکید دارد تا به طور مؤثر در پیچیدگی‌های رعایت استانداردهای FedRAMP حرکت کند. علاوه بر این، تعامل پیچیده میان انطباق، حریم خصوصی و امنیت سایبری را روشن می‌کند. پیامدهای این موضوع برای امنیت ملی و تحلیل اطلاعات چشمگیر است و تأکید می‌کند که نقش FedRAMP در حفظ داده‌های حساس دولتی امری حیاتی است. در نهایت، این تحلیل نشان می‌دهد که دستیابی به انطباق با FedRAMP تنها یک الزام قانونی نیست؛ بلکه یک ضرورت استراتژیک است که نیاز به توجه دقیق به تخصیص منابع، اقدامات امنیتی و شیوه‌های رهبری دارد.

جدول ۵ به عنوان یک خلاصه جامع از کدها و شیوع آن‌ها در مجموعه داده‌ها عمل می‌کند و دیدی فشرده از جنبه‌های بحرانی مرتبط با رعایت استانداردهای FedRAMP ارائه می‌دهد. جدول ۵ مرجع سریعی و اطلاعاتی فراهم می‌کند و شفافیت در مورد میزان تکرار و جوهره هر کد را نمایان می‌سازد. کدها ابعاد مختلفی از FedRAMP را دربر می‌گیرند، از کاهش تهدیدات تا چالش‌های انطباق، و پیچیدگی‌های رعایت مقررات FedRAMP را روشن می‌کنند. علاوه بر این، جدول ۵ نقش FedRAMP را در تحلیل اطلاعات بیان می‌کند، به بررسی خطرات حریم خصوصی داده‌ها و سیاست‌های مربوط به آن پرداخته، تأثیر آن بر امنیت ملی را مورد بررسی قرار می‌دهد و بر یادگیری مستمر و مدیریت تغییر تأکید می‌کند. جدول ۵ همچنین چالش‌های مرتبط با ادغام FedRAMP در سیستم‌های موجود را نیز شناسایی می‌کند. به طور کلی، جدول ۵ تصویری مختصر و مفید از جنبه‌های کلیدی برای درک چشم‌انداز رعایت استانداردهای FedRAMP در دولت فدرال ارائه می‌دهد.

جدول ۵

ماتریس کدگذاری برنامه مدیریت ریسک و مجوز فدرال (FedRAMP)

کد	تعداد (۱)	توضیحات / گزیده
کاهش تهدید در FedRAMP	۴,۲۶۱	کاهش تهدیدها در انطباق با FedRAMP
چالش‌های انطباق با FedRAMP	۴,۲۰۵	چالش‌های مرتبط با انطباق با مقررات FedRAMP
تحلیل اطلاعات در FedRAMP	۴,۲۲۸	استفاده از FedRAMP برای تحلیل اطلاعات
ریسک‌های حریم خصوصی داده‌ها	۲,۳۲۷	ریسک‌های مرتبط با حریم خصوصی داده‌ها در FedRAMP
سیاست‌های مدیریت داده‌ها در FedRAMP	۲,۲۱۲	سیاست‌های مرتبط با مدیریت داده‌ها در FedRAMP
تأثیر بر امنیت ملی	۸۲۹	تأثیر FedRAMP بر امنیت ملی
یادگیری مداوم در FedRAMP	۶۹۸	تأکید بر یادگیری مداوم در FedRAMP
تأثیر بر سیستم‌های قدیمی	۴۶۲	تأثیر FedRAMP بر سیستم‌های قدیمی
مدیریت تغییرات در FedRAMP	۲۵۷	مدیریت تغییرات در فرایندپذیرش FedRAMP
چالش‌های ادغام در FedRAMP	۲۷۲	چالش‌های مرتبط با ادغام FedRAMP

توضیح: این جدول نمای کلی از کدها و میزان شیوع آنها در داده‌ها را ارائه می‌دهد.

جدول ۶

ابعاد استراتژیک و پیچیدگی های FedRAMP

جدول ۶ یک دیدگاه فشرده و سازمان یافته از تم های مرکزی است که از تحلیل رعایت استانداردهای FedRAMP در سازمان های دولتی فدرال به دست آمده است. جدول ۶ این تم ها را در دسته بندی های متمایز سازماندهی می کند و به عنوان یک راهنمای هدایت کننده برای درک چشم انداز چندوجهی FedRAMP عمل می کند. این تم ها از چالش هایی که سازمان ها در تطابق با الزامات FedRAMP با آن ها روبه رو هستند، از جمله محدودیت های منابع و الزامات در حال تغییر، تا ملاحظات حیاتی امنیت، حریم خصوصی و تعادل پیچیده میان حریم خصوصی داده ها و انطباق را شامل می شود. جدول ۶ به بررسی تأثیرات اقتصادی، جنبه های مقرراتی، و نقش عمیق FedRAMP بر امنیت ملی می پردازد. همچنین، این جدول بر نقش محوری رهبری، فرهنگ نوآوری، یادگیری مداوم، و پتانسیل کسب مزیت رقابتی از طریق اعتماد و اعتبار تأکید می کند. در واقع، جدول ۶ به عنوان یک راهنمای ساختاریافته عمل می کند که درک جامعی از ابعاد استراتژیک و پیچیدگی های موجود در دستیابی و حفظ انطباق با FedRAMP در چشم انداز دولت فدرال فراهم می نماید.

جدول ۶

موضوعات نوظهور در برنامه مدیریت ریسک و مجوز فدرال (FedRAMP)

موضوع	زیر موضوعات کلیدی و دیدگاه ها
چالش های انطباق با FedRAMP	چالش های انطباق، محدودیت های منابع، نیازهای در حال تغییر، مدیریت تغییرات، چالش های ادغام، تأثیر بر سیستم های قدیمی
امنیت و حریم خصوصی	کاهش تهدیدها، ریسک های حریم خصوصی داده ها، سیاست های مدیریت داده ها، تعادل بین حریم خصوصی داده ها و تحلیل اطلاعات، اقدامات امنیت
پیامد های اقتصادی	هزینه انطباق، صرفه جویی در هزینه ها، بازگشت سرمایه، تخصیص بودجه
مقررات و انطباق قانونی	مقررات فدرال، انطباق قانونی، چشم انداز مقرراتی
تأثیر بر امنیت ملی	تأثیر بر امنیت ملی، تحلیل اطلاعات، نگرانی های مرتبط با اشتراک گذاری
رهبری و مدیریت تغییرات	چشم انداز رهبری، فرهنگ نوآوری، یادگیری مداوم
مزیت رقابتی	رضایت، اعتماد و اعتبار
رهبری و انطباق مدام	یادگیری مداوم، چالش های ادغام، نیازهای در حال تغییر
تأثیر بر سیستم های قدیمی	تأثیر بر سیستم های قدیمی

توضیح: این جدول موضوعات کلیدی استخراج شده از تحلیل داده ها را خلاصه می کند.

فصل چهارم

پاسخ سؤالات اصلی تحقیق

مزایا و معایب

این فصل نقطه عطفی در این پایان نامه است که در آن محقق به بررسی یافته‌های کلیدی و اهمیت آنها در ارتباط با سؤالات تحقیق پرداخته است. این فصل اطلاعات به دست آمده از مرور سیستماتیک ادبیات، تحلیل کیفی و مصاحبه‌ها/مطالعات متخصصان را ترکیب می‌کند. این یافته‌ها نه تنها به درک عمیق تری از تعامل بین رایانش ابری، هوش مصنوعی داستان‌گویی و پذیرش FedRAMP کمک می‌کنند، بلکه اهمیت زیادی برای زمینه‌های وسیع تر فناوری و انطباق دارند. هدف محقق ارائه یک نقشه راه برای پیمایش در چشم انداز در حال تحول انطباق و نوآوری فناوری است تا اطمینان حاصل شود که سازمان‌های دولتی بتوانند از پتانسیل کامل هوش مصنوعی داستان‌گویی در چارچوب‌های قانونی بهره‌برداری کنند.

۴-۴-۱ چالش‌های پذیرش هوش مصنوعی مکالمه‌ای و یادگیری ماشین در سازمان‌های دولتی فدرال

این تحقیق به دنبال کشف چالش‌های اصلی است که سازمان‌های دولتی فدرال در پذیرش فناوری‌های هوش مصنوعی مکالمه‌ای و یادگیری ماشین در محیط‌های ابری با آن روبرو هستند. یافته‌ها یک چشم‌انداز پیچیده از موانع و مشکلات را نشان می‌دهند که عمدتاً حول امنیت داده‌ها، کمبود تخصص نیروی کار و ناکارآمدی‌های فرایندهای اجرایی متمرکز است.

نگرانی‌های امنیتی و حریم خصوصی: یکی از چالش‌های مهم، حفاظت از اطلاعات حساس و طبقه‌بندی شده است. یکپارچه‌سازی فناوری‌های هوش مصنوعی و یادگیری ماشین نیاز به پردازش حجم زیادی از داده‌ها دارد که خطرات مربوط به نقض داده‌ها و دسترسی غیرمجاز را افزایش می‌دهد. انطباق با استانداردهای امنیتی سخت‌گیرانه مانند آنهایی که توسط FedRAMP اجباری است، لایه‌هایی از پیچیدگی را ایجاد می‌کند.

کمبود نیروی متخصص: برای پیاده‌سازی مؤثر هوش مصنوعی و یادگیری ماشین، مهارت‌های خاص و دانش ویژه‌ای نیاز است. با این حال، سازمان‌های دولتی با چالش‌های عمده‌ای در جذب و نگهداری افرادی که در این زمینه‌ها متخصص باشند، روبرو هستند. این شکاف مهارتی مانعی اساسی برای پذیرش و استفاده بهینه از این فناوری‌هاست.

