نقش هوش مصنوعی در افزایش امنیت تجارت الکترونیک

حسین الیاسی ورگ[1]

اکرم الیاسی ورگ[2]

چکیده

همانطور که تجارت الکترونیک همچنان در حال گسترش است، اهمیت اقدامات امنیتی قوی برای محافظت از تراکنش های دیجیتال و حفظ اعتماد مشتری هرگز به این اندازه حیاتی نبوده است. این مقاله به بررسی نقش چندوجهی هوش مصنوعی (AI) در افزایش امنیت تجارت الکترونیک، پرداختن به تهدیدات رایج امنیت سایبری مانند فیشینگ، نقض داده‌ها و تقلب در پرداخت می‌پردازد. پلتفرم‌های تجارت الکترونیک با استفاده از فناوری‌های هوش مصنوعی، از جمله یادگیری ماشینی و پردازش زبان طبیعی، می‌توانند تشخیص تقلب، احراز هویت مشتری و حفاظت از داده‌ها را بهبود بخشند. ادغام هوش مصنوعی نه تنها عملیات را ساده می کند، بلکه یک محیط خرید آنلاین امن تر را نیز تقویت می کند. این مقاله چالش‌ها و محدودیت‌های فعلی هوش مصنوعی در امنیت تجارت الکترونیک را مورد بحث قرار می‌دهد، در حالی که روندها و نوآوری‌های آینده را برجسته می‌کند که نویدبخش افزایش بیشتر چشم‌انداز امنیتی است.

واژگان کلیدی: امنیت تجارت الکترونیک،هوش مصنوعی،تشخیص تقلب،حفاظت از داده ها، تهدیدات امنیت سایبری

مقدمه

امنیت تجارت الکترونیک برای محافظت از تراکنش های دیجیتال و حفظ اعتماد مشتری بسیار مهم است. این شامل حفاظت از داده ها، احراز هویت و محافظت در برابر دسترسی غیرمجاز است(Khan, ۲۰۱۹; Yasin, Haseeb, & Qureshi, ۲۰۱۲). ابعاد کلیدی امنیت تجارت الکترونیک شامل یکپارچگی، عدم انکار، اصالت، محرمانه بودن، حریم خصوصی و در دسترس بودن است.(SangeethaM & Suchitra, ۲۰۱۸). تکنیک‌های رمزنگاری مختلف، مانند زیرساخت کلید عمومی و امضای دیجیتال، برای افزایش امنیت استفاده می‌شوند(Yasin et al., ۲۰۱۲). با وجود فرصت‌هایی که تجارت الکترونیک ارائه می‌کند، خطرات جدیدی مانند کلاهبرداری سایبری و سرقت هویت را نیز به همراه دارد.(Khan, ۲۰۱۹). امنیت ضعیف در سرورهای تجارت الکترونیک و دستگاه‌های کاربر همچنان یک مانع مهم برای رشد است(Khan, ۲۰۱۹). برای مقابله با این چالش‌ها، کسب‌وکارها باید اقدامات امنیتی جامعی را اجرا کنند و دستورالعمل‌هایی را برای خرید آنلاین امن دنبال کنند(SangeethaM & Suchitra, ۲۰۱۸). همانطور که تجارت الکترونیک به تکامل خود ادامه می دهد، حفظ شیوه های امنیتی قوی برای تقویت اعتماد مشتری و تسهیل تراکنش های دیجیتال ایمن ضروری است.(Khan, ۲۰۱۹).

هوش مصنوعی (AI) با افزایش تجربیات مشتری، ساده‌سازی عملیات و افزایش درآمد، تجارت الکترونیک را متحول می‌کند.(Gaikwad, Ingale, Divekar, Changede, & Bhuwad, ۲۰۲٤). کاربردهای هوش مصنوعی در تجارت الکترونیک شامل تجربه خرید شخصی، پشتیبانی هوشمند از مشتری، و جستجو و کشف محصول بهبود یافته است.(Gaikwad et al., ۲۰۲٤). یادگیری ماشینی، زیرمجموعه‌ای از هوش مصنوعی، شرکت‌های تجارت الکترونیک را قادر می‌سازد تا داده‌های مشتری را تجزیه و تحلیل کنند و بینش‌هایی را ارائه دهند که تجارب مشتری را بهبود می‌بخشد و با تقلب مبارزه می‌کند.(Lari, Vaishnava, & Manu, ۲۰۲۲). راه‌حل‌های تجارت الکترونیک مبتنی بر هوش مصنوعی از روش‌های سنتی بهتر عمل می‌کنند و استفاده از هوش مصنوعی را برای حفظ رقابت بسیار مهم می‌سازند.(Śliwiński, ۲۰۲۱). پلتفرم های بزرگ تجارت الکترونیک مانند آمازون و فلیپ کارت، رویکردهای هوش مصنوعی مانند تجزیه و تحلیل داده ها، یادگیری عمیق و تشخیص الگو را برای درک بهتر ترجیحات مشتری پیاده سازی می کنند.(Saleem & Naseem, ۲۰۲۳). در حالی که هوش مصنوعی مزایای قابل توجهی را ارائه می دهد، چالش هایی را نیز به همراه دارد که باید به آنها توجه شود(Saleem & Naseem, ۲۰۲۳). همانطور که هوش مصنوعی به پیشرفت خود ادامه می دهد، شرکت های تجارت الکترونیک سرمایه گذاری های خود را در این فناوری افزایش می دهند تا رشد کسب و کار را هدایت کنند(Lari et al., ۲۰۲۲).

هدف این مطالعه بررسی نقش تحول آفرین هوش مصنوعی در افزایش امنیت تجارت الکترونیک، رسیدگی به تهدیدات فعلی و پیشنهاد نوآوری های آینده است.

۲. درک تهدیدات امنیتی تجارت الکترونیک

۲.۱. تهدیدات رایج امنیت سایبری در تجارت الکترونیک

پلتفرم‌های تجارت الکترونیک با تهدیدات امنیت سایبری متعددی مواجه هستند که از جمله نگرانی‌های مهم حملات فیشینگ، نقض داده‌ها و تقلب در پرداخت هستند.(R. Gupta, ۲۰۲٤).

حملات فیشینگ تهدید قابل توجهی برای امنیت تجارت الکترونیک است و از آسیب پذیری های کاربران برای سرقت اطلاعات حساس سوء استفاده می کند.(Dadkhah et al., ۲۰۱٦). این حملات اغلب شامل وب‌سایت‌ها یا ایمیل‌های جعلی هستند که منابع قانونی را تقلید می‌کنند و اعتماد بین کاربران و کسب‌وکارهای آنلاین را تضعیف می‌کنند.(Megaw & Flowerday, ۲۰۱۰). عواملی که در حساسیت به فیشینگ نقش دارند عبارتند از فقدان دانش کاربر، دستکاری روانی و نگرانی های مربوط به حریم خصوصی در شبکه های اجتماعی.(Ramadhan & Nurnawati, ۲۰۲۲). برای مبارزه با فیشینگ، استراتژی های پیشگیری مختلفی مانند آموزش کاربر، نرم افزار ضد فیشینگ و احراز هویت چند عاملی پیشنهاد شده است.(Ramadhan & Nurnawati, ۲۰۲۲). علاوه بر این، راه‌حل‌های مبتنی بر سخت‌افزار پیشرفته مانند ماژول پلتفرم مورد اعتماد (TPM) می‌توانند با اتصال اعتبار کاربر به دستگاه‌های خاص، احراز هویت را افزایش دهند و حملات فیشینگ را ناکارآمد نشان دهند.(Latze, ۲۰۰۷). اجرای این اقدامات، همراه با عوامل حیاتی موفقیت مانند تأیید هویت کاربر و وب سایت، تأیید ایمیل و رمزگذاری داده ها، می تواند امنیت تجارت الکترونیک را به طور قابل توجهی بهبود بخشد و اعتماد کاربران را بازگرداند.(Megaw & Flowerday, ۲۰۱۰).

نقض داده ها در تجارت الکترونیک به یک نگرانی مهم تبدیل شده است که هم بر مشاغل و هم بر مصرف کنندگان تأثیر می گذارد. در حالی که نقض داده های وجودی در سطح بالا بر رشد تجارت الکترونیک تأثیر منفی می گذارد، سایر انواع نقض همبستگی مثبتی با گسترش صنعت نشان می دهند.(Dalmadge, ۲۰۱۹). پلتفرم‌های تجارت الکترونیک با تهدیدات مختلف امنیت سایبری از جمله نقض اطلاعات، حملات فیشینگ و باج‌افزار مواجه هستند.(Zade et al., ۲۰۲٤). زمان بندی اعلامیه های نقض بسیار مهم است، زیرا افشای تاخیری منجر به کاهش بیشتر اعتماد مصرف کننده در مقایسه با اعلان های فوری می شود.(Muzatko & Bansal, ۲۰۱۸). تفاوت سنی نقش مهمی در قصد خرید آنلاین پس از نقض بازی دارد، به طوری که افراد مسن بیشتر تحت تأثیر درک شدت نقض و باورهای اعتماد در خدمات تجارت الکترونیک هستند.(Chakraborty, Lee, Bagchi-Sen, Upadhyaya, & Rao, ۲۰۱٦). برای کاهش خطرات، کسب‌وکارهای تجارت الکترونیک باید استانداردهای امنیتی قوی، تاکتیک‌های نظارت مستمر و اقدامات پیشگیرانه را اجرا کنند.(Zade et al., ۲۰۲۴). علاوه بر این، شرکت ها باید برنامه های جامعی را برای اطلاع رسانی به مشتریان در مورد تخلفات و اقدامات پیشنهادی کاهش برای افزایش اعتماد و کاهش ریسک های درک شده آماده کنند.(Chakraborty et al., ۲۰۱٦).

