Voltarea. 2023;1.1.002
ISNN:
DOI:

Article: Review

Internet of things for monitoring electrical systems: architectures, technologies and implementation challenges

Internet of things for monitoring electrical systems: architectures, technologies and implementation challenges

[1]Silvia Elena Mireille Ypanaque Arteaga.

[1]Universidad Nacional de Trujillo, Trujillo – Perú

***Corresponding author:** Silvia Elena Mireille Ypanaque Arteaga

Submitted: 29-12-2022 **Revised:** 04-01-2023 **Accepted:** 23-01-2023 **Published:** 19-02-2023

Cite as:

Ypanaque Arteaga, S. E. M. (2023). Internet of things for monitoring electrical systems: architectures, technologies and implementation challenges. *Voltarea*, *1*(1), 1-17. https://voltarea.dbeditorial.org/index.php/voltarea/article/view/8

ABSTRACT

Introduction: The Internet of Things has established itself as a relevant digital layer to observe electrical assets, integrate distributed measurements, and support operational decisions in increasingly connected energy systems.

Objective: To synthesize the evidence published between 2018 and 2022 on IoT architectures, enabling technologies, monitoring applications, and implementation challenges in electrical systems, identifying development patterns and research gaps.

Methodology: A systematic review was conducted using a structured search, screening, and eligibility process. Records were evaluated by period, thematic relevance, DOI availability, type of publication, and sufficiency of technical information. The final synthesis included 23 studies.

Results: The selected literature evidences a transition from general smart grid architectures to solutions oriented to wireless sensing, edge computing, power quality, equipment monitoring, and data analytics. Interoperability, cybersecurity, communication latency, data quality, and scalability repeatedly appeared as implementation constraints. Methodological heterogeneity limits direct comparison between architectures and rules out a common quantitative measure of effect.

Conclusions: IoT favors more continuous and distributed monitoring, but its practical usefulness depends on integration with legacy infrastructure, reliable data exchange, and security by design. Comparative validations, reproducible reports, and evaluations under representative operating conditions are required.

Keywords: Internet of Things; smart grid; electrical monitoring; interoperability; edge computing

RESUMEN

Introducción: El Internet de las Cosas se ha consolidado como una capa digital relevante para observar activos eléctricos, integrar mediciones distribuidas y apoyar decisiones operativas en sistemas energéticos cada vez más conectados.

Objetivo: Sintetizar la evidencia publicada entre 2018 y 2022 sobre arquitecturas IoT, tecnologías habilitadoras, aplicaciones de monitoreo y desafíos de implementación en sistemas eléctricos, identificando patrones de desarrollo y vacíos de investigación.

Metodología: Se realizó una revisión sistemática mediante un proceso estructurado de búsqueda, cribado y elegibilidad. Los registros se evaluaron por periodo, pertinencia temática, disponibilidad de DOI, tipo de

©2023 por los Autores. Este artículo es de acceso abierto y distribuido según los términos y condiciones bajo una licencia internacional Creative Commons Atribución 4.0. (CC BY 4.0) https://creativecommons.org/licenses/by/4.0/

publicación y suficiencia de información técnica. La síntesis final incluyó 23 estudios.
Resultados: La literatura seleccionada evidencia una transición desde arquitecturas generales de red inteligente hacia soluciones orientadas a sensado inalámbrico, computación en el borde, calidad de energía, supervisión de equipos y analítica de datos. La interoperabilidad, ciberseguridad, latencia de comunicación, calidad de datos y escalabilidad aparecieron reiteradamente como restricciones de implementación. La heterogeneidad metodológica limita la comparación directa entre arquitecturas y descarta una medida cuantitativa común de efecto.
Conclusiones: IoT favorece un monitoreo más continuo y distribuido, pero su utilidad práctica depende de la integración con infraestructura heredada, intercambio confiable de datos y seguridad desde el diseño. Se requieren validaciones comparativas, reportes reproducibles y evaluaciones en condiciones operativas representativas.

Palabras clave: Internet de las Cosas; red eléctrica inteligente; monitoreo eléctrico; interoperabilidad; computación en el borde

INTRODUCTION

During 2018–2022, the digital transformation of the electricity sector changed the way critical infrastructures are observed, interpreted, and managed. In this interval, the Internet of Things (IoT) applied to the monitoring of electrical systems went from occupying a predominantly conceptual space to being integrated into discussions on operation, supervision, automation, and decision-making. The selected literature shows that this evolution did not respond to a single technology, but to the convergence of communications, analytics, digital platforms, and new mechanisms of interaction between physical assets and informational layers (1,2,3). This convergence expanded the possibilities of supervision, but also made more visible the dependence on interoperable architectures, reliable data, and clear criteria to evaluate usefulness, security, and performance.

The scientific problem arises because the rapid expansion of the Internet of Things (IoT) applied to the monitoring of electrical systems produced a heterogeneous body of knowledge. The studies use different vocabularies, scales of analysis, and objectives; some focus on architectures and foundations, others on specific applications, and others on risks, limitations, or conditions of adoption (4,5,6). When these contributions are read in isolation, it is difficult to distinguish which components are more consolidated, which solutions are still experimental, and which challenges are repeated between contexts. A systematic review allows this diversity to be sorted and to avoid that the evaluation of the field depends only on emblematic works or recent technological developments.

The relevance of the problem increases because electrical systems combine requirements for continuity, reliability, security, and responsiveness in close to real time. Therefore, the incorporation of the Internet of Things (IoT) applied to the monitoring of electrical systems cannot be judged solely by technological novelty. Its relationship with data quality, available infrastructure, scalability, interoperability, and the possibility of integrating solutions with legacy systems must also be examined (7,8,9). The literature reviewed shows that technical utility depends on both the method used and the implementation conditions, so that a synthesis focused exclusively on algorithms or devices would offer an incomplete view of the development of the field.

