--Iranian Energy Economics Research ---------
Vol(issue), PP.
jiee.atu.ac.ir
DOI:

ATU PRESS

Review

Received: 05 / October/ 2025
28/ June /2026 Accepted:
ISSN:
eISSN:

A Structured Review of Electricity Consumption Anomaly Detection Approaches with an Emphasis on Unauthorized Consumption in Smart Grids

Nima Abdi — M.Sc. Student in Computer Science, Allameh Tabataba'i University, Tehran, Iran

Fereshteh Azadi Parand* — Associate Professor, Computer Science Dept., Faculty of Computer, Statistic, Mathematics, Allameh Tabataba'i University, Tehran, Iran.

Sepehr Mehregan — M.Sc. Student in Computer Science, Allameh Tabataba'i University, Tehran, Iran

Iman Sharei — M.Sc. Student in Computer Science, Allameh Tabataba'i University, Tehran, Iran

Abstract

Unauthorized electricity consumption and electricity theft are among the most important forms of non-technical losses in electricity distribution networks. In consumption data, they may appear as deviations from normal consumption patterns, abnormal load variations, or discrepancies between delivered and recorded energy. In addition to imposing economic losses on electric utilities, these phenomena affect grid stability, consumption monitoring, and energy policy. This paper provides a structured review of data-driven approaches to electricity consumption anomaly detection in smart grids, with an emphasis on unauthorized consumption and the Iranian context. Statistical methods, machine learning, deep learning, federated learning, and hybrid approaches based on smart meter data are reviewed and compared in terms of data requirements, detection capability, scalability, privacy, implementation cost, and practical limitations. The reviewed studies indicate that hybrid approaches, particularly those combining smart meter data with machine learning and deep learning algorithms, have greater potential to reduce detection errors and identify complex patterns of unauthorized consumption. However, their effective application in Iran depends on the development of smart metering infrastructure, access to reliable data, attention to security and privacy, and the design of corrective policies consistent with energy justice.

Keywords: Smart Grid, Smart Meter, Anomaly Detection, Unauthorized Electricity Consumption, Non-Technical Losses

JEL Classification: Q41, Q48, L94, C45

* Corresponding Author: parand@atu.ac.ir

--پژوهشنامه اقتصاد انرژی ایران---------
دوره ؟، شماره ؟، تابستان، سال ۱۴۰۵، ص ص
jiee.atu.ac.ir
DOI:

مقاله مروری
تاریخ دریافت: ۱۴۰۴/۰۷/۱۳
تاریخ پذیرش: ۱۴۰۵/۰۴/۰۷
ISSN:
eISSN:

مرور ساختاریافته راهکارهای تشخیص ناهنجاری مصرف برق با تأکید بر مصرف غیرمجاز در شبکه‌های هوشمند

نیما عبدی — دانشجوی کارشناسی ارشد رشته علوم کامپیوتر، دانشگاه علامه طباطبائی، تهران، ایران

فرشته آزادی پرند* — دانشیار رشته علوم کامپیوتر، دانشگاه علامه طباطبائی، تهران، ایران

سپهر مهرگان — دانشجوی کارشناسی ارشد رشته علوم کامپیوتر، دانشگاه علامه طباطبائی، تهران، ایران

ایمان شارعی — دانشجوی کارشناسی ارشد رشته علوم کامپیوتر، دانشگاه علامه طباطبائی، تهران، ایران

چکیده

مصرف غیرمجاز برق و برق‌دزدی از مهم‌ترین مصادیق تلفات غیرفنی در شبکه‌های توزیع برق هستند که می‌توانند در داده‌های مصرف به‌صورت انحراف از الگوی عادی مصرف، تغییرات غیرمتعارف بار، یا اختلاف میان انرژی تحویلی و انرژی ثبت‌شده ظاهر شوند. این پدیده‌ها علاوه بر ایجاد زیان اقتصادی برای شرکت‌های برق، بر پایداری شبکه، پایش مصرف و سیاست‌گذاری انرژی نیز اثرگذار است. هدف این مقاله، ارائه یک مرور ساختاریافته از راهکارهای داده‌محور تشخیص ناهنجاری مصرف در شبکه‌های هوشمند برق با تأکید بر مصرف غیرمجاز و شرایط ایران است. در این راستا، روش‌های آماری، یادگیری ماشین، یادگیری عمیق، یادگیری ائتلافی و رویکردهای ترکیبی مبتنی بر کنتورهای هوشمند بررسی و از نظر نوع داده موردنیاز، قابلیت تشخیص، مقیاس‌پذیری، حریم خصوصی، هزینه پیاده‌سازی و محدودیت‌های کاربردی مقایسه می‌شوند. یافته‌های مرور نشان می‌دهد که روش‌های ترکیبی، به‌ویژه ترکیب داده‌های کنتور هوشمند با الگوریتم‌های یادگیری ماشین و یادگیری عمیق، در مطالعات پیشین ظرفیت بیشتری برای کاهش خطای تشخیص و شناسایی الگوهای پیچیده مصرف غیرمجاز داشته‌اند؛ بااین‌حال، به‌کارگیری مؤثر آن‌ها در ایران به توسعه زیرساخت کنتورهای هوشمند، دسترسی به داده‌های معتبر، توجه به امنیت و حریم خصوصی، و طراحی سیاست‌های اصلاحی سازگار با عدالت انرژی وابسته است.

کلیدواژه‌ها: شبکه هوشمند برق، کنتور هوشمند، تشخیص ناهنجاری، مصرف غیرمجاز برق، تلفات غیرفنی

طبقه‌بندی جی‌ای‌ال: Q41, Q48, L94, C45

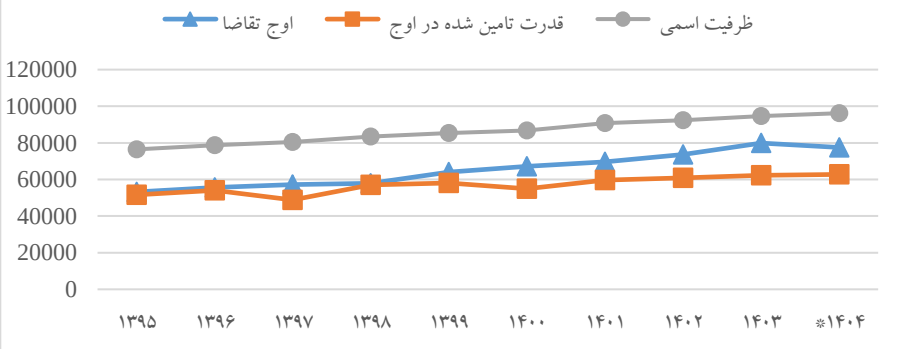
* نویسنده مسئول: parand@atu.ac.ir

۱. مقدمه

انرژی برق یکی از زیرساخت‌های اصلی توسعه صنعتی و اقتصادی است و در سال‌های اخیر، رشد شهرنشینی، گسترش فعالیت‌های صنعتی و برقی‌سازی بخش‌های مختلف اقتصاد، موجب افزایش تقاضای جهانی برق شده است (IEA, 2025). مدیریت این تقاضا، به‌ویژه در کشورهای در حال توسعه مانند ایران، چالشی بزرگ است(Ghorbani & Fartash, 2023; IEA, 2025). همان‌گونه که در شکل ۱ قابل مشاهده است، ظرفیت اسمی تولید برق ایران طی سال‌های ۱۳۹۵ تا ۱۴۰۴ روندی افزایشی داشته است؛ بااین‌حال، رشد اوج تقاضا در سال‌های اخیر سریع‌تر از رشد قدرت تأمین‌شده در زمان اوج بوده و همین مسئله شکاف میان نیاز مصرف و توان قابل تأمین را برجسته‌تر کرده است (مرکز پژوهش‌های مجلس شورای اسلامی، ۱۴۰۳؛ توانیر، ۱۴۰۳).

رکوردشکنی‌های پیاپی مصرف برق در بازه ۱۹ تیر تا ۲ مرداد ۱۴۰۳ (خبرگزاری تسنیم، ۱۴۰۳)، نشان می‌دهد که بار شبکه در دوره‌های گرم سال به‌شدت تحت فشار قرار می‌گیرد. افزون بر این، استخراج رمزارزها نیز به‌عنوان یکی از عوامل افزایش مصرف برق، می‌تواند مدیریت اوج مصرف را دشوارتر کند (Hajiaghapour-Moghimi et al., 2024). این شرایط، ضرورت تقویت زیرساخت‌های سنجش و پایش داده‌محور مصرف را برجسته می‌کند تا بتوان الگوهای غیرعادی را شناسایی و مصرف عادی را از مصرف مشکوک یا غیرمجاز تفکیک کرد.

شکل ۱. روند ظرفیت اسمی، قدرت تأمین شده در اوج و اوج تقاضای برق ایران طی سال‌های ۱۳۹۵ الی ۱۴۰۴



مأخذ: آمار تفصیلی صنعت برق ایران و گزارش‌های پایش شاخص‌های کلان بخش برق مرکز پژوهش‌های مجلس شورای اسلامی (مرکز پژوهش‌های مجلس شورای اسلامی، ۱۴۰۳، ۱۴۰۴؛ توانیر، ۱۴۰۳). داده ۱۴۰۴ مربوط به شش‌ماهه نخست سال است.

شبکه‌های هوشمند برق با فراهم‌کردن داده‌های دقیق‌تر از وضعیت مصرف و عملکرد شبکه، امکان پایش و تحلیل الگوهای غیرعادی را نسبت به شبکه‌های سنتی افزایش می‌دهند (Fang et al., 2012; Gungor et al., 2011). بااین‌حال، تلفات غیرفنی همچنان یکی از چالش‌های مهم شبکه‌های توزیع است و مصرف غیرمجاز، دستکاری تجهیزات اندازه‌گیری و خطاهای ثبت مصرف از مصادیق اصلی آن به‌شمار می‌روند (Depuru et al., 2011; Messinis & Hatziargyriou, 2018). در ایران نیز، با وجود افزایش ظرفیت نصب‌شده نیروگاهی، فاصله میان اوج تقاضا و قدرت تأمین‌شده در زمان اوج نشان می‌دهد که مسئله ناترازی برق همچنان پابرجاست. ازاین‌رو، توسعه روش‌های داده‌محور برای تشخیص مصرف مشکوک می‌تواند به کاهش هزینه‌های نظارت، بهبود مدیریت مصرف و تقویت پایداری شبکه کمک کند (Messinis & Hatziargyriou, 2018; Zheng et al., 2018).

سازوکارهای نظارتی سنتی، به‌ویژه در مقیاس گسترده شبکه توزیع، برای شناسایی همه مصادیق مصرف غیرمجاز محدودیت دارند. بخشی از مصرف غیرمجاز می‌تواند از طریق دستکاری کنتورها، تغییر مسیر اندازه‌گیری یا استفاده از تجهیزات مداخله‌گر در ثبت مصرف رخ دهد (Depuru et al., 2011; Messinis & Hatziargyriou, 2018). این موارد، در صورت نبود داده‌های دقیق و سامانه‌های پایش کافی، به افزایش تلفات غیرفنی و دشواری مدیریت شبکه منجر می‌شوند. در چنین شرایطی، اصلاح هدفمند سیاست‌های یارانه‌ای، تقویت نظارت با کنتورهای هوشمند، به‌کارگیری الگوریتم‌های تشخیص ناهنجاری و هوشمندسازی تدریجی شبکه می‌تواند در کاهش تلفات غیرفنی و بهبود کارایی شبکه نقش داشته باشد.