رشد تجارت الکترونیک منجر به افزایش تقلب در پرداخت و در نتیجه زیان مالی قابل توجهی شده است(Fernandes, ۲۰۱۳). تکنیک های مختلفی برای شناسایی و جلوگیری از فعالیت های متقلبانه در تراکنش های الکترونیکی ایجاد شده است. روش‌های مبتنی بر امضا، انحرافات رفتار کاربر را با مقایسه فعالیت‌های اخیر با الگوهای تثبیت‌شده تحلیل

می‌کنند(Belo, Mota, & Fernandes, ۲۰۱٦). الگوریتم‌های یادگیری ماشین، مانند Random Forest، K-nearest و Isolated Forest، برای شناسایی ناهنجاری‌ها در داده‌های تجارت الکترونیکی استفاده شده‌اند.(Raghava-Raju, ۲۰۱۷). تکنیک‌های هوش محاسباتی، از جمله داده‌کاوی و یادگیری ماشین، نتایج امیدوارکننده‌ای را در کشف تقلب نشان داده‌اند، با سودهای گزارش‌شده تا ۴۳ درصد در معیارهای اقتصادی.(Caldeira, Brandao, & Pereira, ۲۰۱٤). هدف این رویکردها به حداقل رساندن از دست دادن درآمد و افزایش امنیت سیستم های پرداخت الکترونیکی است. از آنجایی که کلاهبرداران تکنیک های پیچیده تری را توسعه می دهند، تحقیقات مداوم و اجرای اقدامات تشخیص و پیشگیری از تقلب برای حفظ یکپارچگی تجارت الکترونیک بسیار مهم است.(Fernandes, ۲۰۱۳).

این تهدیدها به طور فزاینده ای پیچیده می شوند و اغلب از هوش مصنوعی استفاده می کنند و از آسیب پذیری های اینترنت اشیا سوء استفاده می کنند.(R. Gupta, ۲۰۲٤). برای کاهش این خطرات، کسب‌وکارها باید اقدامات فنی مانند رمزگذاری و درگاه‌های پرداخت امن را در کنار شیوه‌های سازمانی مانند آموزش کارکنان و برنامه‌ریزی واکنش به حادثه اجرا کنند.(Zade et al., ۲۰۲٤). رعایت مقرراتی مانند GDPR و CCPA بسیار مهم است(R. Gupta, ۲۰۲٤). فناوری های نوظهور، از جمله احراز هویت بیومتریک و رمزنگاری پس کوانتومی، راه حل های امیدوارکننده ای را برای افزایش امنیت تجارت الکترونیک ارائه می دهند.(Oguta, ۲۰۲٤). تلاقی فناوری، مقررات و آگاهی کاربر در ایجاد یک محیط خرید آنلاین امن بسیار مهم است(Oguta, ۲۰۲٤). نظارت مستمر و استراتژی های پیشگیرانه برای پیشگیری و مدیریت حملات سایبری در بخش تجارت الکترونیک ضروری است.(ANDREIANU, ۲۰۲۳).

۲.۲. تأثیر نقض امنیت بر مشاغل و مصرف کنندگان

نقض امنیت سایبری تأثیرات قابل توجهی بر مشاغل و مصرف کنندگان دارد. شرکت‌های بزرگ با زیان‌های مالی، اختلالات عملیاتی، آسیب‌های اعتباری و چالش‌های قانونی ناشی از انواع نقض مواجه هستند.(Sharma). ارزش بازار شرکت‌ها می‌تواند تقریباً ۱٪ پس از اعلام تخلف کاهش یابد(Goel & Shawky, ۲۰۰۹). همانطور که در یک مطالعه موردی نشان داده شده است، نقض امنیت منجر به هزینه های مستقیم و غیر مستقیم می شود(Wang, D'Cruze, & Wood, ۲۰۱۹). در حالی که نقض حریم خصوصی برای ایجاد اعتماد بسیار مهم است، نقض امنیتی تأثیر قابل توجهی بر رفتار مصرف کننده دارد و "پارادوکس حریم خصوصی" را برجسته می کند.(Nofer, Hinz, Muntermann, & Roßnagel, ۲۰۱٤). پیچیدگی فزاینده تهدیدات سایبری، ناشی از فناوری‌های نوظهور، بر نیاز به استراتژی‌های امنیت سایبری فعال و سازگاری مداوم تأکید می‌کند.(Sharma). برای محافظت از دارایی ها، حفظ اعتماد مصرف کننده و اطمینان از انعطاف پذیری طولانی مدت، کسب و کارها باید در اقدامات امنیتی سایبری قوی در دنیای دیجیتالی فزاینده سرمایه گذاری کنند.(Sharma).

۳. هوش مصنوعی چگونه امنیت تجارت الکترونیک را متحول می کند

۳.۱. فناوری های هوش مصنوعی در حال استفاده

هوش مصنوعی (AI) انقلابی در امنیت و عملیات تجارت الکترونیک ایجاد کرده است. فناوری‌های هوش مصنوعی، به‌ویژه یادگیری ماشینی (ML) و یادگیری عمیق (DL)، برای تقویت جنبه‌های مختلف خرده‌فروشی آنلاین استفاده می‌شوند. اینها شامل بهبود تجربه مشتری از طریق توصیه های شخصی و چت بات ها، بهینه سازی مدیریت موجودی و ساده سازی سیستم های پرداخت می شود.(Halachev, ۲۰۲٤; Mimani, Ramakrishnan, Rohella, Jiwani, & Logeshwaran, ۲۰۲٤). توانایی هوش مصنوعی در تجزیه و تحلیل حجم وسیعی از داده‌ها، پلتفرم‌های تجارت الکترونیک را قادر می‌سازد رفتار و ترجیحات مشتری را بهتر درک کنند و به استراتژی‌های بازاریابی مؤثرتری منجر شوند.(Saleem & Naseem, ۲۰۲۳). علاوه بر این، هوش مصنوعی با افزایش مکانیسم‌های تشخیص تقلب، نقش مهمی در تقویت امنیت تجارت الکترونیک ایفا می‌کند.(Halachev, ۲۰۲٤). علیرغم مزایای بی شماری که دارد، پیاده سازی هوش مصنوعی در تجارت الکترونیک چالش هایی را نیز به همراه دارد که باید به آن توجه شود.(Saleem & Naseem, ۲۰۲۳). به طور کلی، هوش مصنوعی تجارت الکترونیک را به صنعتی کارآمدتر، ایمن و مشتری محور تبدیل می کند(Halachev, ۲۰۲٤).

۳.۲. یادگیری ماشینی

یادگیری ماشینی (ML) امنیت و عملیات تجارت الکترونیک را متحول می کند. تکنیک‌های ML مانند یادگیری تحت نظارت و بدون نظارت، یادگیری تقویتی، و پردازش زبان طبیعی برای بهبود پیش‌بینی رفتار مشتری، تشخیص تقلب، استراتژی‌های قیمت‌گذاری و سیستم‌های توصیه استفاده می‌شوند.(FATUNMBI, ۲۰۲۲). الگوریتم‌های خاص ML مانند درخت‌های تصمیم، جنگل‌های تصادفی و شبکه‌های عصبی در تشخیص تقلب برای معاملات تجارت الکترونیک امیدوارکننده هستند.(Rajkumar et al., ۲۰۲٤). ML همچنین جنبه های مختلف تجارت الکترونیکی، از جمله تجزیه و تحلیل رفتار مصرف کننده، پیش بینی خرید، شخصی سازی و مدیریت موجودی را بهبود می بخشد.(Al-Ebrahim, Bunian, & Nour, ۲۰۲۳). ادغام ML با فناوری وب و ارتباطات سیار منجر به ایجاد بسترهای مالی امن تر و کاربر پسند تر برای تراکنش های آنلاین شده است.(Rath, ۲۰۲۰). با این حال، چالش‌هایی در پیاده‌سازی ML برای تجارت الکترونیک، از جمله امنیت داده‌ها، شفافیت مدل، و یادگیری بی‌درنگ وجود دارد.(FATUNMBI, ۲۰۲۲). توسعه مستمر در این زمینه‌ها برای حفظ رشد و امنیت در محیط‌های تجارت الکترونیک دیجیتالی بسیار مهم است.

۳.۳. پردازش زبان طبیعی

پردازش زبان طبیعی (NLP) نقش مهمی در تجارت الکترونیک ایفا می‌کند و برنامه‌های کاربردی مختلفی مانند جستجوی محصول، سیستم‌های توصیه‌کننده، پاسخ‌گویی به سؤال و تحلیل احساسات را تقویت می‌کند.(Malmasi, Agichtein, Ueffing, Guy, & Rokhlenko, ۲۰۱۹). مجموعه کارگاه های آموزشی ECNLP محققان دانشگاه و صنعت را گرد هم می آورد تا همکاری و اشتراک دانش در این زمینه را تقویت کند.(Malmasi et al., ۲۰۱۹). تحقیقات اخیر پتانسیل تجزیه و تحلیل احساسات و NLP را در افزایش تجربه مشتری و بهبود عملکرد تجارت الکترونیک نشان داده است. با تجزیه و تحلیل نظرات مشتریان و استفاده از تکنیک های NLP، کسب و کارها می توانند فروش را تا ۱۵.۴ درصد افزایش دهند،

سود را تا ۱۵ درصد افزایش دهند و توصیه های مثبت را تا ۱ درصد بهبود بخشند.(**Ismail, Ghareeb, & Youssry**). ادغام **NLP** و تجارت الکترونیک به تکامل خود ادامه می دهد و چت بات ها و دستیاران خرید به عنوان فناوری های تحول آفرین در این بخش ظاهر می شوند.(**Ueffing, Rokhlenko, & Goyal, ۲۰۱۹**). همانطور که روش‌های **NLP** پیشرفت می‌کنند، فرصت‌های امیدوارکننده‌ای را برای بهبود نتایج جستجو، ارائه توصیه‌های شخصی‌سازی شده و تقویت دستیاران مجازی در پلتفرم‌های تجارت الکترونیک ارائه می‌کنند.(**Malmasi et al., ۲۰۱۹**).

