IJEETR

International Journal of Electrical, Electronics, Telecommunications and Robotics (IJEETR)

مجله بین‌المللی مهندسی برق، الکترونیک، مخابرات و رباتیک

https://ijeetr.ir

دوره ۱ – شماره ۱ (پاییز ۱۴۰۴) – صفحه ۲۵ تا ۳۴

# کاربردها و چالش‌های هوش مصنوعی در حفاظت سیستم‌های قدرت: یک بررسی جامع و روش‌مند

**علیرضا جوشن***

کارشناس ارشد برق قدرت گرایش الکترونیک قدرت و ماشین های الکتریکی ،دانشگاه گیلان،گیلان ایران

Alireza.joshan.guilan@gmail.com

## چکیده

با افزایش پیچیدگی شبکه‌های برق با ادغام منابع انرژی تجدیدپذیر، اینترنت اشیا و داده‌های عظیم سنسوری، سیستم‌های حفاظت سنتی دیگر پاسخگوی نیازهای پایداری، قابلیت اطمینان و پاسخ در زمان واقعی نیستند. **هوش مصنوعی (AI)**با توانایی‌های یادگیری از داده‌های تجربی، پردازش بلادرنگ و مدل‌سازی الگوهای غیرخطی نقش مهمی در بهینه‌سازی حفاظت شبکه‌های قدرت ایفا می‌کند. این مقاله مروری سیستماتیک شامل تجزیه و تحلیل بیش از ۱۰۰ مقاله منتشرشده است، کاربردهای کلیدی AIدر تشخیص و طبقه‌بندی خطا، حفاظت تطبیقی، امنیت سایبری و مدیریت اختلالات را بررسی می‌کند، چارچوبی نوین برای مقایسه روش‌ها ارائه می‌دهد و **چالش‌ها و چشم‌اندازهای آتی را با استناد به نتایج تحقیقاتی اخیر** ترسیم می‌کند. این بررسی نشان می‌دهد که روش‌های AIنظیر یادگیری عمیق می‌توانند دقت تشخیص خطا و زمان پاسخ را به‌طور قابل‌توجهی بهبود دهند، اما **مسائل استانداردسازی، تعمیم به داده‌های واقعی، و امنیت سایبری** هنوز به‌طور کامل حل نشده‌اند.

**کلمات کلیدی:** هوش مصنوعی، حفاظت سیستم‌های قدرت، یادگیری ماشین، یادگیری عمیق، تشخیص خطا

## ۱. مقدمه

حفاظت سیستم‌های قدرت به معنای تشخیص سریع وقوع خطا و جداسازی بخش معیوب شبکه برای جلوگیری از گسترش ناپایداری و صدمات تجهیزات است. روش‌های کلاسیک حفاظتی مبتنی بر مقادیر آستانه‌ای (Overcurrent/Distance Protection)و تحلیل‌های تحلیلی، در مواجهه با **شبکه‌های مدرن با منابع توزیع‌شده انرژی، داده‌های عظیم و شرایط غیرخطی** با محدودیت‌هایی مواجه هستند *(Oelhaf et al., 2025)*.

هوش مصنوعی به‌عنوان مجموعه‌ای از الگوریتم‌های داده‌محور، این امکان را فراهم می‌کند که سیستم‌های حفاظتی بتوانند از داده‌های تاریخی و زمان‌واقعی برای **یادگیری الگوهای خطا، سازگاری با تغییرات شبکه و بهبود تصمیم‌گیری در شرایط بحرانی** استفاده کنند *(Mishra & Singh, 2025;* Wörsdörfer et al.,۲۰۲٦).

ادغام AIدر حفاظت سیستم‌های قدرت نه‌تنها باعث افزایش دقت و سرعت پاسخ در تشخیص خطا می‌شود، بلکه کاربردهای پیش‌بینی، تطبیقی و امنیت سایبری را نیز فراهم می‌سازد. این تحولات برای تحقق شبکه‌های برق هوشمند و فراهم کردن قابلیت خودترمیمی امری ضروری محسوب می‌شود.