Between 2018 and 2022, there is also a shift from general descriptions to proposals that are more application-oriented, architecture evaluation, and specific problem solving (10,11,12). This movement justifies jointly analyzing the review studies, applied works, conceptual proposals, and technical developments included in the matrix. Methodological diversity is not interpreted as an automatic weakness; it is a domain characteristic that requires classifying the purpose of each contribution and comparing results within compatible categories. This perspective makes it possible to identify trends without attributing equivalence to designs that answer different questions.

Another difficulty is related to the transfer of results. In electrical systems, a solution demonstrated in a controlled scenario does not necessarily maintain the same performance when integrated into heterogeneous networks, distributed infrastructures, or environments with communication and processing restrictions. Several works in the corpus highlight precisely challenges related to integration, reliability, security, computational load, or information governance (13,14,15). Therefore, the review considers not only what was done, but also under what technological logic it was done and what obstacles were recognized by the studies themselves. This distinction is essential to formulate a research agenda that does not confuse technical availability with maturity of adoption.

The formulation of the problem that guides this study is expressed through the following question: What architectures, enabling technologies, monitoring applications, and implementation challenges characterized the use of IoT in electrical systems between 2018 and 2022? The question integrates four planes: conceptual evolution, technological components, reported applications, and recurrent limitations. Its purpose is not to establish an aggregate effect through meta-analysis, because the designs and results of the studies are too heterogeneous to assume a common metric. Instead, a systematic descriptive and thematic synthesis is adopted, supported by a matrix of selected studies that preserves authorship, year, source, DOI, type of study, and main technique. This decision allows for a correspondence between each synthesis statement and the bibliographic evidence that supports it.

The overall objective was to synthesize the evidence published between 2018 and 2022 on architectures, enabling technologies, monitoring applications, and challenges of the Internet of Things in electrical systems, identifying development patterns and research gaps. To achieve this objective, 23 selected studies with DOIs were examined within the defined period. The review seeks to provide an organized reading of the field and not to substitute for primary experimental evaluations. Consequently, the frequencies used in Results exclusively describe the composition of the corpus and should not be interpreted as population prevalences. The comparison between types of studies, years, and techniques is used to recognize research concentrations, less developed areas, and conceptual relationships that can guide subsequent work.

The contribution of the article lies in integrating dispersed evidence through a reading structure coherent with the problem. First, the conceptual framework that allows interpreting the Internet of Things (IoT) applied to the monitoring of electrical systems is delimited; then the search, eligibility, extraction and synthesis criteria are explained; then the study matrix and the resulting patterns are presented; finally, convergences, tensions and gaps are discussed. This sequence seeks to allow the

reader to move from the general picture to the individual evidence without losing the relationship between question, method and conclusion. By keeping the references in the order of appearance and preserving the DOI of the studies, the review also facilitates the documentary verification of the included sources.

LITERATURE REVIEW

IoT Architectures for Electrical Networks and Systems

The first conceptual dimension of the Internet of Things (IoT) applied to the monitoring of electrical systems is related to the way in which electrical systems incorporate digital layers to represent, communicate, or interpret operating states. The literature does not present a single architecture; rather, it describes combinations of sensors, communications, models, algorithms, and platforms that depend on the purpose of the application. This heterogeneity makes it necessary to differentiate between enabling infrastructure and analytical function. A technology can be central to data acquisition and, at the same time, secondary to the final decision. Corpus studies show that effective integration requires correspondence between sampling frequency, latency, data quality, and operational need. (16,17).

A second axis is interoperability. Electrical digitalization connects equipment with different life cycles, heterogeneous protocols, and unequal computing capabilities. Therefore, the value of the Internet of Things (IoT) applied to the monitoring of electrical systems depends on the possibility of exchanging information without losing meaning, integrity, or opportunity. The selected works point out that open architectures favor integration, but also expand exposure surfaces and governance needs. The problem is not limited to syntactic compatibility; it includes data semantics, temporal synchronization, identity management, and maintenance of models or rules as the infrastructure changes. (17,18).

Distributed computing appears as a response to latency and volume constraints. Processing close to the source can reduce traffic and accelerate decisions, while centralized services facilitate historical storage and larger-scale analysis. The literature reviewed does not consider these approaches as exclusive. A hybrid logic predominates in which functions are assigned according to criticality, response time, availability of communications and computational resources. This organization introduces, however, new problems of coordination, updating and consistency, especially when different components operate with partial information or with different time horizons. (18,19).

Sensing, communication and edge computing

The quality of information is another cross-cutting condition. Digital electrical systems depend on sufficiently complete, synchronized and representative data. Measurement errors, packet losses, topology changes or out-of-distribution data can alter the performance of models and monitoring mechanisms. The literature insists that data augmentation does not automatically guarantee better decisions. Validation procedures, missing handling, anomaly detection and provenance documentation are required. This requirement is particularly important when technological results are used to support operational decisions with consequences on continuity or security. (19,20).

At the application level, studies show an expansion from basic supervision to prognosis, diagnosis, maintenance, control, reliability evaluation, and decision support. The maturity of each application is uneven. Some proposals are supported by conceptual reviews and prototypes, while others employ case studies or empirical data. Therefore, the synthesis must separate feasibility evidence from performance evidence. A well-described architecture can demonstrate conceptual coherence without yet accrediting scalability; in the same way, a favorable result in a particular case does not imply automatic generalization to other systems. (20,21).

The security dimension cuts across the field. As connectivity increases, the need to protect confidentiality, integrity, and availability, but also to preserve operational continuity, grows. Security should be considered by design and not as an added layer after the solution is deployed. The selected studies link risks to communications, devices, platforms, models, and human processes. This broad view is relevant because a technically efficient architecture can generate vulnerabilities if it does not include authentication, segmentation, updating, monitoring, and incident response. (21,22).

Monitoring, interoperability and data management

Scalability represents a different challenge. Solutions that work with few devices or assets can face bottlenecks when the number of nodes, the frequency of data, or the complexity of coordination increases. The literature reviewed discusses scalability in both computational and organizational terms. It is not enough to increase processing capacity; configurations, versions, permissions, models, and rules must also be managed. Sustainable scalability requires modularity and management mechanisms that allow new assets to be incorporated without completely rebuilding the architecture. (22,23).

