electricity

MDPI

Review

Electricity Theft Detection and Prevention Using Technology-Based Models: A Systematic Literature Review

Potego Maboe Kgaphola [1], Senyeki Milton Marebane [1,*] and Robert Toyo Hans [2]

[1] Faculty of Information and Communication Technology, Tshwane University of Technology, eMalahleni 1035, South Africa; kgapholapm@tut.ac.za
[2] Computer Science Department, Tshwane University of Technology, Soshanguve 0152, South Africa; hansr@tut.ac.za
* Correspondence: marebanesm@tut.ac.za

Abstract: Electricity theft comes with various disadvantages for power utilities, governments, businesses, and the general public. This continues despite the various solutions employed to detect and prevent it. Some of the disadvantages of electricity theft include revenue loss and load shedding, leading to a disruption in business operations. This study aimed to conduct a systematic literature review to identify what technology solutions have been offered to solve electricity theft and the effectiveness of those solutions by considering peer-reviewed empirical studies. The systematic literature review was undertaken following the guidelines for conducting a literature review in computer science to assess potential bias. A total of 11 journal articles published from 2012 to 2022 in SCOPUS, Science Direct, and Web of Science were analysed to reveal solutions, the type of theft addressed, and the success and limitations of the solutions. The findings show that the focus in research is channelled towards solving electricity theft in Smart Grids (SGs) and Advanced Metering Infrastructure (AMI); moreover, there is a neglect in the recent literature on finding solutions that can prevent electricity theft in countries that do not have SG and AMI installed. Although the results reported in this study are confined to the analysed research papers, the leading limitation in the selected studies, lack of real-life data for dishonest users. This study's contribution is to show what technology solutions are prevalent in solving electricity theft in recent years and the effectiveness of such solutions.

Keywords: electricity theft; electricity theft detection; electricity theft prevention; systematic literature review; technology solutions

Citation: Kgaphola, P.M.; Marebane, S.M.; Hans, R.T. Electricity Theft Detection and Prevention Using Technology-Based Models: A Systematic Literature Review. *Electricity* **2024**, *5*, 334–350. https://doi.org/10.3390/electricity5020017

Academic Editor: Andreas Sumper

Received: 14 March 2024
Revised: 4 May 2024
Accepted: 31 May 2024
Published: 7 June 2024

1. Introduction

Electricity theft continues to be a major challenge despite various efforts employed to detect and prevent it. According to Arkorful [1], with the exception of credit cards and automobiles, electricity is the third most commonly stolen item in developing countries. Electricity theft harms the financial health of distribution companies and negatively affects future investments in the power sector [2]. Furthermore, Mujuzi [2], Yurtseven [3] stated that developing countries suffer the most because of the nature of their distribution setup, which only records consumption readings from the meter box inside a household. Shahid, et al. [4] outlined common ways in which this theft occurs; these include line hooking, meter bypassing, and meter tempering.

As part of ongoing efforts to reduce electricity theft, researchers have proposed several solutions to curb this challenge. Savian, et al. [5] demonstrated that various regulations had been placed in different countries across the globe to punish perpetrators. Other efforts, such as awareness campaigns on electricity theft, have been explored as stated by Chetty [6]. Furthermore, Adongo, et al. [7] proposed a model for whistleblowing on electricity theft to contribute to mitigating the challenge. Moreover, technology-based models have been

explored Yan and Wen [8], Tanwar, et al. [9], Zheng, et al. [10]. Regardless of these noble efforts to address electricity theft, Ballal, et al. [11] stated that the challenge had reached alarming levels, as shown by the catastrophic impact that the challenge has had on people's lives and various economies across the world. It is on this basis that Mohanty, et al. [12], Leninpugalhanthi, et al. [13] contend for further exploration of technology-based solutions to curb the persistent electricity-theft phenomenon. Such research findings provide the basis for information to develop solutions. A systematic literature review (SLR) can assist in putting together studies that can be used for empirical studies in developing solutions. Furthermore, SLR can serve as a springboard for future research by identifying knowledge gaps [14]. Thus, this study performed an SLR to determine what various technology-based solutions have been developed to address electricity theft and the effectiveness of such solutions. To the best of our knowledge, no research work of this nature was undertaken to address the objective achieved by this study.

This study contributes to the body of knowledge in two-folds, as follows:

(1) Firstly, it provides a holistic view and understanding of existing technology-based solutions for electricity theft detection and prevention.
(2) Secondly, the study provides future solution providers with much-needed knowledge and insights on the current solution's capabilities and effectiveness, as well as their shortcomings.

This study aims to answer the following research questions:

(1) What empirical studies have been performed to address electricity theft, detection, and prevention using technology-based solutions?
(2) Which type of publication and publisher's focuses on technology-based electricity theft detection and prevention methods?
(3) How effective have the proposed/designed solutions been (what are their success and shortcomings)?

2. Literature Review

2.1. The Impact of Electricity Theft on Society

Electricity theft occurs when electricity is used up directly from distribution utilities in an un-metered or illegal way [15]. This includes the meter being made to record low consumption or being made to stop working, referred to as meter bypassing [16]. Another common method of electricity theft, as outlined by Bhalshankar and Thorat [17], is widely known as line or cable hooking, whereby perpetrators tap into the power line just before the distribution box to steal electricity. Furthermore, another common method of stealing electricity is manipulating the electricity bill by tempering with the meter box circuitry; this is known as meter tempering [18]. These types of theft are a global challenge, but the extent to which each type of theft is done depends on the electricity infrastructure of a particular country. This is to say, one type of theft can be prevalent in one country but not so in another.

The theft of electricity has seen governments and state utilities for electricity suffer billions of dollars in revenue loss across the world [19]. Additionally, Mujuzi [2] reported that damage has been done to the power grid, and substations have become overloaded. This becomes frustrating to citizens in affected areas, as they have to deal with unexpected power outages. Countries such as South Africa and Pakistan resort to load shedding in a bid to save electricity [19]. As a result, some businesses lost revenue during this period, while others ceased to operate [6]. Moreover, this challenge affects social lives, disturbs government service delivery, increases criminality, and inhibits the delivery of education and health services. For example, in terms of health, Gehringer, et al. [20] alluded that hospital operations have been negatively affected by load-shedding. As a result, hospitals are constrained from delivering primary health services, and in case of no alternative power supplies, loss of life is unavoidable because doctors are not able to perform critical and life-saving surgeries on patients [21]. Furthermore, this challenge can lead to poverty if the deceased was the only one who was able to provide for their family.

2.2. Electricity Theft Prevention Solutions

To address the challenge of electricity theft, various solutions have been explored by power utilities, governments, and researchers. The following discussion explores different solutions found in the literature.

Electricity theft stems from socio-economic and behavioural factors that require socio-technological solutions, as recommended by Saini [22]. However, Yurtseven [3] argues that prevention should happen before the actual theft; in other words, dealing with consumer behavioural and socio-economic factors might reduce the need to implement engineering and technology-based solutions. Saini [22], Depuru, et al. [23], Yakubu, et al. [24] added that some of the contributing behavioural and socio-economic factors include lower literacy levels, unemployment, corrupt politicians, poor economic conditions of consumers, and weak control systems. Some of these factors could be mitigated if communities were to treat the electricity infrastructure as part of their property and encourage others to get electricity through legal means.

Conventional ways to detect and prevent electricity theft that have been applied include awareness campaigns, conducting physical inspections, disconnecting dishonest users from the grid, and whistleblowing [1,25,26]. It is worth noting that conventional methods are subject to socio-economic factors affecting the consumers; hence, campaigns involve dedicated programmes that encourage communities to join the movement for legitimate power use and seek to influence voluntary behaviour in a sustainable way [27]. Furthermore, Shokoya and Raji [28] added that the Energy Losses Management Programme (ELP), a countrywide campaign launched in 2006 by Eskom, a state utility in South Africa, is directed at educating the public about the issue of electricity theft in the country. They further alluded that making those responsible face justice has successfully reduced electricity theft from 7.12% to 6.43% between 2013 and 2016. This shows that the punishing offenders plays a psychological role in influencing individuals to abstain from illegally consuming electricity.