۳.۴. مزایای هوش مصنوعی در سیستم های امنیتی

هوش مصنوعی (**AI**) به یک نیروی متحول کننده در تجارت الکترونیک تبدیل شده است و مزایای متعددی را در جنبه های مختلف خرده فروشی آنلاین ارائه می دهد. هوش مصنوعی تجربه مشتری را از طریق چت بات‌های هوشمند، عملکردهای جستجوی خودکار و توصیه‌های شخصی‌شده محصول افزایش می‌دهد.(**Mimani et al., ۲۰۲٤**). همچنین با بهینه‌سازی مدیریت موجودی و ساده‌سازی فرآیندهای داخلی کسب‌وکار، کارایی عملیاتی را بهبود می‌بخشد(**Mimani et al., ۲۰۲۴**). در حوزه امنیت، هوش مصنوعی نقش مهمی در تقویت سیستم های پرداخت، کاهش خطرات امنیتی و مبارزه با کلاهبرداری دارد.(**Mimani et al., ۲۰۲٤**). شرکت های تجارت الکترونیک به طور فزاینده ای روی فناوری های هوش مصنوعی سرمایه گذاری می کنند تا به مزیت های رقابتی دست یابند و رشد فروش را افزایش دهند(**Lari et al., ۲۰۲۲**). توانایی هوش مصنوعی در تجزیه و تحلیل حجم زیادی از داده‌ها، کسب‌وکارها را قادر می‌سازد تا تصمیمات مبتنی بر داده‌ها را اتخاذ کنند و تجربیات سفارشی‌سازی شده را برای مشتریان فراهم کنند.(**Shyna & Vishal, ۲۰۱۷**). همانطور که هوش مصنوعی به تکامل خود ادامه می دهد، انتظار می رود که چشم انداز تجارت الکترونیک را بیشتر متحول کند.

۴. شناسایی پیشگیرانه تهدید

۴.۱. سیستم های تشخیص ناهنجاری

سیستم‌های تشخیص ناهنجاری نقش مهمی در تشخیص تهدید فعال برای امنیت تجارت الکترونیک دارند. این سیستم ها ترافیک شبکه و الگوهای تراکنش را برای شناسایی نفوذهای احتمالی و فعالیت های تقلبی تجزیه و تحلیل می کنند(**Massa & Valverde, ۲۰۱٤**). با استفاده از مدل‌های آماری و طبقه‌بندی‌کننده‌های چند متغیره، روش‌های تشخیص ناهنجاری می‌توانند به طور قابل اعتماد حملاتی را با شدت ناهنجاری ترافیکی کمتر از ۳ تا ۵ درصد از ترافیک پس‌زمینه معمولی شناسایی کنند.(**Manikopoulos & Papavassiliou, ۲۰۰۲**). سیستم‌های پیشرفته از داده‌های سری زمانی برای ردیابی و خوشه‌بندی اجزای سیستم مشابه استفاده می‌کنند و امکان شناسایی و گزارش سریع ناهنجاری‌ها را در پلتفرم‌های تجارت الکترونیک در مقیاس بزرگ فراهم می‌کنند.(**İşlek, Aksaylı, & Karamatlı, ۲۰۲۰**). علاوه بر این، الگوریتم‌های تطبیقی برای افزایش تشخیص پیشگیرانه خرابی‌های شبکه و کاهش عملکرد در شبکه‌های تجارت الکترونیک مبتنی بر تراکنش چند سرویس توسعه داده شده‌اند. این الگوریتم‌ها از سوابق تراکنش خام نمونه‌برداری

می‌کنند، آستانه‌های عملکرد تطبیقی ایجاد می‌کنند، و با در نظر گرفتن وابستگی متقابل و همبستگی بین کلاس‌های خدمات مختلف، تشخیص ناهنجاری را در زمان واقعی انجام می‌دهند.(Ho & Papavassiliou, ۲۰۰۰).

۴.۲. تجزیه و تحلیل رفتار

تحقیقات اخیر اهمیت تجزیه و تحلیل رفتاری در افزایش امنیت سایبری، به ویژه در تجارت الکترونیک را برجسته می کند. با تجزیه و تحلیل الگوهای رفتار کاربر، فعالیت شبکه و تعاملات سیستمی، سازمان ها می توانند ناهنجاری هایی را که نشان دهنده تهدیدات بالقوه است، شناسایی کنند.(Ofoegbu, Osundare, Ike, Fakeyede, & Ige, ۲۰۲٤). این رویکرد پیشگیرانه امکان پیش بینی و پیشگیری از حملات را قبل از بروز کامل آنها فراهم می کند. مطالعات نشان داده اند که استفاده از مجموعه داده های بزرگ و تکنیک های تحلیلی پیشرفته می تواند به طور قابل توجهی دقت تشخیص تهدید را بهبود بخشد و در عین حال موارد مثبت کاذب را به حداقل برساند.(Zhao et al., ۲۰۱٦). تجزیه و تحلیل رفتار کاربر (UBA) به عنوان یک مؤلفه حیاتی در شناسایی رفتارهای غیرعادی ظاهر شده است که ممکن است به عوامل مخرب یا حساب های در معرض خطر نشان دهد.(Mihailescu, Nita, Rogobete, & Marascu, ۲۰۲۳). علاوه بر این، ادغام چندین منبع از گزارش‌های امنیتی و استفاده از الگوریتم‌های یادگیری ماشینی می‌تواند اثربخشی سیستم‌های تشخیص نقض را در طول زمان افزایش دهد.(Li & Oprea, ۲۰۱٦). این رویکردهای داده محور نه تنها دفاع سازمانی را تقویت می کنند، بلکه به ایجاد یک اکوسیستم سایبری ایمن تر کمک می کنند.(Ofoegbu et al., ۲۰۲٤).

۴.۳ نظارت بر زمان واقعی

تشخیص تهدید در زمان واقعی در امنیت تجارت الکترونیک برای محافظت در برابر تهدیدات سایبری در حال تکامل بسیار مهم است. پردازش جریان و الگوریتم‌های یادگیری ماشینی امکان تشخیص دقیق و به موقع حملات شناخته شده و روز صفر را فراهم می‌کنند.(Gonzalez, Lobato, Lopez, Carlos, & Duarte). یک چارچوب یکپارچه برای امنیت تجارت الکترونیک می تواند تخصیص منابع را از طریق به حداقل رساندن نظارت بر شبکه بهینه کند، در حالی که نظارت بر رویداد، تجزیه و تحلیل داده ها و ارزیابی ریسک را بدون به خطر انداختن حریم خصوصی کاربر یکپارچه می کند.(Qiu & Li, ۲۰۱۷). تشخیص الگو در جریان رویداد امکان تجزیه و تحلیل رفتار مشتری را در زمان واقعی، استفاده از زبان‌های خاص دامنه و خودکارهای محدود قطعی برای تشخیص کارآمد و مقیاس‌پذیر فراهم می‌کند.(Braik, Morandat, Falleri, & Blanc, ۲۰۱٦). برای مبارزه با کلاهبرداری کارت اعتباری، یک رویکرد جدید با استفاده از نام‌های دامنه یکبار مصرف و سرورهای DNS سفارشی می‌تواند تناقضات تراکنش‌ها را در زمان واقعی شناسایی کند، به تلاش‌های تقلب مبتنی بر پروکسی رسیدگی کند و امنیت کلی تجارت الکترونیک را افزایش دهد.(Patil, Sonkar, Patil, Deshmukh, & Patil,

۲۰۲۳). این پیشرفت‌ها در مجموع به سیستم‌های تشخیص تهدید قوی‌تر و فعال‌تر در چشم‌انداز تجارت الکترونیک کمک می‌کنند.

۵. پیشگیری و مدیریت تقلب

۵.۱. ابزارهای تشخیص تقلب با هوش مصنوعی

ابزارهای تشخیص کلاهبرداری مبتنی بر هوش مصنوعی به دلیل افزایش تراکنش های دیجیتال و کلاهبرداران پیچیده، به طور فزاینده ای برای امنیت تجارت الکترونیک حیاتی می شوند.(Hasan & Rizvi, ۲۰۲۲). این ابزارها از تجزیه و تحلیل داده ها، یادگیری ماشینی و تکنیک های یادگیری عمیق برای تجزیه و تحلیل حجم وسیعی از داده ها در زمان واقعی، شناسایی الگوهای مشکوک و جلوگیری از فعالیت های تقلبی استفاده می کنند.(Vyas, ۲۰۲۳). بررسی متون سیستماتیک نشان می‌دهد که کلاهبرداری از کارت اعتباری بیشترین نوع کلاهبرداری است که تنها چند مطالعه بر پیشگیری از کلاهبرداری متمرکز شده است.(Rodrigues et al., ۲۰۲۲). الگوریتم‌های یادگیری ماشین مانند Random Forest، Support Vector Machine و Gradient Boost برای پیش‌بینی احتمال تراکنش‌های جعلی پیاده‌سازی می‌شوند، در حالی که عدم تعادل کلاس را از طریق نمونه‌برداری بیش از حد و تکنیک‌های پیش پردازش داده‌ها برطرف می‌کنند.(Jhangiani, Bein, & Verma, ۲۰۱۹). با این حال، چالش‌هایی در پیاده‌سازی سیستم‌های تشخیص تقلب مبتنی بر هوش مصنوعی، از جمله حفظ حریم خصوصی داده‌ها، دقت مدل، و مقیاس‌پذیری همچنان وجود دارد.(Vyas, ۲۰۲۳). ادامه تحقیق و توسعه در این زمینه برای افزایش امنیت و قابل اعتماد بودن پلتفرم های تجارت الکترونیک ضروری است.