Performance evaluation is another point of heterogeneity. Studies use different indicators and, in many cases, there is no common metric that allows quantitative aggregation. Some prioritize accuracy or error, others latency, reliability, detection, availability, or interpretability. This diversity justifies a structured narrative synthesis rather than a meta-analysis. Comparison is made by function and purpose, avoiding converting non-equivalent metrics into an artificial ranking. This decision preserves interpretative validity and allows recognizing which dimensions receive more attention and which lack shared evaluation protocols. (23).

The human and organizational factor also conditions adoption. Although much of the literature is technological, implementation occurs within organizations with specific capabilities, responsibilities, and constraints. The usefulness of a solution depends on operators and managers being able to understand their function, maintain it, and respond when the system deviates from what is expected. The most integration-oriented studies show that documentation, competencies, and governance are complements to technical architecture. This dimension is especially important in critical infrastructures, where an automated decision must coexist with supervision and accountability procedures. (23).

Security, Scalability, and Deployment Challenges

From a temporal perspective, the period 2018–2022 captures a stage of rapid conceptual consolidation. The earliest works tend to establish frameworks, taxonomies, or foundations, while a relevant part of the 2021–2022 publications expand applications and challenges. This recent concentration does not mean that the field has reached uniform maturity. On the contrary, the coexistence of reviews, conceptual studies, and specific applications indicates that different subareas are advancing at different rates. The systematic review allows us to observe this transition without projecting the maturity of its most developed examples onto the entire domain. (23).

The evidence also shows that the frontiers of the field are porous. Some selected studies provide methodological or architectural foundations from adjacent domains because they help to understand components necessary for the Internet of Things (IoT) applied to the monitoring of electrical systems. These complementary works must be distinguished from evidence directly focused on electrical systems. The matrix preserves that difference through the type of study and the main technique. This decision avoids artificially expanding the corpus and, at the same time, recognizes that digital electrical innovation is nourished by advances in computing, communications, artificial intelligence, software engineering, and management of complex systems. (23).

Overall, the conceptual framework suggests that the Internet of Things (IoT) applied to the monitoring of electrical systems should be evaluated as a sociotechnical system and not as an isolated technology. Architecture, data, algorithms, communications, security, operation, and human capabilities interact to determine utility and sustainability. This reading guides the synthesis of results: instead of asking which technology is universally superior, it examines what combinations appear, what purposes they pursue, and what constraints they recognize. The framework also allows the gaps in the corpus to be interpreted as concrete research opportunities, especially in comparative validation, interoperability, scalability, real-world evaluation, and reproducible documentation. (23).

The cross-sectional reading of the corpus also allows distinguishing between technological availability and evidence of adoption. A publication can describe a technically viable architecture without yet documenting its behavior under prolonged conditions of operation, maintenance, or change of scale. This difference is decisive for interpreting the literature on electrical systems, because the requirements of continuity and safety make integration a part of performance, not an after-operation. Consequently, the conceptual framework of this review considers maturity as a combination of functional definition, technical demonstration, integration with infrastructure, and evaluation in representative scenarios. This perspective helps to avoid excessive conclusions and allows each study to be positioned according to the type of evidence it actually provides (1,2).

METHOD

Design and scope of the review

The review was proposed as a systematic synthesis focused on the functional architecture of the Internet of Things within electrical systems. The design combined a temporal delimitation from 2018 to 2022 with a comparative reading of sensing, communication, processing, and monitoring solutions.

The documentary unit was each publication with DOI that provided sufficient technical information to recognize the purpose of the system, the components used, and the application context. This choice allowed to jointly examine reviews, architectural studies, and applied developments without treating them as equivalent evidence. The scope was descriptive to characterize the corpus and analytical to relate design decisions to interoperability, data quality, security, latency, and deployment possibilities.

Search strategy and document delimitation

The search was limited to the 2018–2022 interval and combined descriptors of the electrical domain with terms specific to the Internet of Things (IoT) applied to the monitoring of electrical systems. The strategy considered terminological variants in English and Spanish, Boolean operators, and combinations aimed at retrieving publications whose title, abstract, or keywords were directly related to the review question. The documentary process included indexed academic and editorial sources relevant to electrical engineering, energy, and digital technologies. The retrieved records were organized before screening to identify bibliographic matches and prevent the same publication from advancing more than once to the eligibility phase. The temporal delimitation was applied uniformly and the DOI was used as a persistent identifier to distinguish publications with similar titles or versions available in more than one source.

Inclusion criteria

Publications that simultaneously met the following requirements were included: publication date between 2018 and 2022; direct relevance to the Internet of Things (IoT) applied to the monitoring of electrical systems; availability of DOI; access to sufficient information to recognize objective, approach or main technique and relevant results or contributions; and correspondence with the field of electrical systems, smart grids, energy assets or applications closely linked to the research problem. Empirical studies, applied works, reviews, surveys and methodological contributions were admitted when their content provided useful evidence to answer the review question. Inclusion did not depend on all works using the same metric, because the purpose was to characterize the development of the field and its application patterns, not to statistically combine heterogeneous results.

Procedure for exclusion and inclusion of studies

The selection was carried out in successive stages. After the initial identification of 120 records, coincidences and duplicates were filtered, leaving 90 unique references to continue the process. The screening examined titles and abstracts based on thematic correspondence, period and technological field; 55 records advanced to this phase. Subsequently, the potentially relevant full texts were reviewed and those that did not directly answer the question, were outside the defined electrical or energy scope, lacked DOI, presented insufficient information for extraction or corresponded to documents that did not allow the identification of a verifiable technical contribution. 43 full texts were evaluated and finally 23 studies were included. The selection sequence is presented at the end of the methodology using the PRISMA diagram.