Other efforts and strategies include meter auditing, disabling unauthorised connections, looking into theft incidents, collecting tamper fines, and replacing defective meters. Efforts have been made to educate customers to use electricity legally, safely, responsibly, and efficiently, encouraging the public to report electricity-theft suspects, and focusing on high-profile areas [28]. Furthermore, it has been demonstrated that a participatory method in which residents are directly involved by supplying local intelligence is one social channel through which behavioural changes can develop and become effective in combating energy theft [6]. Exploring informal reporting possibilities, such as whistleblowing, becomes critical in this regard.

In countries like South Africa, the IOL [29] reported that communities become hostile to electrical technicians who disconnect them from the grid, and such hostilities result in damage to the electricity supplier's vehicles and equipment. Furthermore, when disconnected, the consumers reconnect immediately after the technician leaves. This behaviour leads to honest users becoming dishonest, as they do not see value in paying for services that others are illegally getting for free.

Governments are also playing a role in combating electricity theft by placing regulations and subsidising electricity [30]. For instance, Turkey's Energy Market Law No. 4628, as revised by Electricity Market Law No. 6446, was enacted in 2001 and paved the way for a free market in the nation's electricity generation and delivery. It established a regulatory body with authority to establish energy prices, provide licenses, and prevent anti-competitive behaviour [5]. Furthermore, governments applied regulatory measures to punish perpetrators. This is demonstrated by Savian, Siluk, Garlet, do Nascimento, Pinheiro and Vale [5] when they allude to the fact that a person who uses deceptive means to interrupt or change the public electrical service in Lebanon faces up to six months in prison and a fine. However, in other developing countries, electricity theft is not treated as a criminal offence, rendering the regulations ineffective [2]. Nonetheless, Yakubu, Babu C and Adjei [24] argue that the high cost of electricity and the subpar quality of the electricity

provided in developing countries should be considered while developing policies to combat electricity theft. In agreement with the previous statement, policy makers should take into account the unemployment and poverty rate in developing countries to accommodate those who are disadvantaged.

Other efforts, such as subsidies for electricity, have been implemented. To subsidise a significant portion of the capital expenditures of electrical connections under the electrification program, the government of South Africa established the National Electrification Fund (NEF). The NEF receives funds from a variety of sources, including grants, budgetary allocations, and the electrical sector [31]. Subsidizing alters attitudes toward legitimacy and affordability, which eventually promotes inclusiveness and adherence to the official framework for electricity use [32].

The development and installation of Smart Girds (SGs) and Advanced Metering Infrastructure (AMI) in the supply of electricity have given rise to the application of technology-based solutions in addressing the issue of electricity theft. Such technology-based solutions include the application of the Internet of Things (IoT), the application of machine learning (ML) and Artificial Intelligence (AI), and the use of data analytics [33,34].

The theft of electricity is a topic that is treated more technically in literature. As such, numerous initiatives are being implemented worldwide to achieve a decrease in electricity theft. For example, Yakubu and Babu. [35] developed a hybrid ML model based on DFT decomposition for forecasting most time-series challenges, and Munikoti et al. [36] applied the voltage sensitivity analysis (VSA) to develop a model that enables the analysis of voltage change stochastically, using low computational resources. In VSA, sensitive voltage levels are compared to variations in system parameters like generation, load, or network topology at different points in the electrical grid.

From the preceding discussion, the solutions can be classified under three categories, namely conventional, government-enabled, and technology-based solutions. Figure 1 summarizes the identified solutions.

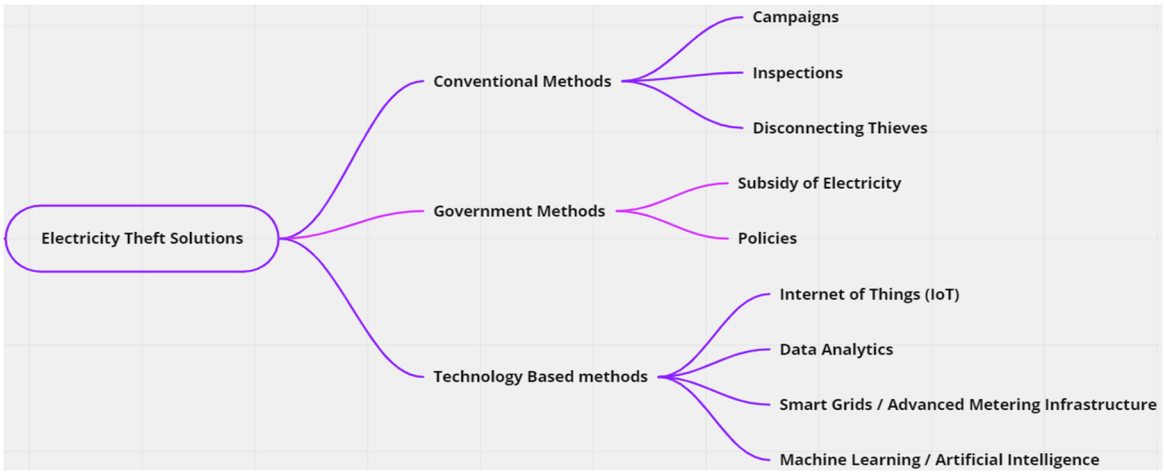

Figure 1. Summary of electricity theft solutions.

3. Methodology

The Preferred Items for Reporting for Systematic Reviews and Meta-Analysis (PRISMA) statement was followed in the development of this systematic review, as recommended by Page et al. [37].

This study used a systematic literature review to fulfil its research objective. According to Xiao and Watson [38], an SLR approach consists of six steps known as systematic review protocol, and these are the formulation of research problem and corresponding questions, article-search plan, selection criteria, quality assessment criteria, data extraction process, and data extraction and synthesis process. Figure 2 depicts a diagrammatic summary of the

six steps. The subsections below present a discussion on how each step was implemented by the study.

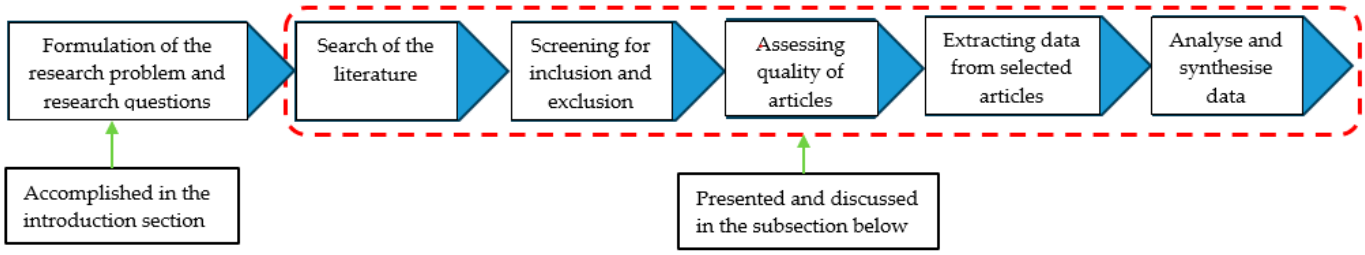

Figure 2. SLR protocol.

3.1. Search for Empirical Studies

Three electronic databases were selected for this study, SCOPUS, Science Direct, and Web of Science, because of the vast number of journals they have from major reputable publishers. This study considered journal articles only because they are the backbone of academic research [39,40]. Search strings used include electricity theft (including detection and/or prevention) and synonyms for electricity (power and energy) and theft (fraud). The combination of the following keywords was used to retrieve relevant empirical studies from the abovementioned databases: ("Electricity" OR "Power" OR "Energy") AND ("theft OR "fraud") AND "detection" OR ("detection" AND "prevention"). The search string terms were customized according to the individual needs and syntax of the individual databases.