با وجود گسترش مطالعات مربوط به شبکه‌های هوشمند برق، کنتورهای هوشمند و روش‌های تشخیص ناهنجاری، همچنان نیاز به مروری ساختاریافته وجود دارد که مسئله مصرف غیرمجاز برق را نه‌فقط از منظر دقت الگوریتم‌ها، بلکه از منظر نوع داده، هزینه پیاده‌سازی، مقیاس‌پذیری، حریم خصوصی و قابلیت اجرا در شرایط ایران بررسی کند (Alkuwari et al., 2022; Messinis & Hatziargyriou, 2018). ازاین‌رو، شکاف

اصلی این پژوهش، نبود یک جمع‌بندی تحلیلی از روش‌های داده‌محور تشخیص مصرف غیرمجاز برق و ارزیابی قابلیت به‌کارگیری آنها در شبکه برق ایران است.

بر این اساس، هدف مقاله حاضر بررسی و طبقه‌بندی راهکارهای تشخیص ناهنجاری مصرف در شبکه‌های هوشمند برق با تأکید بر مصرف غیرمجاز و تلفات غیرفنی است. در این مقاله، منظور از ناهنجاری، انحراف آماری یا رفتاری از الگوی عادی مصرف در داده‌های کنتور یا الگوی بار شبکه است و نه صرفاً وقوع یک تخلف قانونی (Pimentel et al., 2014). بر همین مبنا، برق‌دزدی نه به‌عنوان یک موضوع حقوقی یا اجتماعی مستقل، بلکه به‌عنوان یکی از مصادیق مصرف غیرمجاز بررسی می‌شود که می‌تواند در داده‌های کنتور هوشمند یا الگوی بار مشترکان به‌صورت ناهنجاری قابل تشخیص ظاهر شود. پرسش اصلی پژوهش این است که کدام خانواده از روش‌های تشخیص با توجه به نوع داده، نیاز به داده برچسب‌دار، دقت تشخیص، مقیاس‌پذیری، حریم خصوصی و هزینه پیاده‌سازی، برای شناسایی مصرف غیرمجاز در شبکه‌های هوشمند برق مناسب‌تر است و این روش‌ها در شرایط ایران چه محدودیت‌هایی دارند.

ساختار مقاله به این صورت است: در بخش دوم، مسئله مصرف غیرمجاز برق در ایران و نسبت آن با تلفات غیرفنی، یارانه انرژی و محدودیت زیرساخت‌های نظارتی تبیین می‌شود. در بخش سوم، روش‌شناسی مرور ساختاریافته و معیارهای انتخاب مطالعات توضیح داده می‌شود. در ادامه، مفاهیم پایه شبکه هوشمند، کنتور هوشمند و ناهنجاری مصرف مرور می‌شود و سپس خانواده‌های اصلی روش‌های تشخیص، شامل روش‌های آماری، یادگیری ماشین، یادگیری عمیق، یادگیری ائتلافی و رویکردهای ترکیبی، از منظر قابلیت‌ها و محدودیت‌ها مقایسه می‌شوند. در بخش‌های پایانی نیز مجموعه‌داده‌های پرکاربرد، چالش‌های پیاده‌سازی و دلالت‌های سیاستی برای ایران جمع‌بندی خواهد شد.

۲. بیان مسئله مصرف غیرمجاز برق در ایران

در این مقاله، مصرف غیرمجاز برق به‌عنوان یکی از مصادیق مهم تلفات غیرفنی بررسی می‌شود؛ یعنی وضعیتی که در آن انرژی مصرف‌شده، به‌طور کامل یا صحیح در سامانه اندازه‌گیری و صورت‌حساب ثبت نمی‌شود (Depuru et al., 2011; Messinis & Hatziargyriou, 2018). این پدیده می‌تواند ناشی از انشعاب غیرمجاز پیش از کنتور، دستکاری فیزیکی کنتور، تغییر در مسیر اندازه‌گیری یا ثبت نادرست داده‌های مصرف باشد

(Ali et al., 2023; Depuru et al., 2011; Messinis & Hatziargyriou, 2018). بنابراین، تمرکز این پژوهش بر اثبات حقوقی یا جرم‌شناختی برق‌دزدی نیست، بلکه بر بررسی قابلیت شناسایی الگوهای غیرعادی مصرف در داده‌های کنتور و شبکه متمرکز است. در ایران، تلفات شبکه توزیع همچنان یکی از مسائل مهم بخش برق است (برق‌نیوز، ۱۴۰۳). گزارش‌های منتشرشده در سال ۱۴۰۳، میزان تلفات شبکه توزیع را حدود ۹ تا ۱۰ درصد اعلام کرده‌اند و بخشی از این تلفات به عوامل غیرفنی مانند استفاده غیرمجاز از شبکه، دستکاری تجهیزات اندازه‌گیری و خطاهای ثبت مصرف مربوط می‌شود (برق‌نیوز، ۱۴۰۳؛ Messinis & Hatziargyriou, 2018).

یکی از زمینه‌های اقتصادی مؤثر بر گسترش مصرف غیرمجاز، فاصله قابل توجه میان قیمت فروش برق و هزینه واقعی تأمین آن است. در سال ۱۴۰۵، متوسط قیمت فروش هر کیلووات‌ساعت برق به مشترکان حدود ۸۰۰ تومان اعلام شده، در حالی که قیمت تمام‌شده آن حدود ۱۹۰۰ تومان برآورد شده است (ایرنا، ۱۴۰۵). این شکاف نشان می‌دهد که بخش قابل توجهی از هزینه تأمین برق همچنان در قالب یارانه آشکار یا پنهان پوشش داده می‌شود (ایرنا، ۱۴۰۵؛ Clements et al., 2013). چنین وضعیتی، در کنار ضعف نظارت و محدودیت داده‌های مصرف، می‌تواند انگیزه اقتصادی برای دستکاری کنتورها یا استفاده از انشعاب‌های غیرمجاز را افزایش دهد (Depuru et al., 2011; Messinis & Hatziargyriou, 2018).

بااین‌حال، اصلاح سیاست‌های یارانه‌ای نباید صرفاً به افزایش قیمت برق فروکاسته شود (Clements et al., 2013). در سیاست‌گذاری انرژی، حذف یا کاهش یارانه بدون توجه به فقر انرژی و توان پرداخت خانوارهای آسیب‌پذیر می‌تواند به کاهش عدالت در دسترسی به انرژی منجر شود (Canals Casals et al., 2020; Clements et al., 2013). بخشی از خانوارها حتی در سطح مصرف ضروری نیز نسبت به افزایش قیمت انرژی حساس هستند و تغییر ناگهانی تعرفه می‌تواند فشار اقتصادی بیشتری بر آن‌ها وارد کند. ازاین‌رو، رویکرد مناسب‌تر، اصلاح هدفمند یارانه‌ها همراه با حفظ حمایت از مصرف پایه، طراحی تعرفه‌های پلکانی و استفاده از داده‌های کنتور هوشمند برای تفکیک مصرف عادی از مصرف مشکوک یا غیرمجاز است. چنین رویکردی می‌تواند هم انگیزه مصرف غیرمجاز را کاهش دهد و هم ملاحظات عدالت انرژی را در سیاست‌گذاری برق حفظ کند.

یکی دیگر از عوامل دشواری تشخیص مصرف غیرمجاز در ایران، محدود بودن پوشش کنتورهای هوشمند در مقایسه با تعداد کل مشترکان است. مطابق گزارش‌های منتشرشده تا زمان بازنگری مقاله، بیش از ۵ میلیون دستگاه کنتور هوشمند نصب شده است (برق‌نیوز، ۱۴۰۴ب)؛ این تعداد در مقایسه با حدود ۴۱ میلیون مشترک برق، پوششی در حدود ۱۲ درصد را نشان می‌دهد (برق‌نیوز، ۱۴۰۴الف؛ برق‌نیوز، ۱۴۰۴ب). بنابراین، بخش بزرگی از شبکه توزیع همچنان فاقد داده‌های دقیق، پیوسته و قابل اتکا برای تحلیل الگوی مصرف است (برق‌نیوز، ۱۴۰۴الف؛ برق‌نیوز، ۱۴۰۴ب). در چنین شرایطی، توسعه زیرساخت اندازه‌گیری هوشمند، همراه با طراحی الگوریتم‌های تشخیص متناسب با محدودیت داده، می‌تواند نقش مهمی در شناسایی مصرف غیرمجاز و کاهش تلفات غیرفنی داشته باشد (Ali et al., 2023; Depuru et al., 2011; Messinis & Hatziargyriou, 2018).

بر این اساس، مسئله اصلی صرفاً وجود مصرف غیرمجاز نیست، بلکه دشواری شناسایی آن در شبکه‌ای است که با محدودیت داده، پوشش ناکامل کنتورهای هوشمند، انگیزه‌های اقتصادی ناشی از شکاف قیمتی و ضرورت حفظ عدالت انرژی روبه‌رو است. از این منظر، روش‌های تشخیص ناهنجاری باید نه‌تنها از نظر دقت، بلکه از نظر نیاز به داده برچسب‌دار، هزینه پیاده‌سازی، مقیاس‌پذیری، نرخ مثبت کاذب[1]، حفظ حریم خصوصی و قابلیت اجرا در شرایط شبکه برق ایران ارزیابی شوند. این چارچوب، مبنای بررسی روش‌های تشخیص در بخش‌های بعدی مقاله است (Clements et al., 2013; Messinis & Hatziargyriou, 2018; برق‌نیوز، ۱۴۰۴الف؛ برق‌نیوز، ۱۴۰۴ب).

۳. روش پژوهش: مرور ساختاریافته مطالعات

این پژوهش از نوع مرور ساختاریافته مطالعات است و با هدف شناسایی، غربالگری و تلفیق تحلیلی پژوهش‌های مرتبط با تشخیص ناهنجاری مصرف برق، مصرف غیرمجاز و تلفات غیرفنی در شبکه‌های هوشمند انجام شده است. با توجه به اینکه هدف مقاله حاضر انجام فراتحلیل آماری نیست، بلکه طبقه‌بندی و مقایسه تحلیلی روش‌های موجود از منظر قابلیت کاربرد در شبکه برق ایران است، با الهام از منطق گزارش‌دهی پریزما و اصول مرور ساختاریافته، تنظیم شد (Page et al., 2021; Snyder, 2019; Tricco et al., 2018).

[1] False Positive Rate (FPR)

بر این اساس، پیش از انتخاب مطالعات، پایگاه‌های جست‌وجو، بازه زمانی، کلیدواژه‌ها، معیارهای ورود و خروج و محورهای استخراج داده مشخص شد.