Extraction and organization of evidence

For each included study, authorship, year, title, source of publication, DOI, type of study, technique or main focus, and elements directly related to the objective of the review were recorded. The extraction was organized in a matrix to preserve traceability between each publication and the synthesis presented in Results. The analytical categories were constructed from the recurrent features of the corpus and adjusted to the specific topic of the article, avoiding forcing identical classifications for conceptual contributions, reviews, and empirical applications. When a paper addressed more than one dimension, its content was interpreted according to the main contribution and, when necessary, its contribution to complementary thematic axes was recognized. This organization made it possible to describe temporal trends and contrast approaches without converting methodological differences into unsupported efficacy comparisons.

Synthesis and interpretation

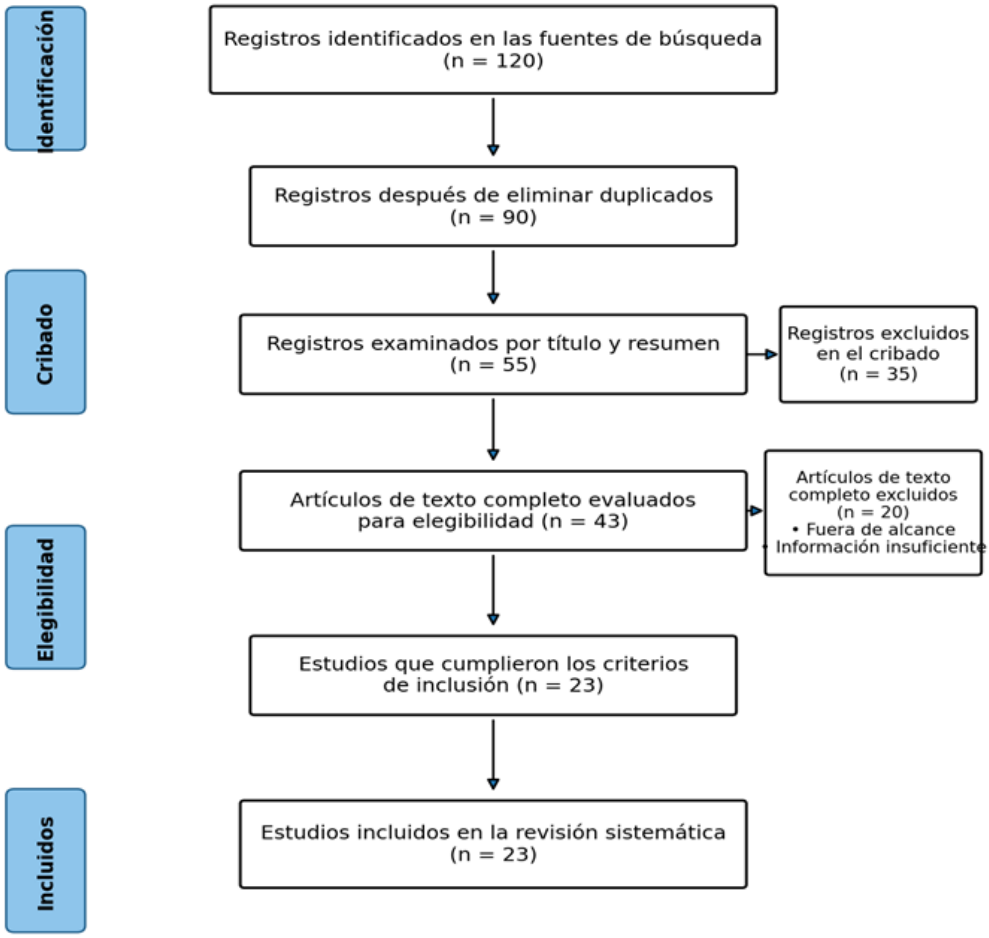
The synthesis integrated comparative reading and thematic grouping of the 23 selected studies. First, the composition of the corpus was characterized by year and nature of the contribution; then, technologies, methods, applications, and recurrent limitations related to the Internet of Things (IoT) applied to the monitoring of electrical systems were examined. The interpretation focused on convergences between studies, differences in scope, and gaps that affect the transfer of results. Descriptive frequencies were used only to represent the internal distribution of the corpus and not as population estimates. Because the publications used different scenarios, indicators, and levels of validation, the findings were discussed according to the function and context of each solution. This procedure allowed linking the study matrix with the research question and conclusions without attributing causality or general superiority to methods that were not compared under equivalent conditions.

Ethical considerations

The research was carried out exclusively with published scientific literature and did not involve intervention on people, access to personally identifiable data, clinical experimentation, or use of animals. Due to the documentary nature of the design, it was not necessary to request informed consent. Academic integrity was preserved through individual identification of publications, preservation of DOIs, and differentiation between results reported by primary studies and interpretation made in the synthesis. The original results were not modified to make them comparable, nor were ethical approvals attributed that did not correspond to the review design. The selection and presentation of evidence remained linked to explicit eligibility criteria and the research question.

Figure 1.

PRISMA flow diagram for study selection



Note. PRISMA flow of identification, screening, full-text eligibility assessment and final inclusion for the systematic review.

RESULTS

The synthesis integrated 23 studies published between 2018 and 2022. All the records of the final corpus have DOIs and were classified by year, type of study, and main technique. The temporal distribution was not uniform: 2020 concentrated 6 publications (26.1%). Overall, the corpus combines reviews, surveys, applied studies, conceptual proposals, and empirical works, which confirms the methodological diversity anticipated in the conceptual framework. The results are presented as a description of the corpus and thematic synthesis; the percentages do not represent prevalence of the universe of publications or aggregate effects of the technologies examined.

The matrix of selected studies allows us to observe that the contributions are not limited to a single function. In the Internet of Things (IoT) applied to the monitoring of electrical systems, the works are distributed between fundamentals, architecture, specific applications, evaluation mechanisms and challenges. This composition favors an evolutionary reading: review and survey studies organize concepts and taxonomies, while applied studies show how certain solutions are transferred to specific problems. The coexistence of both types of evidence suggests that the field simultaneously advanced in conceptual consolidation and technical experimentation during the period analyzed.