The database searches, as depicted in Table 1, were conducted in May 2022 and returned a total of 1017 (111 from Science Direct, 289 from Web of Science and 617 from SCOPUS) articles, inclusive of duplicates, that were published between 2012 and 2022. Mendeley, one of the popular reference management tools, was used to filter out duplicate articles. After the removal of duplicate articles, 622 articles remained for further analysis. Of these, 281 were removed based on the title screening process, while 341 of them were retained for further screening. The abstract screening process resulted in 24 articles considered for inclusion. These articles also met the full selection criteria shown in Figure 3.

Table 1. Database search results.

Search Strings	**Articles Returned per Database**			
	Science Direct	Web of Science	SCOPUS	TOTAL
("Electricity" OR "Power" OR "Energy") AND ("theft OR "fraud") AND "detection" OR ("detection" AND "prevention")	111	289	617	1017

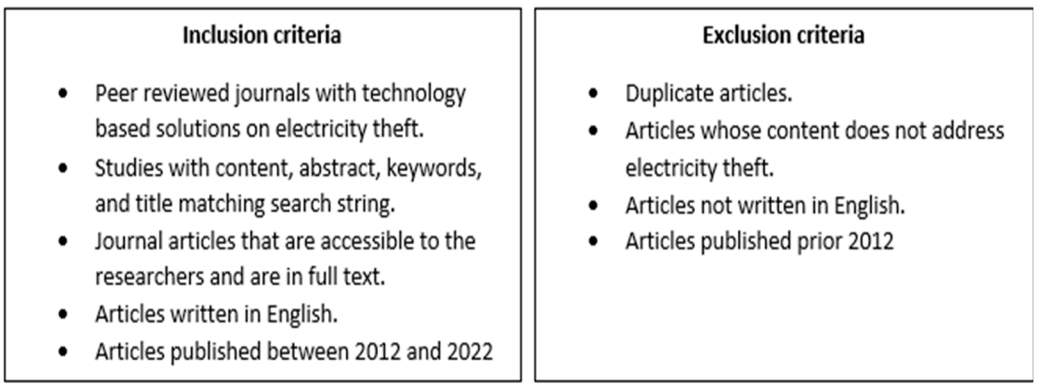

Figure 3. Full selection criteria.

3.2. Quality Assessment of Articles

The remaining 24 articles were quality assessed using the assessment criteria (see Table 2) extracted from the guidelines suggested by Kitchenham and Charters [41]. The results of this process are summarised in Table 3. Of the 24 articles assessed, 17 articles were empirical studies, and 7 were survey studies. The following scoring criteria were used in the assessment process: An article was allocated a score of 1, denoted by "Y" for meeting a quality criterion, and 0 denoted by "N" for failing to meet an assessment criterion. Only 11 articles met all the quality assessment criteria, and, therefore, these articles were considered for data extraction. Using the 11 articles, forward and backward reference searches were performed, and 5 relevant articles were identified. However, the full text of the 5 articles could not be located, and, therefore, they were excluded based on the inclusion/exclusion criteria.

Table 2. Quality assessment criteria.

Quality Assessment Criteria
Q1. Is the study empirical?
Q2. Is the research method clearly defined (data collection and analysis)?
Q3. Are the study's objectives clearly stated and addressed?
Q4. Is there a clear link between data analysis and the study findings that lead to a sound conclusion?

Table 3. Quality assessment criteria results [11,19,25,42–62].

#	Author(s)	Year	Q1	Q2	Q3	Q4	Total
1	Abdulaal et al. [50]	2022	Y	Y	Y	Y	4
2	Arif et al. [52]	2022	Y	Y	Y	Y	4
3	Ibrahim et al. [53]	2021	Y	Y	Y	Y	4
4	Jain et al. [54]	2019	Y	Y	Y	Y	4
5	Javaid et al. [55]	2021	Y	Y	Y	Y	4
6	Lepolesa et al. [56]	2022	Y	Y	Y	Y	4
7	Li et al. [57]	2019	Y	Y	Y	Y	4
8	Micheli et al. [58]	2019	Y	Y	Y	Y	4
9	Shaaban et al. [59]	2021	Y	Y	Y	Y	4
10	Ullah at al. [60]	2021	Y	Y	Y	Y	4
11	Zheng et al. [61]	2018	Y	Y	Y	Y	4
12	Jindal et al. [62]	2016	Y	N	Y	Y	3
13	Ahmed et al. [51]	2022	N	Y	Y	Y	3
14	Althobaiti et al. [25]	2021	N	Y	Y	Y	3
15	Dash et al. [49]	2021	N	Y	Y	Y	3
16	Glauner et al. [48]	2017	N	Y	Y	Y	3
17	Gupta et al. [47]	2020	N	Y	Y	Y	3
18	Takiddin [46]	2021	N	Y	Y	Y	3
29	Xia et al. [45]	2022	N	Y	Y	Y	3
20	Afridi et al. [19]	2021	Y	N	Y	N	2
21	Ballal [44]	2021	Y	N	Y	N	2
22	Ballal et al. [11]	2020	Y	N	Y	N	2
23	Wisetsri et al. [43]	2022	Y	N	N	N	1
24	Yao et al. [42]	2019	Y	N	N	N	1

According to Xiao and Watson [38], a review protocol is vital for reducing potential bias by the researcher, and it should cover all aspects of a review. Figure 2 shows the review protocol for this study, covering the aforementioned guidelines and process steps for an SLR. The protocol was developed by one author (P.M.K) and validated by the other two authors (S.M.M and R.T.H). Furthermore, to alleviate potential bias, the authors followed quality assessment guidelines proposed by Kitchenham and Charters [41].

3.3. Data Extraction and Synthesis of Results

Data were extracted from 11 articles selected based on the selection process shown in Figure 4. The sorting of articles for data extraction was performed using JabRef (Version 5.13), which is an open-source reference manager, and the extracted data were organized and stored in Microsoft Excel (Version 16.0) by the first author (P.M.K.) and verified by the second author (S.M.M.). The data extracted include the author, year of publication, title of the study, publisher, type of electricity theft addressed, proposed solution, detection and prevention technology used, and results of the study.

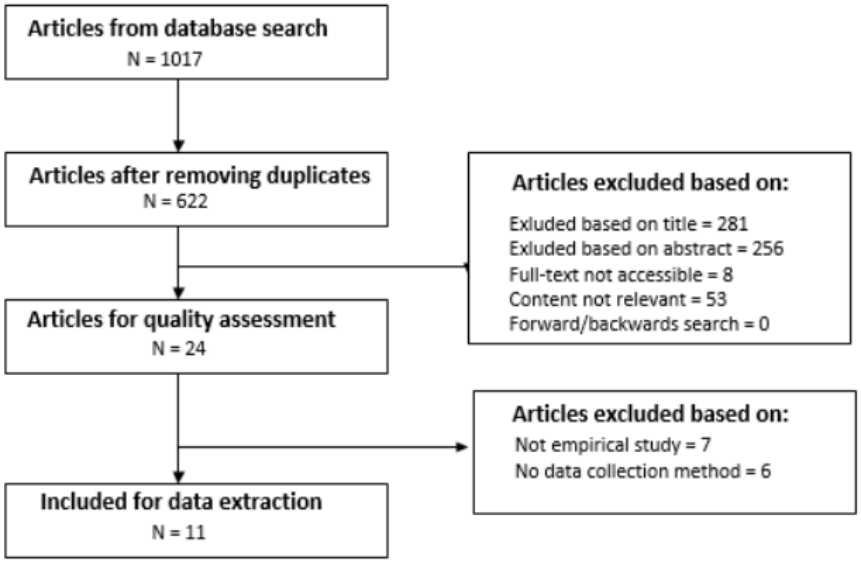

Figure 4. Article search and selection process.

