ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION

Paper ID #49545

Understanding Electricity Theft: Causes, Consequences, and AI-Based Detection

Ethan Scott Stevenson, Marshall University
Jay Cook, Marshall University
Dr. Trevor Bihl, Marshall University

Understanding Electricity Theft: Causes, Consequences, and AI-Based Detection

Abstract

Electricity theft, often overlooked in both public and technical matters, poses a significant economic and social challenge for utilities. Briefly, Electricity theft involves illicitly consuming electric power through various means, from bypassing meters, tampering with meters, to unpaid bills. Beyond technical and safety matters, it is often correlated with poverty, weak infrastructure, and utility/government inefficiencies. The consequences of it extend beyond financial losses, and it contributes to power outages, imbalances in systems, and higher costs for honest consumers. This review covers the scope and impact of electricity theft in America compared to other countries, examining current prevention strategies and emerging solutions. A general review of the role of AI and machine learning is done, which shows promising potential in detecting and mitigating electricity theft through advanced technological approaches.

Introduction

Electricity theft, defined as the unauthorized use of electric power without proper payment, is a critical issue that affects power distribution systems worldwide. In the United States (U.S.), electricity theft leads to an estimated $1.6 billion in annual losses for utility companies, creating a significant financial burden that is ultimately passed on to honest consumers through higher electricity rates [1]. While this issue is not frequently discussed in the U.S., its financial and operational impacts are felt across the energy sector [2]. The challenge lies not only in the monetary losses but also in the inefficiencies and operational difficulties introduced by electricity theft, which compromise the reliability and resilience of power grids.

Globally, electricity theft is recognized as a pervasive problem, particularly in developing and countries where resources for combating the issue are often limited [3]. In these regions, distribution systems are already strained by growing demand and aging infrastructure [2]. The added burden of electricity theft exacerbates these challenges, leading to higher costs for honest consumers, reduced revenues for power distributors, and broader economic and social ramifications [2].

Within power systems, there are naturally losses. Total power lost within a distribution system can be generally expressed as:

$$P_{loss} = P_{delivered} - P_{sold} \quad (1)$$

with total power delivered into the system being $P_{delivered}$ and P_{sold} being the power sold to consumers [4]. Further categorizing P_{loss}, there are two broad categories in power systems: technical and non-technical, as conceptualized in Table 1. Technical losses are from inevitable inefficiencies that come from the physical characteristics of power systems [5]. Non-technical losses include losses due to errors in processes, record keeping, as well as theft [5]. Non-technical losses are especially damaging because they are avoidable, and thus akin to assignable

causes in Six Sigma [6], yet they often persist due to inadequate enforcement mechanisms and resource constraints.

Table 1. Examples of Technical and Nontechnical Losses, from [7]

Technical Losses		Non-Technical Losses
Variable	**Fixed**	
Load	Hysteresis	Accounting Errors
Series	Core	Electricity Theft
Copper	Eddy Current	Faulty Meters (inaccurate and miscalibrated)
Transport Related	No-Load	Faulty Meter Reading Methods
	Shunt	Incorrect Meter Readings
	Iron	Technical Loss Computation Errors

The methods used to steal electricity vary widely, from tampering with meters to illegal connections that bypass billing systems altogether. While utility companies can calculate total system losses by comparing the power delivered to the grid with the power billed to consumers, separating technical from non-technical losses remains a challenge. Technical losses are estimated based on the characteristics of the distribution system, and the remaining losses are attributed to non-technical causes, including theft. This reliance on estimation underscores a fundamental difficulty in quantifying the scale of electricity theft, leaving utility companies to address the issue without precise data.

Traditional methods for detecting electricity theft, such as manual inspections, have been employed for decades. However, these methods are labor-intensive, time-consuming, and increasingly ineffective in identifying theft as perpetrators adopt more sophisticated tactics. The inefficiencies of manual inspections often lead to false positives or negatives, which further complicate efforts to curb electricity theft. In response to these limitations, emerging technologies such as Artificial Intelligence (AI) and Machine Learning (ML) have been explored as innovative solutions for automating theft detection and improving accuracy. These technologies leverage large datasets collected by smart meters and Advanced Metering Infrastructure (AMI) to analyze consumption patterns and identify anomalies indicative of theft.

The social and economic consequences of electricity theft extend beyond financial losses. For power distributors, whether government entities or private companies, theft reduces revenues, limits investment in infrastructure, and undermines the expansion of reliable power systems. For consumers, the indirect costs of electricity theft manifest as higher electricity rates and reduced quality of service. These impacts are particularly pronounced in regions with limited resources to combat theft, where the compounding effects of non-technical losses and infrastructure deficiencies hinder economic development and social progress.