۵.۲. مطالعات موردی پیاده سازی های موفق هوش مصنوعی

تحقیقات اخیر اهمیت روزافزون هوش مصنوعی در پیشگیری از کلاهبرداری برای امنیت تجارت الکترونیک را برجسته می کند. ابزارهای مبتنی بر هوش مصنوعی که از تجزیه و تحلیل داده‌ها و تکنیک‌های یادگیری ماشین استفاده می‌کنند برای افزایش امنیت تراکنش‌ها و شناسایی فعالیت‌های متقلبانه استفاده می‌شوند.(Hasan & Rizvi, ۲۰۲۲). پیاده‌سازی‌های موفق هوش مصنوعی، مانند انبار هوشمند علی‌بابا، ارزش هماهنگی منابع هوش مصنوعی مانند داده‌ها، الگوریتم‌ها و روبات‌ها را با سیستم‌های موجود برای ایجاد قابلیت‌هایی در پیش‌بینی، برنامه‌ریزی و یادگیری نشان می‌دهد.(Zhang, Pee, & Cui, ۲۰۲۱). ادغام هوش مصنوعی، تجزیه و تحلیل داده ها و فناوری های پیشرفته مزایای قابل توجهی را در تشخیص و پیشگیری از تقلب در صنایع ارائه می دهد.(P. Gupta, ۲۰۲٤). سیستم‌های هوش مصنوعی مبتنی بر جاوا به‌ویژه در توسعه راه‌حل‌های هوشمند کشف تقلب، استفاده از یادگیری ماشین و روش‌های یادگیری عمیق برای تجزیه و تحلیل حجم وسیعی از داده‌ها در زمان واقعی و شناسایی الگوهای مشکوک مؤثر هستند.(Vyas, ۲۰۲۳). این پیشرفت ها در مبارزه با کلاهبرداران پیچیده و ایمن تراکنش های مالی در عصر دیجیتال بسیار مهم است.

۵.۳. یادگیری مستمر و سازگاری سیستم های هوش مصنوعی

تکنیک های یادگیری ماشین (ML) و هوش مصنوعی (AI) به عنوان ابزار قدرتمندی برای شناسایی و جلوگیری از تقلب در تجارت الکترونیک ظهور کرده اند.(Idemudia, Agu, & Obeng, ۲۰۲٤). این فناوری‌ها تجزیه و تحلیل بی‌درنگ حجم وسیعی از داده‌های تراکنش، شناسایی الگوهای مشکوک و ناهنجاری‌هایی را که ممکن است نشان‌دهنده فعالیت‌های متقلبانه باشد، امکان‌پذیر می‌سازد.(Reddy et al., ۲۰۲٤). سیستم‌های هوش مصنوعی مبتنی بر جاوا در توسعه برنامه‌های کاربردی تشخیص تقلب مقیاس‌پذیر و قوی نویدبخش بوده‌اند.(Vyas, ۲۰۲۳). مدل‌های مختلف ML، از جمله تکنیک‌های یادگیری تحت نظارت و بدون نظارت، و همچنین روش‌های ترکیبی و گروهی، برای کارایی آنها در تشخیص تقلب مورد ارزیابی قرار گرفته‌اند.(Idemudia et al., ۲۰۲٤). ادغام هوش مصنوعی و ML با تجزیه و تحلیل داده های بزرگ انقلابی در تلاش های پیشگیری از تقلب ایجاد کرده است و به سازمان ها این امکان را می دهد تا به طور فعال خطرات تقلب را شناسایی و کاهش دهند.(Reddy et al., ۲۰۲٤). با این حال، ملاحظات اخلاقی و مسائل مربوط به حریم خصوصی داده ها باید برای اطمینان از استفاده مسئولانه از این فناوری ها در تشخیص و پیشگیری از تقلب مورد توجه قرار گیرد.(Idemudia et al., ۲۰۲٤).

۶. تقویت احراز هویت مشتری

۶.۱. هوش مصنوعی در تأیید هویت

هوش مصنوعی با افزایش تجربه مشتری، امنیت و کارایی عملیاتی، تجارت الکترونیک را متحول می کند. کاربردهای هوش مصنوعی در تجارت الکترونیک عمدتاً بر سیستم‌های توصیه‌کننده، تحلیل احساسات، اعتماد، شخصی‌سازی و بهینه‌سازی تمرکز دارند.(Bawack, Wamba, Carillo, & Akter, ۲۰۲۲). این فناوری‌ها، از جمله یادگیری ماشین، برای درک رفتار مشتری، بهبود خدمات مشتری و مبارزه با تقلب به کار می‌روند(Lari et al., ۲۰۲۲). ابزارهای مبتنی بر هوش مصنوعی مانند توصیه‌های شخصی‌شده، چت‌بات‌ها و تجزیه و تحلیل پیش‌بینی‌کننده، تعاملات و رضایت مشتری را در پلتفرم‌های تجارت الکترونیک جهانی تغییر می‌دهند.(Sulastri, ۲۰۲۳). برای پرداختن به چالش‌های پایدار در مدیریت هویت دیجیتال و کشف تقلب، رویکرد جدیدی برای ادغام بلاک چین و هوش مصنوعی پیشنهاد شده است که از ماهیت غیرمتمرکز بلاک چین و قابلیت‌های تحلیلی هوش مصنوعی بهره می‌برد.(Paschal Kulwa, ۲۰۲٤). در حالی که پذیرش هوش مصنوعی در تجارت الکترونیک مزایای قابل توجهی را ارائه می دهد، نگرانی های اخلاقی را نیز به ویژه در مورد حفظ حریم خصوصی داده ها و شفافیت ایجاد می کند.(Sulastri, ۲۰۲۳). از آنجایی که شرکت‌های تجارت الکترونیک به طور فزاینده‌ای بر روی هوش مصنوعی سرمایه‌گذاری می‌کنند، ایجاد تعادل بین نوآوری‌های فناوری و مسئولیت اخلاقی برای رشد پایدار بسیار مهم است.

۶.۲. راه حل های احراز هویت بیومتریک

احراز هویت بیومتریک به طور فزاینده ای به عنوان یک راه حل حیاتی برای افزایش امنیت در معاملات تجارت الکترونیک شناخته می شود. مطالعات متعدد اهمیت حفاظت از حریم خصوصی مشتری و جلوگیری از سرقت هویت در پرداخت های آنلاین را برجسته می کند(Hosseini & Barkhordari, ۲۰۱۳; Mohammadi & Hosseini). روش‌های بیومتریک مختلفی پیشنهاد شده‌اند، از جمله تشخیص اثر انگشت و عنبیه، که اغلب با پروتکل‌های امنیتی موجود مانند SSL و ۳- D Secure ترکیب می‌شوند (Hosseini & Barkhordari, ۲۰۱۳). برخی از محققان به دلیل منحصر به فرد بودن، استفاده از الگوهای عنبیه رمزگذاری شده را برای احراز هویت مشتری پیشنهاد می کنند(Vangala & Sasi, ۲۰۰٤). علاوه بر این، ادغام بیومتریک با سایر تکنیک‌های امنیتی مانند watermarking، steganography و سیستم‌های رمزنگاری برای تقویت بیشتر قدرت سیستم مورد بررسی قرار گرفته است (Kumar & Sangwan, ۲۰۱٤). در حالی که احراز هویت بیومتریک مزایای متعددی را نسبت به روش‌های سنتی ارائه می‌دهد، طراحی این سیستم‌ها برای مقاومت در برابر حملات احتمالی، به ویژه در برنامه‌های کاربردی از راه دور بدون نظارت مانند محیط‌های تجارت الکترونیک بسیار مهم است (Kumar & Sangwan, ۲۰۱٤).

۶.۳. احراز هویت چند عاملی (MFA) با هوش مصنوعی بهبود یافته است

احراز هویت چند عاملی (MFA) تقویت شده توسط هوش مصنوعی به عنوان یک اقدام امنیتی حیاتی برای پلتفرم های تجارت الکترونیک در حال ظهور است. Aburbeian & Veiga چارچوبی را پیشنهاد می‌کنند که MFA را با یادگیری ماشین ترکیب می‌کند و از تشخیص چهره به عنوان یک عامل تأیید هویت اضافی استفاده می‌کند.(Aburbeian & Fernández-Veiga, ۲۰۲٤). این رویکرد به نرخ‌های دقت بالایی در طبقه‌بندی‌کننده‌های مختلف دست یافت. به طور مشابه، Nugraha و همکاران. یک فرآیند MFA سه مرحله ای برای وب سایت های تجارت الکترونیک، شامل رمز عبور، OTP و سؤالات شخصی پیاده سازی کرد.(Nugraha, Arisandi, & Perdana, ۲۰۲۱). نقش هوش مصنوعی در تجارت الکترونیک فراتر از امنیت، افزایش تجربه مشتری، قابلیت جستجو و توصیه های محصول است.(Mimani et al., ۲۰۲٤). Kakkar & Monga توانایی هوش مصنوعی برای تجزیه و تحلیل حجم زیادی از داده ها را برجسته می کند و توصیه های شخصی را بر اساس رفتار مشتری امکان پذیر می کند.(Kakkar & Monga, ۲۰۲۰). از آنجایی که کسب و کارهای تجارت الکترونیک به طور فزاینده ای از فناوری های هوش مصنوعی استفاده می کنند، ادغام MFA و AI نوید ارائه اقدامات امنیتی قوی در عین بهبود تجربه کلی کاربر و افزایش فروش را می دهد.