The information extracted was combined to answer the study's research questions. The information shown in Table 4 shows the extracted data from the 11 selected articles. The information helps address the study's Questions 1 and 2, which assess what research has been performed on the topic and where the studies have been published, respectively. The information in Table 5, on the other hand, seeks to answer Question 3, which assesses the effectiveness of the proposed solutions by showing the performance measures of the solutions and results of the studies.

Table 4. Identified studies for electricity theft, detection, and prevention.

Author(s)	Title	Publication	Publisher	Study ID
Abdulaal, Ibrahem, Mahmoud, Khalid, Aljohani, Milyani and Abusorrah [50]	"Real-Time Detection of False Readings in Smart Grid AMI Using Deep and Ensemble Learning"	Journal (*IEEE Access*)	Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, United States	A
Arif, Alghamdi, Khan and Javaid [52]	"Towards Efficient Energy Utilization Using Big Data Analytics in Smart Cities for Electricity Theft Detection"	Journal (*Big Data Research*)	Elsevier Inc.: Amsterdam, The Netherlands	B
Ibrahim, Al-Janabi and Al-Khateeb [53]	"Electricity-theft detection in Smart Grids based on deep learning"	Journal (*Bulletin of Electrical Engineering and Informatics*)	Institute of Advanced Engineering and Science: Yogyakarta City, Indonesia	C

Table 4. *Cont.*

Author(s)	Title	Publication	Publisher	Study ID
Jain, Choksi and Pindoriya [54]	"Rule-based classification of energy theft and anomalies in consumers load demand profile"	Journal (*IET Smart Grid*)	Institution of Engineering and Technology: Lucknow, India	D
Javaid, Jan and Javed [55]	"An adaptive synthesis to handle imbalanced big data with deep Siamese network for electricity theft detection in smart grids"	Journal (*Journal of Parallel and Distributed Computing*)	Academic Press Inc.: Cambridge, MA, United States	E
Lepolesa, Achari and Cheng [56]	S	Journal (*IEEE Access*)	Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, United States	F
Li, Han, Yao, Yingchen, Wang and Zhao [57]	"Electricity Theft Detection in Power Grids with Deep Learning and Random Forests"	Journal (*Journal of Electrical and Computer Engineering*)	Hindawi Limited: London, United Kingdom	G
Micheli, Soda, Vespucci, Gobbi and Bertani [58]	"Big data analytics: an aid to detection of non-technical losses in power utilities"	Journal (*Computational Management Science*)	Springer Verlag: Berlin, Germany	H
Shaaban, Tariq, Ismail, Almadani and Mokhtar [59]	"Data-Driven Detection of Electricity Theft Cyberattacks in PV Generation"	Journal (*IEEE Systems Journal*)	Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, United States	I
Ullah, Javaid, Yahaya, Sultana, Al-Zahrani and Zaman [60]	"A Hybrid Deep Neural Network for Electricity Theft Detection Using Intelligent Antenna-Based Smart Meters"	Journal (*Wireless Communications and Mobile Computing*)	Hindawi Limited: London, United Kingdom	J
Zheng, Yang, Niu, Dai and Zhou [61]	"Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids"	Journal (*IEEE Transactions on Industrial Informatics*)	IEEE Computer Society: London, United Kingdom	K

Synthesizing data includes organizing and summarizing the results of the empirical studies included in the systematic review [41]. Therefore, the technologies used for the proposed solutions included in the review are summarized into categories, as displayed in Table 5. This study applied a descriptive synthesis to answer research Question 1 of this study.

Table 5. Technology based solutions for electricity theft detection and prevention.

Study ID	Proposed Solution	Dataset + Performance Measurement + Results	Technology Used	Category
A	Ensemble-based deep-learning detector that enables the System Operator to detect false readings in real time.	***Reference Energy Disaggregation Dataset (REDD):*** The dataset comprises of real consumption readings from honest users recorded at one-minute intervals. The authors generated a new dataset using 10-min intervals for training their model. ***Confusion matrix (False Alarm):*** The detector (equipped with GRU and a fully connected neural network) was able to identify false readings after only about 15 readings, which is significantly fewer than what is required by daily detection methods (144 readings) or weekly detection methods (1008 readings).	Gated Recurrent Unit (GRU)	Classification
B	Tomek Link Borderline Synthetic Minority Oversampling Technique with Support Vector Machine and Temporal Convolutional Network with Enhanced Multi-Layer Perceptron electricity theft detection.	***State Grid Cooperation of China (SGCC) dataset:*** is labelled and consists of honest and fraudulent consumption data recorded over a period of 3 years on a daily basis (has imbalanced data). ***Pakistan Residential Electricity Consumption (PRECON) dataset:*** consumption data of 43 users recorded every minute over a period of a year (contains consumption and auxiliary data). The data was converted to one day intervals for training the model. ***AUC:*** The TCN-EMPL model obtained a higher AUC (83%) reading in low computational resources when compared with other deep learning models such as MLP combined with LSTM (82%—second best). After using auxiliary data, the model improved by 2%.	Temporal Convolutional Network (TCN) + Enhanced Multi-Layer Perceptron (EMLP)	Classification
C	A convolutional neural network (CNN) model for automatic electricity theft detection.	***SGCC dataset:*** The authors filled the missing data with zero values for training their model. ***Accuracy:*** In terms of reducing features to improve performance, the authors applied the blue monkey (BM) algorithm that reduced the number of features from 1035 to 666 and obtained an accuracy score of 92%.	CNN + BM	Classification
D	Rule-based classification of energy theft and anomalies in consumers' load demand profile.	***Dataset***: The dataset utilized in this study belongs to Gujarat Urja Vikas Nigam Limited. It is made up of 15-min interval consumption recordings over a period of a year. ***Accuracy + FPR +Recall + Precision + F1-Score:*** The proposed model addresses user privacy by only using consumer consumption patterns and low sampling rate, while adequately predicting electricity theft.	Hierarchical Clustering + Decision Tree (DT) +	Clustering + Classification

Table 5. *Cont.*

Study ID	Proposed Solution	Dataset + Performance Measurement + Results	Technology Used	Category
E	An adaptive synthesis to handle imbalanced big data with a deep Siamese network for electricity theft detection in Smart Grids	***SGCC dataset:*** The authors used recommended metrics such as AUC and mAP to understand the imbalanced data. ***AUC + MAP:*** The combination of CNN-LSTM and DSN outperforms benchmark methods such as LR, SVM, RF, etc., in terms of AUC and mean average precision (MAP). The model reached the score of 90% for MAP and 93% for AUC, outperforming the benchmark methods who fall in the 70% range and below. This model proved to a better classifier of honest and fraudulent electricity users.	Adaptive Synthesis + CNN + Long Short-Term Memory (LSTM) + Deep Siamese Network (DSN)	Classification
F	Theft detection method, which uses comprehensive features in time and frequency domains in a deep neural network-based classification	***SGCC dataset:*** Data interpolation methods were used to fill out missing and zero values from the dataset. ***Accuracy + AUC:*** Compared to models in other studies using the same dataset, the proposed model reached 91.8% accuracy (second best) and 97% AUC. The model detects electricity theft slightly better (1%) than others in literature.	Deep Neural Network (DNN)	Classification
G	A novel hybrid convolutional neural network-random forest (CNN-RF) model for automatic electricity theft detection.	***Electric Ireland and Sustainable Energy Authority of Ireland (SEAI) dataset:*** smart meter data recorded in 30 min intervals over 525 days. one-hour interval data were generated for training the model. ***Low-Carbon London (LCL) dataset***: consumption readings over a period of 525 days. The authors used one-hour sampling rate. ***AUC:*** Classifiers such as SVM, RF, and GBDT were created and compared to CNN-RF on the same two datasets for electricity theft detection. The CNN-RF model achieved an AUC of 99% and 97% on datasets one and two, respectively, while the runner-up model scored 98% and 96% for the different datasets.	CNN + Random Forest (RF)	Classification
H	An AMI intrusion detection system that uses information fusion to combine the sensors and consumption data from a smart meter to accurately detect energy theft.	***Dataset*:** References a utility database with 96 days' worth of consumption readings recorded in 15 min' intervals. ***Accuracy + Sensitivity + Specificity:*** –In case of incomplete data from meter readings; the proposed multi-linear regression model outperforms classification models in terms of detecting fraudulent users. The model reached 100% accuracy, sensitivity, and specificity when using a very big dataset; for lower dataset sizes, the model prediction is in the 80% range.	Multiple Linear Regression	Regression