فرایندهای تأمین و خرید: همچنین پیچیدگی‌های موجود در فرایندهای تأمین و خرید در سازمان‌های دولتی مطرح شده است. طبیعت فناوری‌های هوش مصنوعی و یادگیری ماشین که به سرعت در حال تحول هستند، غالباً با رویه‌های بوروکراتیک موجود در تضاد قرار می‌گیرد و منجر به تأخیر و ناکارآمدی می‌شود. نتیجه‌گیری: چالش‌های ذکر شده بر لزوم اتخاذ رویکردی جامع برای یکپارچه‌سازی هوش مصنوعی و یادگیری ماشین در فضای ابری در سازمان‌های دولتی فدرال تأکید دارند. این رویکرد باید شامل تقویت تدابیر امنیتی داده‌ها، پرکردن شکاف مهارتی از طریق توسعه نیروی کار و اصلاح سیاست‌های تأمین و خرید باشد.

۴-۴-۲ بهبود عملیات و فرایندهای تصمیم‌گیری در سازمان‌های دولتی فدرال از طریق هوش مصنوعی و یادگیری ماشین

این تحقیق به دنبال بررسی تأثیر تحولی هوش مصنوعی مکالمه‌ای و یادگیری ماشین بر کارایی عملیات و فرایندهای تصمیم‌گیری در سازمان‌های دولتی فدرال است. یافته‌ها مزایای چندجانبه این فناوری‌ها را نشان می‌دهند که شامل خودکارسازی، تعامل با شهروندان و بهبود توانایی‌های تصمیم‌گیری هستند.

خودکارسازی و بهینه‌سازی فرایندها: یکی از مزایای مهم یکپارچه‌سازی هوش مصنوعی و یادگیری ماشین، خودکارسازی وظایف روزمره است. با استفاده از ابزارهای هوش مصنوعی مانند چت‌بات‌ها، سازمان‌ها می‌توانند از بار وظایف اداری و سؤالات تکراری بکاهند.

ارتقای تعامل با شهروندان و ارائه خدمات: فناوری‌های هوش مصنوعی مکالمه‌ای مانند چت‌بات‌ها و دستیاران مجازی نحوه تعامل سازمان‌ها با شهروندان را متحول می‌کند. این ابزارها دسترسی ۷/۲۴ را فراهم کرده و پاسخ‌های دقیق و به‌موقع به سوالات عمومی ارائه می‌دهند.

تصمیم‌گیری مبتنی بر داده‌ها: الگوریتم‌های یادگیری ماشین به بهبود فرایندهای تصمیم‌گیری در سازمان‌ها کمک می‌کنند. با تجزیه و تحلیل داده‌های متنوع، این الگوریتم‌ها می‌توانند بینش‌ها و پیشنهاداتی را تولید کنند که برای سیاست‌گذاری آگاهانه ضروری هستند.

نتیجه‌گیری: یکپارچه‌سازی هوش مصنوعی مکالمه‌ای و یادگیری ماشین می‌تواند پیشرفت‌های قابل‌توجهی در عملیات و حکومت‌داری عمومی ایجاد کند. اما برای تحقق کامل این مزایا، نیاز به توجه به نگرانی‌های مربوط به حریم خصوصی داده‌ها و مسائل اخلاقی است.

۴-۳-۴ پیامدهای اقتصادی پذیرش هوش مصنوعی و یادگیری ماشین در سازمان‌های دولتی فدرال

این تحقیق پیامدهای اقتصادی پیاده‌سازی فناوری‌های هوش مصنوعی مکالمه‌ای و یادگیری ماشین در فضای ابری سازمان‌های دولتی فدرال را بررسی کرده است. یافته‌ها نشان‌دهنده پتانسیل صرفه‌جویی‌های قابل‌توجه در هزینه‌ها، افزایش کارایی عملیاتی و بهبود خدمات عمومی هستند.

صرفه‌جویی در هزینه‌ها و افزایش کارایی: یکی از مزایای اقتصادی اصلی یکپارچه‌سازی هوش مصنوعی و یادگیری ماشین، کاهش هزینه‌های نیروی کار از طریق خودکارسازی است. فناوری‌هایی مانند چت‌بات‌ها و دستیارهای مجازی می‌توانند وظایف اداری روزمره را انجام دهند و این امکان را برای کارکنان دولتی فراهم می‌آورد تا بر روی فعالیت‌های ارزشمندتری تمرکز کنند.

تصمیم‌گیری مبتنی بر داده‌ها و بهینه‌سازی منابع: الگوریتم‌های یادگیری ماشین به بهینه‌سازی تخصیص منابع کمک می‌کنند و همچنین می‌توانند نواحی بالقوه برای کاهش هزینه را شناسایی کنند.

بهبود خدمات شهروندی و رشد اقتصادی: پذیرش هوش مصنوعی و یادگیری ماشین به بهبود خدمات عمومی و افزایش رضایت شهروندان منجر می‌شود. این رضایت می‌تواند منجر به افزایش همکاری با مقررات و سیاست‌ها شده و به کاهش هزینه‌های اجرایی منجر شود.

نتیجه‌گیری: پذیرش هوش مصنوعی مکالمه‌ای و یادگیری ماشین در سازمان‌های دولتی فدرال مزایای اقتصادی قابل‌توجهی از جمله صرفه‌جویی در هزینه‌ها، افزایش کارایی عملیاتی و بهبود خدمات عمومی به دنبال دارد. اما این مزایا باید در برابر هزینه‌های اولیه سرمایه‌گذاری‌ها و تحلیل‌های هزینه - فایده ارزیابی شوند.

۴-۴-۴ ملاحظات قانونی و مقرراتی در پذیرش هوش مصنوعی و یادگیری ماشین

این تحقیق به بررسی چارچوب پیچیده قانونی و مقرراتی در استفاده از هوش مصنوعی مکالمه‌ای و یادگیری ماشین در سازمان‌های دولتی فدرال پرداخته است. یافته‌ها بر اهمیت مدیریت مجموعه‌ای از ملاحظات قانونی تأکید دارند تا از اجرای فناوری به‌صورت توافقی و اخلاقی اطمینان حاصل شود.

مطابقت با حریم خصوصی داده‌ها و امنیت: یکی از چالش‌های قانونی مهم، رعایت قوانین حریم خصوصی داده‌ها و امنیت است. سازمان‌های دولتی با داده‌های حساس سروکار دارند، بنابراین لازم است که با قوانینی مانند HIPAA و FISMA سازگار باشند. این قوانین دستورالعمل‌های سخت‌گیرانه‌ای برای

نحوه پردازش، ذخیره‌سازی و حفاظت از اطلاعات حساس تعیین می‌کنند. فناوری‌های هوش مصنوعی و یادگیری ماشین باید با این الزامات قانونی تطابق داشته باشند تا از حریم خصوصی شهروندان محافظت شده و تمامیت داده‌ها تضمین شود.

ملاحظات اخلاقی و انصاف: استفاده اخلاقی از فناوری‌های هوش مصنوعی امری بسیار مهم است. سازمان‌ها باید متعهد به انصاف، شفافیت و پاسخگویی در استفاده از هوش مصنوعی باشند. این شامل رعایت چارچوب‌هایی مانند GDPR است که توضیحات واضحی برای تصمیمات خودکار و راه‌های اعاده حقوق برای شهروندان فراهم می‌کند. همچنین باید الگوریتم‌های هوش مصنوعی برای شناسایی و جلوگیری از تبعیض و تعصب بررسی شوند تا از پیامدهای قانونی جلوگیری شود.

رعایت قوانین تأمین منابع: خرید و تأمین فناوری‌های هوش مصنوعی و یادگیری ماشین تحت قوانین تأمین منابع انجام می‌شود. رعایت قوانین مانند FAR برای تضمین فرایندهای تأمین شفاف و عادلانه ضروری است.

مقررات انتقال داده‌های فرامرزی: برای راه‌حل‌های مبتنی بر فضای ابری، انتقال داده‌های فرامرزی پیچیدگی‌های قانونی بیشتری ایجاد می‌کند. سازمان‌ها باید مقررات بین‌المللی مانند GDPR را مدنظر قرار دهند که شرایط سخت‌گیرانه‌ای را برای انتقال داده‌های شخصی فراتر از مرزهای اتحادیه اروپا اعمال می‌کند. رعایت این مقررات ممکن است نیازمند پیاده‌سازی مکانیزم‌های خاصی برای حفاظت از داده‌ها باشد.

مالکیت معنوی و مجوزها: پذیرش فناوری‌های هوش مصنوعی همچنین نیاز به درک حقوق مالکیت معنوی و قراردادهای مجوز دارد. سازمان‌های دولتی باید اطمینان حاصل کنند که حقوق و مجوزهای مناسب برای استفاده از الگوریتم‌ها و نرم‌افزارهای هوش مصنوعی را دارند.

نتیجه‌گیری: چارچوب قانونی و مقرراتی برای پذیرش هوش مصنوعی مکالمه‌ای و یادگیری ماشین در سازمان‌های دولتی فدرال چندوجهی و پیچیده است. سازمان‌ها باید به‌دقت از قوانین و مقررات مربوط به حریم خصوصی داده‌ها، امنیت، استفاده اخلاقی، تأمین منابع، انتقال داده‌های فرامرزی و حقوق مالکیت معنوی پیروی کنند. پیمودن این مسیر ضروری است نه تنها برای بهره‌برداری از مزایای هوش مصنوعی و یادگیری ماشین، بلکه برای حفظ اصول قانونی و حفاظت از حقوق شهروندان.