## ۲. روش‌شناسی پژوهش

برای تدوین این مرور، از یک روش سیستماتیک و تکرارپذیر استفاده شد. مراحل اصلی عبارت بودند از:

**جدول۱.مراحل اصلی روش شناسی پژوهش**

| مرحله | شرح |
|---|---|
| تعیین سوالات کلیدی | نقش AIدر حفاظت سیستم‌های قدرت، عملکرد مدل‌ها، چالش‌ها و مسیرهای آتی |
| جستجوی پایگاه‌های علمی | MDPI، Springer، ScienceDirect، IEEE Xplore،Scopus |
| کلمات کلیدی | “Artificial Intelligence”, “Power System Protection”, “Machine Learning”, “Deep Learning”, “Fault Detection” |
| معیارهای ورود | مقالات انگلیسی، مرورها و تحقیقات تجربی تا سال ۲۰۲۵ |
| تجزیه و تحلیل | استخراج کاربردها، روش‌ها، داده‌ها، سنجه‌ها و نتایج |
| ترکیب نتایج | تدوین جدول‌های مقایسه و تحلیل شکاف‌ها |

با این روش، بیش از **۱۰۰ مقاله مروری و تحقیقاتی مرتبط با AIو حفاظت سیستم‌های قدرت** بررسی شد *(Oelhaf et al., 2025)*.

## ۳. طبقه‌بندی کاربردهای AIدر حفاظت سیستم‌های قدرت

در این بخش، کاربردهای AIدر حفاظت سیستم‌های قدرت در چند حوزه کلیدی دسته‌بندی می‌شود:

### ۳.۱-۱-۱. تشخیص، طبقه‌بندی و مکان‌یابی خطا

AIمی‌تواند با یادگیری از داده‌های ولتاژ و جریان، الگوهای خطا را تشخیص دهد و نوع و موقعیت آن را مشخص کند. برای مثال، مدل‌های یادگیری عمیق مانند CNNو LSTMدر تحقیق‌های اخیر در بهبود **دقت تشخیص و موقعیت‌یابی خطا** عملکرد قابل‌توجهی داشته‌اند *(Mishra & Singh, 2025; Oelhaf et al., 2025)*.

### ۳.۲-۱-۲. حفاظت تطبیقی

سیستم‌های حفاظتی باید بتوانند تنظیمات خود را بر اساس شرایط شبکه به‌روزرسانی کنند. AIبا یادگیری رایانه‌ای و روش‌های پیش‌بینی می‌تواند **پارامترهای حفاظتی را به‌صورت بلادرنگ بهینه‌سازی کند** تا دقت و پایداری حفاظت افزایش یابد *(Oelhaf et al., 2025)*.

### ۳.۳-۱-۳. تشخیص ناهنجاری و امنیت سایبری

AIقادر است ناهنجاری‌های جدید در داده‌های سنسوری را تشخیص دهد و در کنار روش‌های امنیت سایبری، **حملات طراحی‌شده را شناسایی و پاسخ دهد** *(Nature Scientific Reports, 2025; Oelhaf et al., 2025)*.

### ۳.۴-۱-۴. ادغام با شبکه‌های هوشمند

هوش مصنوعی با داده‌های IoTو PMU، امکان **تحلیل داده‌های حجیم در زمان‌واقعی و به‌کارگیری استراتژی‌های حفاظتی خودیادگیر** را فراهم می‌کند *(Oelhaf et al., 2025)*.

IJEETR
International Journal of Electrical, Electronics, Telecommunications and Robotics (IJEETR)
مجله بین‌المللی مهندسی برق، الکترونیک، مخابرات و رباتیک
https://ijeetr.ir
دوره ۱ – شماره ۱ (پاییز ۱۴۰۴) – صفحه ۲۵ تا ۳۴

### ۴. الگوریتم‌ها و تکنیک‌های AIدر حفاظت سیستم‌های قدرت

جدول۲. **الگوریتم‌ها و تکنیک‌های AIدر حفاظت سیستم‌های قدرت**

| تکنیک AI | کاربرد اصلی | مزایا | محدودیت‌ها |
|---|---|---|---|
| **شبکه عصبی عمیق (DL)** | تشخیص و طبقه‌بندی خطا | قابلیت استخراج ویژگی‌های پیچیده | نیاز به داده بسیار |
| **یادگیری ماشین سنتی (ML)** | تشخیص ابتدایی و طبقه‌بندی خطا | ساختار ساده | محدودیت در داده‌های پیچیده |
| **یادگیری تقویتی (RL)** | بهینه‌سازی تطبیقی | تصمیم‌گیری پویا | پیچیدگی پیاده‌سازی |
| **الگوریتم‌های ترکیبی** | حفاظت تطبیقی و چندوظیفه‌ای | تقویت کارایی | محاسبات سنگین |