Table 5. *Cont.*

Study ID	Proposed Solution	Dataset + Performance Measurement + Results	Technology Used	Category
I	A data-driven approach based on machine learning to detect electricity thefts.	***Dataset*:** generated from historical records of temperature and solar irradiance data. ***Sensitivity + Specificity + Precision + Negative Predictive Value (NPV) + Accuracy + False Alarm:*** The TDU detects cyber-attacks in distributed generators. When compared with SVM, ARIMA, and LSE detectors in the same context. ARIMA and SVM performed better in terms of NPV and Sensitivity whereas the TDU outperformed them in the other metrics.	Regression Tree	Regression
J	A hybrid deep neural network, which combines convolutional neural network, particle swarm optimization, and gated recurrent unit.	***SGCC dataset:*** The authors used SMOTE to balance data. ***AUC + Accuracy + F1-Score + Recall + Precision*** Several models were trained to resolve data imbalance when predicting electricity theft. The CNN-GRU-PSO model was tested against SVM, LR, LSTM, CNN-LSTM, and CNN-GRU. SVM was 1% higher than the proposed CNN-GRU-PSO model in terms of accuracy (94%). The proposed model outperformed all the other models in all the remaining performance matrices recording 94% for Precision and F1-Score, and 95% for Recall and AUC.	CNN + GRU + Particle swarm optimization (PSO)	Classification
K	A novel electricity-theft detection method based on wide and deep convolutional neural networks (CNN).	***SGCC dataset****:* The dataset was balanced using data interpolation. Data were analysed using one-week intervals. ***AUC + MAP:*** Detects the periodic patterns of electricity consumption and non-periodic consumption to classify dishonest (non-periodic) and honest (periodic) users of electricity. For this challenge, the proposed model outperformed LR, SVM, RF, and CNN in predicting electricity theft.	Wide and deep CNN	Classification

4. Results and Discussion

A database search was conducted on SCOPUS, Science Direct, and Web of Science which resulted in 1017 articles spanning from 2012 to 2022. The screening process resulted in the removal of 395 duplicate articles and the exclusion of 281 articles based on title, 256 based on abstract, 53 based on irrelevant content, 8 based on full text not available, and 13 failing to meet the quality criteria. Eleven articles met all quality assessment criteria and were considered for data extraction. Additionally, through forward and backward reference searches, five relevant articles were identified, but full texts could not be located, resulting in their exclusion.

The discussions in the following subsections aim to present insight into the study's results and findings. Section 4.1 discusses the research results regarding empirical studies that address electricity theft detection and prevention using technology. It further provides information on where such studies have been published. Therefore, the first subsection presents information and findings which fulfil the first two objectives of the study, namely to identify empirical studies that have been performed to address electricity theft, detection, and prevention using technology-based solutions; and to identify which journals and publishers focus on technology-based electricity theft, detection, and prevention methods. Section 4.2 discusses the study's research results, addressing the following research objective: to determine how effective the proposed/designed solutions have been (determination of their success and shortcomings).

4.1. Existence of Empirical Studies to Address Electricity-Related Problems

The information presented in Tables 3–5 shows that many countries have adopted the use of SG and AMI to combat the challenge of electricity theft. This finding agrees with the observation made by Otuoze, et al. [63], who state that SG has become the prevalent solution in combating electricity theft. Furthermore, SG and AMI offer benefits such as the generation of electricity bills by a central processing unit and the detection of meter tempering. As such, studies by Ibrahim, Al-Janabi and Al-Khateeb [53], Li, Han, Yao, Yingchen, Wang and Zhao [57], Micheli, Soda, Vespucci, Gobbi and Bertani [58] are focused on finding solutions for detecting and preventing illegal electricity consumption by means of manipulating consumption readings (meter bypassing) because SG and AMI do not offer such functionality. However, SG and AMI have sum check meters which are designed to track the overall energy input into a particular segment of the grid. They then compare the energy input with the total energy consumption measured by individual consumer meters within that segment. The information from sum check meters can be used as ground truth to validate data-processing algorithms' ability to detect actual electricity theft, as implemented by Micheli, Soda, Vespucci, Gobbi and Bertani [58], Shaaban, Tariq, Ismail, Almadani and Mokhtar [59]. However, this technique has been neglected by the majority of the selected studies. Data-processing algorithms detect electricity theft through analysing consumption patterns and anomalies to classify potential theft.

Moreover, this study observed that machine learning (ML), deep learning, and big data analytics are prevalent technology methods for detecting meter bypassing in SG and AMI. The proposed models in the selected studies employ classification, regression, and clustering techniques to differentiate between fraudulent and honest users. It is further observed that classification is the most preferred method for detecting electricity theft, as shown in Table 5. However, using a single classification method is not sufficient to produce satisfactory results, and, therefore, a combination of these techniques has been used by Abdulaal, Ibrahem, Mahmoud, Khalid, Aljohani, Milyani and Abusorrah [50], Arif, Alghamdi, Khan and Javaid [52], Javaid, Jan and Javed [55], Li, Han, Yao, Yingchen, Wang and Zhao [57], Ullah, Javaid, Yahaya, Sultana, Al-Zahrani and Zaman [60] to better detect electricity theft. Furthermore, the authors Shaaban, Tariq, Ismail, Almadani and Mokhtar [59] have successfully applied regression and clustering techniques to detect and prevent electricity theft in SG and AMI. This study further discovered that a majority of the journals that address the issue at hand are from the Institute of Electrical and Electronics

Engineers (IEEE). However, the lack of publications of non-SG and AMI studies in detecting and preventing electricity theft in the past decade points to the need to investigate suitable mechanisms to deploy in countries that do not have SG and AMI. On the contrary, this may suggest a potential bias in journals and publication houses in regard to accepting and publishing studies of such a nature.

The next discussion is on the effectiveness of the existing technological solutions in addressing electricity theft detection and prevention. The proposed solutions in the listed studies are grouped according to their categories: classification models, classification with clustering models, and regression models.

4.2. The Effectiveness of the Existing Solutions in Addressing Electricity-Related Problems

4.2.1. Classification Models

The research results of this study show that machine-learning classification models are a more efficient way to separate fraudulent consumption of electricity from honest consumption, as stipulated in Table 5. These findings are drawn from studies by Abdulaal, Ibrahem, Mahmoud, Khalid, Aljohani, Milyani and Abusorrah [50], Arif, Alghamdi, Khan and Javaid [52], Ibrahim, Al-Janabi and Al-Khateeb [53], Javaid, Jan and Javed [55], Lepolesa, Achari and Cheng [56], Li, Han, Yao, Yingchen, Wang and Zhao [57], Ullah, Javaid, Yahaya, Sultana, Al-Zahrani and Zaman [60], Zheng, Yang, Niu, Dai and Zhou [61], Huang and Xu [64], who have all applied classification techniques to detect electricity theft. Of the applied classification techniques, CNN is the most used. The benefit of using CNN is its autonomous ability to detect important features, and also it is friendly to computational requirements of the Central Processing Unit (CPU) and Random Access Memory (RAM), as indicated by Javaid, Jan and Javed [55]. Nonetheless, this study discussed how CNN alone does not provide optimal classification results; it is, therefore, no surprise that studies by Abdulaal, Ibrahem, Mahmoud, Khalid, Aljohani, Milyani and Abusorrah [50], Javaid, Jan and Javed [55], Li, Han, Yao, Yingchen, Wang and Zhao [57], Ullah, Javaid, Yahaya, Sultana, Al-Zahrani and Zaman [60] combined CNN with other classification techniques to produce models with better prediction accuracy for the detection of electricity theft.