۷. حفاظت از داده ها و حریم خصوصی

۷.۱. هوش مصنوعی در رمزگذاری داده ها

هوش مصنوعی به طور فزاینده ای در تجارت الکترونیک ادغام می شود و تعاملات و عملیات با مشتری را افزایش می دهد(Jakkula, ۲۰۲٤). تحقیقات در مورد هوش مصنوعی در تجارت الکترونیک عمدتاً بر سیستم های توصیه کننده، تجزیه و تحلیل احساسات، اعتماد، شخصی سازی و بهینه سازی متمرکز است.(Bawack et al., ۲۰۲۲). با این حال، استفاده از هوش مصنوعی در تجارت الکترونیک نگرانی های قابل توجهی را در مورد حفظ حریم خصوصی و امنیتی ایجاد می کند. قراردادهای هوشمند، ضمن بهبود کارایی و کاهش هزینه‌ها، با آسیب‌پذیری‌های امنیتی روبرو هستند که می‌تواند کل شبکه‌های بلاک چین را به خطر بیندازد.(Gupta et al., ۲۰۲۰). برای رسیدگی به این مسائل، محققان در حال بررسی تکنیک‌های هوش مصنوعی برای محافظت از حریم خصوصی قراردادهای هوشمند هستند. علاوه بر این، فناوری بلاک چین برای ایجاد سیستم‌های توصیه‌گر حفظ حریم خصوصی با هوش مصنوعی ادغام می‌شود. به عنوان مثال، پلت فرم Private-Rec، یک محیط امن برای استفاده از داده ها در سیستم های توصیه فراهم می کند و به کاربران انگیزه هایی برای به اشتراک گذاری داده های خود ارائه می دهد.(Bosri, Rahman, Bhuiyan, & Al Omar, ۲۰۲۰). هدف این پیشرفت‌ها ایجاد تعادل بین مزایای هوش مصنوعی در تجارت الکترونیک با حفاظت از داده‌ها و اقدامات حفظ حریم خصوصی است.

۷.۲. مطابقت با مقررات (GDPR، CCPA)

مطالعات اخیر چالش های انطباق حفاظت از داده ها در تجارت الکترونیک را برجسته می کند. تجزیه و تحلیل ۳۶۰ وب سایت تجارت الکترونیک نشان داد که عدم انطباق گسترده با مقرراتی مانند GDPR و CCPA، با ۷۳٪ از کوکی های شخص ثالث به عنوان ردیاب و ۸۵٪ در برابر حملات XSS آسیب پذیر هستند.(Nivedita Singh et al., ۲۰۲٤). برای پرداختن به این مسائل، به شرکت‌های فناوری ایالات متحده توصیه می‌شود که تیم‌های متقابل ایجاد کنند، روی آموزش کارکنان سرمایه‌گذاری کنند، حریم خصوصی را با اصول طراحی اجرا کنند و فرهنگ بهبود مستمر را تقویت کنند.(Chukwurah & Aderemi, ۲۰۲٤). اهمیت اعتماد در محیط‌های تجارت الکترونیک با توصیه‌هایی برای ادغام فناوری‌های پیشرفته افزایش حریم خصوصی و رعایت استانداردهای نظارتی دقیق مورد تاکید قرار گرفته است.(Morić, Dakic, Djekic, & Regvart, ۲۰۲۴). علی‌رغم این تلاش‌ها، تخلفات همچنان ادامه دارد و نیاز به بررسی جامع انطباق وب‌سایت‌های تجارت الکترونیک با مقررات حفاظت از داده است.(Nivedita Singh et al., ۲۰۲٤). این یافته‌ها بر نیاز فوری به سیاست‌های کوکی یکسان و مکانیسم‌های اجرایی قوی برای اطمینان از حفاظت از داده‌ها در تجارت الکترونیک تأکید می‌کند.

۷.۳. نقش هوش مصنوعی در حفظ اعتماد مصرف کننده

هوش مصنوعی نقش مهمی در شکل دادن به اعتماد مصرف کننده و افزایش تجربه مشتری در تجارت الکترونیک ایفا می کند. فناوری‌های هوش مصنوعی مانند سیستم‌های توصیه، ربات‌های گفتگو و تشخیص تقلب امنیت و شخصی‌سازی را بهبود می‌بخشند، اما نگرانی‌های اخلاقی را در مورد حریم خصوصی داده‌ها و تعصب الگوریتمی نیز افزایش می‌دهند.(Akbar, Nabil, Iqbal, & Islam, ۲۰۲٤). استفاده روزافزون از هوش مصنوعی در اپلیکیشن‌های موبایل و پلتفرم‌های تجارت الکترونیک، ارزیابی مجدد مدل‌های اعتماد را با در نظر گرفتن عواملی مانند تمایل به اعتماد و حساسیت درک شده اطلاعات شخصی ضروری می‌کند.(Zarifis & Fu, ۲۰۲۳). شخصی‌سازی مبتنی بر هوش مصنوعی در تبلیغات از یادگیری ماشینی و تحلیل‌های پیش‌بینی‌کننده برای تطبیق تجربیات مصرف‌کننده استفاده می‌کند، در حالی که بر اهمیت پرداختن به نگرانی‌های مربوط به حریم خصوصی و ملاحظات اخلاقی تأکید می‌کند.(Navdeep Singh & Adhikari). پلتفرم‌های تجارت الکترونیک جهانی از هوش مصنوعی برای توصیه‌های شخصی‌شده و عملیات ساده‌شده استفاده می‌کنند، که بر نیاز به تعادل بین نوآوری‌های تکنولوژیکی و مسئولیت‌های اخلاقی برای حفظ اعتماد مصرف‌کننده و دستیابی به رشد پایدار تأکید می‌کند.(Sulastri, ۲۰۲۳).

۸. چالش ها و محدودیت های هوش مصنوعی در امنیت تجارت الکترونیک

۸.۱. مثبت و منفی کاذب

فناوری‌های هوش مصنوعی پتانسیل قابل‌توجهی برای افزایش امنیت تجارت الکترونیک، به‌ویژه در تشخیص تقلب و توصیه‌های شخصی‌سازی شده، ارائه می‌کنند. تکنیک های یادگیری ماشینی مانند رگرسیون لجستیک و درختان تصمیم می توانند به کاهش مثبت کاذب در تشخیص تقلب کارت اعتباری کمک کنند.(Patil et al., ۲۰۲۳). سیستم های پیشرفته با استفاده از احراز هویت و پروفایل DNS می توانند به تلاش های تقلب مبتنی بر پروکسی رسیدگی کنند و امنیت تجارت الکترونیک را تقویت کنند.(Patil et al., ۲۰۲۳). سیستم‌های توصیه مبتنی بر هوش مصنوعی، مانند SmartCart، از CNN و GAN برای ارائه پیشنهادات محصول شخصی‌شده بر اساس آپلود تصاویر استفاده می‌کنند.(Dharwadkar, Veena, Manohar, Jayanthi, & Kannadaguli, ۲۰۲٤). با این حال، چالش‌ها از جمله تهدیدات امنیت سایبری، هک و سرقت هویت همچنان ادامه دارند(Khan, ۲۰۱۹). برای پرداختن به این مسائل، تکنیک‌های هوش مصنوعی جدید مخصوص امنیت سایبری مانند سیستم‌های مبتنی بر دانش و استدلال احتمالی برای کنترل موارد مثبت و منفی کاذب در امنیت برنامه‌های کاربردی وب مورد نیاز است.(Morel, ۲۰۱۱). علیرغم محدودیت هایی مانند کیفیت داده ها و تعصبات مدل، هوش مصنوعی همچنان نقش مهمی در بهبود امنیت تجارت الکترونیک و تجربه کاربر ایفا می کند.

۸.۳. نگرانی های حفظ حریم خصوصی داده ها

با ادامه رشد تراکنش های آنلاین، نگرانی های امنیت و حفظ حریم خصوصی تجارت الکترونیک اهمیت زیادی پیدا کرده است(Arora, ۲۰۲۳). نقض داده ها، حملات فیشینگ، و آسیب پذیری های درگاه پرداخت، هم برای کسب و کارها و هم برای مصرف کنندگان تهدیدات قابل توجهی است.(Oguta, ۲۰۲٤). چالش‌های کلیدی شامل حفاظت از داده‌های مصرف‌کننده، درک اطلاعات جمع‌آوری‌شده و ارائه توصیه‌های شخصی‌شده است (نوریان و همکاران، ۲۰۲۰). برای پرداختن به این مسائل، محققان در حال بررسی راه حل های نوآورانه ای مانند احراز هویت بیومتریک، رمزنگاری پس کوانتومی و فناوری های حفظ حریم خصوصی هستند.(Oguta, ۲۰۲٤). اجرای اقدامات امنیتی قوی برای تقویت اعتماد مشتری و تسهیل رشد تجارت الکترونیک بسیار مهم است.(Khan, ۲۰۱۹). علاوه بر این، مقررات دولتی و چارچوب های قانونی نقشی حیاتی در حفظ استانداردهای حفظ حریم خصوصی داده ها ایفا می کنند(Arora, ۲۰۲۳). همانطور که تجارت الکترونیک به تکامل خود ادامه می دهد، تلاقی فناوری، مقررات و آگاهی کاربر در ایجاد یک محیط خرید آنلاین امن و قابل اعتماد حیاتی است.(Khan, ۲۰۱۹).