Addressing electricity theft also represents an interdisciplinary challenge at the intersection of engineering, policy, and technology. By examining electricity theft through the lens of engineering problem-solving, this paper introduces students and educators to real-world applications of electrical engineering, artificial intelligence, and data science. It provides a case study that combines technical challenges, societal impacts, and innovative solutions, illustrating the broader relevance of engineering to pressing global issues. Additionally, the paper

emphasizes the importance of integrating AI and advanced technologies into engineering curricula, preparing students to tackle complex, interdisciplinary problems in their future careers.

This paper seeks to provide a comprehensive review of electricity theft by examining its causes, methods, and impacts, as well as the effectiveness of current and emerging solutions. By comparing the prevalence of electricity theft in the U.S. with that in other countries, this review aims to contextualize the issue within a global framework. The paper will also explore how advanced technologies like AI can be leveraged to combat electricity theft and discuss the limitations and potential future developments in this field. Ultimately, addressing electricity theft requires a multifaceted approach that combines technological innovation, policy measures, and public awareness to reduce losses and enhance the efficiency of power distribution systems worldwide. This holistic perspective further aims to foster engineering innovation and education.

Societal Causes of Electricity Theft

To understand possible causes of electricity theft, it is worthwhile to examine countries by the prevalence of electricity theft. Notably, electricity theft is generally prevalent in developing countries and minimal in developed nations. For example, in the United States non-technical losses are estimated to be 2% of total electricity generated [5]; in Brazil, these losses are estimated to be about 5% of their total generated energy [8]; whereas in India, these losses are estimated to be about 15% [8]. An example of the relationship between economic factors and non-technical losses is seen in Figure 1, for India, where as the GDP per capita Purchase Power Parity (PPP) rises by year, the non-technical losses are seen to decrease.

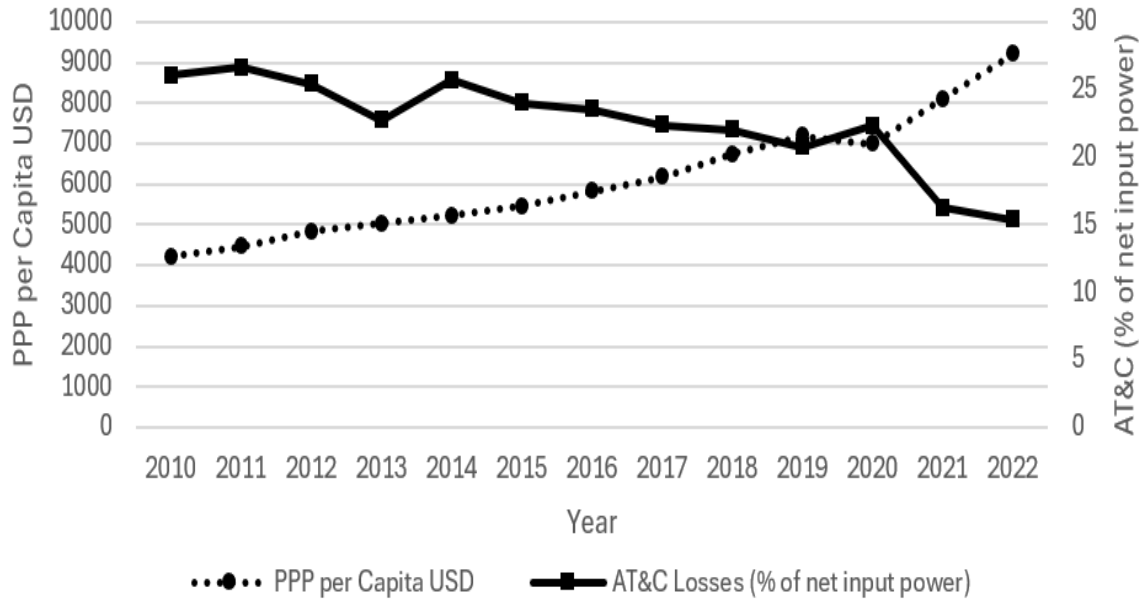

Figure 1. Indian PPP per Capita GDP in USD and Non-Technical Losses (% of net input power). Percentages retrieved from annual PFC reports: [9]**. Annual PPP per capita in USD retrieved from World Bank Group** [10]**.**

Studies exploring reasons for theft found that regions and countries with high rates of electricity theft areas were found to have several correlated factors, including GDP to taxation ratio, corruption, poverty, low literacy, unemployment, urbanization, and collection efficiency [11]. As mentioned in [12], as electricity prices become an appreciable percentage of income, the rewards to theft outweigh the risks. Of course, poverty is not the only driver of electricity theft. Studies have found a relationship between electricity theft and overall corruption; with one predictor being the GDP to taxation ratio, which has indicated a relationship between the honesty of taxpayers and the strength of tax code enforcement with electricity theft [11]. Findings have also shown that private utilities achieved lower theft rates, indicating that a focus on profits and the inability to trade power for votes allowed private utilities to achieve less non-technical losses [11].