The performance of the classification models was largely measured using AUC, followed by accuracy metrics. Based on these findings, one might assume that using both metrics to measure the performance of a classification model will give an advantage in prediction accuracy over using them separately. However, the findings of this study (see Table 5) show that selecting a good combination of ML algorithms is the factor that gives one model an advantage over the other in terms of prediction accuracy. Furthermore, from the selected studies, classification models that were combined with CNN show to have AUC and accuracy readings above 90%.

While reducing the frequency of recordings (sampling rate) can affect the ability of a model to predict accurately, authors such as [50,61,65] carefully considered the trade-offs between data resolution and prediction accuracy to produce models that performed satisfactory regardless of the reduced sampling rate. Moreover, reducing the sampling rate may also help in identifying the periodicity of the data which may be difficult to identify when data are recorded in short intervals, as seen in [61]. Furthermore, being able to apply feature reduction techniques that are best suited for your dataset and ML algorithm(s) is pivotal in terms of increasing the detection rate of your model. These techniques include the blue monkey algorithm and Minimum Redundancy Maximum Relevance, as displayed in studies by [53,56]. However, computational resources play a big role in determining the response time of ML models.

4.2.2. Classification with Clustering Models

In agreement with Saeed, et al. [66], the evaluation of the selected articles shows that clustering techniques are good for reducing the amount of processing needed for classification because they excel at grouping similar users of different consumption patterns. Moreover, clustering offers benefits such as low-sampling rates and minimal usage of meta-

data and communication layer, which afforded researchers Jain, Choksi and Pindoriya [54] the flexibility to create a model that protect user privacy. However, it is worth noting that clustering techniques are not favourable for pinpointing electricity thieves because of their inability to produce deep insight into fraudulent users. These findings are in sync with the declarations of Savian, Siluk, Garlet, do Nascimento, Pinheiro and Vale [5]. Thus, clustering techniques have been used with other techniques to detect electricity theft in AMI.

4.2.3. Regression Models

With regards to regression models, the selected studies show that regression models perform satisfactorily irrespective of the size of data used; hence, Micheli, Soda, Vespucci, Gobbi and Bertani [58] model leveraged the strength of the regression technique by outperforming data mining models in terms of identifying electricity theft even when analysing a small dataset. Furthermore, regression models are good when used to predict continuous data; hence, Shaaban, Tariq, Ismail, Almadani and Mokhtar [59] used a regression tree to detect electricity theft performed in the distributed generation domain as opposed to detecting theft from the consumption domain. Accuracy, specificity, and sensitivity were the common metrics that were used for determining the performance of regression models.

The common limitation amongst the included studies is a lack of fraudulent user data, which affects the ability of the models to detect theft in complex real-life situations, as reported by Jain, Choksi and Pindoriya [54], Shaaban, Tariq, Ismail, Almadani and Mokhtar [59], Ullah, Javaid, Yahaya, Sultana, Al-Zahrani and Zaman [60]. Other limitations include the lack of adequate computing power, which limits the model's ability to analyse fine details of the data, as reported by [52]. Further limitations include theft detection not being performed in real time, and the neglect of data privacy. Furthermore, a notable portion of the selected studies, including those by Abdulaal, Ibrahem, Mahmoud, Khalid, Aljohani, Milyani and Abusorrah [50], Ibrahim, Al-Janabi and Al-Khateeb [53], Javaid, Jan and Javed [55], Micheli, Soda, Vespucci, Gobbi and Bertani [58], Zheng, Yang, Niu, Dai and Zhou [61], have not reported their limitations.

5. Conclusions

Xiao and Watson [38] state that the systematic review process must be reported exhaustively so that it can be reliable and repeatable. This study transparently outlined its review process and reported its findings on searching the literature, the screening process, quality screening, and the research results.

A detailed systematic review of the literature on technology-based solutions used to detect and prevent electricity theft and their effectiveness from three major databases, namely SCOPUS, Science Direct, and Web of Science, for the period 2012 to 2022, was presented in the preceding sections. The study focused on the proposed solutions, technology used, type of theft addressed, results, and limitations. It is well documented in the literature that electricity theft is a global phenomenon that affects both developed and developing countries. Electricity theft affects human lives negatively, paralyses economies, and is costly to governments. Various technological solutions have been implemented in efforts to address the different forms of electricity theft.

The results of this study show that there is significant neglect in the literature regarding the electricity theft crisis in countries where SG and AMI are not implemented. Most studies published in recent years focus on preventing theft in SG and AMI. Nonetheless, current solutions for detecting theft in SG and AMI lack datasets with sufficient fraudulent consumer data. There is, therefore, a need to explore models that will use sufficient real-life fraudulent user datasets to exceed the existing models in terms of electricity-theft detection.

Furthermore, the current solutions do not offer real-time prevention; rather, they detect and report on electricity theft instances for later preventative measures by electricity providers. This creates a view that journals that publish articles on the matter at hand portray detecting and reporting as the ultimate solution for preventing electricity theft in SG and AMI. Therefore, this study recommends that researchers and publishers focus on

providing solutions to prevent electricity theft in real time. This study further discovered that machine learning and big data analytics are the dominant technology used for detecting electricity theft in SG and AMI. Moreover, classification techniques have proven to be prevalent among the technology used in solving this challenge, with CNN being the popular classification technique that was included as part of the provided solutions. To measure the effectiveness of the provided solutions, AUC and accuracy metrics were the most used in the selected studies. Although these synthesised results are useful for future research aimed at developing solutions for combating electricity theft, the findings of this study are limited to articles found in the selected databases. To obtain a broader view of the matter, the authors recommend including more databases in future reviews.

Author Contributions: Conceptualisation, P.M.K.; literature review, P.M.K. and S.M.M.; protocol, P.M.K.; protocol validation, S.M.M. and R.T.H.; quality review and validation, P.M.K., S.M.M. and R.T.H.; data extraction and synthesis, P.M.K.; verification, S.M.M.; reporting P.M.K., S.M.M. and R.T.H.; report review, S.M.M. and R.T.H. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by Tshwane University of Technology.