Examination of the main techniques shows a strong dependence on the application context. There is no dominant method that can be considered sufficient for the entire domain. Instead, solutions are selected according to monitoring, security, forecasting, control, maintenance, interoperability, or interpretation needs. This diversity supports a central conclusion of the review: technology maturity should be assessed by function and context, not by a general comparison of heterogeneous studies. Works closer to operational applications provide evidence of feasibility, but generalization continues to be conditioned by architecture, data, and deployment environment.

Table 1.

Matrix of the 23 studies selected for the systematic review

No.	Authors	Year	Study	Type	Method	DOI
1	Alireza Ghasempour	2019	Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges	Review	IoT-SG Architecture Review	https://doi.org/10.3390/inventions4010022
2	Al-Turjman F, Abujubbeh M	2019	IoT-enabled smart grid via SM: An overview	Review	Smart meters + IoT	https://doi.org/10.1016/j.future.2019.02.012
3	Y. Saleem; N. Crespi; M.H. Rehmani; R. Copeland	2019	Internet of Things-Aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions	Survey	IoT-SG	https://doi.org/10.1109/ACCESS.2019.2913984

No.	Authors	Year	Study	Type	Method	DOI
4	Reka SS, Dragicevic T	2018	Future effectual role of energy delivery: A comprehensive review of Internet of Things and smart grid	Review	IoT + smart grid	https://doi.org/10.1016/j.rser.2018.03.089
5	S.R. Mukundan; T. Vijayakumar	2019	Review on IoT Based Smart Grid Architecture Implementations	Review	IoT-SG Architectures	https://doi.org/10.36548/jeea.2019.1.002
6	Khan F, Siddiqui MAB, Rehman AU, Khan J, Sadiq MT, Asad A	2020	IoT Based Power Monitoring System for Smart Grid Applications	Prototype	ThingSpeak + sensores	https://doi.org/10.1109/ICEET48479.2020.9048229
7	Lilia Tightiz; Hyosik Yang	2020	A Comprehensive Review on IoT Protocols' Features in Smart Grid Communication	Review	IoT Protocols	https://doi.org/10.3390/en13112762
8	Bagdadee AH, Hoque MZ, Zhang L	2020	IoT Based Wireless Sensor Network for Power Quality Control in Smart Grid	Studio/Prototype	WSN + IoT	https://doi.org/10.1016/j.procs.2020.03.417

No.	Authors	Year	Study	Type	Method	DOI
9	Rohan Pal; Suresh Chavan; Deepak Gupta; Ashish Khanna; Sanjeevikumar Padmanaban ; Basim Khan; Joel J.P.C. Rodriguez	2021	A comprehensive review on IoT-based infrastructure for smart grid applications	Review	IoT Infrastructure	https://doi.org/10.1049/rpg2.12272
10	Sartika N, Sukmana Y, Effendi MR, Rusliana I, Khomisah, Yuningsih Y	2021	A Systematic Literature Review on IoT-based Smart Grid	Systematic review	SLR IoT-SG	https://doi.org/10.1109/ICWT52862.2021.9678415
11	Alavikia Z, Shabro M	2022	A comprehensive layered approach for implementing internet of things-enabled smart grid: A survey	Survey	Layered architecture	https://doi.org/10.1016/j.dcan.2022.01.002
12	Aranda JAS, Costa RDS, Vargas VW, Pereira PRDS, Barbosa JLV, Vianna MP	2022	Context-aware Edge Computing and Internet of Things in Smart Grids: A systematic mapping study	Systematic mapping	IoT + edge + context	https://doi.org/10.1016/j.compeleceng.2022.107826

No.	Authors	Year	Study	Type	Method	DOI
13	Jesús Jaime Moreno Escobar et al.	2021	A Comprehensive Review on Smart Grids: Challenges and Opportunities	Review	Smart grid/sensores	https://doi.org/10.3390/s21216978
14	Dileep G	2020	A survey on smart grid technologies and applications	Survey	SG Technologies	https://doi.org/10.1016/j.renene.2019.08.092
15	Deepak Kumar Panda; Saptarshi Das	2021	Smart grid architecture model for control, optimization and data analytics of future power networks with more renewable energy	Review	SHAM	https://doi.org/10.1016/j.jclepro.2021.126877
16	Ananthavijayan R, Shanmugam PK, Sanjeevikumar P, Holm-Nielsen JB, Blaabjerg F, Fedak V	2019	Software Architectures for Smart Grid System—A Bibliographical Survey	Review	Software architecture	https://doi.org/10.3390/en12061183
17	Yang Zhang; Tao Huang; Ettore Francesco Bompard	2018	Big data analytics in smart grids: a review	Review	Big data/AMI	https://doi.org/10.1186/s42162-018-0007-5

No.	Authors	Year	Study	Type	Method	DOI
18	Liu D.; Liang H.; Zeng X.; Zhang Q.; Zhang Z.; Li M.	2022	Edge Computing Application, Architecture, and Challenges in Ubiquitous Power Internet of Things	Review	Edge + UPIoT	https://doi.org/10.3389/fenrg.2022.850252
19	Molokomme DN, Onumanyi AJ, Abu-Mahfouz AM	2022	Edge Intelligence in Smart Grids: A Survey on Architectures, Offloading Models, Cyber Security Measures, and Challenges	Survey	Edge intelligence	https://doi.org/10.3390/jsan11030047
20	Lei T, Lv F, Liu J, Feng J, Sun G	2022	Research on Electrical Equipment Monitoring and Early Warning System Based on Internet of Things Technology	Applied study	IoT + Early Warning	https://doi.org/10.1155/2022/6255277
21	Muhammed Zekeriya Gunduz; Resul Das	2020	Cyber-security on smart grid: Threats and potential solutions	Review	IoT/SG Security	https://doi.org/10.1016/j.comnet.2019.107094

No.	Authors	Year	Study	Type	Method	DOI
22	Ferrag MA, Babaghayou M, Yazici MA	2020	Cyber security for fog-based smart grid SCADA systems: Solutions and challenges	Survey	Fog/SCADA	https://doi.org/10.1016/j.jisa.2020.102500
23	Rafał Leszczyna	2018	Cybersecurity and privacy in standards for smart grids – A comprehensive survey	Survey	SG Standards	https://doi.org/10.1016/j.csi.2017.09.005

Note. The matrix reproduces the final selected corpus documented in the evidence workbook. DOI links are retained for verification.