Other factors like weak legal regulations and poor infrastructure contribute to this disparity [11]. Finally, some studies suggest electricity theft can be driven by culture [12], where in many countries electricity theft can become normalized through sheer amount or other circumstances, and a theft culture is established [12] [13]. An argument for strong law enforcement, incorrupt government, private utility ownership, and public education campaigns can be made from these findings. For example, in Ghana many electricity theft reports are of people that are not relatively poor, with many electricity thieves being churches, businesses, and consumers [14]. Thus, electricity theft can be strongly driven by corruption and other factors, and the issue cannot be solely linked to poverty [14].

Economic and Other Impacts

Worldwide non-technical losses are significant and estimated (2014) at $89.3 billion a year [15]. Detecting and mitigating electricity theft has historically involved a combination of usage analysis. In the United States, while the overall rate of non-technical losses is relatively low (approximately 2-3%), the cost is high and costs approximately $1.6 billion dollars each year [1]. Other countries have similar costs, for example, in Brazil, these losses are estimated to be about 5% of their total generated energy, which comes out to be about $2.4 billion lost per year [8]. South Africa loses approximately $350 million to theft; Columbia loses about $24 million per year, and Jamaica estimates approximately $46 million in losses in a year [8].

Beyond economic impacts, electricity theft strains power systems since losses due to theft are unpredictable and cannot be planned for. An example of an extreme case of this can be seen in India in 2012, when non-technical losses were 25% of all power distributed [16]. The stress of theft helped cause a blackout in 2012 which affected 700 million, or 8.5% of the global population [11] [17].

Electricity Theft Methods

Techniques used to steal electricity are varied. The general idea is simply to access distributed electricity without paying for it. The methods used range from simple to sophisticated, where participants only need to avoid electric meters or bills. Simple methods generally bypass or avoid meters, and sophisticated techniques can involve skilled tampering with meters. Deceiving the

utility in some way is also a common electricity theft method. As discussed in [7], electricity theft is generally of three types:

A. *Billing Related Theft:*
    - *Deliberate non-payment* of bills.
    - *Malicious billing irregularities*, such as intentional efforts to bribe officials to ignore use
    - *Billing irregularities*, unintentional theft such as accounting errors and faulty meters, faulty meter reading methods, incorrect meter readings, technical loss computation errors
B. *Fraud*, whereby customers change their apparent usage via:
    - *Bypassing* a meter to prevent it from measuring the power consumed
    - *Tampering* with a meter to cause it to output a more favorable reading for the customer. This is subdivided into mechanical and digital/smart meter methods
C. *Outright Theft* where customers directly steal electricity, such as through:
    - *Tapping* an overhead line to create a new, illegal connection
    - *Induction Coupling* whereby energy from a power line is collected by electromagnetic induction without physically connecting to the line.

Billing related theft involves corruption or inaccurate equipment, with utilities billing customers for less money than what the power would be properly billed for [13]. Additionally, this includes deliberate non-payment where consumers simply do not pay their bills [13]. When there are no repercussions, corruption or other governmental and cultural factors are indicated to be present [13]. In many circumstances and definitions, not paying bills is not "theft" per se; however, unpaid bills can account for large amounts of unpaid power [13] [18].

Fraud related theft involves modifying their meters or modifying what is read by the meters so that they measure less electricity usage than actual [13]. This can involve tampering with physical meters. Figure 2 highlights various places that meters can be modified to make mechanical metering gears slower or sense incorrect values [19] [5]. For digital meters, Figure 3, cyber-attacks to steal credentials to modify their operations have been seen in use [20]. Related fraud methods include merely bypassing the meter, e.g. Figure 4, where clients with a meter simply connect wires to either transmission lines or client lines before their meter and make a connection to the service line after the meter [13] [5]. Fraud related theft can also occur whereby meters are removed, conductors are placed to make direct connections, as seen in Figure 5, and then the meters are returned when meter readings are expected.