Data Availability Statement: The material used in this study is publicly available from the sourced databases.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Arkorful, V.E. Unravelling Electricity Theft Whistleblowing Antecedents Using the Theory of Planned Behavior and Norm Activation Model. *Energy Policy* **2022**, *160*, 112680. [CrossRef]
2. Mujuzi, J. Electricity Theft in South Africa: Examining the Need to Clarify the Offence and Pursue Private Prosecution? *Obiter* **2020**, *40*, 78–87. [CrossRef]
3. Yurtseven, Ç. The Causes of Electricity Theft: An Econometric Analysis of the Case of Turkey. *Util. Policy* **2015**, *37*, 70–78. [CrossRef]
4. Shahid, M.B.; Shahid, M.O.; Tariq, H.; Saleem, S. Design and Development of an Efficient Power Theft Detection and Prevention System through Consumer Load Profiling. In Proceedings of the 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Swat, Pakistan, 24–25 July 2019; pp. 1–6.
5. Savian, F.d.S.; Siluk, J.C.M.; Garlet, T.B.; do Nascimento, F.M.; Pinheiro, J.R.; Vale, Z. Non-Technical Losses: A Systematic Contemporary Article Review. *Renew. Sustain. Energy Rev.* **2021**, *147*, 111205. [CrossRef]
6. Chetty, V.G. *The Combating of Unauthorised Electrical Connections in Kwazulu-Natal, South Africa*; Magister Technologiae, University of South Africa: Pretoria, South Africa, 2018.
7. Adongo, C.A.; Taale, F.; Bukari, S.; Suleman, S.; Amadu, I. Electricity Theft Whistleblowing Feasibility in Commercial Accommodation Facilities. *Energy Policy* **2021**, *155*, 112347. [CrossRef]
8. Yan, Z.; Wen, H. Electricity Theft Detection Base on Extreme Gradient Boosting in AMI. *IEEE Trans. Instrum. Meas.* **2021**, *70*, 2504909. [CrossRef]
9. Tanwar, S.; Kumari, A.; Vekaria, D.; Raboaca, M.S.; Alqahtani, F.; Tolba, A.; Neagu, B.-C.; Sharma, R. GrAb: A Deep Learning-Based Data-Driven Analytics Scheme for Energy Theft Detection. *Sensors* **2022**, *22*, 4048. [CrossRef]
10. Zheng, K.; Chen, Q.; Wang, Y.; Kang, C.; Xia, Q. A Novel Combined Data-Driven Approach for Electricity Theft Detection. *IEEE Trans. Ind. Inform.* **2019**, *15*, 1809–1819. [CrossRef]
11. Ballal, M.S.; Suryawanshi, H.; Mishra, M.K.; Jaiswal, G. Online Electricity Theft Detection and Prevention Scheme for Smart Cities. *IET Smart Cities* **2020**, *2*, 155–164. [CrossRef]
12. Mohanty, S.; Iqbal, M.; Thampi, P. Controlling and Monitoring of Power Theft Using Internet of Things. In Proceedings of the 2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C), Bangalore, India, 11–12 June 2021. [CrossRef]
13. Leninpugalhanthi, P.; Janani, R.; Nidheesh, S.; Mamtha, R.V.; Keerthana, I.; Kumar, R.S. Power Theft Identification System Using Iot. In Proceedings of the 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS), Coimbatore, India, 15–16 March 2019.
14. Munn, Z.; Peters, M.D.J.; Stern, C.; Tufanaru, C.; McArthur, A.; Aromataris, E. Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. *BMC Med. Res. Methodol.* **2018**, *18*, 143. [CrossRef]
15. Khonjelwayo, B.; Nthakheni, T. Determining the causes of electricity losses and the role of management in curbing them: A case study of City of Tshwane Metropolitan Municipality, South Africa. *J. Energy S. Afr.* **2021**, *32*, 45–57. [CrossRef]

16. Jawale, P.; Jain, A.; Deokate, S.; Kapse, A. Iot Based Smart Energy Meter Monitoring with Identification of Electricity Theft. In Proceedings of the 3rd International Conference on Communication & Information Processing (ICCIP) 2021, Haldia, India, 25 May 2021.
17. Bhalshankar, S.; Thorat, C. Direct Hooking Electric Theft: Silicone Rubber Piping over Bear Overhead Electric Conductors Technical Enforcement Mechanisms. *Int. J. Sci. Res.* **2018**, *7*, 739–740.
18. Chandel, P.; Thakur, T.; Sawale, B.A. Energy Meter Tampering: Major Cause of Non-Technical Losses in Indian Distribution Sector. In Proceedings of the International Conference on Electrical Power and Energy Systems (ICEPES), Bhopal, India, 14–16 December 2016; pp. 368–371.
19. Afridi, A.; Wahab, A.; Khan, S.; Ullah, W.; Khan, S.; Islam, S.Z.U.; Hussain, K. An Efficient and Improved Model for Power Theft Detection in Pakistan. *Bull. Electr. Eng. Inform.* **2021**, *10*, 1828–1837. [CrossRef]
20. Gehringer, C.; Rode, H.; Schomaker, M. The Effect of Electrical Load Shedding on Pediatric Hospital Admissions in South Africa. *Epidemiol. Author Manuscr.* **2018**, *29*, 841–847. [CrossRef] [PubMed]
21. Khwela, H. An Exploratory Study on Electricity Theft in Staram Informal Settlement in Tongaat in Durban, KwaZulu-Natal Province. Ph.D. Thesis, University of Kwazulu-natal, Durban, South Africa, 2019.
22. Saini, S. Social and Behavioral Aspects of Electricity Theft—An Explorative Review. *Int. J. Res. Econ. Soc. Sci.* **2017**, *7*, 26–37.
23. Depuru, S.S.S.R.; Wang, L.; Devabhaktuni, V. Electricity Theft: Overview, Issues, Prevention and a Smart Meter Based Approach to Control Theft. *Energy Policy* **2011**, *39*, 1007–1015. [CrossRef]
24. Yakubu, O.; Babu, C.N.; Adjei, O. Electricity Theft: Analysis of the Underlying Contributory Factors in Ghana. *Energy Policy* **2018**, *123*, 611–618. [CrossRef]
25. Althobaiti, A.; Jindal, A.; Marnerides, A.K.; Roedig, U. Energy Theft in Smart Grids: A Survey on Data-Driven Attack Strategies and Detection Methods. *IEEE Access* **2021**, *9*, 159291–159312. [CrossRef]
26. Mutebi, R.; Otim, J.; Sebitosi, A. Towards a Persuasive Technology for Electricity Theft Reduction in Uganda. In Proceedings of the eInfrastructure and e-Services for Developing Countries 9th International Conference, AFRICOMM 2017, Lagos, Nigeria, 11–12 December 2017. [CrossRef]
27. Landie, C. Power up against Electricity Theft. *Inst. Munic. Eng. S. Afr.* **2011**, *36*, 63.
28. Shokoya, O.; Raji, A. Electricity Theft: A Reason to Deploy Smart Grid in South Africa. In Proceedings of the 2019 International Conference on the Domestic Use of Energy (DUE), Wellington, South Africa, 25–27 March 2019.
29. IOL. Cape Izinyoka-Nyoka Cost Eskom Millions. Available online: https://www.iol.co.za/capetimes/news/cape-izinyoka-nyoka-cost-eskom-millions-73538605-296d-47cc-8f8c-381119b68cb4 (accessed on 14 June 2023).
30. Mbanjwa, T. An Analysis of Electricity Theft: The Case Study of Kwaximba in Ethekwini, Kwazulu-Natal. Ph.D. Thesis, University of Kwazulu-Natali, Durban, South Africa, 2017.
31. Davidson, O.; Mwakasonda, S.A. Electricity Access for the Poor: A Study of South Africa and Zimbabwe. *Energy Sustain. Dev.* **2004**, *8*, 26–40. [CrossRef]
32. Okpoudhu, U.; Oniemola, P.K.; Wifa, E.L. The Dilemma of Electricity Pricing and Cost Recovery in Nigeria: Repositioning the Law to Balance the Interests of Investors and Consumers. *Afr. Nazarene Univ. Law J.* **2019**, *7*, 115–137.
33. Sahoo, S.; Nikovski, D.N.; Muso, T.; Tsuru, K. Electricity Theft Detection Using Smart Meter Data. In Proceedings of the 2015 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Montevideo, Uruguay, 5–7 October 2015.
34. Kumarana, K.; Ananthib, N.; Saranyac, G.; Priyadharshinid, S.; Thiviyabalae, T.; Vaishnavif, K. Power Theft Detection and Alert System Using Iot. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 1135–1139.
35. Yakubu, O.; Babu, N. Electricity Consumption Forecasting Using Dft Decomposition Based Hybrid Arima-Dlstm Model. *Indones. J. Electr. Eng. Comput. Sci.* **2021**, *24*, 1107–1120. [CrossRef]
36. Munikoti, S.; Jhala, K.; Lai, K.; Natarajan, B. Analytical Voltage Sensitivity Analysis for Unbalanced Power Distribution System. In Proceedings of the 2020 IEEE Power & Energy Society General Meeting (PESGM), Montreal, QC, Canada, 2–6 August 2020; pp. 1–5.
37. Page, M.J.; Moher, D.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E. Prisma 2020 Explanation and Elaboration: Updated Guidance and Exemplars for Reporting Systematic Reviews. *Bmj* **2021**, *372*, n160. [CrossRef] [PubMed]
38. Xiao, Y.; Watson, M. Guidance on Conducting a Systematic Literature Review. *J. Plan. Educ. Res.* **2019**, *31*, 93–112. [CrossRef]
39. Thyer, B. The Importance of Journal Articles. *Oxf. Acad.* **2008**, 1–12. [CrossRef]
40. Palmatier, R.W.; Houston, M.B.; Hulland, J. Review Articles: Purpose, Process, and Structure. *J. Acad. Mark. Sci.* **2018**, *46*, 1–5. [CrossRef]
41. Kitchenham, B.; Charters, S. *Guidelines for Performing Systematic Literature Reviews in Software Engineering*; Keele University: Keele, UK, 2007; Volume 2.
42. Yao, D.; Wen, M.; Liang, X.; Fu, Z.; Zhang, K.; Yang, B. Energy Theft Detection with Energy Privacy Preservation in the Smart Grid. *IEEE Internet Things J.* **2018**, *6*, 7659–7669. [CrossRef]
43. Wisetsri, W.; Qamar, S.; Verma, G.; Verma, D.; Kakar, V.K.; Chansongpol, T.; Somtawinpongsai, C.; Tan, C.C. Electricity Theft Detection and Localization in Smart Grids for Industry 4.0. *Intell. Autom. Soft Comput.* **2022**, *33*, 1473–1483. [CrossRef]
44. Ballal, M.S. Online electrical energy theft detection and prevention scheme for direct hook-line activity. *J. Inst. Eng. (India) Ser. B* **2021**, *102*, 1007–1018. [CrossRef]