۴-۴-۵ نگرانی‌های حریم خصوصی و حفاظت از داده‌ها در استفاده از مدل‌های زبانی بزرگ (LLMs)

این تحقیق به بررسی جنبه‌های مهم حریم خصوصی و حفاظت از داده‌ها در کاربرد مدل‌های زبانی بزرگ در سازمان‌های دولتی فدرال پرداخته است. استفاده از LLM ها که داده‌های متنی گسترده‌ای را پردازش می‌کنند، چالش‌ها و ملاحظات متعددی در حوزه حریم خصوصی داده‌ها و استفاده اخلاقی به وجود می‌آورد.

- **حریم خصوصی داده‌ها و انطباق:** یکی از نگرانی‌های اصلی، نحوه پردازش اطلاعات حساس توسط LLM هاست، به‌ویژه باتوجه‌به مجموعه داده‌های وسیعی که برای آموزش این مدل‌ها موردنیاز است. سازمان‌های دولتی باید این نگرانی‌ها را با دقت مدیریت کنند تا از افشای یا سوءاستفاده تصادفی از داده‌های شهروندان جلوگیری کنند. رعایت مقررات سخت‌گیرانه‌ای مانند GDPR و HIPAA برای حفظ حقوق حریم خصوصی فردی و یکپارچگی داده‌ها حیاتی است.

- **شفافیت و توضیح پذیری:** پیچیدگی های LLM ها اغلب باعث می شود که آن ها به عنوان "جعبه های سیاه" تلقی شوند و درک چگونگی رسیدن آن ها به تصمیمات خاص دشوار باشد. این عدم شفافیت می تواند نگرانی هایی در مورد تعصب و نتایج ناعادلانه ایجاد کند، به ویژه در برنامه های حیاتی. سازمان ها باید بر روی افزایش شفافیت این مدل ها و ارائه توضیحات قابل فهم برای تصمیمات خودکار متمرکز شوند تا این نگرانی ها برطرف شوند.
- **افشای تصادفی داده ها:** یکی از خطرات مهم مربوط به LLM ها، افشای غیر مقصود اطلاعات حساس یا شناسایی ناپذیر شخصی است. پیاده سازی تدابیر سخت گیرانه برای جلوگیری از چنین افشاسازی ضروری است تا از پیامدهای قانونی و آسیب های احتمالی به اعتبار جلوگیری شود.
- **کاهش تعصب و استفاده اخلاقی:** LLM ها مستعد یادگیری تعصبات موجود در داده های آموزشی خود هستند که می تواند منجر به نتایج ناعادلانه یا تبعیض آمیز شود. سازمان ها باید به طور فعال برای کاهش این تعصبات از طریق اطمینان از تنوع و نمایندگی داده های آموزشی و استفاده از تکنیک های شناسایی و اصلاح تعصب اقدام کنند.
- **تدابیر امنیتی داده ها:** حفاظت از LLM ها در برابر دسترسی غیرمجاز، حملات سایبری و نقض داده ها با نگرانی های حریم خصوصی ارتباط نزدیکی دارد. تدابیر امنیتی قوی مانند رمزگذاری و کنترل دسترسی برای حفظ امنیت این مدل ها ضروری است.
- **رعایت مقررات بین المللی حفاظت از داده ها:** برای سازمان های دولتی که با داده های بین المللی سروکار دارند، رعایت مقررات انتقال داده های فرامرزی اهمیت ویژه ای دارد. رعایت مقرراتی مانند GDPR ممکن است نیازمند اقدامات اضافی، از جمله محلی سازی داده ها یا مکانیزم های خاص برای انتقال داده ها باشد.
- **نتیجه گیری:** سؤال تحقیق ۵ بر اهمیت رسیدگی به نگرانی های حریم خصوصی و حفاظت از داده ها در استفاده از مدل های زبانی بزرگ در کاربردهای هوش مصنوعی مکالمه ای و یادگیری ماشین در سازمان های دولتی فدرال تأکید دارد. سازمان ها باید این نگرانی ها را با دقت مدیریت کنند تا استفاده اخلاقی و مسئولانه از LLM ها را تضمین کنند، اولویت دادن به حریم خصوصی فردی، ارتقای شفافیت و حفاظت در برابر نقض داده ها و تعصب ها.

۴-۴-۶ مدیریت خطرات امنیتی در LLM ها برای سازمان های دولتی

- این تحقیق بر جنبه امنیتی استفاده از مدل های زبانی بزرگ در سازمان های دولتی فدرال تمرکز دارد، به ویژه در حوزه های هوش مصنوعی مکالمه ای و یادگیری ماشین. این بحث تهدیدات امنیتی مختلف را بررسی کرده و استراتژی های جامعی برای کاهش این خطرات پیشنهاد می دهد.
- **تهدیدات امنیتی سایبری:** مانند بسیاری از فناوری های دیجیتال، LLM ها در برابر تهدیدات مختلف امنیتی سایبری آسیب پذیر هستند که از حملات هکری خارجی تا نقض های داخلی داده ها را شامل می شود. پیاده سازی تدابیر امنیتی قوی شامل استفاده از فایروال ها، سیستم های شناسایی نفوذ و پروتکل های رمزگذاری برای حفاظت از LLM ها و داده های حساس ضروری است.

- **حریم خصوصی داده‌ها و محرمانگی:** پردازش و سیع داده‌های متنی توسط LLM ها که برخی از آن‌ها ممکن است محرمانه باشند، نیازمند تدابیر سخت‌گیرانه حفاظت از حریم خصوصی و محرمانگی است. رمزگذاری، کنترل دسترسی و تکنیک‌های ناشناس‌سازی داده‌ها برای حفاظت از اطلاعات حساس از دسترسی یا افشای غیرمجاز ضروری هستند.
- **حملات خصمانه: LLM ها** در برابر حملات خصمانه آسیب‌پذیر هستند که در آن داده‌های ورودی به منظور تولید خروجی‌های نادرست یا مضر دست‌کاری می‌شوند. این حملات می‌تواند در زمینه‌های حیاتی تصمیم‌گیری آسیب‌زا باشد. سرمایه‌گذاری در تحقیقات و فناوری‌ها برای شناسایی و مقابله با این حملات برای تقویت امنیت و پایداری LLM ها ضروری است.
- **ریسک‌های زنجیره تأمین:** وابستگی LLM ها به مدل‌های پیش آموزش داده شده و کتابخانه‌های شخص ثالث، خطرات مربوط به زنجیره تأمین را معرفی می‌کند. ارزیابی و اطمینان از امنیت این اجزاء برای جلوگیری از آسیب‌پذیری‌های ناشی از وابستگی‌های خارجی ضروری است.
- **ملاحظات اخلاقی و تعصب‌ها:** نگرانی‌های امنیتی در LLM ها همچنین شامل مسائل اخلاقی مانند تعصب در داده‌های مدیریت ریسک: پروژه‌های هوش مصنوعی و یادگیری ماشین با ریسک‌ها و عدم اطمینان‌های ذاتی همراه هستند. رهبران باید توانایی شناسایی، ارزیابی و کاهش این ریسک‌ها را داشته باشند تا از شکست‌های احتمالی پروژه جلوگیری کرده و نتایج پایداری را تضمین کنند.
- **رهبری اخلاقی:** باتوجه به پیامدهای اخلاقی هوش مصنوعی و یادگیری ماشین، به‌ویژه در زمینه‌های دولتی، رهبران باید از شیوه‌های اخلاقی حمایت کنند. این شامل تضمین این است که الگوریتم‌های هوش مصنوعی منصفانه، شفاف، بدون تعصب و هم‌راستا با اصول اخلاقی در مدیریت داده‌ها و تصمیم‌گیری باشند.
- **نوآوری و انطباق:** ماهیت سریع‌الوصول فناوری نیازمند فرهنگ نوآوری و انطباق‌پذیری است. رهبران باید آزمایش با فناوری‌های نوظهور را تشویق کرده و آماده تغییر استراتژی‌ها در پاسخ به پیشرفت‌های تکنولوژیکی باشند.
- **معیارهای عملکرد و پاسخگویی:** ایجاد معیارهای واضح برای عملکرد و پاسخگویی تیم‌ها به نتایج پروژه‌های هوش مصنوعی و یادگیری ماشین ضروری است. این رویکرد به رهبران این امکان را می‌دهد که پیشرفت را پیگیری کرده، موفقیت را اندازه‌گیری کنند و اطمینان حاصل کنند که ابتکارات به اهداف موردنظر خود دست می‌یابند.
- **مشارکت ذی‌نفعان:** رهبران مؤثر باید به طور فعال با ذی‌نفعان از جمله شهروندان، سیاست‌گذاران و شرکای صنعتی تعامل داشته باشند. مدیریت انتظارات، درخواست بازخورد و حفظ شفافیت در طول فرایند پیاده‌سازی از جمله کلیدهای موفقیت در مشارکت ذی‌نفعان هستند.
- **استراتژی بلندمدت:** رهبری پیشگامانه شامل توسعه استراتژی‌های بلندمدت است که تغییرات تکنولوژیکی آینده و نیازهای تکاملی مأموریت‌ها را پیش‌بینی می‌کند. رهبران باید بر روی رویکردهای پایدار که قادر به انطباق با پیشرفت‌های آینده در زمینه هوش مصنوعی و یادگیری ماشین باشند، تمرکز کنند.
- **نتیجه‌گیری:** رهبری مؤثر برای پذیرش و پیاده‌سازی موفقیت‌آمیز پروژه‌های هوش مصنوعی مکالمه‌ای و یادگیری ماشین در نهادهای دولتی فدرال حیاتی است. رهبری با چشم‌انداز، مدیریت تغییر ماهرانه، همکاری چندوظیفه‌ای، ملاحظات اخلاقی و تعهد به نوآوری از جمله ارکان اساسی برای

موفقیت هستند. رهبران باید پیچیدگی‌های پذیرش هوش مصنوعی را به طور ماهرانه‌ای هدایت کرده و اولویت را به شیوه‌های اخلاقی و حکمرانی داده‌ها بدهند و فرهنگی را برای نوآوری و موفقیت بلندمدت پرورش دهند.