### ۵. مرور و مقایسه مطالعات کلیدی

در جدول ۳ چند مقاله مروری مهم در این حوزه و نقاط کلیدی آن‌ها آورده شده است:

**جدول۳. مطالعات کلیدی پژوهش**

| مرجع | تکنیک‌ها | دامنه کاربرد | نکته برجسته |
|---|---|---|---|
| Oelhaf et al. (۲۰۲۵) | ML, DL | حفاظت و مدیریت اختلال | چارچوب Scoping Reviewبا بیش از ۱۰۰ مطالعه *(Oelhaf et al., 2025)* |
| Mishra & Singh (۲۰۲۵) | DL | تکنیک‌های یادگیری عمیق در حفاظت | بررسی جامع DLو روندهای کاربردی *(Mishra & Singh, 2025)* |
| Nasim et al. (۲۰۲٤) | DL | تشخیص و تشخیص خطاها | بررسی مقایسه‌ای روش‌های DLدر تشخیص خطا *(Aziz et al., 2024)* |

| | | | |
|---|---|---|---|
| بهبود دقت تشخیص و کاهش خطای در سیستم‌های حفاظتی *(Upadhyay & Yadav, ۲۰۲٤)* | حفاظت شبکه برق | ML, ANN, Fuzzy | AI Based Protection Schemes (۲۰۲٤) |
| تشخیص ناهنجاری‌ها و حملات سایبری *(Nature Scientific Reports, 2025)* | امنیت سیستم‌های قدرت | ML, DL | AI-Driven Cyber Security (۲۰۲٥) |

## ۶. جدول مقایسه عملکرد روش‌ها

جدول۴. **مقایسه عملکرد روش‌ها**

| مرجع | داده‌های آزمایشی | زمان پاسخ | دقت تشخیص | روش |
|---|---|---|---|---|
| *(Mishra & Singh, 2025)* | داده‌های سنسوری واقعی | خیلی سریع | ۹۵٪> | DL (CNN, LSTM) |
| *(Oelhaf et al., 2025)* | داده‌های شبیه‌سازی | متوسط | ۹۰٪~ | MLسنتی |
| *(Upadhyay & Yadav, 2024)* | داده‌های صنعتی | سریع | ۹۵.۷٪ | ANN + Fuzzy |
| *(Nature Scientific Reports, ۲۰۲٥)* | داده‌های واقعی و شبیه‌سازی | سریع | ۹۳٪~ | Cybersecurity AI |

## ۷. چالش‌ها و محدودیت‌ها

اگرچه هوش مصنوعی (AI)توانسته است عملکرد حفاظت سیستم‌های قدرت را به‌طور قابل‌توجهی بهبود دهد، مجموعه‌ای از چالش‌های اساسی و محدودیت‌های تحقیقاتی و عملی همچنان مانع از کاربرد گسترده، مطمئن و پایدار این فناوری در شبکه‌های برق واقعی است.

یکی از مهم‌ترین محدودیت‌ها کمبود داده‌های واقعی، عمومی و با کیفیت برای آموزش و ارزیابی مدل‌های هوش مصنوعی است. بسیاری از مطالعات موجود بر روی داده‌های شبیه‌سازی‌شده انجام شده‌اند که ممکن است نتوانند پیچیدگی‌ها، نویزها و عدم قطعیت‌های داده‌های عملیاتی در شبکه‌های برق حقیقی را بازتاب دهند. عدم دسترسی به دیتاست‌های بزرگ و استاندارد باعث می‌شود که اعتبارسنجی دقیق و مقایسه عملکرد مدل‌ها در سناریوهای واقعی دشوار شود، زیرا داده‌های در دسترس محدود یا متعلق به شرکت‌های خصوصی هستند که به‌طور عمومی منتشر نمی‌شوند *(Oelhaf et al., 2025;* Ncube et al.. ۲۰۲٦).