Table 1 confirms that the final evidence base contains 23 individually identifiable studies with DOI. The matrix also shows that the corpus is methodologically mixed rather than dominated by a single design. This diversity is analytically useful because it combines conceptual consolidation with application-oriented evidence, but it also prevents treating all reported outcomes as directly comparable. The study type and technique columns therefore function as interpretive qualifiers: conclusions are drawn within compatible groups and are not converted into a single pooled effectiveness estimate.

DISCUSSION

Integration, Data and Operation

The findings show that the electric IoT makes sense when sensors, communications, processing, and monitoring form a coherent chain. The architectures reviewed do not simply connect devices; they organize the measurement journey from asset to decision. That continuity explains why latency, synchronization, and data quality appear alongside connectivity in architecture and protocol studies. A network with numerous nodes can provide little value if the data arrives out of time or without operational context. The discussion of the corpus leads, therefore, to evaluate the architecture for its ability to sustain useful and traceable information, especially when monitoring feeds maintenance, protection, or control. (1,7,16)

The transition to specific applications is one of the most visible changes of the period reviewed. Power quality, equipment monitoring, and edge processing studies shift the emphasis from the general promise of the smart grid to defined operational problems. Such specialization improves the relevance of assessments, but makes it difficult to compare results between jobs pursuing different

functions. An architecture optimized for detecting disturbances does not necessarily respond in the same way to maintenance or distributed control. Therefore, metrics should correspond to the purpose of each solution and include, in addition to the main indicator, response times, availability, resource consumption, and fault tolerance. (8,12,20)

Interoperability appears as a structural condition and not as a secondary feature. Electrical systems combine equipment with long lifecycles, heterogeneous protocols, and platforms incorporated at different times. Integrating these components requires communication compatibility, but also semantic correspondence between variables, timestamps, and operational states. Corpus reviews warn that a technically successful connection can continue to produce ambiguous information if systems interpret the same measurement differently. Consequently, modularity and well-defined data models are relevant for onboarding new assets without rebuilding the entire platform. Interoperability should be evaluated during design, testing, and sustained operation. (2,7,11)

The usefulness of monitoring depends on the quality of the data circulating through the architecture. Packet losses, incomplete measurements, temporal misalignment, or lack of provenance can alter diagnoses and decisions even if the communication infrastructure is functioning properly. The studies reviewed suggest that increasing the volume of information does not solve these problems by itself. Validation rules, missing handling, anomaly identification, and documentation of the origin of signals are required. This point becomes important in distributed networks, where multiple sources can describe related states with different update frequencies. Data governance should be considered part of IoT performance and not a post-deployment administrative task. (17-20)

Scalability, security and sustainability

The expansion of connected devices increases the exposure surface of the electrical system and forces cybersecurity to be linked to operational continuity. The included works that address threats and protection show that authentication, segmentation, updating and monitoring of events should not be added after installing the solution. When an IoT platform participates in supervision or control, the alteration of measurements can affect both information and operation. Hence, the technical evaluation needs to simultaneously consider connectivity, latency and resistance to unauthorized access or tampering. The corpus supports a security approach integrated into the design cycle, with response and maintenance mechanisms in line with the criticality of each function. (21-23)

Edge computing appears as a response to applications that cannot rely exclusively on centralized processing. Bringing analytical capability close to the source reduces traffic and can shorten response times, but it also distributes responsibilities for updating, coordination, and security. The studies reviewed do not justify a simple opposition between edge and cloud; rather, they describe functions that can be distributed according to criticality, data volume, and availability of communications. Immediate tasks can be solved locally, while historical analysis and global management remain in centralized layers. The methodological challenge is to document this functional assignment and demonstrate how consistency, traceability, and recovery are maintained when different nodes process partial information. (12,18,19)

Scalability must be interpreted beyond the number of sensors that a platform can support. As the network grows, so do configurations, credentials, software versions, data flows, and dependencies between services. A proven solution with few devices may face difficulties when incorporated into a distributed infrastructure with heterogeneous assets. Corpus studies show that technology scaling requires management mechanisms and not just greater computational capacity. It is useful to evaluate how new nodes are added, how they are updated without interrupting critical functions, and how compatibility with existing components is preserved. This dimension brings experimental research closer to the conditions of prolonged operation of a power grid. (11-14)

The life cycle introduces a demand that is not very visible in short-term evaluations. Sensors, gateways, platforms, and protocols do not age at the same rate as the electrical assets to which they are connected. The sustainability of an architecture depends on being able to replace components, update software, renew credentials, and modify interfaces without losing service continuity. The studies reviewed allow us to infer that an initially functional solution can become a costly dependency if it does not contemplate maintenance and evolution. Therefore, technological maturity should incorporate criteria of maintainability, future compatibility, and change management. This reading complements the immediate performance metrics and brings the evaluation of the IoT closer to the needs of infrastructures with long operating horizons. (13-16)

The 23 included studies present a diversity of scenarios, objectives, and metrics, a circumstance that limits the construction of a single quantitative comparison. This heterogeneity does not invalidate the results; it forces them to be interpreted within the function and context for which they were obtained. Architecture tests, prototypes, and reviews answer different questions and should not be ordered by a common performance indicator. The synthesis shows the convenience of reporting configurations, datasets, communication conditions, and evaluation criteria in greater detail. A more uniform documentation would allow reproducing experiences and distinguishing whether the differences observed come from the method, infrastructure, or scenario used. (1-23)