جست‌وجوی اصلی در پایگاه اسکوپوس انجام شد و برای تکمیل منابع، پایگاه‌های ساینس‌دایرکت[1]، آی‌تریپل‌ئی اکسپلور[2] و گوگل اسکالر[3] نیز بررسی شدند. بازه زمانی جست‌وجو از سال ۲۰۱۵ تا ۲۰۲۶ در نظر گرفته شد و آخرین جست‌وجو در خرداد ۱۴۰۵ انجام گرفت. منابع قدیمی‌تر فقط زمانی استفاده شدند که برای تعریف مفاهیم پایه مانند شبکه هوشمند، کنتور هوشمند، تشخیص تازگی یا روش‌های پایه یادگیری ماشین ضروری بودند. کلیدواژه‌های جست‌وجو شامل ترکیبی از معادل‌های فارسی و انگلیسی «شبکه هوشمند برق»، «کنتور هوشمند»، «زیرساخت اندازه‌گیری پیشرفته»، «تشخیص ناهنجاری»، «مصرف غیرمجاز برق»، «برق‌دزدی»، «تلفات غیرفنی»، «تشخیص تقلب»، «یادگیری ماشین»، «یادگیری عمیق»، «یادگیری ائتلافی» و «روش‌های ترکیبی» بود.

معیارهای ورود به مرور شامل ارتباط مستقیم مطالعه با شبکه هوشمند، کنتور هوشمند یا داده‌های مصرف برق؛ تمرکز بر تشخیص ناهنجاری، مصرف غیرمجاز، تقلب یا تلفات غیرفنی؛ ارائه روش، مجموعه‌داده، شاخص ارزیابی یا بحث اجرایی قابل استفاده برای مقایسه؛ انتشار به‌صورت مقاله مجله، مقاله کنفرانس معتبر، گزارش رسمی یا مجموعه‌داده قابل استناد؛ و دسترسی به متن کامل بود. در مقابل، مطالعاتی حذف شدند که صرفاً به توضیح عمومی الگوریتم‌های یادگیری ماشین پرداخته بودند، ارتباط مستقیمی با داده‌های مصرف برق یا شبکه هوشمند نداشتند، فقط از منظر حقوقی، اجتماعی یا اقتصادی به برق‌دزدی پرداخته بودند، متن کامل یا اطلاعات روش‌شناختی کافی نداشتند، یا در پایگاه‌های مختلف تکراری بودند.

فرایند غربالگری در چند مرحله انجام شد. ابتدا رکوردهای بازیابی‌شده از اسکوپوس و منابع تکمیلی تجمیع و موارد تکراری حذف شدند. سپس عنوان و چکیده مطالعات بر اساس معیارهای ورود و خروج بررسی شد. در مرحله بعد، متن کامل مطالعات باقی‌مانده بررسی شد و موارد نامرتبط یا فاقد اطلاعات کافی کنار گذاشته شد. در نهایت، مطالعات منتخب به‌عنوان مبنای تحلیل در بخش‌های بعدی مقاله استفاده شدند. واحد تحلیل در این پژوهش،

[1] ScienceDirect
[2] IEEE Xplore
[3] Google Scholar

مقاله، گزارش رسمی یا مجموعه‌داده مرتبط با تشخیص ناهنجاری مصرف برق بود و به دلیل ماهیت مروری پژوهش، مداخله انسانی یا گردآوری داده میدانی انجام نشد.

استخراج داده‌ها بر چند محور انجام گرفت: نوع داده ورودی، نوع ناهنجاری یا تهدید، خانواده روش تشخیص، شاخص‌های ارزیابی، محدودیت‌های عملی و دلالت‌های اجرایی برای ایران. بر این اساس، از هر مطالعه اطلاعاتی درباره نوع داده مورد استفاده، نوع مسئله، خانواده روش، معیارهای ارزیابی و محدودیت‌های اجرایی استخراج شد. این چارچوب، مبنای مرور مفاهیم پایه و سپس مقایسه روش‌های تشخیص در ادامه مقاله قرار گرفت.

۱.۳ شبکه هوشمند برق

شبکه‌های هوشمند برق سیستمی یکپارچه از تجهیزات، حسگرها و فناوری‌های دیجیتال و ارتباطی هستند که با جمع‌آوری و تحلیل بلادرنگ داده‌ها، امکان مدیریت خودکار و بهینه تولید، انتقال، توزیع و مصرف انرژی را فراهم می‌کند (Fang et al., 2012; Gungor et al., 2011). در چنین شبکه‌ای، تبادل دوطرفه اطلاعات و انرژی میان بخش‌های تولید، انتقال، توزیع و مصرف، امکان پایدارسازی ولتاژ و فرکانس، مدیریت بار و پاسخ‌گویی سریع‌تر به اختلالات را فراهم می‌سازد (Fang et al., 2012; Abrahamsen et al., 2021).

طراحی شبکه هوشمند برق متناسب با اهداف، سطح زیرساخت و ظرفیت‌های فنی هر کشور انجام می‌شود. در این زمینه، مؤسسه ملی استاندارد و فناوری ایالات متحده[1] چارچوبی برای شبکه هوشمند ارائه کرده است که در آن بازیگران و کارکردهای اصلی شبکه در حوزه‌هایی مانند مشتری، بازار، ارائه‌دهنده خدمات، عملیات، تولید، انتقال و توزیع سازمان‌دهی می‌شوند (Gopstein et al., 2021).

[1] NIST

جدول ۱: حوزه‌های اصلی شبکه هوشمند در چارچوب مؤسسه ملی استاندارد و فناوری ایالات متحده[۱]

حوزه	نقش‌ها/خدمات موجود در حوزه
مشتری[۲]	کاربران نهایی برق که ممکن است تولید، ذخیره‌سازی و مدیریت مصرف انرژی را نیز انجام دهند. به‌طور سنتی، سه نوع مشتری با زیرحوزه‌های مربوطه مطرح می‌شوند: **مسکونی**، **تجاری**، و **صنعتی**.
بازارها[۳]	تسهیل‌گران و مشارکت‌کنندگان در بازارهای برق و سایر سازوکارهای اقتصادی که برای تحریک اقدامات و بهینه‌سازی نتایج سیستم استفاده می‌شوند.
ارائه‌دهنده خدمات[۴]	سازمان‌هایی که خدمات را به مشتریان برق و شرکت‌های توزیع ارائه می‌دهند.
عملیات[۵]	مدیران جریان برق در شبکه
تولید (شامل منابع انرژی توزیع‌شده)[۶]	تولیدکنندگان برق که ممکن است انرژی را نیز ذخیره کنند. این حوزه شامل **منابع تولید سنتی** (نیروگاه‌های حرارتی، نیروگاه‌های آبی بزرگ‌مقیاس و مزارع تجدیدپذیر متصل به شبکه انتقال) و **منابع انرژی توزیع‌شده** می‌شود. منابع انرژی توزیع‌شده معمولاً در حوزه‌های مشتری و توزیع (ذخیره‌سازی، پاسخ به تقاضا) یا توسط ارائه‌دهندگان خدمات به‌صورت تجمیع‌شده عمل می‌کنند.
انتقال[۷]	انتقال‌دهندگان برق با ولتاژ بالا در مسافت‌های طولانی که ممکن است برق را ذخیره یا تولید نیز کنند.
توزیع[۸]	توزیع برق به مشتریان و دریافت برق از منابع تولید پراکنده یا ذخیره‌سازهای متصل به شبکه توزیع

بر اساس چارچوب این مؤسسه کنتورهای هوشمند در نقطه اتصال میان حوزه مشتری و حوزه توزیع قرار می‌گیرند و نقش رابط اصلی میان مصرف‌کننده، شرکت توزیع و سامانه‌های عملیاتی شبکه را ایفا می‌کنند. از آنجا که داده‌های ثبت‌شده توسط این کنتورها مبنای اصلی تحلیل الگوی مصرف و تشخیص رفتارهای غیرعادی است، بخش بعدی به بررسی کنتورهای هوشمند اختصاص دارد (Gopstein et al., 2021).

۲.۳ کنتورهای هوشمند

کنتورهای هوشمند نسل جدیدی از تجهیزات اندازه‌گیری انرژی هستند که در شبکه‌های برق هوشمند به‌کار گرفته می‌شوند (Gungor et al., 2011; Abrahamsen et al., 2021). این کنتورها با قابلیت‌های پیشرفته ارتباطی، امکان ثبت و انتقال داده‌های مصرف را

---

[۱] برگرفته از گوپستاین و همکاران (۲۰۲۱)

[2] Customer
[3] Markets
[4] Service Provider
[5] Operation
[6] Generation, including Distributed Energy Resources (DER)
[7] Transmission
[8] Distribution

به‌صورت دوره‌ای یا نزدیک به بلادرنگ برای کاربران و اپراتورهای شبکه فراهم می‌کنند. برخلاف کنتورهای سنتی که تنها میزان کلی مصرف انرژی را ثبت می‌کنند، کنتورهای هوشمند داده‌های تفصیلی‌تری مانند زمان‌بندی مصرف و پروفایل‌های انرژی را ارائه می‌دهند (Gungor et al., 2011).

از منظر تشخیص ناهنجاری، اهمیت اصلی کنتور هوشمند در تولید داده‌های زمانی مصرف است؛ زیرا بسیاری از روش‌های آماری، یادگیری ماشین و یادگیری عمیق برای تفکیک مصرف عادی از مصرف مشکوک یا غیرمجاز، به همین داده‌ها متکی هستند (Messinis & Hatziargyriou, 2018; Zheng et al., 2018). از منظر زیرساخت ارتباطی، کنتورهای هوشمند را می‌توان به سه دسته کلی تقسیم کرد؛ این دسته‌بندی از آن جهت اهمیت دارد که نوع ارتباط بر هزینه پیاده‌سازی، پوشش شبکه، تأخیر ارسال داده و امکان تشخیص سریع ناهنجاری اثر می‌گذارد (Abrahamsen et al., 2021; Gungor et al., 2011).

کنتورهای مبتنی بر پی‌ال‌سی[1]: این کنتورها داده‌ها را از طریق خطوط برق موجود ارسال می‌کنند. هزینه پایین زیرساخت و استفاده از شبکه موجود از مزایای این فناوری است (Artale et al., 2018)، اما اختلالات و محدودیت پهنای باند ممکن است عملکرد ارتباطی آن را مختل کند (Ferreira et al., 2010).

کنتورهای مبتنی بر شبکه‌های بی‌سیم: این کنتورها از فناوری‌هایی مانند زیگبی[2]، لورا[3]، اینترنت اشیای باند باریک[4] یا وای‌فای برای انتقال داده استفاده می‌کنند. بسته به نوع فناوری، این روش می‌تواند برای محیط‌های شهری، مناطق پراکنده یا مکان‌هایی که دسترسی به زیرساخت سیمی دشوار است، مناسب باشد (Abrahamsen et al., 2021; Gungor et al., 2011).