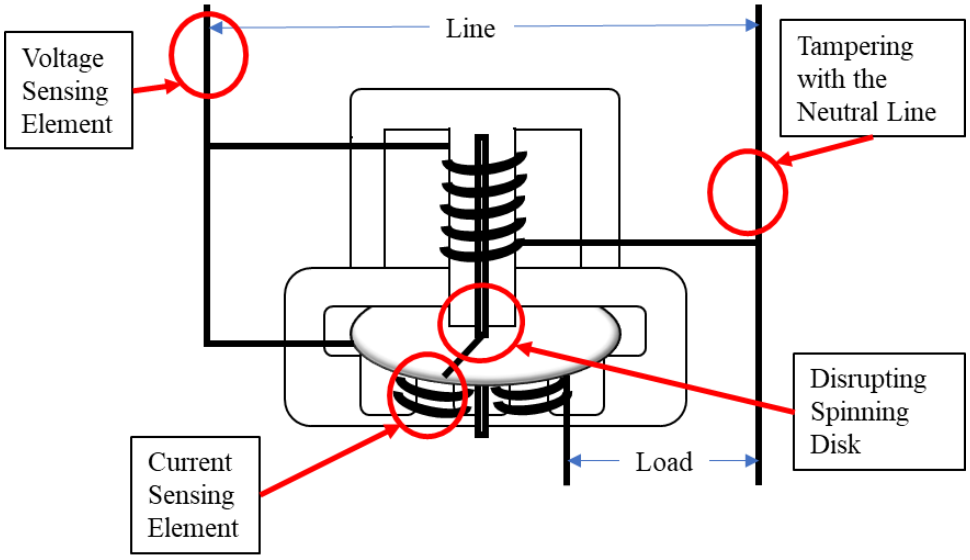

Figure 2. Conceptualization of a single-phase mechanical watt-hour meter with locations susceptible to theft highlighted, recreated from [21]

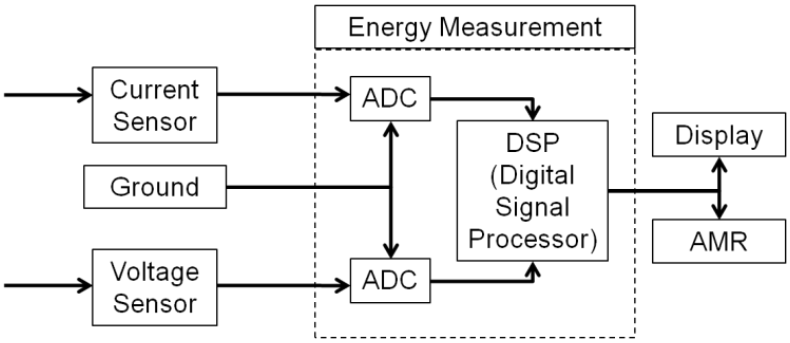

Figure 3. Conceptualization of parts of a digital meter, from [7]

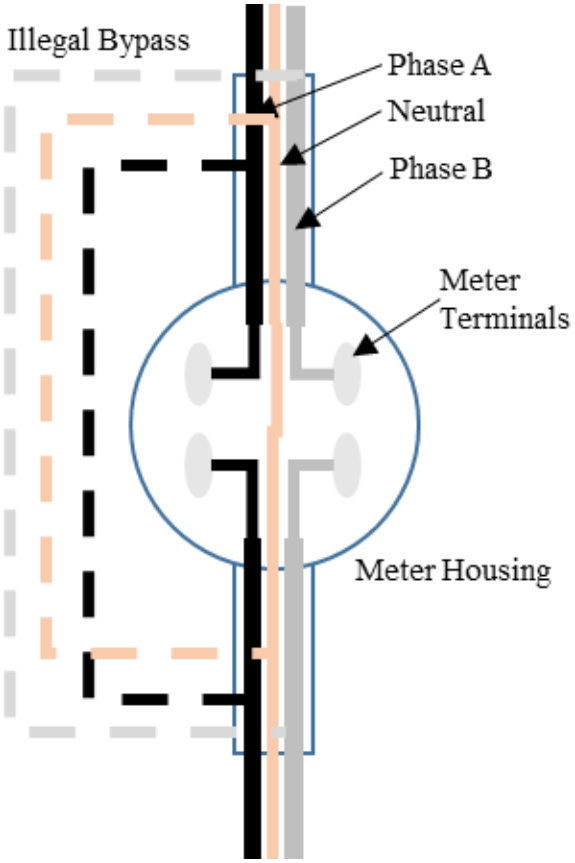

Figure 4. Example of meter bypass showing typical 2-phase connection, i.e. United States houses, with a bypass making a connection around the meter, from [5]