مرتبط با این موضوع، عدم وجود معیارها و استانداردهای ارزیابی مشترک برای سنجش عملکرد روش‌های AIدر حفاظت سیستم‌های قدرت یک چالش بزرگ دیگر است. بررسی‌های اخیر نشان می‌دهند که مطالعات مختلف از مجموعه معیارهای متفاوتی استفاده می‌کنند و اغلب ارزیابی‌ها تنها بر اساس چند معیار ساده مانند دقت انجام می‌شود، در حالی که سنجش‌های مقاومتی، پایداری در برابر نویز، و مقایسه عملکرد در سناریوهای عملیاتی واقعی به‌طور سازگار گزارش نمی‌شوند. این پراکندگی در معیارهای ارزیابی، مقایسه عادلانه و منصفانه بین روش‌ها را دشوار کرده و توسعه راه‌حل‌های استاندارد را با مشکل مواجه می‌سازد *(Oelhaf et al., 2025)*.

چالش بعدی پیچیدگی محاسباتی و هزینه‌های سخت‌افزاری است. بسیاری از مدل‌های پیشرفته، به‌ویژه شبکه‌های عصبی عمیق یا معماری‌های پیچیده‌تر، برای آموزش و استنتاج نیازمند منابع محاسباتی بسیار بالا، حافظه زیاد و مصرف انرژی قابل‌توجه هستند. این مسئله باعث افزایش هزینه‌های پیاده‌سازی و مانع از اجرای این مدل‌ها در زمان واقعی بر روی سخت‌افزارهای لبه (Edge)یا در محیط‌های با منابع محدود می‌شود. در شرایطی که سیستم‌های حفاظتی باید در کسری از ثانیه پاسخ دهند، نیاز به سخت‌افزارهای قدرتمند و بهینه می‌تواند یکی از موانع اصلی پیاده‌سازی عملی باشد (Energy Informatics., ۲۰۲۵).

امنیت و اعتماد به مدل‌های AIنیز از دیگر چالش‌های اساسی در این حوزه هستند. شبکه‌های قدرت جزء زیرساخت‌های حیاتی محسوب می‌شوند و حملات سایبری می‌توانند تأثیرات مخرب و حتی فاجعه‌باری داشته باشند. مدل‌های هوش مصنوعی، به‌خصوص آنهایی که به‌صورت «جعبه سیاه» عمل می‌کنند، می‌توانند در برابر داده‌های مخرب، حملات تزریق خطا یا تهدیدات سایبری آسیب‌پذیر باشند. همچنین عدم شفافیت در نحوه تصمیم‌گیری مدل‌ها باعث می‌شود که اپراتورها نتوانند دلایل پیش‌بینی یا واکنش حفاظتی AI را به‌طور کامل تبیین کنند، که این موضوع می‌تواند اعتماد کاربران و ناظران به چنین سیستم‌هایی را کاهش دهد. تحقیقات نشان داده‌اند که حتی در کاربردهای هوشمند شبکه‌های انرژی، موضوع قابل تفسیر بودن و قابل توضیح بودن **(**Explainability**)**مدل‌ها یکی از مسائل کلیدی است که باید مورد توجه قرار گیرد تا اطمینان‌پذیری و پذیرش عملی افزایش یابد (Henao & Edgell., ۲۰۲۵; Sarun et al.,۲۰۲٦; Vignes et al.,۲۰۲۵;Kilaru et al.,۲۰۲۵).

یکی دیگر از محدودیت‌ها ی کپارچه‌سازی AIبا زیرساخت‌های سنتی و تجهیزات موجود است. بسیاری از شبکه‌های قدرت فعلی بر اساس اصول سنتی طراحی شده‌اند و افزودن لایه‌های هوشمند نیازمند تغییرات اساسی در معماری نرم‌افزاری و سخت‌افزاری، استانداردهای ارتباطی، و ابزارهای اندازه‌گیری است. توسعه چارچوب‌های نرم‌افزاری، پروتکل‌های ارتباطی جدید و راهکارهای ارتباطی امن برای سنجش و انتقال داده‌ها موضوعی است که هنوز به‌طور کامل حل نشده باقی مانده است (Henao & Edgell., ۲۰۲۵; Amani et al.. ۲۰۲٦; Khalil et al.,۲۰۲٦).