کنتورهای مبتنی بر شبکه سلولی[5]: این کنتورها برای انتقال داده از شبکه‌های تلفن همراه، مانند نسل چهارم و پنجم، استفاده می‌کنند. پوشش گسترده و امکان انتقال داده در مقیاس وسیع از مزایای این فناوری است، اما هزینه‌های عملیاتی و وابستگی به کیفیت پوشش شبکه می‌تواند محدودیت ایجاد کند (Abrahamsen et al., 2021).

---

[1] PLC: Power Line Carrier
[2] Zigbee
[3] LoRa
[4] NB-IoT
[5] Cellular

کنتورهای هوشمند از منظر شیوه ارسال داده نیز به دو دسته کلی تقسیم می‌شوند (Abrahamsen et al., 2021; Gungor et al., 2011).

کنتورهای بلادرنگ[1]: این کنتورها داده‌های مصرف را در بازه‌های زمانی کوتاه ثبت و ارسال می‌کنند و امکان پایش سریع‌تر بار و تشخیص زودهنگام تغییرات غیرعادی را فراهم می‌سازند.

کنتورهای ذخیره‌سازی داده: این کنتورها اطلاعات مصرف را در بازه‌های زمانی مشخص ذخیره کرده و در دوره‌های معین، مانند روزانه یا هفتگی، ارسال می‌کنند. این روش می‌تواند هزینه‌های ارتباطی را کاهش دهد، اما برای تشخیص سریع ناهنجاری‌های کوتاه‌مدت محدودیت بیشتری دارد.

انتخاب نوع کنتور هوشمند به کاربرد، زیرساخت ارتباطی، تراکم مشترکان، هزینه پیاده‌سازی و نیاز زمانی سامانه تشخیص بستگی دارد (Abrahamsen et al., 2021; Gungor et al., 2011). در کاربردهایی که تشخیص سریع ناهنجاری و مدیریت بار اهمیت بیشتری دارد، کنتورهای دوطرفه با قابلیت ارسال داده در بازه‌های کوتاه مناسب‌ترند؛ اما در مناطق دورافتاده یا کم‌تراکم، فناوری‌های کم‌مصرف یا کنتورهای ذخیره‌سازی داده می‌توانند گزینه عملی‌تری باشند. در ایران، محدود بودن پوشش کنتورهای هوشمند باعث می‌شود کیفیت، پیوستگی و دسترس‌پذیری داده‌های مصرف یکی از محدودیت‌های اصلی اجرای روش‌های تشخیص ناهنجاری باشد (برق‌نیوز، ۱۴۰۴الف؛ برق‌نیوز، ۱۴۰۴ب).

۳.۳ سامانه نظارت، کنترل و گردآوری داده‌های شبکه برق[2]

کنتورهای هوشمند داده‌های مصرف مشترکان را فراهم می‌کنند، اما پایش وضعیت عملیاتی شبکه به داده‌هایی مانند ولتاژ، جریان، وضعیت تجهیزات، رخدادهای حفاظتی و فرمان‌های کنترلی نیز نیاز دارد (Stouffer et al., 2023). این داده‌ها معمولاً از طریق سامانه اسکادا گردآوری و پایش می‌شوند. اسکادا سامانه‌ای برای کنترل نظارتی و گردآوری داده در زیرساخت‌های صنعتی و شبکه‌های برق است و در نیروگاه‌ها، پست‌های برق و شبکه‌های توزیع برای مشاهده وضعیت تجهیزات و پشتیبانی از تصمیم‌گیری بهره‌برداران استفاده می‌شود (Stouffer et al., 2023).

---

[1] Real-Time Meters
[2] SCADA: Supervisory Control and Data Acquisition

معماری اسکادا معمولاً از حسگرها، تجهیزات اندازه‌گیری، واحدهای پایانه‌ای، کنترل‌گرهای منطقی و مرکز کنترل تشکیل می‌شود (Stouffer et al., 2023). داده‌های گردآوری‌شده در مرکز کنترل برای پایش لحظه‌ای، ثبت رخدادها، تحلیل روندهای عملیاتی و پشتیبانی از تصمیم‌گیری استفاده می‌شوند. در صورت اتصال این داده‌ها به روش‌های آماری یا مدل‌های یادگیری ماشین، امکان تفکیک بهتر رفتار عادی شبکه از رویدادهای غیرعادی، مانند تغییرات غیرمعمول بار، خطاهای تجهیزاتی یا داده‌های مشکوک، فراهم می‌شود (Nguyen et al., 2025; Zibaeirad et al., 2024).

در کاربردهای عملی، داده‌های اسکادا می‌توانند برای تولید هشدار، اولویت‌بندی رخدادها و پشتیبانی از اقدامات اصلاحی استفاده شوند. بااین‌حال، اتصال این سامانه‌ها به شبکه‌های ارتباطی، سطح حمله سایبری را افزایش می‌دهد و ممکن است خود سامانه پایش و کنترل را به هدف حمله تبدیل کند. بنابراین، امنیت ارتباطات، کنترل دسترسی و حفاظت از داده‌های عملیاتی، پیش‌شرط استفاده قابل‌اعتماد از داده‌های اسکادا در تشخیص ناهنجاری و مدیریت شبکه است (Nguyen et al., 2025; Stouffer et al., 2023).

٤ ناهنجاری در داده‌های شبکه هوشمند برق و عوامل مؤثر بر تشخیص آن

در این مقاله، ناهنجاری به معنای انحراف آماری یا رفتاری از الگوی عادی داده‌های مصرف یا وضعیت عملیاتی شبکه است (Pimentel et al., 2014; Fährmann et al., 2024). شناسایی ناهنجاری ابتدا به تعریف وضعیت عادی نیاز دارد. این وضعیت می‌تواند بر اساس متغیرهایی مانند الگوی بار، توان مصرفی، ولتاژ، فرکانس، زمان مصرف و رفتار تاریخی مشترک تعیین شود. بنابراین، هر تغییر غیرمعمول الزاماً ناهنجاری محسوب نمی‌شود (Pimentel et al., 2014; Fährmann et al., 2024)؛ زیرا بخشی از تغییرات مصرف می‌تواند ناشی از نوسانات طبیعی، شرایط آب‌وهوایی، تعطیلات یا تغییرات عادی رفتار مصرف‌کننده باشد. بنابراین، در این مقاله ناهنجاری به‌عنوان یک نشانه داده‌ای برای بررسی بیشتر تلقی می‌شود، نه به‌عنوان اثبات قطعی مصرف غیرمجاز.

تعیین وضعیت عادی می‌تواند با روش‌های ساده آماری، مانند میانگین متحرک و انحراف معیار، یا با مدل‌های پیشرفته‌تر یادگیری ماشین انجام شود (Ahmed et al., 2016; Pimentel et al., 2014). در هر دو حالت، هدف اصلی تعیین آستانه یا مرز تصمیمی است که رفتار عادی را از رفتار غیرعادی یا مشکوک جدا کند (Miljković, 2010; Pimentel

et al., 2014). بااین‌حال، مشاهده ناهنجاری در داده‌های مصرف به‌تنهایی به معنای اثبات مصرف غیرمجاز نیست، بلکه نشانه‌ای برای بررسی بیشتر، تطبیق با داده‌های عملیاتی و ارزیابی میدانی است.

از سوی دیگر، داده‌های شبکه هوشمند ممکن است تحت تأثیر خطاهای تجهیزاتی، اختلالات ارتباطی یا حملات سایبری قرار گیرند. برای مثال، تزریق داده نادرست می‌تواند داده‌های مصرف یا وضعیت شبکه را تغییر دهد و در نتیجه، دقت الگوریتم‌های تشخیص ناهنجاری را کاهش دهد (Zibaeirad et al., 2024). ازاین‌رو، در ادامه، آسیب‌پذیری‌های اصلی شبکه و کنتور هوشمند از منظر فیزیکی، سایبری و الگوریتمی مرور می‌شود.

۱.٤ آسیب‌پذیری‌های مؤثر بر تشخیص ناهنجاری در شبکه و کنتور هوشمند

دقت روش‌های تشخیص ناهنجاری به کیفیت، صحت و پیوستگی داده‌های کنتور هوشمند و سامانه‌های پایش شبکه وابسته است (Nguyen et al., 2025; Stouffer et al., 2023). دستکاری فیزیکی کنتور، اختلال ارتباطی، تزریق داده نادرست یا حمله به مدل‌های تشخیص می‌تواند باعث ایجاد هشدار نادرست، پنهان‌ماندن مصرف مشکوک یا کاهش قابلیت اعتماد نتایج شود (Nguyen et al., 2025; Zibaeirad et al., 2024; Zhu et al., 2023). از این منظر، آسیب‌پذیری‌های مرتبط با شبکه و کنتور هوشمند را می‌توان در سه گروه فیزیکی، سایبری و الگوریتمی دسته‌بندی کرد. جدول ۲ نمونه‌های اصلی این آسیب‌پذیری‌ها و اثر آنها بر داده و تشخیص ناهنجاری را نشان می‌دهد.

جدول ۲. نمونه آسیب‌پذیری‌های مؤثر بر داده و تشخیص ناهنجاری در شبکه هوشمند برق

حمله/آسیب‌پذیری	لایه	توضیحات	منابع مرتبط
دستکاری فیزیکی کنتور و سیم‌کشی[1]	فیزیکی	اتصال غیرمجاز، تغییر مسیر اندازه‌گیری، تغییر تنظیمات داخلی یا خرابکاری سخت‌افزاری کنتور می‌تواند موجب ثبت ناقص یا نادرست مصرف و پنهان‌ماندن مصرف مشکوک شود.	(Jeffin et al., 2020; Nguyen et al., 2025)
خرابکاری یا خرابی تجهیزات اندازه‌گیری[2]	فیزیکی	آسیب عمدی یا خرابی سنسورها، کابل‌ها و تجهیزات کنترلی می‌تواند داده ناقص، غیرواقعی یا الگوهای مشابه ناهنجاری تولید کند و تفکیک خطای تجهیزاتی از مصرف غیرمجاز را دشوار سازد	(Nguyen et al., 2025; Stouffer et al., 2023)
شنود، بازپخش و حمله مرد میانی[3]	ارتباطی	رهگیری، بازپخش یا تغییر پیام‌ها و بسته‌های داده در مسیر ارتباطی می‌تواند حریم خصوصی مشترکان را تهدید کرده و صحت داده‌های مصرف یا فرمان‌های کنترلی را کاهش دهد	(Nguyen et al., 2025; Zibaeirad et al., 2024)
انکار سرویس[4]	ارتباطی	اشباع کانال پی‌ال‌سی یا شبکه‌های بی‌سیم با ترافیک جعلی برای قطع ارتباط. می‌تواند باعث قطع، تأخیر یا ناقص‌شدن داده‌ها و اختلال در تشخیص سریع ناهنجاری شود.	(Ortega-Fernandez & Liberati, 2023; Nguyen et al., 2025)
تزریق داده جعلی[5]	داده	ارسال یا ثبت مقادیر غیرواقعی مصرف یا وضعیت شبکه می‌تواند الگوی مصرف جعلی ایجاد کند، مصرف مشکوک را پنهان سازد یا نرخ خطای تشخیص را افزایش دهد.	(Lin et al., 2023; Nguyen et al., 2025)
نصب بدافزار در کنتور یا سامانه کنترل[6]	نرم‌افزاری	بارگذاری نرم‌افزار مخرب روی کنتور، درگاه ارتباطی یا سرور کنترل می‌تواند موجب حذف، تغییر، تأخیر یا دستکاری داده‌های مورد استفاده در تشخیص ناهنجاری شود.	(Bouramdane, 2023; Nguyen et al., 2025; Stouffer et al., 2023)
مسموم‌سازی داده و حمله خصمانه[7]	الگوریتم	تزریق داده آلوده در فرایند آموزش یا ایجاد تغییرات کوچک در ورودی مدل می‌تواند باعث کاهش دقت، افزایش مثبت کاذب یا طبقه‌بندی نادرست نمونه‌های مصرف شود.	(Zhu et al., 2023; Bouramdane, 2023)
حملات به مدل در یادگیری توزیع‌شده یا ائتلافی[8]	الگوریتم	ارسال به‌روزرسانی‌های نادرست از سوی گره‌های مخرب، استنتاج داده‌های آموزشی یا استخراج مدل می‌تواند اعتمادپذیری، محرمانگی و پایداری مدل‌های تشخیص ناهنجاری را کاهش دهد.	(Zhang et al., 2026; Zhao et al., 2025)