45. Xia, X.; Xiao, Y.; Liang, W.; Cui, J. Detection Methods in Smart Meters for Electricity Thefts: A Survey. *Proc. IEEE* **2022**, *110*, 273–319. [CrossRef]
46. Takiddin, A.; Ismail, M.; Zafar, U.; Serpedin, E. Robust electricity theft detection against data poisoning attacks in smart grids. *IEEE Trans. Smart Grid* **2020**, *12*, 2675–2684. [CrossRef]
47. Gupta, A.K.; Routray, A.; Naikan, V.A. Detection of power theft in low voltage distribution systems: A review from the Indian perspective. *IETE J. Res.* **2020**, *68*, 4180–4197. [CrossRef]
48. Glauner, P.; Meira, J.A.; Valtchev, P.; State, R.; Bettinger, F. The challenge of non-technical loss detection using artificial intelligence: A survey. *Int. J. Comput. Intell. Syst.* **2017**, *10*, 760–775. [CrossRef]
49. Dash, S.K.; Roccotelli, M.; Khansama, R.R.; Fanti, M.P.; Mangini, A.M. Long Term Household Electricity Demand Forecasting Based on RNN-GBRT Model and a Novel Energy Theft Detection Method. *Appl. Sci.* **2021**, *11*, 8612. [CrossRef]
50. Abdulaal, M.J.; Ibrahem, M.I.; Mahmoud, M.M.E.A.; Khalid, J.; Aljohani, A.J.; Milyani, A.H.; Abusorrah, A.M. Real-Time Detection of False Readings in Smart Grid Ami Using Deep and Ensemble Learning. *IEEE Access* **2022**, *10*, 47541–47556. [CrossRef]
51. Ahmed, M.; Khan, A.; Ahmed, M.; Tahir, M.; Jeon, G.; Fortino, G.; Piccialli, F. Energy theft detection in smart grids: Taxonomy, comparative analysis, challenges, and future research directions. *IEEE/CAA J. Autom. Sin.* **2022**, *9*, 578–600. [CrossRef]
52. Arif, A.; Alghamdi, T.A.; Khan, Z.A.; Javaid, N. Towards Efficient Energy Utilization Using Big Data Analytics in Smart Cities for Electricity Theft Detection. *Big Data Res.* **2022**, *27*, 100285. [CrossRef]
53. Ibrahim, N.M.; Al-Janabi, S.T.F.; Al-Khateeb, B. Electricity-Theft Detection in Smart Grids Based on Deep Learning. *Bull. Electr. Eng. Inform.* **2021**, *10*, 2285–2292. [CrossRef]
54. Jain, S.; Choksi, K.A.; Pindoriya, N.M. Rule-Based Classification of Energy Theft and Anomalies in Consumers Load Demand Profile. *IET Smart Grid* **2019**, *2*, 612–624. [CrossRef]
55. Javaid, N.; Jan, N.; Javed, M.U. An Adaptive Synthesis to Handle Imbalanced Big Data with Deep Siamese Network for Electricity Theft Detection in Smart Grids. *J. Parallel Distrib. Comput.* **2021**, *153*, 44–52. [CrossRef]
56. Lepolesa, L.J.; Achari, S.; Cheng, L. Electricity Theft Detection in Smart Grids Based on Deep Neural Network. *IEEE Access* **2022**, *10*, 39638–39655. [CrossRef]
57. Li, S.; Han, Y.; Yao, X.; Yingchen, S.; Wang, J.; Zhao, Q. Electricity Theft Detection in Power Grids with Deep Learning and Random Forests. *J. Electr. Comput. Eng.* **2019**, *2019*, 4136874. [CrossRef]
58. Micheli, G.; Soda, E.; Vespucci, M.T.; Gobbi, M.; Bertani, A. Big Data Analytics: An Aid to Detection of Non-Technical Losses in Power Utilities. *Comput. Manag. Sci.* **2019**, *16*, 329–343. [CrossRef]
59. Shaaban, M.; Tariq, U.; Ismail, M.; Almadani, N.; Ahmed, M. Data-Driven Detection of Electricity Theft Cyberattacks in Pv Generation. *IEEE Syst. J.* **2021**, *16*, 3349–3359. [CrossRef]
60. Ullah, A.; Javaid, N.; Yahaya, A.S.; Sultana, T.; Al-Zahrani, F.A.; Zaman, F. A Hybrid Deep Neural Network for Electricity Theft Detection Using Intelligent Antenna-Based Smart Meters. *Wirel. Commun. Mob. Comput.* **2021**, *2021*, 9933111. [CrossRef]
61. Zheng, Z.; Yang, Y.; Niu, X.; Dai, H.N.; Zhou, Y. Wide and Deep Convolutional Neural Networks for Electricity-Theft Detection to Secure Smart Grids. *IEEE Trans. Ind. Inform.* **2018**, *14*, 1606–1615. [CrossRef]
62. Jindal, A.; Dua, A.; Kaur, K.; Singh, M.; Kumar, N.; Mishra, S. Decision tree and SVM-based data analytics for theft detection in smart grid. *IEEE Trans. Ind. Inform.* **2016**, *12*, 1005–1016. [CrossRef]
63. Otuoze, A.O.; Mustafa, M.W.; Sofimieari, I.E.; Dobi, A.M.; Sule, A.H.; Abioye, A.E.; Saeed, M.S. Electricity Theft Detection Framework Based on Universal Prediction Algorithm. *Indones. J. Electr. Eng. Comput. Sci.* **2019**, *15*, 758–768. [CrossRef]
64. Huang, Y.; Xu, Q. Electricity Theft Detection Based on Stacked Sparse Denoising Autoencoder. *Int. J. Electr. Power Energy Syst.* **2021**, *125*, 106448. [CrossRef]
65. Lin, G.Y.; Feng, X.F.; Guo, W.C.; Cui, X.Y.; Liu, S.Y.; Jin, W.C.; Lin, Z.Z.; Ding, Y. Electricity Theft Detection Based on Stacked Autoencoder and the Undersampling and Resampling Based Random Forest Algorithm. *IEEE Access* **2021**, *9*, 124044–124058. [CrossRef]
66. Saeed, M.S.; Mustafa, M.W.; Hamadneh, N.N.; Alshammari, N.A.; Sheikh, U.U.; Jumani, T.A.; Khalid, S.B.A.; Khan, I. Detection of Non-Technical Losses in Power Utilities—A Comprehensive Systematic Review. *Energies* **2020**, *13*, 4727. [CrossRef]