Validation and technological maturity

Coexistence with legacy infrastructure is a critical point in moving IoT proposals from prototypes to real networks. Electrical systems are rarely replaced in a comprehensive manner; new digital layers must coexist with equipment, protocols, and procedures already in place. This condition modifies interface, security, and maintenance requirements and may limit advantages observed in controlled environments. The literature reviewed suggests that effective adoption depends on designing progressive integration mechanisms and documenting dependencies between new and existing components. Assessing compatibility, migration effort, and operational consequences allows the feasibility of a solution to be assessed more accurately than an isolated demonstration of connectivity or processing. (7,11,16)

A methodological consequence of the review is the need to choose metrics related to the operational function. Accuracy, latency, availability, energy consumption, or data loss rate describe different dimensions and should not be combined as if they represented a single result. For power quality monitoring, temporal fidelity may be central; for distributed monitoring, availability and delay may

become more important. The comparison between studies becomes clearer when each indicator is related to the stated objective and the constraints of the scenario. This practice would also allow identifying trade-offs between performance, computational cost, security, and scalability, aspects that are often found separately in the literature analyzed. (8,12,17)

Reproducibility is a condition for the progress of the period to be accumulated. Describing only the final result makes it difficult to determine how much of the performance depends on parameters, topology, sampling frequency, or network conditions. The reviewed papers show enough diversity to warrant more detailed reporting protocols, especially in applied studies. Publishing configurations, assumptions, preprocessing procedures, and test criteria would favor independent comparisons. When data cannot be shared, it is still possible to document their structure, provenance, and limitations. Such transparency would help separate improvements attributable to the architecture from those derived from particular conditions of the experiment and would strengthen the transfer to different electrical scenarios. (14,17,20)

The big picture allows us to situate the maturity of the electric IoT in the integration of several dimensions and not in the isolated optimization of a component. Architecture, interoperability, data quality, security, scalability and maintenance interact during actual operation. A proposal can exhibit good analytical performance and remain difficult to adopt if it depends on closed interfaces, fragile configurations or unclear upgrade processes. The research agenda should move towards representative evaluations that combine technical indicators with sustained operating conditions. Comparing solutions under equivalent functional requirements, documenting failures and considering the life cycle would provide more useful evidence to decide when an architecture is ready to be integrated into existing electrical infrastructure. (11-23)

CONCLUSIONS

The systematic review allowed to answer the general objective by integrating the evidence of 23 studies on the Internet of Things (IoT) applied to the monitoring of electrical systems within the period 2018–2022. The results show an expanding field whose evolution combines conceptual consolidation and increasingly specific applications. The main conclusion is that the usefulness of the solutions does not depend only on the novelty of a technique, but also on its correspondence with specific operational needs, the quality of the information used and the possibility of being consistently incorporated into electrical infrastructures that have their own technical and organizational constraints.

The corpus shows that technological integration is a central criterion for interpreting the results on the Internet of Things (IoT) applied to the monitoring of electrical systems. Interoperability, data availability, scalability, security, maintainability and compatibility with existing systems appear recurrently as conditions that can favor or limit the observed performance. Therefore, the positive results obtained in particular scenarios should not be automatically generalized to other networks, assets or contexts. The future evaluation should incorporate these conditions as part of the performance and not treat them as separate secondary aspects of the main solution.

The methodological heterogeneity identified explains why it is not appropriate to establish a universal ranking of methods or to calculate an aggregate effect from results that respond to different objectives and metrics. The review provides greater value by organizing convergences, contrasts, and gaps within comparable categories. This conclusion guides the reading of the tables and figures: the frequencies describe the composition of the corpus and the matrices allow individual evidence to be traced, while the thematic interpretation relates the findings to the research problem without attributing equivalence to designs that were not designed to answer the same question.

Subsequent research should strengthen reproducibility through complete descriptions of data, configurations, procedures, and metrics, as well as incorporating comparisons under representative conditions and predefined evaluation criteria. It is also necessary to expand validation outside of controlled scenarios and clearly document transfer constraints. More comparable evidence would make it possible to determine which solutions maintain their performance in the face of changes in scale, topology, load, data quality, or communications infrastructure, and would make it easier for academic results to be translated into engineering decisions with less uncertainty.

Finally, the synthesis confirms that the development of the Internet of Things (IoT) applied to the monitoring of electrical systems should be understood as a multidimensional process in which technology, data, architecture, and operational context converge. The selected studies offer a sufficient basis to identify consolidated lines and persistent challenges, but also show the need for more comprehensive evaluations. The future agenda should prioritize verifiable, secure, interoperable, and technically justified solutions, with indicators linked to the actual purpose of use. This orientation would allow progress from feasibility demonstrations to cumulative evidence capable of supporting responsible adoptions in electrical systems.

BIBLIOGRAPHIC REFERENCES

1. Alireza Ghasempour. Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges. Inventions. 2019; 4(1):22. https://doi.org/10.3390/inventions4010022
2. Al-Turjman F, Abujubbeh M. IoT-enabled smart grid via SM: An overview. Future Gener Comput Syst. 2019;96:579-590. https://doi.org/10.1016/j.future.2019.02.012
3. Y. Saleem, N. Crespi, M.H. Rehmani, R. Copeland. Internet of Things-Aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions. IEEE Access. 2019;7:62962-63003. https://doi.org/10.1109/ACCESS.2019.2913984
4. Reka SS, Dragicevic T. Future effectual role of energy delivery: A comprehensive review of Internet of Things and smart grid. Renew Sustain Energy Rev. 2018;91:90-108. https://doi.org/10.1016/j.rser.2018.03.089
5. S.R. Mugunthan, T. Vijayakumar. Review on IoT Based Smart Grid Architecture Implementations. Journal of Electrical Engineering and Automation. 2019; 1(1):20-27. https://doi.org/10.36548/jeea.2019.1.002
6. Khan F, Siddiqui MAB, Rehman AU, Khan J, Sadiq MT, Asad A. IoT Based Power Monitoring System for Smart Grid Applications. In: 2020 International Conference on Engineering and Emerging Technologies (ICEET). IEEE; 2020. p. 1-5. https://doi.org/10.1109/ICEET48479.2020.9048229