۷-۴-۴ ادغام هوش مصنوعی و یادگیری ماشین در زیرساخت‌های دولت فدرال

این تحقیق مراحل و ملاحظات حیاتی برای مهاجرت و ادغام مؤثر فناوری‌های هوش مصنوعی مکالمه‌ای و یادگیری ماشین در زیرساخت‌های موجود نهادهای دولتی فدرال را بررسی می‌کند. یافته‌ها ماهیت چندبعدی این فرآیند و استراتژی‌های لازم برای پیاده‌سازی موفقیت‌آمیز را برجسته می‌کنند.

- **ارزیابی زیر ساخت:** اولین گام برای نهادهای ارزیابی کامل زیرساخت‌های فعلی خود است که شامل سخت‌افزار، نرم‌افزار، قابلیت‌های شبکه و سیستم‌های ذخیره‌سازی داده‌ها می‌شود. این ارزیابی جامع برای شناسایی نواحی که ممکن است نیاز به ارتقا یا اصلاحات داشته باشند، ضروری است.
- **تحلیل سازگاری:** اطمینان از سازگاری میان سیستم‌های موجود و فناوری‌های جدید هوش مصنوعی/یادگیری ماشین از اهمیت ویژه‌ای برخوردار است. نهادهای باید ارزیابی کنند که آیا سیستم‌های فعلی آنها می‌توانند با این فناوری‌های جدید یکپارچه شوند یا نیاز به اصلاحات دارند. پرداختن به مسائل سازگاری به‌صورت پیشگیرانه ضروری است تا از اختلالات در عملیات جلوگیری شود.
- **آمادگی داده‌ها:** باتوجه به ماهیت داده‌محور هوش مصنوعی و یادگیری ماشین، نهادهای باید کیفیت، حجم و دسترسی به داده‌های خود را ارزیابی کنند. آماده‌سازی داده‌ها برای پردازش هوش مصنوعی شامل پاک‌سازی، استانداردسازی و اطمینان از دسترسی به آنها است. ایجاد شیوه‌های حکمرانی داده‌ها نیز کلید تضمین امنیت و انطباق داده‌ها است.
- **ملاحظات مقیاس‌پذیری:** مقیاس‌پذیری باید عنصر بنیادی ابتکارات هوش مصنوعی و یادگیری ماشین باشد. حتی اگر پروژه‌ها با طرح‌های آزمایشی شروع شوند، طراحی باید امکان گسترش را برای رفع نیازهای آینده فراهم کند.
- **اقدامات امنیتی:** ادغام هوش مصنوعی و یادگیری ماشین در سیستم‌های دولتی نیاز به اقدامات امنیتی تقویت شده دارد. نهادهای باید رمزنگاری، کنترل دسترسی و سیستم‌های نظارت مستمر را برای حفاظت از داده‌های حساس و پیشگیری از تهدیدات سایبری پیاده‌سازی کنند.
- **بین عملکردی بودن:** باتوجه به تنوع نرم‌افزارها و سیستم‌های مورد استفاده توسط نهادهای دولتی، اطمینان از بین عملکردی بودن ضروری است. رابط‌ها و پروتکل‌های استاندارد می‌توانند این ادغام را تسهیل کنند.
- **آموزش و توسعه مهارت‌ها:** آمادگی نیروی کار برای ادغام هوش مصنوعی و یادگیری ماشین ضروری است. این شامل آموزش و ارتقا مهارت‌های کارکنان در مفاهیم و ابزارهای مرتبط با این فناوری‌ها است.
- **مدیریت تغییر:** پرداختن به جنبه‌های انسانی ادغام فناوری از طریق مدیریت تغییر مؤثر بسیار حیاتی است. استراتژی‌ها برای تسهیل انتقال شامل ارتباطات روشن، آموزش جامع و پرداختن به مقاومت در برابر تغییرات در روندها و فرایندهای جدید است.

- **همکاری با تأمین کنندگان:** همکاری نزدیک با تأمین کنندگان فناوری هوش مصنوعی و یادگیری ماشین ضروری است. این همکاری اطمینان می‌دهد که نهادها نیازهای سیستم را درک کرده، پشتیبانی لازم را دریافت کنند و به‌روزرسانی‌ها و تعمیرات ضروری را به‌موقع انجام دهند.
- **آزمون و اعتبارسنجی:** قبل از پیاده‌سازی در مقیاس کامل، آزمون‌ها و اعتبارسنجی‌های دقیق برای شناسایی و حل مشکلات ضروری است. این مرحله برای کاهش اختلالات و تضمین عملکرد صحیح فناوری پس از پیاده‌سازی حیاتی است.
- **انطباق و مقررات:** نهادها باید اطمینان حاصل کنند که پیاده‌سازی‌های هوش مصنوعی و یادگیری ماشین آن‌ها با تمامی مقررات و استانداردهای فدرال مرتبط مطابقت دارند. این انطباق غیرقابل مذاکره است و برای استقرار قانونی و اخلاقی فناوری‌ها ضروری است.
- **نظارت و ارزیابی مستمر:** موفقیت مداوم نیازمند نظارت و ارزیابی مستمر است. ایجاد شاخص‌های عملکرد کلیدی (KPI) برای ارزیابی تأثیر فناوری‌های هوش مصنوعی و یادگیری ماشین بر عملیات و فرایندهای تصمیم‌گیری از اجزای اصلی این ارزیابی مستمر است.
- **نتیجه‌گیری:** مهاجرت و ادغام فناوری‌های هوش مصنوعی و یادگیری ماشین در زیر ساخت‌های نهادهای دولتی فدرال نیازمند برنامه‌ریزی دقیق، ارزیابی همه‌جانبه و اجرای دقیق است. با پرداختن به ملاحظات کلیدی مانند سازگاری، مقیاس‌پذیری، امنیت و انطباق، نهادها می‌توانند به طور مؤثر از پتانسیل تحول‌آفرین هوش مصنوعی و یادگیری ماشین بهره‌برداری کنند، درحالی‌که کارایی و امنیت عملیاتی را حفظ می‌کنند.

۴-۴-۸ پیامدهای هوش مصنوعی مکالمه‌ای و یادگیری ماشین در امنیت ملی و اطلاعات

- این سؤال به پیامدهای پذیرش هوش مصنوعی مکالمه‌ای و یادگیری ماشین (CAIML) برای تحلیل امنیت ملی و اطلاعات در دولت فدرال می‌پردازد. این یک حوزه حساس است که پذیرش فناوری می‌تواند پیامدهای قابل توجهی داشته باشد.
- **تحلیل اطلاعات بهبود یافته:** پذیرش CAIML می‌تواند توانمندی‌های تحلیلگران اطلاعاتی را به طور قابل توجهی افزایش دهد. این فناوری‌ها می‌توانند حجم وسیعی از داده‌ها را به‌سرعت پردازش و تحلیل کنند و به تحلیلگران کمک کنند تا الگوها، روندها و تهدیدات بالقوه را به طور کارآمدتری شناسایی کنند.
 - **شناسایی تهدیدات به‌صورت بلادرنگ:** CAIML می‌تواند شناسایی تهدیدات و هشداردهی در زمان واقعی را فراهم کند. با نظارت مستمر بر جریان‌های داده، این فناوری‌ها می‌توانند فعالیت‌های مشکوک یا تهدیدات امنیت
 - **ی را سریع شناسایی کرده و امکان پاسخ‌دهی سریع فراهم کنند.**
 - **تحلیل پیش‌بینی:** الگوریتم‌های یادگیری ماشین می‌توانند برای پیش‌بینی تهدیدات امنیتی یا ریسک‌ها بر اساس داده‌های تاریخی آموزش‌دیده و این رویکرد پیشگیرانه به نهادها این امکان را می‌دهد که اقدامات پیشگیرانه انجام دهند.
 - **ادغام داده‌ها:** CAIML می‌تواند داده‌ها را از منابع مختلف، از جمله اطلاعات منبع‌باز، رسانه‌های اجتماعی و اطلاعات محرمانه ادغام کند. این ادغام داده‌ها، درک جامع‌تری از تهدیدات امنیتی ایجاد می‌کند.