[1] Wiring Tampering / Hardware Tampering
[2] Sabotage / Equipment Damage
[3] Replay Attack / Man-in-the-Middle Attack
[4] Denial of Service / Distributed Denial of Service
[5] False Data Injection
[6] Malware Deployment
[7] Data Poisoning / Adversarial Attack
[8] Byzantine Faults / Membership Inference / Model Extraction

۱.۱.٤ آسیب‌پذیری‌های فیزیکی

در آسیب‌پذیری‌های فیزیکی، دستکاری سیم‌کشی، تغییر مسیر اندازه‌گیری یا خرابکاری سخت‌افزاری کنتور می‌تواند موجب ثبت ناقص یا نادرست مصرف شود (Jeffin et al., 2020; Nguyen et al., 2025; Stouffer et al., 2023). افزون بر حملات عمدی، خرابی طبیعی حسگرها و تجهیزات اندازه‌گیری نیز ممکن است داده‌هایی مشابه رفتار غیرعادی تولید کند. بنابراین، سامانه تشخیص باید تا حد امکان میان مصرف مشکوک، خطای تجهیزاتی و تغییرات عادی مصرف تمایز قائل شود.

۲.۱.٤ حملات سایبری

در آسیب‌پذیری‌های سایبری، ضعف لایه‌های ارتباطی و داده‌ای می‌تواند موجب شنود، بازپخش، تغییر یا تزریق داده‌های مصرف و وضعیت شبکه شود (Bouramdane, 2023; Nguyen et al., 2025; Ortega-Fernandez & Liberati, 2023). چنین حملاتی نه‌تنها حریم خصوصی مشترکان را تهدید می‌کنند، بلکه می‌توانند الگوهای جعلی در داده ایجاد کرده یا داده‌های واقعی مصرف غیرمجاز را پنهان کنند. ازاین‌رو، امنیت ارتباطات، احراز هویت و کنترل دسترسی برای قابل اعتماد بودن نتایج تشخیص ناهنجاری ضروری است.

۳.۱.٤ حملات علیه مدل‌های هوش مصنوعی

با ورود یادگیری ماشین و یادگیری عمیق به فرآیند تشخیص ناهنجاری، خود داده آموزشی و مدل تشخیص نیز به سطح حمله تبدیل می‌شوند. در حملاتی مانند مسموم‌سازی داده[1]، نمونه‌های آلوده وارد فرایند آموزش می‌شوند و در حملات خصمانه، تغییرات کوچک در ورودی می‌تواند خروجی مدل را به‌اشتباه تغییر دهد (Zhang et al., 2026; Zhu et al., 2023). در محیط‌های توزیع‌شده یا یادگیری ائتلافی نیز ارسال به‌روزرسانی‌های نادرست از سوی گره‌های مخرب می‌تواند عملکرد مدل را تضعیف کند. بنابراین، ارزیابی روش‌های تشخیص باید علاوه بر دقت، به مقاومت مدل در برابر داده آلوده و حملات الگوریتمی نیز توجه کند.

[1] Data Poisoning

۲.٤ طبقه‌بندی روش‌های تشخیص ناهنجاری مصرف

در تشخیص ناهنجاری مصرف برق، باید میان الگوی جدید و الگوی واقعاً غیرعادی تمایز گذاشت. برای مثال، تغییر مصرف یک مشترک ممکن است ناشی از تغییر فصل، تغییر الگوی کاری، اضافه‌شدن یک وسیله پرمصرف یا تغییر تعداد ساکنان باشد و الزاماً به معنای مصرف غیرمجاز نیست. ازاین‌رو، روش‌های تشخیص معمولاً با تعیین آستانه تصمیم[1] یا امتیاز ناهنجاری[2]، رفتار عادی، رفتار جدید و رفتار مشکوک را از یکدیگر تفکیک می‌کنند (Miljković, 2010; Pimentel et al., 2014)؛ اما این تفکیک باید با داده‌های تکمیلی و ارزیابی میدانی تفسیر شود.

روش‌های تشخیص ناهنجاری مصرف را می‌توان به سه گروه کلی تقسیم کرد: بررسی دستی، روش‌های آستانه‌گذاری و آماری، و روش‌های داده‌محور مبتنی بر یادگیری ماشین یا یادگیری عمیق (Ahmed et al., 2016; Fährmann et al., 2024; Pimentel et al., 2014). جدول ۳ این سه گروه را از نظر مقیاس‌پذیری، قابلیت تشخیص سریع، دقت و هزینه پیاده‌سازی مقایسه می‌کند. بر این اساس، انتخاب روش تشخیص تنها به دقت مدل وابسته نیست، بلکه به کیفیت داده، وجود یا نبود برچسب، هزینه اجرا، نرخ خطای مثبت کاذب، امکان پردازش سریع و محدودیت‌های زیرساختی شبکه نیز بستگی دارد.

جدول ۳: مقایسه کلی گروه‌های اصلی تشخیص ناهنجاری مصرف برق

	دستی	آستانه‌گذاری ثابت	یادگیری ماشین/یادگیری عمیق
مقیاس‌پذیری	پایین	متوسط	بالا، مشروط به زیرساخت پردازش و داده
تشخیص بلادرنگ	پایین	بالا برای الگوهای ساده	وابسته به مدل، داده و زیرساخت ارتباطی
دقت تشخیص	وابسته به تجربه کارشناس	مناسب برای تغییرات آشکار و قواعد ساده	مناسب برای الگوهای پیچیده و غیرخطی
هزینه پیاده‌سازی	پایین تا متوسط	متوسط	متوسط تا بالا
هزینه نگه‌داری	بالا	متوسط	وابسته به کیفیت داده، آموزش مجدد و به‌روزرسانی مدل
محدودیت اصلی	خطای انسانی و مقیاس‌پذیری پایین	حساسیت به آستانه ثابت و تغییر الگوی مصرف	نیاز به داده کافی، تنظیم مدل و کنترل خطای مثبت کاذب

[1] Novelty Score
[2] Anomaly Score

۱.۲.٤ روش‌های آستانه‌گذاری و آماری

در این دسته از روش‌ها، برای شناسایی ناهنجاری از معیارهایی مانند میانگین، انحراف معیار، نسبت‌های آماری، آزمون‌های فرضیه و آستانه‌های ثابت یا پویا استفاده می‌شود (Ahmed et al., 2016; Pimentel et al., 2014). برای مثال، در داده‌های مصرف برق می‌توان با استفاده از میانگین متحرک یا تعیین مرزهای آستانه، رفتار عادی مصرف را از تغییرات غیرعادی یا مشکوک تفکیک کرد. با وجود سادگی و سرعت محاسبات، این روش‌ها معمولاً در برابر تغییرات تدریجی، الگوهای فصلی و رفتارهای پیچیده مصرف محدودیت دارند.

به‌عنوان نمونه، پاسرینی و تونلو (۲۰۱۹) استفاده از مودم‌های خط برق را به‌عنوان حسگر در شبکه‌های هوشمند برای تشخیص و مکان‌یابی ناهنجاری‌هایی مانند تغییرات امپدانس و نقص‌های الکتریکی بررسی کردند. در این روش، اندازه‌گیری‌های جاری با مقدار مرجع مقایسه می‌شود و عبور اختلاف یا نسبت اندازه‌گیری‌ها از آستانه‌ای مشخص، نشانه وقوع ناهنجاری در نظر گرفته می‌شود. این نمونه نشان می‌دهد که روش‌های آستانه‌گذاری می‌توانند برای تشخیص سریع و کم‌هزینه برخی ناهنجاری‌های فنی مفید باشند؛ بااین‌حال، کارایی آنها به انتخاب آستانه مناسب و پایداری شرایط مرجع وابسته است.

بنابراین، روش‌های آستانه‌گذاری و آماری به دلیل سادگی، سرعت و هزینه کمتر، برای پایش اولیه و شرایطی که الگوی عادی مصرف پایدار است مناسب‌اند؛ اما در صورت تغییر رفتار مصرف، وجود داده‌های نامتوازن یا پیچیده‌شدن الگوهای مصرف غیرمجاز، احتمال مثبت کاذب، منفی کاذب و کاهش دقت افزایش می‌یابد (Ahmed et al., 2016; Pimentel et al., 2014). همین محدودیت‌ها زمینه استفاده از روش‌های داده‌محور مانند یادگیری ماشین و یادگیری عمیق را فراهم می‌کند.

۲.۲.٤ روش‌های مبتنی بر یادگیری ماشین و یادگیری عمیق

در تشخیص ناهنجاری مصرف برق، روش‌های یادگیری ماشین و یادگیری عمیق زمانی اهمیت می‌یابند که الگوهای مصرف، غیرخطی، زمان‌مند یا متأثر از متغیرهای متعدد باشند (Ahmed et al., 2016; Alkuwari et al., 2022; Fährmann et al., 2024). این روش‌ها می‌توانند از داده‌های کنتور هوشمند، الگوی بار، ویژگی‌های زمانی و داده‌های

عملیاتی برای تفکیک رفتار عادی از رفتار مشکوک استفاده کنند. بااین‌حال، کارایی آنها به کیفیت داده، وجود داده برچسب‌دار، نامتوازنی نمونه‌های عادی و غیرعادی، هزینه پردازش و کنترل خطای مثبت کاذب وابسته است.

روش‌های یادگیری ماشین کلاسیک شامل رویکردهای نظارت‌شده، بدون‌نظارت و نیمه‌نظارتی هستند. در تشخیص ناهنجاری مصرف، روش‌های نظارت‌شده زمانی کاربرد دارند که نمونه‌های عادی و غیرعادی برچسب‌گذاری شده باشند؛ در مقابل، روش‌های بدون‌نظارت برای شرایطی مناسب‌اند که داده برچسب‌دار محدود یا در دسترس نباشد.