Figure 5. Examples of bypassing a metering through the use of automobile jumper cab les (a) and screwdrivers (b), from [7]**.**

The methods mentioned above all related to electricity thieves who are (or were) customers of a utility. However, not all thieves are customers with a meter or bills to avoid, *Outright Theft* methods involve directly connecting to transmission or service lines to steal power, this is commonly called “tapping” [5]. Tapping and Meter tampering/bypassing can each be done with

simple materials. Wire, jumper cables, and metal objects are commonly used for tapping, tampering, and bypassing [5]. An example is seen in Figure 6. Notably, line tapping, meter tampering, and meter bypassing are all inherently dangerous, as they involve working either around or directly with live power lines. Many reports are made of the electrocution of people attempting these techniques [13]. However, developments in this approach include a patent to safely tap power lines for emergency or military use [22].

However, other methods of outright theft include theft by induction whereby electricity is stolen via induction coupling or energy harvesting. While such methods are generally cost prohibitive to steal a significant amount of electricity due to the large investment required [23], their technical feasibility and public consciousness make them notable. Additionally, recent developments in small electronics, e.g. [24], "harvest" "free electricity" in the environment to charge small electronic device. Notably, widespread adoption of such methods of electricity theft, as advocated by many [25] [26], could result in significant electricity theft and reduced abilities of utilities to plan.

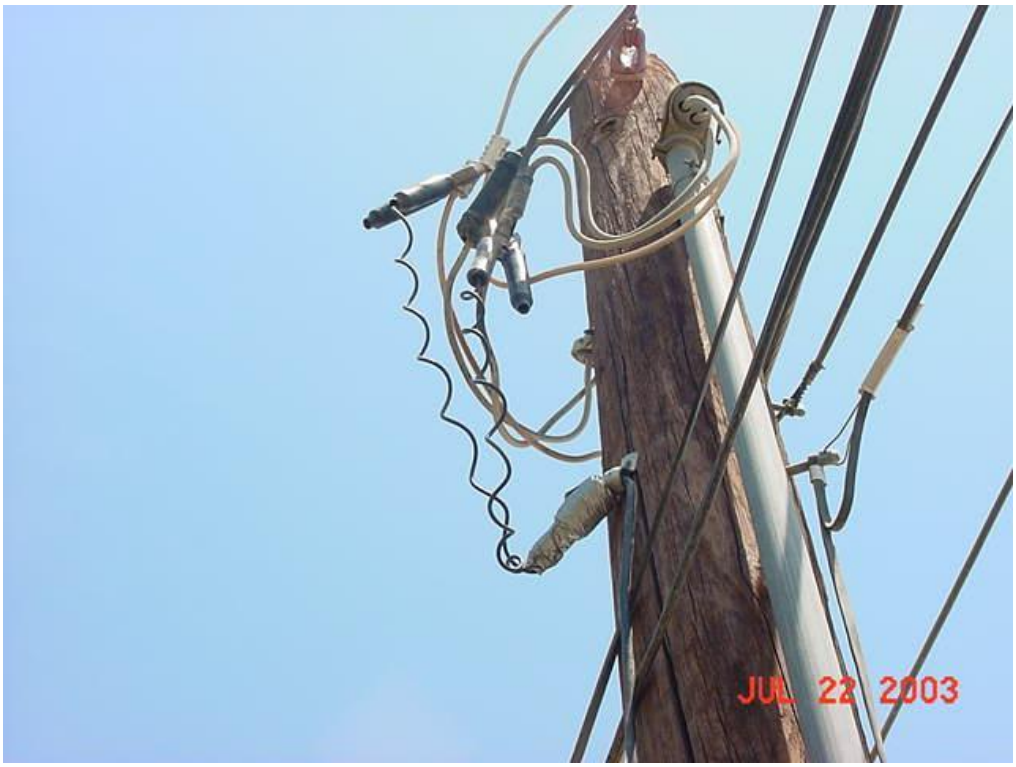

Figure 6. Example of Tapping in America, from [7]

Electricity Theft Detection and Prevention

Beyond large scale cultural changes, preventing and detecting electricity theft are often highly related, but some distinctions can be made. Preventing theft includes both active and passive means. While detecting theft includes both active and reactive methods. An example of both a deterrent and detection method are regular meter readings; a deterrent since knowing the meter

could be inspected at any time deters some theft, it is also a valuable detection method since a meter inspector can find damage, alterations, and suspicious behavior which corresponds to theft.