- **شناسایی ناهنجاری‌ها CAIML:** در شناسایی ناهنجاری‌ها مهارت دارد که برای شناسایی الگوهای غیرعادی یا غیرمنتظره در داده‌ها بسیار مهم است. این می‌تواند به‌ویژه در کشف فعالیت‌های پنهانی یا نقض‌های امنیت سایبری مفید باشد.
- **امنیت سایبری:** امنیت ملی به شدت وابسته به تدابیر امنیت سایبری قوی است. CAIML می‌تواند با نظارت مستمر بر ترافیک شبکه، شناسایی آسیب‌پذیری‌ها و پاسخ‌دهی به تهدیدات در زمان واقعی، امنیت سایبری را تقویت کند.
- **کاهش خطای انسانی:** اتوماسیون از طریق CAIML می‌تواند خطر خطای انسانی در تحلیل‌های اطلاعاتی را کاهش دهد. تحلیلگران می‌توانند بر تصمیم‌گیری‌های سطح بالاتر تمرکز کنند درحالی‌که هوش مصنوعی به پردازش داده‌ها و ارزیابی‌های اولیه می‌پردازد.
- **بهینه‌سازی منابع CAIML:** می‌تواند تخصیص منابع را بهینه‌سازی کرده و نواحی با ریسک یا اولویت بالا را شناسایی کند. این اطمینان می‌دهد که منابع محدود به جایی که بیشترین نیاز را دارند هدایت می‌شوند.
- **ملاحظات اخلاقی:** استفاده از CAIML در امنیت ملی و اطلاعات نگرانی‌های اخلاقی از جمله مسائل حریم خصوصی و تعصبات در الگوریتم‌ها را به همراه دارد. دستیابی به تعادل بین امنیت و حقوق فردی یک چالش پیچیده است.
- **همکاری انسان و هوش مصنوعی:** ادغام موفقیت‌آمیز CAIML در عملیات امنیت ملی نیاز به همکاری مؤثر بین سیستم‌های هوش مصنوعی و تحلیلگران انسانی دارد. نهادها باید فرایندهایی برای تعامل معنی‌دار انسان و هوش مصنوعی ایجاد کنند.
- **انطباق با مقررات:** نهادهای دولتی باید از چارچوب‌های قانونی و مقرراتی در استفاده از CAIML برای امنیت ملی پیروی کنند. رعایت قوانین مربوط به حریم خصوصی داده‌ها، نظارت و فعالیت‌های اطلاعاتی ضروری است.
- **شفافیت و پاسخگویی:** تضمین شفافیت در تصمیم‌گیری‌های هوش مصنوعی و حفظ پاسخگویی در قبال نتایج تولید شده توسط هوش مصنوعی از اهمیت ویژه‌ای برخوردار است. این شامل توضیح چگونگی رسیدن هوش مصنوعی به نتایج یا پیشنهادها خاص است.
- **حملات متقابل:** نهادهای امنیت ملی باید برای حملات متقابل به سیستم‌های هوش مصنوعی آماده باشند. تهدیدگران ممکن است سعی کنند مدل‌های هوش مصنوعی را دستکاری کرده تا عملیات اطلاعاتی را فریب داده یا مختل کنند.
- **یادگیری و انطباق مستمر:** مدل‌های CAIML باید به طور مداوم یاد بگیرند و به تهدیدات در حال تکامل سازگار شوند. نهادها به مکانیزم‌هایی برای به‌روزرسانی و آموزش دوباره مدل‌های هوش مصنوعی نیاز دارند تا از حریفان جلوتر بمانند.
- **نتیجه‌گیری:** پذیرش CAIML در تحلیل امنیت ملی و اطلاعات در دولت فدرال پیامدهای دوردست و چالش‌های اخلاقی، قانونی و پاسخگویی را به همراه دارد. درحالی‌که این فناوری‌ها پتانسیل بهبود شناسایی تهدیدات، تحلیل پیش‌بینی و بهینه‌سازی منابع را دارند، چالش‌های اخلاقی و حقوقی نیز وجود دارد. دستیابی به تعادل صحیح بین امنیت و حقوق فردی، رعایت مقررات و آمادگی برای حملات متقابل از اجزای مهم بهره‌برداری موفقیت‌آمیز از CAIML برای امنیت ملی است. یک رویکرد مسئولانه و سازگار برای استفاده از این فناوری‌ها درحالی‌که منافع ملی حفظ می‌شود، ضروری است.

نتیجه‌گیری

در نتیجه، پرورش یک فرهنگ نوآوری و یادگیری مداوم برای موفقیت در پذیرش CAIML در رایانش ابری در سازمان‌های دولتی فدرال از اهمیت بالایی برخوردار است. چنین فرهنگی آزمایش، همکاری و انطباق‌پذیری را تشویق می‌کند که همگی در چشم‌انداز در حال تکامل سریع فناوری‌های هوش مصنوعی و یادگیری ماشین ضروری هستند. تعهد رهبری، توانمندسازی کارکنان و تمرکز بر شیوه‌های اخلاقی به ساختن فرهنگی کمک می‌کند که از نوآوری حمایت می‌کند و اطمینان می‌دهد که سازمان‌های دولتی فدرال می‌توانند از تمام پتانسیل CAIML برای بهبود عملیات و تصمیم‌گیری‌ها بهره‌برداری کنند.

بررسی پتانسیل هوش مصنوعی داستان‌گویی در تقویت امنیت داده‌ها و تطابق با FedRAMP به بینش‌های مهمی دست‌یافت. هوش مصنوعی داستان‌گویی یک رویکرد نوآورانه برای تجزیه و تحلیل و تجسم الگوهای داده‌ای ارائه داد که به شناسایی تهدیدات و نظارت کمک کرد. این فناوری امکان تحلیل تهدیدات در زمان واقعی و شناسایی تهدیدات نوظهور امنیت سایبری را فراهم کرد. علاوه بر این، هوش مصنوعی داستان‌گویی به توسعه روایت‌هایی کمک کرد که در مدل‌سازی تهدیدات و ادغام اطلاعات تهدیدات مفید بود. نقش آن در تقویت قابلیت‌های ارزیابی تهدید و تسریع شناسایی تهدیدات چشمگیر بود. با بهره‌برداری از قدرت هوش مصنوعی داستان‌گویی، سازمان‌های دولتی فدرال می‌توانند تدابیر امنیتی داده‌های خود را تقویت کرده و با الزامات FedRAMP هم‌راستا شوند.

فصل پنجم

جمع‌بندی و پیشنهادها

در چشم‌انداز پویای پذیرش فناوری و امنیت در سازمان‌های دولتی فدرال، این تحقیق وارد قلمروهای ناشناخته‌ای شده است تا یک اکتشاف جامع و روشن از تعاملات پیچیده بین رایانش ابری، هوش مصنوعی داستان‌گویی و برنامه مدیریت ریسک و مجوز فدرال (FedRAMP) ارائه دهد. در این تحقیق، محقق ضمن بررسی چالش‌ها و فرصت‌ها، به شناسایی راه‌حل‌ها و مسیرهای عملی برای عبور از پیچیدگی‌های این میدان پرداخته است. در عصری که به شدت تحت‌تأثیر فناوری است، درک پیچیدگی‌های اجرای راه‌حل‌های فناوریانه پیشرفته در سازمان‌های دولتی ضروری است. این مطالعه یک بررسی جامع از چشم‌انداز پیچیده و پویا در رایانش ابری، هوش مصنوعی داستان‌گویی و تطابق با برنامه مدیریت ریسک و مجوز فدرال (FedRAMP) در سازمان‌های دولتی فدرال ارائه می‌دهد. یافته‌های ارائه شده چالش‌ها و فرصت‌های پیچیده موجود در پذیرش فناوری را روشن می‌کند. همچنین، این یافته‌ها درک دقیقی از نحوه تعامل راه‌حل‌های فناوری نوآورانه با الزامات سخت‌گیرانه امنیت داده و انطباق قانونی ارائه می‌دهند. این تحقیق بینش‌های حیاتی در خصوص نحوه ادغام مؤثر فناوری‌های نوین مانند رایانش ابری و هوش مصنوعی در سازمان‌های دولتی فراهم می‌کند، درحالی‌که استانداردهای امنیتی و انطباقی سخت‌گیرانه را حفظ می‌کند، در دوران انقلاب فناوریانه جاری. اهمیت این مطالعه در تحلیل عمیق آن از دشواری‌ها، امکانات و آثار این ادغام‌های فناوری نهفته است، همراه با پیشنهادها خاص برای سیاست‌گذاران، سازمان‌های دولتی و جامعه پژوهشی.

۵-۱ نتایج حاصل از تحقیق

۵-۱-۱ شناسایی موانع اصلی پذیرش فناوری‌های هوشمند در سازمان‌های دولتی

این تحقیق نشان داد که موانع فرهنگی، قانونی، و امنیتی از اصلی‌ترین چالش‌های پذیرش هوش مصنوعی و رایانش ابری در سازمان‌های دولتی هستند. به طور خاص، موارد زیر شناسایی شدند:

- **نگرانی‌های امنیتی:** بسیاری از سازمان‌های دولتی نگرانی‌های زیادی در خصوص حریم خصوصی داده‌ها و امنیت اطلاعات دارند. این نگرانی‌ها به‌ویژه در استفاده از رایانش ابری که داده‌ها باید در سرورهای خارج از سازمان ذخیره شوند، بیشتر احساس می‌شود.
- **مقررات قانونی:** قوانین موجود در بسیاری از کشورها هنوز برای مدیریت و نظارت بر فناوری‌های نوین به‌ویژه در زمینه حریم خصوصی و امنیت داده‌ها به‌روز نشده‌اند. به همین دلیل، سازمان‌های دولتی با مشکلاتی در پیاده‌سازی این فناوری‌ها روبه‌رو هستند.
- **مقاومت فرهنگی و ساختاری:** بسیاری از کارکنان دولتی به دلیل ترس از تغییر و مقاومت در برابر نوآوری‌ها، از پذیرش فناوری‌های جدید امتناع می‌کنند. این مقاومت به‌ویژه در سیستم‌های دولتی با ساختارهای بوروکراتیک و فرایندهای سنتی وجود دارد.

۵-۱-۲ مزایای پذیرش فناوری‌های هوشمند

نتایج تحقیق نشان داد که پذیرش هوش مصنوعی و رایانش ابری می‌تواند به‌شدت به افزایش بهره‌وری، کاهش هزینه‌ها و بهبود کیفیت خدمات در سازمان‌های دولتی کمک کند:

- **افزایش کارایی:** استفاده از هوش مصنوعی برای تحلیل داده‌ها و پیش‌بینی روندها می‌تواند فرایندهای تصمیم‌گیری را سریع‌تر و دقیق‌تر کند.
- **کاهش هزینه‌ها:** با استفاده از رایانش ابری، سازمان‌های دولتی می‌توانند از زیرساخت‌های مقیاس‌پذیر بهره‌مند شوند و هزینه‌های مربوط به نگهداری و به‌روزرسانی سرورها را کاهش دهند.
- **بهبود خدمات عمومی:** استفاده از این فناوری‌ها باعث می‌شود که سازمان‌ها بتوانند خدمات خود را به‌طور مؤثرتری به شهروندان ارائه دهند، به‌ویژه در زمینه درخواست‌های آنلاین، پرداخت‌ها و پیگیری امور اداری.