۸.۴. نیاز به نظارت انسانی

ادغام هوش مصنوعی در تجارت الکترونیک و خدمات مالی مزایای قابل توجهی را ارائه می دهد اما همچنین چالش هایی را ایجاد می کند که نظارت انسانی را ضروری می کند. در حالی که هوش مصنوعی کارایی را در زمینه هایی مانند خدمات مشتری و کشف تقلب افزایش می دهد، نگرانی هایی در مورد امنیت سایبری، حریم خصوصی و از دست دادن بالقوه همدلی انسانی در تعاملات با مشتری وجود دارد.(Jakkula, ۲۰۲۳). قانون پیشنهادی هوش مصنوعی اتحادیه اروپا با هدف رسیدگی به این مسائل با معرفی الزامات نظارت انسانی برای سیستم‌های هوش مصنوعی پرخطر است، اگرچه سؤالاتی در مورد ویژگی‌های پیاده‌سازی باقی مانده است.(Enqvist, ۲۰۲۳). برای متعادل کردن اتوماسیون با همدلی و کاهش خطرات، استراتژی هایی مانند ترکیب عناصر انسانی در سیستم های هوش مصنوعی، طراحی اخلاقی، مقررات، آموزش و حفظ نظارت انسانی توصیه می شود.(Jakkula, ۲۰۲۳). هدف این اقدامات افزایش رضایت مشتری، محافظت در برابر تهدیدات سایبری و اطمینان از استقرار هوش مصنوعی در تجارت الکترونیک و خدمات مالی است.

۹. آینده هوش مصنوعی در امنیت تجارت الکترونیک

۹.۱. گرایش ها و نوآوری های نوظهور

نوآوری های اخیر در امنیت تجارت الکترونیک و برنامه های کاربردی هوش مصنوعی، صنعت را متحول کرده، تجارب مشتری و کارایی عملیاتی را افزایش می دهد. شخصی‌سازی مبتنی بر هوش مصنوعی، واقعیت افزوده و چت‌بات‌ها رضایت کاربر را بهبود می‌بخشد و تحول دیجیتال را در خرده‌فروشی به پیش می‌برد.(Mathur & Gupta, ۲۰۲٤). فناوری‌های هوش مصنوعی مانند Google AI Cloud Platform و IBM Watson برای قیمت‌گذاری محصول و استراتژی‌های توزیع

مورد استفاده قرار می‌گیرند.(Kamesh & Binu, ۲۰۲٤). ادغام هوش مصنوعی در تجارت الکترونیک، شخصی سازی، اتوماسیون و راحتی را برای مشتریان افزایش می دهد و در عین حال کارایی و سودآوری را برای مشاغل افزایش می دهد.(Fatima, ۲۰۲۳). با این حال، بازار دیجیتال در حال گسترش با چالش‌های امنیتی در حال تحول، از جمله نقض اطلاعات و حملات فیشینگ مواجه است. برای پرداختن به این مسائل، فناوری‌های نوظهور مانند احراز هویت بیومتریک، رمزنگاری پس کوانتومی و فناوری‌های حفظ حریم خصوصی در حال بررسی هستند تا امنیت تجارت الکترونیک را افزایش دهند.(Oguta, ۲۰۲٤). آینده امنیت تجارت الکترونیک در تلاقی فناوری، مقررات و آگاهی کاربر برای ایجاد یک محیط خرید آنلاین امن و قابل اعتماد نهفته است.

۹.۲. پیش بینی ها برای پذیرش هوش مصنوعی در امنیت تجارت الکترونیک

پیش بینی می شود که استفاده از هوش مصنوعی در امنیت تجارت الکترونیک با افزایش شخصی سازی، اتوماسیون و کارایی عملیاتی صنعت را متحول کند.(Fatima, ۲۰۲۳). انتظار می‌رود سیستم‌های امنیت سایبری مبتنی بر هوش مصنوعی راه‌حل‌های پیشگیرانه و تطبیقی را ارائه دهند و دقت تشخیص تهدید و زمان پاسخگویی را در بخش‌های مختلف از جمله تجارت الکترونیک بهبود بخشند.(N G, ۲۰۲٤). ادغام هوش مصنوعی در تجارت الکترونیک، مدل‌ها و استراتژی‌های کسب‌وکار را متحول می‌کند و باعث افزایش تجارب مشتری و کارایی عملیاتی می‌شود.(Zelda, Prabowo, & Satato, ۲۰۲٤). با این حال، چالش هایی مانند نگرانی های حفظ حریم خصوصی داده ها، سوگیری های الگوریتمی، و پیامدهای نیروی کار باید مورد توجه قرار گیرند.(N G, ۲۰۲٤). انتظار می‌رود که همگرایی فناوری‌های بلاک چین و هوش مصنوعی در تجارت الکترونیک، امنیت داده‌ها و تراکنش‌ها را افزایش دهد و به مسائل امنیتی فعلی در معاملات آنلاین رسیدگی کند.(Suradi, ۲۰۲٤). همانطور که این فناوری‌ها به تکامل خود ادامه می‌دهند، شرکت‌های تجارت الکترونیکی که این تغییرات را پذیرفته و با آن سازگار می‌شوند، احتمالاً در بازار رقابتی آنلاین رشد خواهند کرد.(Fatima, ۲۰۲۳).

۹.۳. آماده شدن برای چشم انداز تهدید فردا

پلتفرم‌های تجارت الکترونیک با چشم‌اندازی در حال تحول از تهدیدات امنیت سایبری، از جمله حملات فیشینگ، بدافزارها، نقض‌های داده‌ها و تهدیدات داخلی مواجه هستند.(R. Gupta, ۲۰۲٤). این تهدیدها پیچیده تر می شوند و مجرمان سایبری از هوش مصنوعی و یادگیری ماشینی استفاده می کنند(R. Gupta, ۲۰۲٤). آسیب‌پذیری‌های کلیدی شامل مشکلات سمت کلاینت، اتصالات شبکه، وب سرورها و نرم‌افزارهای شخص ثالث است(Dakov & Malinova, ۲۰۲۱). برای کاهش این خطرات، کسب‌وکارها اقدامات فنی مانند رمزگذاری، دروازه‌های پرداخت امن، و سیستم‌های تشخیص نفوذ را در کنار شیوه‌های سازمانی مانند آموزش کارکنان و برنامه‌ریزی واکنش به حادثه اجرا می‌کنند.(R. Gupta, ۲۰۲٤). فناوری‌های نوظهور مانند احراز هویت بیومتریک و رمزنگاری پس کوانتومی راه‌حل‌های امیدوارکننده‌ای را برای افزایش امنیت تجارت الکترونیک ارائه می‌کنند.(Oguta, ۲۰۲٤). مطابقت با مقرراتی مانند GDPR و CCPA و رعایت

استانداردهای امنیتی مانند انطباق با PCI بسیار مهم است.(Dakov & Malinova, ۲۰۲۱). پرداختن به این چالش های امنیتی برای حفظ اعتماد مشتری و تسهیل رشد مداوم تجارت الکترونیک ضروری است(Khan, ۲۰۱۹)

۱۰. نتیجه گیری

ادغام هوش مصنوعی در امنیت تجارت الکترونیک فرصتی متحول کننده برای افزایش ایمنی و قابلیت اطمینان تراکنش های آنلاین است. فناوری‌های هوش مصنوعی، از جمله یادگیری ماشینی و پردازش زبان طبیعی، به طور قابل‌توجهی تشخیص تقلب، احراز هویت مشتری و حفاظت از داده‌ها را بهبود می‌بخشند. با این حال، چالش‌هایی مانند موارد مثبت کاذب، نگرانی‌های مربوط به حریم خصوصی داده‌ها و نیاز به نظارت انسانی باید برای اطمینان از استقرار هوش مصنوعی مسئولانه برطرف شوند. همانطور که تجارت الکترونیک به تکامل خود ادامه می دهد، تلاقی فناوری، مقررات و آگاهی کاربران در ایجاد یک محیط خرید آنلاین امن بسیار مهم خواهد بود. نوآوری های آینده، از جمله احراز هویت بیومتریک و رمزنگاری پس کوانتومی، نویدبخش تقویت بیشتر امنیت تجارت الکترونیک هستند. کسب‌وکارهای تجارت الکترونیک باید این پیشرفت‌ها را برای حفظ اعتماد مشتری و تسهیل رشد مداوم در بازار دیجیتال بپذیرند.

مراجع

Aburbeian, A. M., & Fernández-Veiga, M. (۲۰۲٤). Secure Internet Financial Transactions: A Framework Integrating Multi-Factor Authentication and Machine Learning. *AI*, *5*(۱), ۱۷۷-۱۹٤ .

Akbar, M. U., Nabil, S. J., Iqbal, K. A., & Islam, A. (۲۰۲٤). The Influence of Artificial Intelligence on Consumer Trust in E-Commerce: Opportunities and Ethical Challenges. *European Journal of Theoretical and Applied Sciences*, ۲(٦), ۲٥۰-۲٥۹ .

Al-Ebrahim, M. A., Bunian, S., & Nour, A. A. (۲۰۲۳). Recent Machine-Learning-Driven Developments in E-Commerce: Current Challenges and Future Perspectives. *Engineered Science*, *28*, ۱۰٤٤ .

ANDREIANU, G. (۲۰۲۳). *Protecting Your E-Commerce Business. Analysis on Cyber Security Threats.* Paper presented at the Proceedings of the International Conference on Cybersecurity and Cybercrime-۲۰۲۳.