در مجموع، این چالش‌ها اعم از دسترسی محدود به داده‌های واقعی، ضعف در استانداردسازی ارزیابی، نیازمند منابع محاسباتی سنگین، مسائل امنیتی و اعتماد، و دشواری‌های یکپارچه‌سازی با زیرساخت‌های موجود نشان می‌دهند که توسعه‌ی کاربردی و عملی هوش مصنوعی در حفاظت سیستم‌های قدرت هنوز در مراحل اولیه قرار دارد و نیازمند تلاش‌های تحقیقاتی متمرکز، توسعه استانداردهای مشترک، و همکاری بین صنعت و دانشگاه است.

### ۸. چشم‌اندازهای آتی

با توجه به پیشرفت‌های قابل توجه هوش مصنوعی در حوزه حفاظت سیستم‌های قدرت، مسیر تحقیقات آینده بیش از پیش نیازمند تمرکز بر توسعه و بهبود ابزارها و روش‌های هوشمند است. یکی از مهم‌ترین نیازها، توسعه دیتاست‌های استاندارد و عمومی است که بتوانند به عنوان مرجع ارزیابی عملکرد مدل‌های هوش مصنوعی مورد استفاده قرار گیرند. در حال حاضر، بسیاری از مدل‌های یادگیری ماشین بر روی داده‌های محدود یا شبیه‌سازی‌شده آموزش داده می‌شوند که این موضوع محدودیت‌هایی در ارزیابی عملکرد واقعی آنها ایجاد می‌کند. فراهم آوردن دیتاست‌های جامع و استاندارد می‌تواند امکان مقایسه مستقیم الگوریتم‌ها و اطمینان از کیفیت و دقت آنها را فراهم سازد.

از سوی دیگر، بهبود قابلیت تعمیم مدل‌ها به داده‌های واقعی و نویزی یکی از چالش‌های اصلی پژوهشی است. داده‌های عملیاتی شبکه‌های قدرت غالباً دارای نویز، خطاهای اندازه‌گیری و شرایط غیرایده‌آل هستند که مدل‌ها باید بتوانند با آنها به‌صورت پایدار و مطمئن کار کنند. تحقیقات آینده باید به طراحی الگوریتم‌هایی بپردازند که نه تنها در شرایط شبیه‌سازی شده، بلکه در محیط‌های واقعی با داده‌های نامطمئن و متغیر نیز عملکرد قابل قبولی ارائه دهند (Mishra & Singh., ۲۰۲۵; Kassar et al.,۲۰۲٦; Sarun et al.,۲۰۲٦).

یکی دیگر از جنبه‌های مهم، هوش مصنوعی قابل توضیح (Explainable AI) است که می‌تواند اعتماد اپراتورها و مهندسان شبکه را به مدل‌های هوشمند افزایش دهد. مدل‌های فعلی اغلب به عنوان «جعبه سیاه» عمل می‌کنند و توضیح دقیقی از تصمیمات حفاظتی ارائه نمی‌دهند. توسعه روش‌های هوش مصنوعی شفاف و قابل تفسیر، امکان بررسی دلایل تصمیم‌گیری‌های مدل‌ها و اطمینان از انطباق آنها با استانداردهای ایمنی و عملیاتی را فراهم می‌کند و به تسهیل پذیرش فناوری‌های هوشمند در صنعت کمک می‌کند (Al Battashi et al.,۲۰۲٦; Adadi et al.,۲۰۱۸; Arrieta et al.,۲۰۲۰; Haque et al.,۲۰۲۳).

علاوه بر این، ادغام هوش مصنوعی با روش‌های امنیت سایبری و شبکه‌های توزیع‌شده چشم‌انداز مهمی برای آینده حفاظت سیستم‌های قدرت به شمار می‌آید. با توجه به افزایش پیچیدگی شبکه‌های هوشمند و اتصال گسترده منابع انرژی تجدیدپذیر و توزیع‌شده، مدل‌های هوشمند باید توانایی شناسایی و مقابله با تهدیدات سایبری و نوسانات شبکه را به صورت یکپارچه داشته باشند. این موضوع به توسعه سیستم‌های محافظتی پیش‌بینی‌کننده و مقاوم کمک کرده و سطح اطمینان شبکه را به شکل چشمگیری ارتقاء می‌دهد (Kilaru et al.,۲۰۲۵).