۱-۵-۳ نقش امنیت داده‌ها در پذیرش فناوری‌های هوشمند

یکی از یافته‌های مهم تحقیق این است که سازمان‌های دولتی برای پذیرش فناوری‌های جدید نیاز به سیاست‌های امنیتی قوی و مشخص دارند. استفاده از الگوریتم‌های هوش مصنوعی برای شناسایی تهدیدات سایبری و تقویت امنیت داده‌ها می‌تواند به این سازمان‌ها کمک کند تا از مزایای این فناوری‌ها بهره‌برداری کنند.

۲-۵-۴ ضرورت به‌روزرسانی قوانین و مقررات

تحقیق نشان داد که چالش‌های قانونی یکی از موانع عمده در پذیرش این فناوری‌ها در سازمان‌های دولتی است. قوانین موجود بسیاری از کشورها هنوز به طور کامل پذیرش فناوری‌های نوین را تسهیل نمی‌کنند. به همین دلیل، اصلاح قوانین و مقررات برای هم‌راستایی با پیشرفت‌های فناوری ضروری است.

۵-۲-۲ پیشنهادات برای تحقیق

۱-۵-۲ بررسی تأثیرات بلندمدت پذیرش فناوری‌های هوشمند در سازمان‌های دولتی

یکی از پیشنهادات برای تحقیقات آینده، مطالعه تأثیرات بلندمدت پذیرش هوش مصنوعی و رایانش ابری در سازمان‌های دولتی است. تحقیقات بیشتری باید به بررسی اینکه چگونه این فناوری‌ها می‌توانند در طولانی‌مدت تأثیرات مثبتی بر پاسخ‌دهی به شهروندان، کیفیت خدمات دولتی و حفظ امنیت داده‌ها بگذارند، پردازند.

۲-۵-۲ توسعه مدل‌های پذیرش فناوری به‌ویژه برای بخش‌های دولتی

پژوهش‌های بیشتری باید به طراحی مدل‌های پذیرش فناوری اختصاص یابد که مخصوص بخش دولتی باشد. مدل‌های پذیرش فناوری که در بخش خصوصی مورد استفاده قرار می‌گیرند ممکن است به طور کامل برای سازمان‌های دولتی قابل اجرا نباشند، زیرا ویژگی‌های فرهنگی، قانونی و سازمانی متفاوتی دارند؛ بنابراین، مدل‌های اختصاصی پذیرش برای بخش دولتی نیاز به توسعه دارند.

۲-۵-۳ تحلیل چالش‌های مرتبط با امنیت داده‌ها در سطح جهانی

در تحقیقاتی آینده، باید به چالش‌های امنیتی جهانی در پذیرش فناوری‌های هوشمند در سازمان‌های دولتی پرداخته شود. به‌ویژه در زمینه حریم خصوصی اطلاعات، که با توجه به استانداردهای مختلف جهانی (مانند GDPR در اروپا) متفاوت است. مقایسه چالش‌های امنیتی در کشورهای مختلف می‌تواند به شناسایی بهترین شیوه‌ها برای مدیریت داده‌های حساس دولتی کمک کند.

۲-۵-۴ مطالعه بر روی مدل‌های آموزشی برای کارکنان دولتی

یکی از موانع اصلی پذیرش فناوری‌های جدید در سازمان‌های دولتی، مقاومت کارکنان به دلیل ناشناسی یا عدم توانایی در استفاده از این فناوری‌ها است؛ بنابراین، تحقیقات آینده باید بر روی مدل‌های آموزشی برای ارتقای توانمندی‌های کارکنان دولتی در استفاده از فناوری‌های نوین، به‌ویژه هوش مصنوعی و رایانش ابری متمرکز شود.

۲-۵-۵ بررسی تأثیرات اجتماعی و فرهنگی پذیرش فناوری در سازمان‌های دولتی

برای پذیرش موفقیت‌آمیز فناوری‌های نوین در سازمان‌های دولتی، باید موانع فرهنگی و اجتماعی مورد بررسی قرار گیرند. تحقیقات بیشتری باید به تحلیل فرهنگ سازمانی در بخش دولتی و مقاومت کارکنان در برابر فناوری‌های جدید پردازد و راهکارهای مناسب برای مدیریت این تغییرات را پیشنهاد دهد.

۲-۵-۶ تحلیل قوانین و مقررات برای تسهیل پذیرش فناوری های نوین

تحقیقات آینده باید به تحلیل و پیشنهاد اصلاحات قانونی در زمینه پذیرش هوش مصنوعی و رایانش ابری در سازمان های دولتی پردازد. این تحقیق می تواند به سیاست گذاران و مقامات قانونی کمک کند تا مقررات جدیدی تدوین کنند که از یک طرف پذیرش فناوری ها را تسهیل کرده و از طرف دیگر امنیت اطلاعات را تضمین کند.

۵-۳ توصیه ها

باتوجه به یافته های تحقیق، محقق توصیه های عملی زیر را ارائه می دهد که هم قابل اجرا و هم قابل انطباق هستند و به ذی نفعان مختلف در زمینه پذیرش فناوری و امنیت در آژانس های دولتی فدرال کمک می کنند.

۵-۳-۱ برای آژانس های دولتی فدرال

- **بازبینی و اصلاح سیاست ها**

آژانس های دولتی فدرال باید یک بازبینی جامع از سیاست ها و مقررات موجود در زمینه رایانش ابری، هوش مصنوعی داستان گویی و انطباق با FedRAMP انجام دهند. این بازبینی باید باهدف شناسایی شکاف ها و ناکارآمدی ها صورت گیرد و به روزرسانی سیاست ها به گونه ای انجام شود که با فناوری های نوظهور و چالش های امنیتی هم راستا باشد.

- **سرمایه گذاری در آموزش و توسعه مهارت ها**

آژانس ها باید سرمایه گذاری در برنامه های آموزشی و توسعه مهارت برای کارکنان خود را در اولویت قرار دهند. باتوجه به تغییرات سریع فناوری، یادگیری مداوم ضروری است. فراهم کردن فرصت هایی برای کارکنان جهت کسب مهارت های جدید و به روز ماندن با بهترین شیوه های صنعتی از اهمیت بالایی برخوردار است.

- **تقویت فرهنگ نوآوری**

آژانس ها باید به طور فعال فرهنگ نوآوری را ترویج کنند، به طوری که کارکنان تشویق شوند تا به کاوش راه حل ها و روش های جدید بپردازند. ایجاد محیطی که خلاقیت و حل مسئله را ارج می نهد می تواند به واکنش های مؤثرتر نسبت به چالش های در حال تحول منجر شود.

۵-۳-۲ برای سیاست گذاران

- **ایجاد همکاری میان صنعت ها**

سیاست گذاران باید همکاری و تبادل دانش میان آژانس های دولتی فدرال و دیگر صنایع که با چالش های مشابه فناوری روبه رو هستند، تسهیل کنند. این تبادل میان صنعت ها می تواند به پذیرش بهترین شیوه ها و توسعه سیاست های قوی تر منجر شود.

- **حمایت از تحقیق و توسعه**

سیاست گذاران باید منابعی را برای حمایت از تلاش های تحقیق و توسعه در زمینه های رایانش ابری، هوش مصنوعی داستان گویی و انطباق با FedRAMP تخصیص دهند. ابتکارات تأمین مالی می تواند به نوآوری و توسعه فناوری های امن متناسب با نیازهای دولتی منجر شود.

۵-۳-۳ برای محققان

- **کاوش تهدیدات نوظهور**

محققان باید به شناسایی و تحلیل تهدیدات و چالش های نوظهور در تقاطع رایانش ابری، هوش مصنوعی داستان گویی و FedRAMP بپردازند. پیش بینی این مسائل می تواند به توسعه راه حل های پیشگیرانه کمک کند.

- **ارزیابی اثرات بلندمدت**
محققان باید مطالعات طولانی مدت برای ارزیابی اثرات بلندمدت تغییرات سیاستی و پذیرش فناوری در آژانس‌های دولتی فدرال انجام دهند. درک چگونگی تکامل این تغییرات در طول زمان برای بهبود مستمر ضروری است.

۵-۳-۴ برای تمامی ذینفعان

- **انعطاف‌پذیری را حفظ کنید**
تأکید بر اهمیت انعطاف‌پذیری در محیطی که به طور مداوم در حال تغییر است. ذی‌نفعان باید آماده باشند تا استراتژی‌ها و سیاست‌های خود را به طور مداوم بررسی و در پاسخ به پیشرفت‌های فناوری و تهدیدات امنیتی در حال تحول، تغییر دهند.
- **امنیت را در اولویت قرار دهید**
تأکید بر اهمیت حیاتی امنیت در تمامی جنبه‌های ادغام فناوری. این شامل پیاده‌سازی تدابیر سخت‌گیرانه حفاظت از داده‌ها، سیستم‌های پیشرفته شناسایی تهدیدات و شیوه‌های نظارتی مستمر می‌شود.
- **همکاری برای یافتن راه‌حل‌ها**
تشویق به تلاش‌های مشترک در میان بخش‌های مختلف. با گردآوری منابع و تخصص‌ها، آژانس‌های فدرال، سیاست‌گذاران، محققان و کارشناسان صنعت می‌توانند استراتژی‌های مؤثرتری برای مقابله با چالش‌های پذیرش فناوری و امنیت طراحی کنند.