Arora, D. (۲۰۲۳). Data privacy issues with e-commerce. *International Journal of Social Science & Economic Research* .

Bawack, R. E., Wamba, S. F., Carillo, K. D. A., & Akter, S. (۲۰۲۲). Artificial intelligence in E-Commerce: a bibliometric study and literature review. *Electronic markets*, *32*(۱), ۲۹۷-۳۳۸ .

Belo, O., Mota, G., & Fernandes, J. (٢٠١٦). *A signature based method for fraud detection on e-commerce scenarios.* Paper presented at the Analysis of Large and Complex Data.

Bosri, R., Rahman, M. S., Bhuiyan, M. Z. A., & Al Omar, A. (٢٠٢٠). Integrating blockchain with artificial intelligence for privacy-preserving recommender systems. *IEEE Transactions on Network Science and Engineering, 8*(٢), ١٠٠٩-١٠١٨ .

Braik, W., Morandat, F., Falleri, J.-R., & Blanc, X. (٢٠١٦). *Real time streaming pattern detection for ecommerce.* Paper presented at the Proceedings of the ٣١st Annual ACM Symposium on Applied Computing.

Caldeira, E., Brandao, G., & Pereira, A. C .(٢٠١٤) .*Fraud analysis and prevention in e-commerce transactions.* Paper presented at the ٢٠١٤ ٩th Latin American Web Congress.

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Rao, H. R. (٢٠١٦). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems, 83*, ٤٧-٥٦ .

Chukwurah, E. G., & Aderemi, S. (٢٠٢٤). Harmonizing teams and regulations: strategies for data protection compliance in US technology companies. *Computer Science & IT Research Journal, 5*(٤), ٨٢٤-٨٣٨ .

Dadkhah, M., Jazi, M. D., Mobarakeh, M. S., Shamshirband, S., Wang, X., & Raste, S. (٢٠١٦). An overview of phishing attacks and their detection techniques. *International Journal of Internet Protocol Technology, 9*(٤), ١٨٧-١٩٥ .

Dakov, S., & Malinova, A. (٢٠٢١). A Survey of E-Commerce Security Threats and Solutions. *Proceedings of CBU in Natural Sciences and ICT, 2*, ١-٩ .

Dalmadge, C. L. (٢٠١٩). IMPACTS OF DATA BREACHES ON ECOMMERCE GROWTH. *International Journal of Business Research* .

Dharwadkar, V., Veena, R., Manohar, S., Jayanthi, M., & Kannadaguli, P. (٢٠٢٤). *Smart Cart: Revolutionizing E-Commerce in India with AI-Powered Personalized Product Recommendations Overview.* Paper presented at the ٢٠٢٤ ٥th International Conference on Circuits, Control, Communication and Computing (I٤C).

Enqvist, L. (٢٠٢٣). 'Human oversight'in the EU artificial intelligence act: what, when and by whom? *Law, Innovation and Technology, 15*(٢), ٥٠٨-٥٣٥ .

Fatima, S. (٢٠٢٣). AI Implementation in an E-commerce. *International Journal For Multidisciplinary Research* .

FATUNMBI, T. O. (٢٠٢٢). Impact of data science and cybersecurity in e-commerce using machine learning techniques. *World Journal of Advanced Research and Reviews, 13*(١), ٨٣ .٢-٨٤٦

Fernandes, L. (٢٠١٣). Fraud in electronic payment transactions: Threats and countermeasures. *Asia Pacific Journal of Marketing & Management Review*_____ *ISSN, 2319*, ٢٨٣٦ .

Gaikwad, D., Ingale, P., Divekar, P., Changede, S., & Bhuwad, S. (٢٠٢٤). AI Enabled E-commerce Platform. *International Journal of Advanced Research in Science, Communication and Technology* .

Goel, S., & Shawky, H. A. (٢٠٠٩). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*(٧), ٤٠٤-٤١٠ .

Gonzalez, A., Lobato, P., Lopez, M. A., Carlos, O., & Duarte, M. B. *An Accurate Threat Detection System through Real-time Stream Processing*.

Gupta, P. (٢٠٢٤). Securing Tomorrow: The Intersection of AI, Data, and Analytics in Fraud Prevention. *Asian Journal of Research in Computer Science, 17*(٣), ٧٥-٩٢ .

Gupta, R. (٢٠٢٤). Cybersecurity Threats in E-Commerce: Trends and Mitigation Strategies. *Journal of Advanced Management Studies, 1*(٣), ١-١٠ .

Gupta, R ,.Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (٢٠٢٠). Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges. *IEEE Access, 8*, ٢٤٧٤٦-٢٤٧٧٢ .

Halachev, P. (٢٠٢٤). The Influence of Artificial Intelligence on the Automation of Processes in Electronic Commerce. *Data and Metadata* .

Hasan, I., & Rizvi, S. (٢٠٢٢). *AI-driven fraud detection and mitigation in e-commerce transactions.* Paper presented at the Proceedings of Data Analytics and Management: ICDAM ٢٠٢١, Volume ١.

Ho, L., & Papavassiliou, S. (٢٠٠٠). *Network and service anomaly detection in multi-service transaction-based electronic commerce wide area networks.* Paper presented at the Proceedings ISCC ٢٠٠٠. Fifth IEEE Symposium on Computers and Communications.

Hosseini, Z. Z., & Barkhordari, E. (٢٠١٣). *Enhancement of security with the help of real time authentication and one time password in e-commerce transactions.* Paper presented at the The ٥th Conference on Information and Knowledge Technology.

Idemudia, C., Agu, E. E., & Obeng, S. (٢٠٢٤). Analysis of machine learning techniques in detecting and preventing e-commerce fraud effectively. *International Journal of Frontiers in Science and Technology Research* .

İşlek, İ., Aksaylı, N. D., & Karamatlı, E. (٢٠٢٠). *Proactive Anomaly Detection Using Time Series Data of a Large Scale Platform.* Paper presented at the ٢٠٢٠ ٢٨th Signal Processing and Communications Applications Conference (SIU).

Ismail, W. S., Ghareeb, M. M., & Youssry, H. Enhancing Customer Experience through Sentiment Analysis and Natural Language Processing in E-commerce .

Jakkula, A. R. (٢٠٢٣). The Human Element in AI: Balancing Automation with Empathy in E-Commerce. *Journal of Artificial Intelligence & Cloud Computing* .

Jakkula, A. R. (٢٠٢٤). Ensuring Data Privacy and Security in AI-Enabled E-commerce Platforms. *Journal of Artificial Intelligence & Cloud Computing* .

Jhangiani, R., Bein, D., & Verma, A. (٢٠١٩). *Machine learning pipeline for fraud detection and prevention in e-commerce transactions.* Paper presented at the ٢٠١٩ IEEE ١٠th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON).

Kakkar, S., & Monga, V. (٢٠٢٠). *A Study on Artificial Intelligence in E - Commerce*.

Kamesh, S., & Binu, G .(٢٠٢٤) .Personalization and Customer Experience in E-Commerce. *International Journal of Innovative Science and Research Technology (IJISRT)* .

Khan, D. S. W. (٢٠١٩). *Cyber security issues and challenges in E-commerce.* Paper presented at the Proceedings of١٠ th international conference on digital strategies for organizational success.

Kumar, A., & Sangwan, S. (٢٠١٤). Biometric Security Systems. *International Journal of Engineering Trends and Technology, 11*, ١٦٩-١٧٠ .

Lari, H. A., Vaishnava, K., & Manu, K .(٢٠٢٢) .Artifical intelligence in E-commerce: Applications, implications and challenges. *Asian Journal of Management, 13*(٣), ٢٣٥-٢٤٤ .

Latze, C. (٢٠٠٧). Stronger Authentication in E-Commerce-How to protect even naıve Users against Phishing, Pharming, and MITM attacks. *RVS Retreat 2007 at Quarten*, ١١١-١١٦ .

Li, Z., & Oprea, A. (٢٠١٦). *Operational security log analytics for enterprise breach detection.* Paper presented at the ٢٠١٦ IEEE Cybersecurity Development (SecDev).

Malmasi, S., Agichtein, E., Ueffing ,N., Guy, I., & Rokhlenko, O. (٢٠١٩). *First international workshop on e-commerce and NLP (ECNLP) chairs' welcome.* Paper presented at the ٢٠١٩ World Wide Web Conference, WWW ٢٠١٩.

Manikopoulos, C., & Papavassiliou, S. (٢٠٠٢). Network intrusion and fault detection: a statistical anomaly approach. *IEEE Communications Magazine, 40*(١٠), ٧٦-٨٢ .

Massa, D., & Valverde, R. (٢٠١٤). A fraud detection system based on anomaly intrusion detection systems for e-commerce applications. *Computer and Information Science, 7* .١١٧-١٤٠ ,(٢)

Mathur, D., & Gupta, V. (٢٠٢٤). Emerging trends in e-commerce and their applications: Driving digital transformation in retail. *World Journal of Advanced Research and Reviews* .

Megaw, G., & Flowerday, S. V. (٢٠١٠). *Phishing within e-commerce :A trust and confidence game.* Paper presented at the ٢٠١٠ Information Security for South Africa.

Mihailescu, M. I., Nita, S. L., Rogobete, M., & Marascu, V. (٢٠٢٣). *Unveiling Threats: Leveraging User Behavior Analysis for Enhanced Cybersecurity.* Paper presented at the ٢٠٢٣ ١٥th International Conference on Electronics, Computers and Artificial Intelligence (ECAI).