7. Lilia Tightiz, Hyosik Yang. A Comprehensive Review on IoT Protocols' Features in Smart Grid Communication. Energies. 2020; 13(11):2762. https://doi.org/10.3390/en13112762
8. Bagdadee AH, Hoque MZ, Zhang L. IoT Based Wireless Sensor Network for Power Quality Control in Smart Grid. Procedia Comput Sci. 2020;167:1148-1160. https://doi.org/10.1016/j.procs.2020.03.417
9. Rohan Pal, Suresh Chavhan, Deepak Gupta, Ashish Khanna, Sanjeevikumar Padmanaban, Baseem Khan, Joel J.P.C. Rodrigues. A comprehensive review on IoT-based infrastructure for smart grid applications. IET Renew Power Gener. 2021; 15(14):3061-3090. https://doi.org/10.1049/rpg2.12272
10. Sartika N, Sukmana Y, Effendi MR, Rusliana I, Khomisah, Yuningsih Y. A Systematic Literature Review on IoT-based Smart Grid. In: 2021 7th International Conference on Wireless and Telematics (ICWT). IEEE; 2021. https://doi.org/10.1109/ICWT52862.2021.9678415
11. Alavikia Z, Shabro M. A comprehensive layered approach for implementing internet of things-enabled smart grid: A survey. Digit Commun Netw. 2022; 8(3):388-410. https://doi.org/10.1016/j.dcan.2022.01.002
12. Aranda JAS, Costa RDS, Vargas VW, Pereira PRDS, Barbosa JLV, Vianna MP. Context-aware Edge Computing and Internet of Things in Smart Grids: A systematic mapping study. Comput Electr Eng. 2022;99:107826. https://doi.org/10.1016/j.compeleceng.2022.107826
13. Jesus Jaime Moreno Escobar et al.. A Comprehensive Review on Smart Grids: Challenges and Opportunities. Sensors. 2021; 21(21):6978. https://doi.org/10.3390/s21216978
14. Dileep G. A survey on smart grid technologies and applications. Renew Energy. 2020;146:2589-2625. https://doi.org/10.1016/j.renene.2019.08.092
15. Deepak Kumar Panda, Saptarshi Das. Smart grid architecture model for control, optimization and data analytics of future power networks with more renewable energy. J Clean Prod. 2021;301:126877. https://doi.org/10.1016/j.jclepro.2021.126877
16. Ananthavijayan R, Shanmugam PK, Sanjeevikumar P, Holm-Nielsen JB, Blaabjerg F, Fedak V. Software Architectures for Smart Grid System-A Bibliographical Survey. Energies. 2019; 12(6):1183. https://doi.org/10.3390/en12061183
17. Yang Zhang, Tao Huang, Ettore Francesco Bompard. Big data analytics in smart grids: a review. Energy Inform. 2018; 1(1):8. https://doi.org/10.1186/s42162-018-0007-5
18. Liu D., Liang H., Zeng X., Zhang Q., Zhang Z., Li M.. Edge Computing Application, Architecture, and Challenges in Ubiquitous Power Internet of Things. Front Energy Res. 2022; 10: https://doi.org/10.3389/fenrg.2022.850252
19. Molokomme DN, Onumanyi AJ, Abu-Mahfouz AM. Edge Intelligence in Smart Grids: A Survey on Architectures, Offloading Models, Cyber Security Measures, and Challenges. J Sens Actuator Netw. 2022; 11(3):47. https://doi.org/10.3390/jsan11030047
20. Lei T, Lv F, Liu J, Feng J, Sun G. Research on Electrical Equipment Monitoring and Early Warning System Based on Internet of Things Technology. Math Probl Eng. 2022;2022:6255277. https://doi.org/10.1155/2022/6255277
21. Muhammed Zekeriya Gunduz, Resul Das. Cyber-security on smart grid: Threats and potential solutions. Comput Netw. 2020;169:107094. https://doi.org/10.1016/j.comnet.2019.107094

22. Ferrag MA, Babaghayou M, Yazici MA. Cyber security for fog-based smart grid SCADA systems: Solutions and challenges. J Inf Secur Appl. 2020;52:102500. https://doi.org/10.1016/j.jisa.2020.102500
23. Rafał Leszczyna. Cybersecurity and privacy in standards for smart grids – A comprehensive survey. Comput Stand Interfaces. 2018;56:134-149. https://doi.org/10.1016/j.csi.2017.09.005

ETHICAL CONSIDERATIONS

Not applicable. This study is a review of published literature and did not involve direct participation of human beings, animals, interventions, or collection of identifiable personal data.

ARTIFICIAL INTELLIGENCE (AI) USE STATEMENT

The authors declare that the generative artificial intelligence tool ChatGPT (OpenAI) was used exclusively to support the organization of the article and translation of text. Its use did not determine the scientific content, study design, source selection, data analysis, interpretation of results, or conclusions. Full responsibility for the content remains with the authors.

FUNDING

This research did not receive any financial support.

CONFLICT OF INTEREST

The authors declare no conflicts of interest.

AUTHOR CONTRIBUTION

Author Names and Initials: Silvia Elena Mireille Ypanaque Arteaga (SEMYA)

1. **Conceptualization:** SEMYA
2. **Data curation:** SEMYA
3. **Formal analysis:** SEMYA
4. **Acquisition of financing:** not applicable
4. **Investigation:** SEMYA
5. **Methodology:** SEMYA
6. **Project administration:** SEMYA
7. **Resources:** SEMYA
8. **Software:** not applicable
9. **Supervision:** SEMYA
10. **Validation:** SEMYA
12. **View:** SEMYA
13. **Original draft writing:** SEMYA
14. **Writing, review and editing:** SEMYA