ماشین بردار پشتیبان[1] و نسخه‌های یک‌کلاسه آن از روش‌های رایج برای تفکیک نمونه‌های عادی از نمونه‌های دورافتاده هستند. در مسئله تشخیص ناهنجاری مصرف برق، این روش‌ها به‌ویژه زمانی مفیدند که حجم داده محدود باشد یا هدف، تعیین مرزی میان رفتار عادی و رفتار مشکوک باشد. مزیت اصلی آنها توانایی مدل‌سازی مرزهای غیرخطی با استفاده از توابع هسته است؛ اما کارایی آنها به انتخاب هسته، تنظیم پارامترها و حساسیت آستانه وابسته است. همچنین در داده‌های بزرگ کنتورهای هوشمند، پیچیدگی محاسباتی و نیاز به تنظیم دقیق می‌تواند کاربرد عملی آنها را محدود کند (Ahmed et al., 2016; Schölkopf et al., 1999; Tax & Duin, 2004). در برخی مطالعات نیز از ترکیب این روش‌ها با رویکردهای دیگر برای تشخیص خطا یا ناهنجاری در شبکه هوشمند استفاده شده است (De Santis et al., 2015).

درخت تصمیم و جنگل تصادفی[2] با تقسیم داده‌ها بر اساس ویژگی‌های مصرف، امکان طبقه‌بندی نمونه‌های عادی و مشکوک را فراهم می‌کنند. جنگل تصادفی با ترکیب چندین درخت تصمیم، معمولاً در برابر نویز و تغییرات داده مقاوم‌تر از یک درخت منفرد است. مزیت مهم این گروه، تفسیرپذیری نسبی و امکان استخراج اهمیت ویژگی‌هاست؛ برای مثال، می‌توان بررسی کرد که کدام ویژگی‌های زمانی یا مصرفی در تشخیص ناهنجاری نقش بیشتری داشته‌اند. بااین‌حال، عملکرد این روش‌ها همچنان به کیفیت ویژگی‌های استخراج‌شده و توازن داده‌ها وابسته است (Primartha & Tama, 2017).

[1] SVM: Support Vector Machine
[2] Decision Tree and Random Forest

الگوریتم‌های خوشه‌بندی (مانند کا-میانگین[1] و دیبی اسکن[2]) نمونه‌های مصرف را بر اساس شباهت رفتاری گروه‌بندی می‌کنند و نمونه‌هایی را که از الگوهای غالب فاصله دارند، به‌عنوان رفتار غیرعادی یا مشکوک در نظر می‌گیرند. این روش‌ها در شرایط کمبود داده برچسب‌دار مفیدند، اما به انتخاب معیار فاصله، تعداد خوشه‌ها، مقداردهی اولیه و تغییرات فصلی مصرف حساس‌اند. روش‌های کاهش ابعاد، مانند تحلیل مؤلفه اصلی[3]، نیز می‌توانند برای فشرده‌سازی ویژگی‌های مصرف و آشکارسازی تغییرات غیرمعمول به‌کار روند، اما در مسئله مصرف غیرمجاز معمولاً نقش کمکی دارند و به‌تنهایی برای تفکیک رفتار مشکوک از تغییرات عادی مصرف کافی نیستند (Ahmed et al., 2016; Pimentel et al., 2014).

در گروه روش‌های یادگیری عمیق، مدل‌هایی مانند خودرمزگذارها، شبکه‌های بازگشتی، شبکه‌های کانولوشنی و معماری‌های ترکیبی برای استخراج الگوهای پیچیده از داده‌های زمانی یا عملیاتی به‌کار می‌روند. به‌عنوان نمونه، سینیوسوگلو و همکاران (۲۰۲۱) سامانه تشخیص نفوذ منسا[4] را برای تشخیص ناهنجاری و طبقه‌بندی حملات سایبری در محیط‌های شبکه هوشمند ارائه کردند. این رویکرد با استفاده از معماری عمیق مبتنی بر خودرمزگذار و شبکه مولد خصمانه، داده‌های عملیاتی را تحلیل کرده و میان نمونه‌های عادی و حملات مختلف تمایز ایجاد می‌کند. اهمیت این نمونه برای مقاله حاضر در آن است که نشان می‌دهد روش‌های عمیق در محیط شبکه هوشمند می‌توانند الگوهای پیچیده و چندکلاسه را مدل‌سازی کنند؛ بااین‌حال، تعمیم چنین روش‌هایی به تشخیص مصرف غیرمجاز مشترکان نیازمند داده مصرف معتبر، برچسب قابل اعتماد و کنترل نرخ مثبت کاذب است.

در مجموع، روش‌های یادگیری ماشین و یادگیری عمیق نسبت به روش‌های آستانه‌گذاری توان بیشتری در مدل‌سازی الگوهای پیچیده مصرف دارند؛ اما برتری آنها مطلق نیست و انتخاب آنها باید با توجه به دسترسی به داده معتبر، امکان برچسب‌گذاری، هزینه پردازش، نرخ مثبت کاذب، حفظ حریم خصوصی و قابلیت پیاده‌سازی در شبکه برق

[1] K-Means
[2] DBSCAN: Density-based spatial clustering of applications with noise
[3] Principal Component Analysis (PCA)
[4] MENSA

ایران انجام شود (Alkuwari et al., 2022; Fährmann et al., 2024; Messinis & Hatziargyriou, 2018).

۵. داده‌های موجود برای تحلیل روش‌های تشخیص

انتخاب مجموعه‌داده مناسب یکی از عوامل تعیین‌کننده در ارزیابی روش‌های تشخیص ناهنجاری مصرف برق است (Alkuwari et al., 2022; Fährmann et al., 2024). در مطالعات پیشین، مجموعه‌داده‌های مختلفی برای تحلیل مصرف، تشخیص تقلب، ارزیابی حملات سایبری و بررسی رفتار شبکه‌های هوشمند استفاده شده‌اند (Alkuwari et al., 2022; Fährmann et al., 2024; Takiddin et al., 2022). بااین‌حال، داده‌های مرتبط با ناهنجاری مصرف معمولاً با چالش‌هایی مانند نبود برچسب دقیق، نامتوازنی شدید میان نمونه‌های عادی و غیرعادی، داده‌های گمشده و تفاوت در بازه‌های نمونه‌برداری مواجه‌اند (Fährmann et al., 2024; Takiddin et al., 2022; Zheng et al., 2018).

جدول ۴ نمونه‌ای از مجموعه‌داده‌های پرکاربرد در مطالعات تشخیص ناهنجاری، مصرف غیرمجاز و امنیت شبکه‌های هوشمند را نشان می‌دهد. این مجموعه‌داده‌ها از نظر نوع داده، بازه زمانی، وجود یا نبود برچسب، مقیاس نمونه‌ها و هدف کاربردی تفاوت دارند؛ ازاین‌رو، نتایج مدل‌های تشخیص در مطالعات مختلف همیشه به‌طور مستقیم قابل مقایسه نیستند (Fährmann et al., 2024; Takiddin et al., 2022).

جدول ٤: مجموعه‌داده‌های پرکاربرد در تشخیص ناهنجاری و مصرف غیرمجاز در شبکه‌های هوشمند

نام مجموعه‌داده	توضیحات
خیابان پیکان/دیتاپورت[1]	داده‌های با وضوح تا یک‌ثانیه‌ای از مصرف برق، آب، گاز و تولید خورشیدی صدها خانه مسکونی آمریکا برای تحلیل الگوها و تشخیص ناهنجاری.
مجموعه‌داده تشخیص سرقت برق شرکت شبکه برق دولتی چین[2]	سری‌های زمانی مصرف روزانه ٤٢ هزار کاربر مسکونی چین با برچسب «دزدی» یا «عادی» برای آزمون مقیاس‌پذیر الگوریتم‌های تشخیص تقلب
نمودارهای بار برق ۲۰۱۱ تا ۲۰۱٤[3]	پروفایل ۱۵دقیقه‌ای مصرف برق ۳۷۰ خانوار پرتغالی طی چهار سال برای پیش‌بینی بار و پرکردن داده‌های گمشده.
پروژه کنتور هوشمند کمیسیون تنظیم مقررات انرژی ایرلند[4]	مصرف نیم‌ساعتی حدود ۳٦۰۰ خانوار ایرلندی در ۱۸ ماه با تمرکز بر تحلیل پاسخ به تعرفه و تشخیص ناهنجاری.
مجموعه‌داده تقاضای ساعتی آی‌اس‌او نیوانگلند[5]	داده‌های ساعتی بار شبکه، دما و قیمت در نه منطقه از سال ۲۰۰۳ تاکنون برای طراحی بازار و پیش‌بینی قیمت.
داده‌های مصرف انرژی کنتور هوشمند خانوارهای لندن[6]	مصرف نیم‌ساعتی ٥٥٦۷ خانوار لندن از ۲۰۱۱ تا ۲۰۱٤ برای تحلیل مدیریت بار و پاسخ به تعرفه‌های هوشمند.
مجموعه‌داده اینترنت اشیای ۲۳ [7]	مجموعه‌داده ترافیک شبکه ۲۰ نمونه بدافزار و ۳ نمونه عادی دستگاه‌های اینترنت اشیاء برای توسعه سامانه‌های تشخیص نفوذ.

بر اساس جدول ۴، بخش مهمی از مجموعه‌داده‌های موجود برای تحلیل الگوی مصرف، مدیریت بار یا امنیت شبکه طراحی شده‌اند و همه آنها به‌طور مستقیم برای تشخیص مصرف غیرمجاز برچسب‌گذاری نشده‌اند. بنابراین، انتخاب مجموعه‌داده باید متناسب با هدف مطالعه انجام شود؛ برای مثال، داده‌های مصرف خانوار برای تحلیل الگوی بار مناسب‌اند، اما برای ارزیابی دقیق تشخیص برقدزدی به برچسب‌های معتبر، داده‌های میدانی و اطلاعات تکمیلی

[1] Pecan Street / Dataport
[2] State Grid Corporation of China (SGCC) electricity-theft dataset
[3] Electricity Load Diagrams 2011–2014
[4] CER Smart Metering Project – Electricity Customer Behaviour Trial, 2009–2010
[5] ISO New England hourly demand dataset
[6] SmartMeter Energy Consumption Data in London Households
[7] IoT-23

درباره وضعیت کنتور یا شبکه نیاز است (Messinis & Hatziargyriou, 2018; Takiddin et al., 2022; Zheng et al., 2018). ازاین‌رو، مقایسه دقت روش‌ها بدون توجه به نوع مجموعه‌داده، وجود یا نبود برچسب مصرف غیرمجاز و شدت نامتوازنی داده‌ها می‌تواند گمراه‌کننده باشد (Fährmann et al., 2024; Takiddin et al., 2022).