Mimani, S., Ramakrishnan, R., Rohella, P., Jiwani, N., & Logeshwaran, J. (٢٠٢٤). *The Utilization of AI Extends Beyond Payment Systems to E-Commerce Store Development.* Paper presented at the ٢٠٢٤ ٢nd International Conference on Disruptive Technologies (ICDT).

Mohammadi, S., & Hosseini, S. Z. Enhancement of security via real time authentication with biometric methods in e-commerce transactions .

Morel, B. (٢٠١١). *Artificial intelligence and the future of cybersecurity.* Paper presented at the Proceedings of the ٤th ACM workshop on Security and artificial intelligence.

Morić, Z., Dakic, V., Djekic, D., & Regvart, D. (٢٠٢٤). Protection of Personal Data in the Context of E-Commerce. *Journal of cybersecurity and privacy, 4*(٣), ٧٣١-٧٦١ .

Muzatko, S., & Bansal, G. (٢٠١٨). *Timing of data breach announcement and e-commerce trust.* Paper presented at the The proceedings of Midwest Association for Information Systems Conference.

N G, S. G. (٢٠٢٤). Review on Harnessing Artificial Intelligence: A Paradigm Shift in Cybersecurity for a Safer Digital Future. *International Journal for Research in Applied Science and Engineering Technology* .

Nofer, M., Hinz, O., Muntermann, J., & Roßnagel, H. (٢٠١٤). The economic impact of privacy violations and security breaches: A laboratory experiment. *Business & Information Systems Engineering, 6*, ٣٣٩-٣٤٨ .

Nugraha, M. A., Arisandi, D., & Perdana, N. J. (٢٠٢١). Pengamanan Website E-Commerce Menggunakan Multi-Factor Authentication. *Jurnal Ilmu Komputer dan Sistem Informasi, 9*(١), ١٥٨-١٦٢ .

Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (٢٠٢٤). Data-Driven Cyber Threat Intelligence: Leveraging Behavioral Analytics for Proactive Defense Mechanisms .

Oguta, G. C. (٢٠٢٤). Securing the virtual marketplace: Navigating the landscape of security and privacy challenges in E-Commerce. *GSC Advanced Research and Reviews, 18*(١), ٠٨٤-١١٧ .

Paschal Kulwa, C. (٢٠٢٤ .(Blockchain and Artificial Intelligence: A Synergistic Approach for Digital Identity and Security in E-Commerce. *International Journal of Science and Research (IJSR* .(

Patil, P., Sonkar, M., Patil, P., Deshmukh, P., & Patil, T. (٢٠٢٣). A Comprehensive Strategy for Detecting Credit Card Fraud in E-Commerce Utilizing DNS Authentication. *International Journal of Soft Computing and Engineering (IJSCE)* .

Qiu, L., & Li, J. (٢٠١٧). Covering the Monitoring Network: A Unified Framework to Protect E-Commerce Security. *Complexity, 2017*(١), ٦٢٥٤٨٤٢ .

Raghava-Raju, A. (٢٠١٧). Predicting Fraud in Electronic Commerce: Fraud Detection Techniques in E-Commerce. *International Journal of Computer Applications, 171*(٢), ١٨-٢٢ .

Rajkumar, K. V., Yadav, O. V., Bhyrapuneni, S ,.Sudha, M. V., Ratnagiri, D., & Thota, K. K. (٢٠٢٤). *Enhancing E-Commerce Security: A Machine Learning Framework for Fraud Detection.* Paper presented at the ٢٠٢٤ ٨th International Conference on Electronics, Communication and Aerospace Technology (ICECA).

Ramadhan, I. H., & Nurnawati, E. K. (٢٠٢٢). Analisis ancaman phishing dalam layanan e-commerce. *PROSIDING SNAST*, E٣١-٤١ .

Rath, M. (٢٠٢٠). Machine learning and its use in e-commerce and e-business. In *Handbook of research on applications and implementations of machine learning techniques* (pp. ١١١-١٢٧): IGI Global.

Reddy, S. R. B., Kanagala, P., Ravichandran, P., Pulimamidi, R., Sivarambabu, P., & Polireddi, N. S. A. (٢٠٢٤). Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics. *Measurement: Sensors, 33*, ١٠١١٣٨ .

Rodrigues, V. F., Policarpo, L. M., da Silveira, D. E., da Rosa Righi, R., da Costa, C. A., Barbosa, J. L. V., . . . Arcot, T. (٢٠٢٢). Fraud detection and prevention in e-commerce: A systematic literature review. *Electronic Commerce Research and Applications, 56*, ١٠١٢٠٧ .

Saleem, S. A. M., & Naseem, S. M. B. (٢٠٢٣). *A Comprehensive Review of the Artificial Intelligence (AI) shift in E-commerce.* Paper presented at the ٢٠٢٣ ٦th International Conference on Advances in Science and Technology (ICAST).

SangeethaM, K., & Suchitra, R. (٢٠١٨). The Study of E-Commerce Security Issues and Solutions. *International journal of engineering research and technology, 4* .

Sharma, A. THE IMPACT OF CYBERSECURITY BREACHES ON BIG BUSINESSES. *International Journal of Advanced Research, 12* .(١٠)

Shyna, K., & Vishal, M. (٢٠١٧). A study on artificial intelligence E-commerce. *International Journal of Advances in Engineering & Scientific Research, 4*(٤), ٦٢-٦٨ .

Singh, N., & Adhikari, D .AI-Driven Personalization in eCommerce Advertising. In: Academic Press.

Singh, N., Do, Y., Yu, Y., Fouad, I., Kim, J., & Kim, H. (٢٠٢٤). Crumbled Cookies: Exploring E-commerce Websites? Cookie Policies with Data Protection Regulations. *ACM Transactions on the Web* .

Śliwiński, R. (٢٠٢١). Artificial Intelligence: A Prerequisite for Competitive Advantage in E-Commerce. In *Competition, Strategy, and Innovation* (pp. ١٥-٣٤): Routledge.

Sulastri, L. (٢٠٢٣). The Role of Artificial Intelligence in Enhancing Customer Experience: A Case Study of Global E-commerce Platforms. *International Journal of Science and Society* .

Suradi, A. (٢٠٢٤). Blockchain and AI Technology Convergence: Applications in E-Commerce. *Journal of Information System, Technology and Engineering* .٢٦٩-٢٧٩ ,(٣)٢ ,

Ueffing, N., Rokhlenko, O., & Goyal, A. K. (٢٠١٩). First International Workshop on e-Commerce and NLP (ECNLP) Chairs' Welcome. *Companion Proceedings of The 2019 World Wide Web Conference* .

Vangala, R. R., & Sasi, S. (٢٠٠٤). *Biometric authentication for e-commerce transaction.* Paper presented at the ٢٠٠٤ IEEE International Workshop on Imaging Systems and Techniques (IST)(IEEE Cat. No. ٠٤EX٨٩٦).

Vyas, B. (٢٠٢٣). Java in Action: AI for Fraud Detection and Prevention. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, ٥٨-٦٩ .

Wang, P., D'Cruze, H., & Wood, D. (٢٠١٩). ECONOMIC COSTS AND IMPACTS OF BUSINESS DATA BREACHES. *Issues in Information Systems, 20* .(٢)

Yasin, S., Haseeb, K., & Qureshi, R. J. (٢٠١٢). Cryptography based e-commerce security: a review. *International Journal of Computer Science Issues (IJCSI), 9*(٢), ١٣٢ .

Zade, S., Barhanpure, S., Jaiswal, S. V., Kaur, G., Agrawal, P., & Pinjarkar, L. (٢٠٢٤). *E-Commerce Cybersecurity: A Comprehensive Review of Types, Breaches and Best Practices.* Paper presented at the ٢٠٢٤ ١٠th International Conference on Electrical Energy Systems (ICEES).

Zarifis, A., & Fu, S. (٢٠٢٣). Re-Evaluating Trust and Privacy Concerns When Purchasing a Mobile App :Re-Calibrating for the Increasing Role of Artificial Intelligence. *Digital, 3*(٤), ٢٨٦-٢٩٩ .

Zelda, Y. C., Prabowo, B. A., & Satato, Y. R. (٢٠٢٤). Kebangkitan E-commerce Bertenaga AI: Mengubah Lanskap Bisnis di Tahun ٢٠٢٤. *Prosiding Seminar Nasional Ilmu Manajemen Kewirausahaan dan Bisnis* .

Zhang, D., Pee, L., & Cui, L. (۲۰۲۱). Artificial intelligence in E-commerce fulfillment: A case study of resource orchestration at Alibaba's Smart Warehouse. *International journal of information management*, *57*, ۱۰۲۳۰٤ .

Zhao, J., Lau, R. Y., Zhang, W., Zhang, K., Chen, X., & Tang, D. (۲۰۱٦). Extracting and reasoning about implicit behavioral evidences for detecting fraudulent online transactions in e-Commerce. *Decision Support Systems*, *86*, ۱۰۹-۱۲۱ .

The role of artificial intelligence in increasing e-commerce security

Hossein elyasi varg

Akram elyasi varg

Abstract

As e-commerce continues to expand, the importance of robust security measures to protect digital transactions and maintain customer trust has never been more critical. This article explores the multifaceted role of artificial intelligence (AI) in enhancing e-commerce security, addressing common cybersecurity threats such as phishing, data breaches, and payment fraud. By leveraging AI technologies, including machine learning and natural language processing, e-commerce platforms can improve fraud detection, customer authentication, and data protection. Integrating AI not only streamlines operations but also fosters a safer online shopping environment. This article discusses the current challenges and limitations of AI in e-commerce security, while highlighting future trends and innovations that promise to further enhance the security landscape.

Keywords:E-commerce security, artificial intelligence, fraud detection, data protection, cybersecurity threats