۵-۳-۵ توصیه‌های خاص

- **بهترین شیوه‌های امنیت داده‌ها**
پیشنهاد می‌شود آژانس‌های دولتی بهترین شیوه‌های امنیت داده‌ها را پذیرفته و به‌طور جدی آن‌ها را اجرا کنند. این شامل استفاده از رمزگذاری، کنترل‌های دسترسی سخت‌گیرانه و ارزیابی‌های منظم امنیتی به‌منظور حفاظت از اطلاعات حساس است.
- **ادغام هوش مصنوعی داستان‌گویی**
پیشنهاد می‌شود که هوش مصنوعی داستان‌گویی در چارچوب‌های امنیت سایبری ادغام شود. این می‌تواند توانایی‌ها را در زمینه‌هایی مانند شناسایی تهدیدات، مدل‌سازی تهدیدات و تحلیل تهدیدات به‌صورت بلادرنگ افزایش دهد و رویکردی پویا به امنیت ارائه دهد.
- **همکاری بین آژانس‌ها**
تأکید بر نیاز به تلاش‌های مشترک میان آژانس‌های فدرال. به‌اشتراک‌گذاری اطلاعات تهدیدات و بینش‌های امنیتی می‌تواند به ارزیابی‌های ریسک جامع‌تر و تقویت امنیت ملی منجر شود.
- **به‌روزرسانی سیاست‌ها**
پیشنهاد می‌شود سیاست‌گذاران به طور دوره‌ای مقررات را بازبینی و به‌روزرسانی کنند تا ملاحظات فناوری‌های نوظهور مانند هوش مصنوعی داستان‌گویی را در بر گیرد. این اطمینان می‌دهد که دستورالعمل‌ها مرتبط و مؤثر در زمینه پیشرفت‌های فناوری مدرن باقی بمانند.
- **ادامه تحقیقات**
تشویق به تحقیق مداوم در زمینه پذیرش فناوری، امنیت و انطباق. تلاش‌های تحقیقاتی مستمر برای پیشی‌گرفتن از چالش‌های جدید و بهره‌برداری از فرصت‌های نوظهور در این حوزه ضروری است.

۵-۴ جمع‌بندی و نتیجه‌گیری

تحقیق حاضر نشان می‌دهد که پذیرش فناوری‌های هوشمند در سازمان‌های دولتی، باوجود مزایای چشمگیر مانند افزایش کارایی، کاهش هزینه‌ها و بهبود کیفیت خدمات، با چالش‌های امنیتی، موانع فرهنگی و مقاومت در برابر تغییر روبه‌رو است. این تحقیق بر لزوم اصلاح مقررات و توسعه مدل‌های پذیرش فناوری برای بخش دولتی تأکید دارد و پیشنهادهایی برای تحقیقات آینده در این زمینه ارائه کرده است. این تحقیق به‌عنوان یک سند جامع در زمینه پذیرش

فناوری و امنیت در سازمان‌های دولتی فدرال به‌ویژه در رابطه با هوش مصنوعی داستان‌گویی و FedRAMP به حساب می‌آید و مسیرهای جدیدی برای تحقیق و پیشرفت در این زمینه‌ها فراهم می‌آورد. این تحقیق دیدگاه‌های جامع و عمیقی درباره پذیرش رایانش ابری، ادغام هوش مصنوعی در داستان‌گویی و انطباق با FedRAMP در سازمان‌های دولتی فدرال ارائه می‌دهد. کمک‌های نظری کلیدی این تحقیق بر اهمیت برنامه‌ریزی استراتژیک، توسعه نیروی کار ماهر، اقدامات امنیتی و حاکمیت رهبری به‌منظور مدیریت مؤثر پیچیدگی‌های این تکنولوژی‌ها تأکید دارد. این درک، مبنای تحقیق و تدوین سیاست‌های آینده در پیشرفت‌های فناوری در بخش عمومی را فراهم می‌آورد. این تحقیق به بررسی ادغام داستان‌گویی مبتنی بر هوش مصنوعی در سازمان‌های دولتی فدرال می‌پردازد و بر چالش‌ها، فرصت‌ها و ملاحظات استراتژیک تمرکز دارد. این تحقیق پیچیدگی‌های پیاده‌سازی داستان‌گویی مبتنی بر هوش مصنوعی در عملیات دولتی را آشکار کرده و دیدگاه‌های دقیقی از موانع و فرصت‌های موجود ارائه می‌دهد.

مراجع

- Aarestrup, F. M., Albeyatti, A., Armitage, W. J., Auffray, C., Augello, L., Balling, R.,... & Van Oyen, H. (٢٠٢٠). Towards a European health research and innovation cloud (HRIC). *Genome medicine*, ١٢, ١-١٤.
<https://doi.org/10.1186/s13073-020-0113-z>
- Abdulmajeed, M., & Fahmy, N. (٢٠٢٢). Meta-analysis of AI Research in Journalism: Challenges, Opportunities and Future Research Agenda for Arab Journalism. *From the Internet of Things to the Internet of Ideas: The Role of Artificial Intelligence: Proceedings of EAMMIS ٢٠٢٢, ٢١٣- ٢٢٥*.
- AbuMusab, S. (٢٠٢٣). Generative AI and human labor: who is replaceable?. *AI & SOCIETY*, ١-٣.
- Adams, W. C. (٢٠١٥). Conducting semi- structured interviews. *Handbook of practical program evaluation*, ٤٩٢-٥٠٥.
- Ahmad, R., Siemon, D., Gnewuch, U., & Robra-Bissantz, S. (٢٠٢٢, January). A Framework of Personality Cues for Conversational Agents. In *Proceedings of the ٥٥th Hawaii International Conference on System Sciences*.
- Akoury, N., Salz, R., & Iyyer, M. (٢٠٢٣). Towards Grounded Dialogue Generation in Video Game Environments.
- Al Batayneh, R. M., Taleb, N., Said, R. A., Alshurideh, M. T., Ghazal, T. M., & Alzoubi, H. M. (٢٠٢١, May). IT governance framework and smart services integration for future development of Dubai infrastructure utilizing AI and big data, its reflection on the citizens standard of living. In *The international conference on artificial intelligence and computer vision* (pp. ٢٣٥-٢٤٧). Cham: Springer International Publishing.
- Alam, M. K. (٢٠٢١). A systematic qualitative case study: questions, data collection, NVivo analysis and saturation. *Qualitative Research in Organizations and Management: An International Journal*, ١٦(١), ١-٣١.

- Ali, M. A., & ALQARAGHULI, A. (٢٠٢٣). A Survey on the Significance of Artificial intelligence (AI) in Network cybersecurity. *Babylonian Journal of Networking*, ٢٠٢٣, ٢١-٢٩.
- Ali, O. M. S. H. (٢٠١٦). The perceived benefits of cloud computing technology for regional municipal governments and barriers to adoption (Doctoral dissertation, University of Southern Queensland).
- Allen, Greg, and Taniel Chan. Artificial intelligence and national security. Cambridge, MA: Belfer Center for Science and International Affairs, ٢٠١٧.
- Alliance, B. B. E., & Bureau, C. C. F. P. FPAO third-party assessment organization under the FedRAMP requirements programme API application programming interface AWS Amazon Web Services BCRs Binding Corporate Rules.
- Alshammari, R. F. N., Arshad, H., Abd Rahman, A. H., & Albahri, O. S. (٢٠٢٢). Robotics utilisation in automatic vision-based assessment systems from artificial intelligence perspective: A systematic review. *IEEE Access*.
- Alsheibani, S., Messom, C., & Cheung, Y. (٢٠٢٠). Re-thinking the competitive landscape of artificial intelligence.
- Alves-Oliveira, P., Sequeira, P., Melo, F. S., Castellano, G., & Paiva, A. (٢٠١٩). Empathic robot for group learning: A field study. *ACM Transactions on Human-Robot Interaction (THRI)*, ٨(١), ١-٣٤.
- Amato, G., Behrmann, M., Bimbot, F., Caramiaux, B., Falchi, F., Garcia, A.,... & Vincent, E. (٢٠١٩).
 - AI in the media and creative industries. *arXiv preprint arXiv:١٩٠٥.٠٤١٧٥*.
- Amjad, B., Zeeshan, M., & Beg, M. O. (٢٠٢٣). EMP-EVAL: A Framework for Measuring Empathy in Open Domain Dialogues. *arXiv preprint arXiv:٢٣٠١.١٢٥١٠*.
- Anand, A., & Kumar, A. THE RISE OF ARTIFICIAL INTELLIGENCE IN VIDEO GAMES.