در مجموع، چشم‌اندازهای آتی هوش مصنوعی در حفاظت سیستم‌های قدرت شامل تمرکز بر استانداردسازی داده‌ها، بهبود قابلیت تعمیم، افزایش شفافیت تصمیم‌گیری و یکپارچه‌سازی با امنیت سایبری و شبکه‌های توزیع‌شده است. پیشرفت در این زمینه‌ها نه تنها عملکرد حفاظتی را بهبود می‌بخشد، بلکه مسیر توسعه شبکه‌های برق هوشمند، پایدار و مقاوم در برابر تهدیدات را هموار می‌کند و نقش هوش مصنوعی را به عنوان یک ابزار کلیدی و غیرقابل جایگزین در مدیریت آینده انرژی تثبیت می‌نماید.

## ۹. نتیجه‌گیری

هوش مصنوعی به عنوان یک ابزار نوین، تأثیر قابل توجهی بر عملکرد و کارایی سیستم‌های قدرت داشته است. استفاده از الگوریتم‌های پیشرفته یادگیری ماشین و یادگیری عمیق باعث شده است که تشخیص خطا در شبکه‌های برق سریع‌تر و دقیق‌تر انجام شود، که این امر به کاهش زمان خاموشی‌ها و افزایش قابلیت اطمینان سیستم منجر می‌شود. علاوه بر این، هوش مصنوعی توانایی تطبیق‌پذیری بالایی در شرایط متغیر شبکه، بارهای ناپایدار و منابع انرژی تجدیدپذیر دارد و می‌تواند پاسخ‌های محافظتی بهینه‌ای ارائه دهد که فراتر از توان سیستم‌های حفاظتی سنتی است.

علاوه بر بهبود عملکرد حفاظتی، هوش مصنوعی در ارتقاء امنیت سیستم‌های قدرت نیز نقش مهمی ایفا می‌کند. الگوریتم‌های هوشمند قادر به شناسایی الگوهای غیرمعمول و تهدیدات سایبری هستند و می‌توانند پیش از بروز خطاهای جدی یا حملات سایبری، اقدام‌های پیشگیرانه انجام دهند. این ویژگی‌ها به ویژه در شبکه‌های برق هوشمند و سیستم‌های انرژی توزیع‌شده اهمیت دوچندان دارند، جایی که پیچیدگی و میزان داده‌های ورودی بسیار بالاست.

با این حال، استفاده گسترده از هوش مصنوعی در حفاظت سیستم‌های قدرت با چالش‌هایی نیز همراه است. از جمله می‌توان به نیاز به استانداردسازی الگوریتم‌ها و فرآیندهای حفاظتی، دسترسی به داده‌های واقعی و با کیفیت برای آموزش مدل‌ها، و مسائل امنیت سایبری اشاره کرد. این چالش‌ها نشان می‌دهد که علی‌رغم پیشرفت‌های چشمگیر، پژوهش‌های آینده باید بر ایجاد چارچوب‌های قابل اعتماد، مقاوم و قابل ارزیابی تمرکز کنند تا اطمینان حاصل شود که هوش مصنوعی می‌تواند در شرایط عملیاتی واقعی به صورت پایدار و ایمن عمل کند.

در مجموع، هوش مصنوعی نه تنها قابلیت بهبود عملکرد حفاظتی و امنیتی سیستم‌های قدرت را دارد، بلکه زمینه را برای توسعه شبکه‌های هوشمند و پایدارتر فراهم می‌کند. با ادامه تحقیقات در زمینه استانداردسازی، ارتقاء کیفیت داده‌ها و افزایش مقاومت سیستم‌ها در برابر تهدیدات سایبری، می‌توان انتظار داشت که نقش هوش مصنوعی در حفاظت سیستم‌های قدرت به طور روزافزون کلیدی و غیرقابل جایگزین شود.

## مراجع

Mishra, M., & Singh, J. G. (۲۰۲۵). *A comprehensive review on deep learning techniques in power system protection: Trends, challenges, applications and future directions*. **Results in Engineering, ۲۵,** ۱۰۳۸۸٤.