٦. چالش‌ها و کارهای آتی

یکی از مهم‌ترین چالش‌های اجرای روش‌های تشخیص ناهنجاری مصرف برق، مقیاس‌پذیری و پردازش به‌موقع داده‌هاست (Alkuwari et al., 2022; Fährmann et al., 2024). افزایش تعداد کنتورهای هوشمند، حسگرها و سامانه‌های پایش شبکه، حجم زیادی از داده‌های زمانی و عملیاتی تولید می‌کند (Abrahamsen et al., 2021; Gungor et al., 2011). در چنین شرایطی، روش‌های تشخیص باید علاوه بر دقت، از نظر هزینه پردازش، سرعت پاسخ‌گویی و قابلیت اجرا در زیرساخت‌های موجود نیز ارزیابی شوند (Fährmann et al., 2024; Messinis & Hatziargyriou, 2018).

چالش دوم به کیفیت داده و قابلیت اعتماد نتایج مربوط است. داده‌های مصرف معمولاً با مشکلاتی مانند نبود برچسب دقیق، نامتوازنی میان نمونه‌های عادی و غیرعادی، داده‌های گمشده و تفاوت در بازه‌های نمونه‌برداری روبه‌رو هستند (Fährmann et al., 2024; Takiddin et al., 2022; Zheng et al., 2018). این عوامل می‌توانند موجب افزایش مثبت کاذب یا منفی کاذب شوند و در نتیجه، تشخیص مصرف مشکوک یا غیرمجاز را دشوارتر کنند (Fährmann et al., 2024; Takiddin et al., 2022). بنابراین، پژوهش‌های آینده باید علاوه بر توسعه مدل‌های دقیق‌تر، بر بهبود داده، اعتبارسنجی میدانی و طراحی معیارهای ارزیابی قابل مقایسه تمرکز کنند.

حریم خصوصی و امنیت داده نیز از چالش‌های اساسی این حوزه است (Nguyen et al., 2025; Stouffer et al., 2023). داده‌های کنتور هوشمند می‌توانند اطلاعات حساسی درباره الگوی زندگی یا فعالیت مصرف‌کنندگان آشکار کنند و حملاتی مانند تزریق داده نادرست، حملات خصمانه، مسموم‌سازی داده و حملات بیزانسی می‌توانند عملکرد سامانه‌های تشخیص را مختل کنند (McMahan et al., 2017; Nguyen et al., 2025). روش‌هایی مانند یادگیری ائتلافی می‌توانند با نگه‌داشتن داده خام در محل تولید و تبادل به‌روزرسانی‌های مدل، وابستگی به انتقال مستقیم داده‌های مصرف را کاهش دهند؛ بااین‌حال،

ناهمگونی داده‌های محلی، هزینه ارتباطی و امکان ارسال به‌روزرسانی‌های مخرب همچنان از چالش‌های اصلی این رویکرد است (McMahan et al., 2017; Zhang et al., 2026).

در شرایط ایران، چالش اصلی تنها انتخاب الگوریتم دقیق‌تر نیست، بلکه فراهم‌کردن زیرساخت داده، افزایش پوشش کنتورهای هوشمند، استانداردسازی ثبت و تبادل داده، حفظ حریم خصوصی و طراحی سیاست‌های اجرایی سازگار با عدالت انرژی است. ازاین‌رو، مسیرهای آینده پژوهش می‌تواند شامل توسعه مدل‌های سبک و قابل استقرار، روش‌های مقاوم در برابر داده ناقص و حملات سایبری، و چارچوب‌های تصمیم‌گیری باشد که میان دقت تشخیص، هزینه اجرا و ملاحظات اجتماعی و سیاستی توازن برقرار کنند.

۷. جمع‌بندی

این مقاله با رویکرد مرور ساختاریافته، راهکارهای تشخیص ناهنجاری مصرف برق را با تأکید بر مصرف غیرمجاز و تلفات غیرفنی در شبکه‌های هوشمند بررسی کرد. جمع‌بندی مطالعات نشان می‌دهد که تشخیص مصرف غیرمجاز صرفاً یک مسئله حقوقی یا اقتصادی نیست، بلکه در سطح فنی به تحلیل داده‌های مصرف، شناسایی انحراف از الگوی عادی و تفکیک رفتار مشکوک از تغییرات طبیعی مصرف وابسته است. ازاین‌رو، مشاهده ناهنجاری در داده‌های مصرف باید به‌عنوان نشانه‌ای برای بررسی بیشتر در نظر گرفته شود و نه اثبات قطعی مصرف غیرمجاز.

مرور روش‌ها نشان داد که روش‌های آستانه‌گذاری و آماری به دلیل سادگی و هزینه کمتر، برای پایش اولیه و شرایطی که الگوی مصرف پایدار است مناسب‌اند، اما در برابر الگوهای پیچیده، تغییرات تدریجی و داده‌های نامتوازن محدودیت دارند. در مقابل، روش‌های یادگیری ماشین و یادگیری عمیق توان بیشتری در مدل‌سازی روابط غیرخطی و الگوهای پیچیده مصرف دارند، ولی کارایی آنها به کیفیت داده، وجود برچسب معتبر، هزینه پردازش، کنترل خطای مثبت کاذب و قابلیت پیاده‌سازی بستگی دارد. روش‌های ترکیبی و رویکردهایی مانند یادگیری ائتلافی نیز ظرفیت مهمی برای آینده دارند، اما بدون زیرساخت داده، امنیت ارتباطات و سازوکارهای اعتبارسنجی قابل اتکا، نمی‌توان آنها را راه‌حل قطعی دانست (Alshehri et al., 2024; Zhang et al., 2026).

برای ایران، مهم‌ترین دلالت این مرور آن است که کاهش تلفات غیرفنی و شناسایی مصرف مشکوک تنها با انتخاب الگوریتم دقیق‌تر محقق نمی‌شود. این هدف به توسعه پوشش کنتورهای هوشمند، دسترسی به داده‌های معتبر، استانداردسازی تبادل داده، حفاظت از حریم خصوصی، کاهش خطاهای تشخیص و طراحی سیاست‌های اصلاحی سازگار با عدالت انرژی نیاز دارد. ازاین‌رو، این جمع‌بندی می‌تواند مبنایی برای انتخاب روش‌های تشخیص متناسب با محدودیت‌های داده، هزینه اجرا و شرایط شبکه برق ایران فراهم کند.

یافته‌های این پژوهش می‌تواند برای شرکت‌های توزیع برق، سیاست‌گذاران انرژی و پژوهشگران حوزه شبکه هوشمند کاربرد داشته باشد. برای شرکت‌های توزیع، نتایج مقاله نشان می‌دهد که انتخاب روش تشخیص باید بر اساس کیفیت داده، پوشش کنتورهای هوشمند، نرخ مثبت کاذب و هزینه پیاده‌سازی انجام شود. برای سیاست‌گذاران، یافته‌ها نشان می‌دهد که اصلاح یارانه و مدیریت مصرف باید همراه با توجه به فقر انرژی و حمایت از مصرف پایه باشد تا تشخیص و کنترل مصرف غیرمجاز به کاهش عدالت در دسترسی به انرژی منجر نشود (Canals Casals et al., 2020; Clements et al., 2013). برای پژوهش‌های آینده نیز پیشنهاد می‌شود مدل‌های سبک، مقاوم در برابر داده ناقص و قابل اجرا در زیرساخت واقعی شبکه برق ایران توسعه و با داده‌های معتبر میدانی ارزیابی شوند.

تعارض منافع

نویسندگان اعلام می‌کنند که هیچ‌گونه تعارض منافعی در ارتباط با پژوهش حاضر وجود ندارد.

سپاسگزاری

نویسندگان از سردبیر و داوران محترم نشریه بابت ارائه دیدگاه‌ها و پیشنهادهای اصلاحی ارزشمند سپاسگزاری می‌کنند. این پژوهش از هیچ نهاد یا سازمانی حمایت مالی دریافت نکرده است.

منابع

ایرنا. (۱۴۰۵، ۴ خرداد). قیمت تمام‌شده هر کیلووات ساعت برق ۱۹۰۰ تومان است/ تشدید یارانه پنهان بخش انرژی. خبرگزاری جمهوری اسلامی . https://www.irna.ir/news/86164083

برق‌نیوز. (۱۴۰۳، ۴ مهر). تلفات شبکه برق کشور تا پایان برنامه هفتم به ۱۰ درصد کاهش می‌یابد https://barghnews.com/fa/news/59453 .

برق‌نیوز. (۱۴۰۴الف، ۸ اردیبهشت). ۹۶۲ هزار مشترک جدید برق در سال ۱۴۰۳ به شبکه سراسری پیوستند https://barghnews.com/fa/news/62216 .

برق‌نیوز. (۱۴۰۴ب، ۲۲ اردیبهشت). نصب ۹ میلیون کنتور هوشمند در کشور تا پاییز سال آینده https://barghnews.com/fa/news/62424 .

توانیر. (۱۴۰۳). آمار تفصیلی صنعت برق ایران در سال ۱۴۰۲: ویژه مدیریت راهبردی. شرکت مادر تخصصی تولید، انتقال و توزیع نیروی برق ایران.

خبرگزاری تسنیم. (۱۴۰۳). رکوردشکنی مصرف برق در تابستان ۱۴۰۳. خبرگزاری تسنیم . https://tn.ai/3127521

مرکز پژوهش‌های مجلس شورای اسلامی. (۱۴۰۳). پایش شاخص‌های کلان بخش برق (۱): سال ۱۴۰۲. مرکز پژوهش‌های مجلس شورای اسلامی . https://doi.org/10.22034/report.2024.17156.1924

مرکز پژوهش‌های مجلس شورای اسلامی. (۱۴۰۴). پایش شاخص‌های کلان بخش برق (۴): شش‌ماهه اول سال ۱۴۰۴. دفتر مطالعات انرژی، صنعت و معدن. https://doi.org/10.22034/mrc.report.21284

References

Abrahamsen, F. E., Ai, Y., & Cheffena, M. (2021). Communication technologies for smart grid: A comprehensive survey. Sensors, 21(23), 8087. https://doi.org/10.3390/s21238087

Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

Ali, S., Min, Y., & Ali, W. (2023). Prevention and detection of electricity theft of distribution network. Sustainability, 15(6), 4868. https://doi.org/10.3390/su15064868

Alkuwari, A. N., Al-Kuwari, S., & Qaraqe, M. (2022). Anomaly detection in smart grids: A survey from cybersecurity perspective. In 2022 3rd International Conference on Smart Grid and Renewable Energy (SGRE) (pp. 1–7). IEEE. https://doi.org/10.1109/SGRE53517.2022.9774221

Alshehri, A., Badr, M. M., Baza, M., & Alshahrani, H. (2024). Deep anomaly detection framework utilizing federated learning for electricity theft zero-day cyberattacks. Sensors, 24(10), Article 3236. https://doi.org/10.3390/s24103236

Artale, G., Cataliotti, A., Cosentino, V., Di Cara, D., Fiorelli, R., Guaiana, S., Panzavecchia, N., & Tinè, G. (2018). A new PLC-based smart metering architecture for medium/low voltage grids: Feasibility and experimental characterization. Measurement, 129, 479–488. https://doi.org/10.1016/j.measurement.2018.07.070

Bouramdane, A.-A. (2023). Cyberattacks in smart grids: Challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. Journal of Cybersecurity and Privacy, 3(4), 662–705. https://doi.org/10.3390/jcp3040031

Canals Casals, L., Tirado Herrero, S., Barbero, M., & Corchero, C. (2020). Smart meters tackling energy poverty mitigation: Uses, risks and approaches. In 2020 IEEE Electric Power and Energy Conference (EPEC) (pp. 1–6). IEEE. https://doi.org/10.1109/EPEC48502.2020.9320062

Clements, B., Coady, D., Fabrizio, S., Gupta, S., Alleyne, T., & Sdralevich, C. (Eds.). (2013). Energy subsidy reform: Lessons and implications.