Theft Prevention Methods

Passive means include reducing access to the lines and meters. Utilities commonly attempt simple anti-theft measures like meter locks and seals that show when the lock or seal is broken, indicating theft [31] [28] [29]. Reducing access to the lines further makes tapping increasingly difficult [27]. Locks and seals aren't a very quick method of detection, nor do they offer much defense against tampering [31], thus smart meters can include sensors to detect and report unauthorized access [30]. Active means reduce theft and create publicity through successful prosecutions [31], publicity on dangers, both physical and criminal, through word of mouth [32], and the known potential for random checks [33].

Theft Detection Methods

Electricity theft is not always an easy thing to detect. Methods like smart meters and power draw analytics can help identify and locate electricity theft [4]. Expanding on this, the detection of electricity theft can largely be grouped into a few categories:

1. Traditional
2. Hardware based methods
3. Data driven methods

Traditional methods of theft detection are primarily from regular, and random, meter reader detection [33]. Additionally, many utilities have anonymous reporting lines, and public informants are a reliable way to find thieves [33]. Utility line tapping may also be detected, drops of voltage or current reversing may be sensed and reported which show that a region of a power grid is using more power than expected [31]. Check meters and traditional analysis to pinpoint regions of the grid with high losses have also been used for well over 100 years, c.f. [34] [35]. Randomly checking neighborhoods with expected high incidence of theft has been found to be an effective way to find theft [36]. Heuristic methods, whereby records are monitored to find large changes in usage are known as reliable means to find accounts with probable theft [37].

Hardware-based methods include advanced meters and additional sensors being placed. Smart meters, electronic meters which have the ability to communicate to the utility, can help identify and locate electricity theft [4]. For their use, two primary communication schemes are used: power line communication and wireless transmissions to the utility [38]. Additionally, smart meters with additional sensor based approaches, also known as [39], uses extremely additional sensors to detect tampering or check meters at adjacent location to provide a comparison of reported amounts and transmit results to a monitoring location [39]. Unfortunately, such hardware-based methods are very expensive as they require additional electronics for each meter or supplemental equipment [39].

Data driven methods, including AI/ML methods, use algorithmic means to find anomalous usage patterns [40]. Data driven methods use algorithmic means to find patterns in data. Such

methods are generally of two types: statistical analysis which focuses on primary data analysis, e.g. asking specific questions of the data, and data mining, which is a form of secondary data analysis, with data broadly collected and then processed to find meaningful patterns [41] [42]. Colloquially, such methods are now often referred to as AI/ML.

AI/ML for Electricity Theft Detection

Current approaches primarily used in electricity theft detection involve various families of methods. These include *prediction* methods to characterize patterns, *associating* (clustering) methods to group usage patterns together, *classification* methods to identify customers as thieves, and *anomaly* detection to find seemingly extreme data records [7]. Notably, many other domains have benefit from data science by posting challenge datasets for the public and academia to explore; however, the proprietary nature of real electricity usage data has made data availability a problem [5] [39]. Compounding this general data availability issue is that smart meters themselves, the primary source of data for AI-based electricity theft detection methods, are themselves prone to logging incomplete and inaccurate data.

AI/ML methods generally approach electricity theft through a few means. The first is a predictive approach where the amount of electricity billed is compared with the total theoretical power that is delivered from the generation site [1]. In such approaches, reliable estimations and broad comparisons with other customers are needed to make appropriate models and then appropriate heuristics are needed to understand what changes are possibly due to theft and not lifestyle events.

A second means to electricity theft detection through AI/ML is through anomaly detection. In such applications, statistical or relative anomalous behaviors are found through combining AI/ML methods for classification with extreme samples being labeled anomalous and possibly due to theft [20]. Recent expansions of this general concept include leveraging the state of the art in AI algorithms, such as convolutional neural networks (CNNs) and transformer networks [11], to make sense of the large messy data inherent in the multitude of customer records.

A third method for AI/ML use involves classification whereby records of dishonest customers are used to create a model that reliably identifies theft. From here, all records are passed and customers that are classified as theft are further investigated. Recent work in this area includes using three-phase power data to simulate the usage from three types of dishonest users: evasion, interference, and data tampering [7]. While such methods have what appears to be high accuracy (98.25%), significant work is needed since 17,000 customers per million would need investigating with a 1.75% error rate.

A fourth methods for AI/ML use involve clustering. Clustering is a form of classification, but for unsupervised means whereby one is interested in finding groups in data [44]. Ideally, such groups would be an *electricity theft* group and the *non-theft* group of honest consumers [45] [46]. However, clustering in electricity theft usage analysis can useful when theft patterns are not reliably known.