- Anderson, J. B. (٢٠٢١). Inadequacy of Risk Acceptance Criteria for Cloud Services Adoption: A Qualitative Generic Study (Doctoral dissertation, Capella University).
- Anoir, L., Khaldi, M., & Erradi, M. (٢٠٢٢). Personalization in Adaptive E-Learning. In *Designing User Interfaces With a Data Science Approach* (pp. ٤٠-٦٧). IGI Global.
- Ante, C., & Ante, C. (٢٠١٦). Comparison and Conclusion. *The Europeanisation of Vocational Education and Training*, ١٩٣-٢٢٩.
- Ash, E., & Hansen, S. (٢٠٢٢). *Text Algorithms in Economics*.
- Audibert, R. B. (٢٠٢٢). On the evolution of AI and machine learning: analyses of impact, leadership and influence over the last decades.
- Audibert, R. B., Lemos, H., Avelar, P., Tavares, A. R., & Lamb, L. C. (٢٠٢٢). On the Evolution of AI and Machine Learning: Towards Measuring and Understanding Impact, Influence, and Leadership at Premier AI Conferences. arXiv preprint arXiv:٢٢٠٥.١٣١٣١.
- Axelsson, M., Spitale, M., & Gunes, H. (٢٠٢٢). Robots as mental well-being coaches: Design and ethical recommendations. arXiv preprint arXiv:٢٢٠٨.١٤٨٧٤.
- Azah, A. S. A. (٢٠٢١). Manpower, AI, robot, Re-imagining the Workforce. Bachner, J. (٢٠٢٢). Optimizing analytics for policymaking and governance.
- Baiheng, L., & Wen, Z. (٢٠٢٠, December). Rethinking of Artificial Intelligence Storytelling of Digital Media. In ٢٠٢٠ International Conference on Innovation Design and Digital Technology (ICIDDT) (pp. ١١٢-١١٥). IEEE.
- Baraka, K., Alves-Oliveira, P., & Ribeiro, T. (٢٠٢٠). An extended framework for characterizing social robots. *Human-Robot Interaction: Evaluation Methods and Their Standardization*, ٢١-٦٤.
- Barros, A. P., & Dumas, M. (٢٠٠٦). The rise of web service ecosystems. *IT professional*, ٨(٥), ٣١-٣٧.
- Barta, G., & Göröcsi, G. (٢٠٢١). Risk management considerations for artificial intelligence business applications. *International Journal of Economics and Business Research*, ٢١(١), ٨٧-١٠٦.

- Basting, E. J., Munshi, I., Harangozo, J., Dongarra, M. S., & Goncy, E. A. (۲۰۲۳). When does technology use within dating relationships cross the line? A thematic analysis of semistructured interviews with young adults. *Psychology of Violence*.
- Batarseh, F. A., & Yang, R. (Eds.). (۲۰۱۷). *Federal data science: Transforming government and agricultural policy using artificial intelligence*. Academic Press.
- Belgodere, B., Dognin, P., Ivankay, A., Melnyk, I., Mroueh, Y., Mojsilovic, A.,... & Young, R. A. (۲۰۲۳). Auditing and Generating Synthetic Data with Controllable Trust Trade-offs. *arXiv preprint arXiv:۲۳.۰۴.۱۰۸۱۹*.
- Bettoni, Andrea, Davide Matteri, Elias Montini, Bartłomiej Gładysz, and Emanuele Carpanzano. "An AI adoption model for SMEs: A conceptual framework." *IFAC-PapersOnLine* ۵۴, no. ۱ (۲۰۲۱): ۷۰۲-۷۰۸.
- Bhushan, S. B., Reddy, P., Subramanian, D. V., & Gao, X. Z. (۲۰۱۸). Systematic survey on evolution of cloud architectures. *International Journal of Autonomous and Adaptive Communications Systems*, ۱۱(۱), ۱۴-۳۸.
- Biermann, O. C., Ma, N. F., & Yoon, D. (۲۰۲۲, June). From tool to companion: Storywriters want AI writers to respect their personal values and writing strategies. In *Designing Interactive Systems Conference* (pp. ۱۲۰۹-۱۲۲۷).
- Biersmith, L., & Laplante, P. (۲۰۲۲, October). Introduction to AI Assurance for Policy Makers. In ۲۰۲۲ IEEE ۲۹th Annual Software Technology Conference (STC) (pp. ۵۱-۵۶). IEEE.
- Blanchard, A., & Taddeo, M. (۲۰۲۳). The Ethics of Artificial Intelligence for Intelligence Analysis: a Review of the Key Challenges with Recommendations. *Digital Society*, ۲(۱), ۱-۲۸.
- Blau, J. (۲۰۲۰). Europe's great digital gap. *Research-Technology Management*, ۶۳(۲), ۳-۶.
<https://www.questia.com/library/journal/۱G۱-۶۱۶۰۴۷۳۹۳/europe-s-great-digital-gap>

- Bodemer, O. (۲۰۲۳). Artificial Intelligence in Governance: A Comprehensive Analysis of AI Integration and Policy Development in the German Government. Authorea Preprints.
- Boukhari, M. (۲۰۲۱). The Impact of Artificial Intelligence on the B۲B Sales Funnel.
-
- Bouma, D., Canbaloglu, G., Treur, J., & Wiewiora, A. (۲۰۲۳). Adaptive network modeling of the influence of leadership and communication on learning within an organization. *Cognitive Systems Research*, ۷۹, ۵۵-۷۰.
- Braga, J., Regateiro, F., Stiubiener, I., & Braga, J. C. (۲۰۲۲). A proposal to improve research in AI algorithm and data governance. OSF Preprints. September, ۱۵.
- Braun, V., & Clarke, V. (۲۰۰۶). Using thematic analysis in psychology. *Qualitative research in psychology*, ۳(۲), ۷۷-۱۰۱.
- Breit, A., Waltersdorfer, L., Ekaputra, F. J., Sabou, M., Ekelhart, A., Ia...A., ... & van Harmelen, F. (۲۰۲۳). Combining machine learning and semantic web: A systematic mapping study. *ACM Computing Surveys*.
- Bringsjord, S., & Ferrucci, D. (۱۹۹۹). Artificial intelligence and literary creativity: Inside the mind of brutus, a storytelling machine. Psychology Press.
- Bruno, F., Cardoso, P., & Faltay, P. The National Employment System.
-
- Burtell, M., & Woodside, T. (۲۰۲۳). Artificial influence: An analysis of AI-driven persuasion. arXiv preprint arXiv:۲۳۰۳.۰۸۷۲۱.
- Calo, R. (۲۰۱۸). Artificial intelligence policy: A primer and roadmap. *U. Bologna L. Rev.*, ۳, ۱۸۰. Carenini, G., & Duplessis, A. Investigating the Intuitive Logic behind Autoregressive Language Models.
- Carney, W. T. (۲۰۱۹). A Case Study of the United States Air Force Adoption of Cloud Computing (Doctoral dissertation, Robert Morris University).

واژه نامه

واژگان انگلیسی به فارسی :

هوش مصنوعی	Artificial Intelligence
رایانش ابری	Cloud Computing
حریم خصوصی	Privacy
یادگیری ماشین	Machine Learning
امنیت داده‌ها	Data Security
نوآوری	Innovation
رهبری	Leadership
تصمیم‌گیری	Decision-Making
تحلیل داده‌ها	Data Analysis
چالش‌ها	Challenges
فرصت‌ها	Opportunities
مجوز	Authorization
قانون‌گذاری	Legislation
ارزیابی	Evaluation
زیرساخت	Infrastructure
آموزش	Training
مقررات	Regulations
توسعه	Development
بهره‌وری	Efficiency
امنیت سایبری	Cybersecurity
شفافیت	Transparency
شبکه	Network
سیستم	System
نظارت	Supervision
سیاست‌گذاری	Policy-Making
محیط سازمانی	Organizational Environment
تحلیل محتوا	Content Analysis
پژوهش	Research
اخلاقیات	Ethics
همکاری	Collaboration

واژگان فارسی به انگلیسی

Artificial Intelligence	هوش مصنوعی
Machine Learning	یادگیری ماشین
Cloud Computing	رایانش ابری
Privacy	حریم خصوصی
Data Security	امنیت داده‌ها
Innovation	نوآوری
Language Model	مدل زبانی
Decision-Making	تصمیم‌گیری
Leadership	رهبری
Data Analysis	تحلیل داده‌ها
Infrastructure	زیرساخت
Challenges	چالش‌ها
Opportunities	فرصت‌ها
Legislation	قانون‌گذاری
Authorization	مجوز
Evaluation	ارزیابی
Organizational Environment	محیط سازمانی
Information Technology	فناوری اطلاعات
Research	پژوهش
Training	آموزش
Regulations	مقررات
Supervision	نظارت
Development	توسعه
Efficiency	بهره‌وری
Cybersecurity	امنیت سایبری
Content Analysis	تحلیل محتوا
Network	شبکه
System	سیستم
Transparency	شفافیت
Policy-Making	سیاست‌گذاری

Abstract

Abstract This dissertation examines challenges and opportunities in federal government Conversational AI and Machine Learning (CAIML) integration. It emphasizes Conversational AI (CAI)'s impact on decision-making across sectors and its improvement of human-technology interactions, particularly in IoT and cloud computing. The study reviews AI storytelling, including NLP, character generation, VR/AR, deep learning, leadership, and FedRAMP compliance. Qualitative research follows PRISMA and uses NVivo for data analysis. A comprehensive literature review, qualitative analysis, and expert interviews reveal CAIML adoption challenges and opportunities. Leadership, economic and legal factors, privacy, data protection, and national security are studied. The dissertation concludes with a summary of its findings and research questions on federal agency CAI and ML adoption barriers, operational improvements, legal/regulatory issues, privacy, data protection, security threats, and effective leadership strategies. CAI and ML integration into federal infrastructure and national security and intelligence implications are also discussed. The dissertation recommends federal agencies prioritize personnel training, migration planning, and solution sustainability to advance CAIML adoption. It helps federal policymakers and practitioners adopt CAIML technologies by highlighting their transformative potential and challenges.

Keywords: CAIML Integration, Federal Government, Cloud Computing, Data Privacy and Protection, Leadership Practices.



Payam Noor University

Faculty of Engineering

Seminar Report

Department of Computer Engineering and Information Technology

The Technology Adoption Model for Cloud Computing, Storytelling Artificial Intelligence, and the Federal Risk and Authorization Management Program

Reza Azadmehr

Supervisor:

Dr. Alirreza Razavi

Jan ۲۰۲۰