International Monetary Fund.
https://doi.org/10.5089/9781475558111.071

Commission for Energy Regulation. (2012). CER Smart Metering Project – Electricity Customer Behaviour Trial, 2009–2010 [Data set]. Irish Social Science Data Archive. SN: 0012-00.
https://www.ucd.ie/issda/data/commissionforenergyregulationcer/

De Santis, E., Livi, L., Sadeghian, A., & Rizzi, A. (2015). Modeling and recognition of smart grid faults by a combined approach of dissimilarity learning and one-class classification. Neurocomputing, 170, 368–383. https://doi.org/10.1016/j.neucom.2015.05.112

Depuru, S. S. S. R., Wang, L., & Devabhaktuni, V. (2011). Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft. Energy Policy, 39(2), 1007–1015.
https://doi.org/10.1016/j.enpol.2010.11.037

Fährmann, D., Martín, L., Sánchez, L., & Damer, N. (2024). Anomaly detection in smart environments: A comprehensive survey. IEEE Access, 12, 64006–64049.
https://doi.org/10.1109/ACCESS.2024.3395051

Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart grid—The new and improved power grid: A survey. IEEE Communications Surveys & Tutorials, 14(4), 944–980.
https://doi.org/10.1109/SURV.2011.101911.00087

Ferreira, H. C., Lampe, L., Newbury, J., & Swart, T. G. (2010). Power line communications: Theory and applications for narrowband and broadband communications over power lines. Wiley.
https://doi.org/10.1002/9780470661291

Garcia, S., Parmisano, A., & Erquiaga, M. J. (2020). IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0) [Data set]. Zenodo. https://doi.org/10.5281/zenodo.4743746

Ghorbani, A., & Fartash, K. (2023). Challenges of smart grid technology deployment in developing countries: Case study of Iran. In

Handbook of Smart Energy Systems (pp. 2551–2572). Springer. https://doi.org/10.1007/978-3-030-97940-9_74

Gopstein, A., Nguyen, C., O'Fallon, C., Hastings, N., & Wollman, D. A. (2021). NIST framework and roadmap for smart grid interoperability standards, release 4.0 (NIST Special Publication 1108r4). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1108r4

Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. IEEE Transactions on Industrial Informatics, 7(4), 529–539. https://doi.org/10.1109/TII.2011.2166794

Hajiaghapour-Moghimi, M., Heydari Tafreshi, O., Hajipour, E., Vakilian, M., & Lehtonen, M. (2024). Investigating the cryptocurrency mining loads' high penetration impact on electric power grid. IEEE Access, 12, 153643–153663. https://doi.org/10.1109/ACCESS.2024.3482098

International Energy Agency. (2025). Electricity 2025: Analysis and forecast to 2027. IEA. https://www.iea.org/reports/electricity-2025

ISO New England. (n.d.). Hourly real-time system demand [Data set]. Energy, Load, and Demand Reports. https://www.iso-ne.com/isoexpress/web/reports/load-and-demand/-/tree/dmnd-rt-hourly-sys

Jeffin, M. J., Minu, B., & Babu, A. V. (2020). Internet of things enabled power theft detection and smart meter monitoring system. In 2020 International Conference on Communication and Signal Processing (ICCSP) (pp. 262–267). IEEE. https://doi.org/10.1109/ICCSP48568.2020.9182144

Lin, X., An, D., Cui, F., & Zhang, F. (2023). False data injection attack in smart grid: Attack model and reinforcement learning-based detection method. Frontiers in Energy Research, 10, Article 1104989. https://doi.org/10.3389/fenrg.2022.1104989

McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. y. (2017). Communication-efficient learning of deep networks from decentralized data. In Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS) (Proceedings of Machine Learning Research, Vol. 54, pp. 1273–1282). PMLR.

Messinis, G. M., & Hatziargyriou, N. D. (2018). Review of non-technical loss detection methods. Electric Power Systems Research, 158, 250–266. https://doi.org/10.1016/j.epsr.2018.01.005

Miljković, D. (2010). Review of novelty detection methods. In Proceedings of the 33rd International Convention MIPRO (pp. 593–598). IEEE.

Nguyen, L.-H., Nguyen, V.-L., Hwang, R.-H., Kuo, J.-J., Chen, Y.-W., Huang, C.-C., & Pan, P.-I. (2025). Toward secured smart grid 2.0: Exploring security threats, protection models, and challenges. IEEE Communications Surveys & Tutorials, 27(4), 2581–2620. https://doi.org/10.1109/COMST.2024.3493630

Ortega-Fernandez, I., & Liberati, F. (2023). A review of denial of service attack and mitigation in the smart grid using reinforcement learning. Energies, 16(2), Article 635. https://doi.org/10.3390/en16020635

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Passerini, F., & Tonello, A. M. (2019). Smart grid monitoring using power line modems: Anomaly detection and localization. IEEE Transactions on Smart Grid, 10(6), 6178–6186. https://doi.org/10.1109/TSG.2019.2899264

Pecan Street Inc. (n.d.). Dataport [Data set]. https://www.pecanstreet.org/dataport/

Pimentel, M. A. F., Clifton, D. A., Clifton, L., & Tarassenko, L. (2014). A review of novelty detection. Signal Processing, 99, 215–249. https://doi.org/10.1016/j.sigpro.2013.12.026

Primartha, R., & Tama, B. A. (2017). Anomaly detection using random forest: A performance revisited. In 2017 International Conference on Data and Software Engineering (ICoDSE) (pp. 1–6). IEEE. https://doi.org/10.1109/ICODSE.2017.8285847

Schölkopf, B., Williamson, R. C., Smola, A. J., Shawe-Taylor, J., & Platt, J. C. (1999). Support vector method for novelty detection. In Advances in Neural Information Processing Systems 12 (pp. 582–588). MIT Press.

Siniosoglou, I., Radoglou-Grammatikis, P., Efstathopoulos, G., Fouliras, P., & Sarigiannidis, P. (2021). A unified deep learning anomaly detection and classification approach for smart grid environments. IEEE Transactions on Network and Service Management, 18(2), 1137–1151. https://doi.org/10.1109/TNSM.2021.3078381

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Stouffer, K., Pease, M., Tang, C. Y., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). Guide to operational technology (OT) security (NIST Special Publication 800-82 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3

Takiddin, A., Ismail, M., Zafar, U., & Serpedin, E. (2022). Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids. IEEE Systems Journal, 16(3), 4106–4117. https://doi.org/10.1109/JSYST.2021.3136683

Tax, D. M. J., & Duin, R. P. W. (2004). Support vector data description. Machine Learning, 54, 45–66. https://doi.org/10.1023/B:MACH.0000008084.60811.49

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., Moher, D., Peters, M. D. J., Horsley, T., Weeks, L., Hempel, S., Akl, E. A., Chang, C., McGowan, J., Stewart, L., Hartling, L., Aldcroft, A., Wilson, M. G., Garritty, C., ... Straus, S. E. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation. Annals of Internal Medicine, 169(7), 467–473. https://doi.org/10.7326/M18-0850

Trindade, A. (2015). ElectricityLoadDiagrams20112014 [Data set]. UCI Machine Learning Repository. https://doi.org/10.24432/C58C86

UK Power Networks. (n.d.). SmartMeter energy consumption data in London households [Data set]. London Datastore. https://data.london.gov.uk/dataset/smartmeter-energy-consumption-data-in-london-households-vqm0d/

Zhang, Z., Rath, S., Xu, J., & Xiao, T. (2026). Federated learning for smart grid: A survey on applications and potential vulnerabilities. ACM Transactions on Cyber-Physical Systems, 10(1), 1–26. https://doi.org/10.1145/3760788

Zhao, K., Li, L., Ding, K., Gong, N. Z., Zhao, Y., & Dong, Y. (2025). A survey of model extraction attacks and defenses in distributed computing environments. arXiv. https://arxiv.org/abs/2502.16065

Zheng, Z., Yang, Y., Niu, X., Dai, H.-N., & Zhou, Y. (2018). Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids. IEEE Transactions on Industrial Informatics, 14(4), 1606–1615. https://doi.org/10.1109/TII.2017.2785963

Zhu, Y., Wen, H., Zhao, R., Jiang, Y., Liu, Q., & Zhang, P. (2023). Research on data poisoning attack against smart grid cyber–physical system based on edge computing. Sensors, 23(9), Article 4509. https://doi.org/10.3390/s23094509

Zibaeirad, A., Safavi, A. A., & Sarbishaei, O. (2024). A comprehensive survey on the security of smart grid: Challenges, mitigations, and future research opportunities. arXiv. https://arxiv.org/abs/2407.07966

Persian References Translated into English

Bargh News. (2024, September 25). Electricity network losses in the country will be reduced to 10 percent by the end of the Seventh Development Plan. Bargh News. https://barghnews.com/fa/news/59453 (In Persian)

Bargh News. (2025a, April 28). 962 thousand new electricity subscribers joined the national grid in 2024/2025. Bargh News. https://barghnews.com/fa/news/62216 (In Persian)

Bargh News. (2025b, May 12). Installation of 9 million smart meters in the country by next autumn. Bargh News. https://barghnews.com/fa/news/62424 (In Persian)

Islamic Parliament Research Center. (2024). Monitoring macro indicators of the electricity sector (1): Year 1402. Islamic Parliament Research Center. https://doi.org/10.22034/report.2024.17156.1924 (In Persian)

Islamic Parliament Research Center. (2025). Monitoring macro indicators of the electricity sector (4): First half of 1404. Office of Energy, Industry and Mining Studies. https://doi.org/10.22034/mrc.report.21284 (In Persian)

Islamic Republic News Agency. (2026, May 25). The cost price of each kilowatt-hour of electricity is 1,900 tomans / Intensification of hidden subsidies in the energy sector. IRNA. https://www.irna.ir/news/86164083 (In Persian)

Tasnim News Agency. (2024). Record-breaking electricity consumption in the summer of 2024. Tasnim News Agency. https://tn.ai/3127521 (In Persian)

Tavanir. (2024). Detailed statistics of Iran's electric power industry in 1402: Strategic management edition. Iran Power Generation, Transmission and Distribution Management Company. (In Persian)

استناد به این مقاله: ۱۴۰۵. مرور ساختاریافته راهکارهای تشخیص ناهنجاری مصرف برق با تأکید بر مصرف غیرمجاز در شبکه‌های هوشمند. *پژوهشنامه اقتصاد انرژی ایران*، سال(شماره)، ص آغاز-ص پایان.