Notably, once a reliable AI/ML method is trained, companies can utilize these methods in real-time to automatically detect possible theft by routing smart meter data to a cloud server to process and analyze records [7]. Such approaches could flag possible theft, and notify/schedule meter readers to perform proactive visits to identified consumers. Such an approach would allow power companies to catch thieves faster and stop the problem before they lose a significant amount of power.

Conclusions

Electricity theft, which can take the form of direct theft, fraud, or billing issues, is a multifaceted challenge with far-reaching economic, operational, and societal consequences. Electricity theft is a major problem in the developing world, but also one of serious concern in the developed world. While electricity theft accounts for a relatively small percentage of total power produced in many developed nations, the financial burden they impose is significant. In developing countries, where resources are scarce, the impacts are even more pronounced, exacerbating infrastructure challenges and undermining economic progress.

It should also be concern not only for the utilities, but also consumers due to it resulting in added cost of electricity. There are several methods that are currently being used to attempt to detect and prevent electricity theft, but many of these methods are preventative and related to regular inspections via meter readings. Emerging technologies, particularly AI and ML, offer promising solutions for detecting and mitigating theft. These data-driven approaches can provide utilities with powerful tools to identify anomalies, streamline operations, and proactively combat fraudulent activities. However, implementing these solutions demands access to reliable data, robust infrastructure, and a commitment to addressing broader systemic issues such as corruption and weak enforcement mechanisms.

Future efforts must focus on fostering cross-disciplinary collaboration among engineers, policymakers, and educators to develop innovative solutions. Public awareness is limited and increasing awareness can play a pivotal role in reducing theft and promoting a culture of accountability. By leveraging advanced technologies and aligning them with socio-political measures, it is possible to minimize electricity theft, enhance grid reliability, and ensure fair access to energy resources for all. This paper contributes to this ongoing dialogue by providing a foundation for further research and actionable insights for stakeholders invested in creating resilient, equitable energy systems.

References

[1] T. Ahmad, H. Chen, J. Wang and Y. Guo, "Review of Various Modeling Techniques for the Detection of Electrcity Theft in Smart Grid Environment," *Renewable and Sustainable Energy Reviews,* vol. 82, no. 3, pp. 2916-2933, 2018.

[2] F. Jamil, "On the electricity shortage, price and electricity theft nexus," *Energy Policy,* pp. 267-272, 2013.

[3] I. N. Kessides, "Chaos in power: Pakistan's electricity crisis.," *Energy Policy*, vol. 55, pp. 271-285, 2013.
[4] A. Tanveer, "Non-technical loss analysis and prevention using smart meters," *Renewable and Sustainable Energy Reviews*, pp. 573-589, 2017.
[5] T. Bihl and A. and Zobaa, "Data-mining methods for electricity theft detection.," in *Big Data Analytics in Future Power Systems*, CRC Press, 2018, pp. 107-124.
[6] T. Abdelhamid, "Six Sigma in lean construction systems: opportunities and challenges," *Proceedings of the 11th Annual Conference for Lean Construction*, pp. 22-24, 2003.
[7] T. J. Bihl and S. Hajjar, "Electricity Theft Concerns within Advanced Energy Technologies," *IEEE National Aerospace & Electronics Conference (NAECON)*, 2017.
[8] D. Carr and Thomson, M., "Non-Technical Electricity Losses," *Energies*, vol. 15, no. 6, p. 2218, 2022.
[9] Power Finance Corporation, *The Performance of State Power Utilities for the Years 2010-2022*. Power Finance Corporation, 2022. [Online]. Available: https://pfcindia.com/ensite/Home/VS/29.
[10] "World Bank National Accounts Data," World Bank Group, [Online]. Available: data.worldbank.org/indicator/NY.GDP.PCAP.CD. [Accessed 10 11 2024].
[11] V. Gaur and E. & Gupta, "The determinants of electricity theft: An empirical analysis of indian states," *Energy Policy*, pp. 127-136, 2016.
[12] D. Carr and M. Thomson, "Non-technical Electricity Losses," *Energies*, p. 2218, 2022.
[13] T. B. Smith, "Electricity theft: a comparative analysis," *Energy Policy*, pp. 2067-2076, 2004.
[14] O. Yakubu, B. C., &. A. N. and O., "Electricity theft: Analysis of the underlying contributory factors in ghana.," *Energy Policy*, pp. 611-618, 2018.
[15] Northeast Group, "Emerging Markets Smart Grid: Outlook 2015," Northeast Group, Washington, DC, 2014.
[16] The Performance of State Power Utilities for the years 2010-2011 to 2012-13, Power Finance Corporation Ltd..
[17] "World Population Data Sheet," Population Reference Bureau, 2012. [Online]. Available: https://www.prb.org/wp-content/uploads/2012/07/2012-population-data-sheet_eng.pdf.
[18] Report on Performance of Power Utilities 2022-2023, Power Finance Corporation, 2024.
[19] H. D. Morton, "US Patent No. 2,019,866.". 20 Oct. 1933.
[20] S. McLaughlin, B. Holbert, A. Fawaz, R. Berthier and S. Zonouz, "A multi-sensor energy theft detection framework for advanced metering infrastructures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1319-1330, 2013.
[21] D. Suriyamongkol, "Non-technical losses in electrical power systems," *Master's thesis*, Nov. 2002.
[22] P. Marshall, "Power line sentry charging". U.S. Patent 7,398,946., 2008.
[23] D. L. Deardorff, "A Solution to the RWP for Exam 1 - Stealing Power," Summer 2006. [Online]. Available: http://user.physics.unc.edu/~deardorf/phys25/rwp/exam1rwpsolution.html. [Accessed 28 Aug. 2015].
[24] D. Siegel, "Dennis Siegel," 2017. [Online]. Available: http://dennissiegel.de/. [Accessed 10 Jun. 2017].