Aziz, S., Qaiser, A., Kulsoom,U., & Ahmed, S. (۲۰۲٤). *Fault detection and fault diagnosis in power system using AI: A review*. **Sir Syed University Research Journal of Engineering & Technology, ۱٤(۱),** ۲۷–۳۲.

Upadhyay, A., & Yadav, A. K. (۲۰۲٤). *AI based protection schemes of electrical grid system*. **Acta Scientiae, ۲۵(۲),** ۱۹٦–۲۰۵. Retrieved from

AI-Driven Cybersecurity Framework for Anomaly Detection in Power Systems. (۲۰۲۵). ***Scientific Reports*.**

**Oelhaf, J., Kordowich, G., Pashaei, M., Bergler, C., Maier, A., Jäger, J., & Bayer, S.** (۲۰۲۵). *A scoping review of machine learning applications in power system protection and disturbance management. International Journal of Electrical Power & Energy Systems*, ۱۷۲, ۱۱۱۲۵۷.

**Vignes, V. M., Sri Harini, M. P., Rahul Satheesh & Vipin Das, Padmanaban, S.** (۲۰۲۵). *AI-driven cybersecurity framework for anomaly detection in power systems. Scientific Reports*, ۱۵, Article ۳۵۵۰۶.

**Henao, F., & Edgell, R.** (۲۰۲۵). *AI in power systems: a systematic review of key matters of concern. Energy Informatics*, ۸, Article ۷۶.

Amani,F., Ardali,F.,&Kargarian,A.(۲۰۲۶). Event-Driven Deep RL Dispatcher for Post-Storm Distribution System Restoration.arXiv preprint arXiv:۲۶۰۱-۱۰۰۴۴.

Wörsdörfer, M. (۲۰۲۶). Ten reasons why—the case for more and better AI regulation. *AI and Ethics*, *6*(۱), ۶۲.

Ncube, P. D., Dzvapatsva, G. P., Matobobo, C., & Ranga, M. M. (۲۰۲۶). Redefining student assessment in AI-infused learning environments: a systematic review of challenges and strategies for academic integrity. *AI and Ethics*, *6*(۱), ۶۸.

Kassar, M., & Jizi, M. (۲۰۲۶). Artificial intelligence and robotic process automation in auditing and accounting: a systematic literature review. *Journal of Applied Accounting Research*, *27*(۱), ۲۱۷-۲۴۱.

Sarun, H., Rotana, S., & Chhunla, C. (۲۰۲۶). The Role and Significance of Artificial Intelligence in Transforming Modern Society: Opportunities, Challenges, and Future Directions. *Journal of Agriculture and Environment*, *3*(۱), ۱۳۳-۱۴۱.

Khalil, R. A., Ahmad, K., & Ali, H. (۲۰۲۶). Redefining Elderly Care with Agentic AI: challenges and opportunities. *IEEE Open Journal of the Computer Society*.

Al Battashi, M. A., Adnan, M. A., Jamil, A. I. B., & Al-Battashi, M. A. (۲۰۲۶). Mapping Research Trends in AI-Driven Personalized Learning Pathways: A Scoping Review. *Generators, Bots, and Tutors: Creative Approaches to Human-AI Synergy in Classroom Instruction*, ۱-۳۰.

Adadi, A., & Berrada, M. (۲۰۱۸). *Peeking inside the black-box: A survey on explainable artificial intelligence (XAI).* IEEE Access, ۶, ۵۲۱۳۸–۵۲۱۶۰.

Arrieta, A. B., et al. (۲۰۲۰). *Explainable Artificial Intelligence (XAI): Definitions, taxonomies, fundamentals, and challenges.* Information Fusion, ۵۸, ۸۲–۱۱۵.

Haque, A. K. M. B. (۲۰۲۳). *Explainable AI (XAI) from an end user perspective: A systematic literature review.* Technological Forecasting and Social Change, ۱۸٦, ۱۲۲۰٦٤.

Kilaru,M.,Potluri,R.M.,&Khan,R.(۲۰۲٥).Application of Explainable Artificial Intelligence(XAI) and Blochchain Technology in Indian Sustainable,Green Supply Chain Management Practices.In Explainable AI and Blochchain for Secure and Agile Supply Chains(pp.۱۲۹-۱٤۱). Chapman and Hall/CRC.