[25] m. dansie, "Free Electricity From Thin Air," 28 Jun. 2013. [Online]. Available: http://revolution-green.com/free-electricity-from-thin-air/. [Accessed 10 Jun. 2017].
[26] H. von der Gracht, M. Salcher and N. Graf Kerssenbrock, The Energy Challenge, München: Redline Verlag, Münchner Verlagsgruppe GmbH, 2016.
[27] H. R. Wade, "Kansas city service drop obviates theft, tree problems, contacts," *Electrical World*, pp. 110-111, 1 Mar. 1955.
[28] W. S. Davis, "Means for precluding tampering with electric meters". US Patent 1,612,420, 28 Dec. 1926.
[29] S. B. Clark, "Iron-clad services protect against theft," *Electrical World*, vol. 91, no. 7, p. 347, 18 Feb. 1928.
[30] J. H. Stokes, J. I. Clark and C. E. Maxwell, "Anti-energy diversion system for electric utility meters". US Patent 4,565,995, 21 Jan. 1986.
[31] J. Weslowski, "Utilities launch assault to halt theft of power," *Electric Light and Power*, vol. 54, no. 10, pp. 25-26, 1 Oct 1976.
[32] Electrical Light and Power, "Electricity diversion reduced through media and in-house publicity," *Electrical Light and Power*, p. 54, Dec. 1979.
[33] M. Anderson, "How to identify electricity theft in apartments without hardware or software investmnets," BluTrend LLC, 2006.
[34] J. H. Hallberg, "Theft of current: how to detect, prosecute and prevent I.," *Electrical World and Engineer*, vol. 45, no. 17, pp. 794-796, 1905.
[35] C. J. Bandim, J. E. Alves, A. V. Pinto, F. C. Souza, M. R. Loureiro, C. A. Magalhaes and F. Galvez-Durand, "Identification of energy theft and tampered meters using a central observer meter: A mathematical approach," *IEEE PES Transmission and Distribution Conference and Exposition*, pp. 163-168, 2003.
[36] B. Nesbit, "Thieves lurk, the sizable problem of stolen electricity," *Electrcial world*, pp. 31-35, Sep./Oct. 2000.
[37] K. A. Seger and D. J. Icover, "Power theft the silent crime," *FBI Law Enforcement Bulletin*, pp. 20-25, Mar. 1988.
[38] D. P. a. P. M. Stephen McLaughlin, "Energy Theft in the Advanced Metering," [Online]. Available: https://patrickmcdaniel.org/pubs/critis09.pdf.
[39] W. Bai, L. Xiong, Y. Liao, Z. Tan, J. Wang and Z. Zhang, "Detection Method for Three-Phase Electrcity Theft Based on Multi-Dimensional Feature Extraction," *Sensors*, vol. 24, no. 18, p. 6057, 2024.
[40] A. Goldman and P. Sweet, "“Flash! Stealing electricity is risky business," *Las Vegas Sun*, 29 May 2008.
[41] N. Shahzadi, N. Javaid, M. Akbar, A. Aldegheishem, N. Alrajeh and S. H. Bouk, "A Novel Data Driven Approach for Combating Energy Theft in Urbanized Smart Grids Using Artificial Intelligence," *Expert Systems with Applications*, vol. 253, 2024.
[42] S. S. S. R. Depuru, L. Wang and V. Devabhaktuni, "Support vector machine based data classification for detection of electricity theft," in *Power Systems Conference and Exposition*, 2011.