Evaluating Energy Efficiency and Security for Internet of Things: A Systematic Review

Luciana P. Oliveira[1(✉)], Moroni N. Vieira[2], Gabriel B. Leite[1], and Edson L. V. de Almeida[1]

[1] IFPB Campus João Pessoa, Av. Primeiro de Maio, 720 - Jaguaribe, João Pessoa, PB, Brazil
luciana.oliveira@ifpb.edu.br, gabriel.bezerra@academico.ifpb.edu.br, edson.l.v.almeida@outlook.com

[2] IFRN Campus Currais Novos, Rua Manoel Lopes Filho, 773 - Valfredo Galvão, Currais Novos, RN, Brazil
moroni.neres@ifrn.edu.br

Abstract. The Internet of Things (IoT) contains devices to collect and transmit information that should not be captured by third parties. Although devices have internet connectivity, some devices have battery limited energy. Therefore, it is important the conducting of evaluations to investigate, compare and propose security mechanisms with energy-efficient. However, there is a very low number of research using practical evaluations with real devices, as measurement approach takes a long time to perform the experiments. Therefore, the aim of this paper is to analyze, categorize analytically and statistically the methodologies which have been presented in the area of IoT based on the Systematic Literature Review (SLR) method, in order to extract features of the research protocols (definition of a set of equipment, topology, traffic, parameters, metrics and other variables) to be used in new research that addresses the concepts of security, energy and IoT. The weaknesses and highlighting of each study is discussed as well as presenting some hints for addressing future research with lower execution times of experiments, as it will be possible to reuse the results of measurements already published for the same parameter and metrics.

1 Introduction

The Internet of Things (IoT) is constituted of devices that have similar characteristics to WSN (Wireless Sensor Networks) sensors, having limited energy to collect and transmit information that should not be captured by third parties. Therefore, works such as [1] consider IoT as the result of WSN with Internet access, being possible to remotely access several information from the environment in which wireless sensors were deployed [2,3]. In addition, changing batteries in WSN and some IoT solutions should be avoided, so it is important to use security mechanisms with energy efficiency. This is because in some cases

L. Barolli et al. (Eds.): AINA 2020, AISC 1151, pp. 217–228, 2020.
https://doi.org/10.1007/978-3-030-44041-1_20

the devices are deployed in a hostile environment where there is no possibility of replacing or recharging the batteries. Therefore, the choice of low-energy security mechanisms is critical, and for this reason this research found more than 800 papers that evaluated energy consumption of WSN and IoT security solutions through simulations, analytical modeling or practical experiments by measurement.

This work found 362 secondary technical papers (surveys and reviews) and only 49 contained information about the IoT, energy and security. However, none of the secondary work have been focused to comprehend practical evaluations with real devices. Although it possible to find 927 papers that executed an evaluation, only 72 works described the evaluation through a practical experiments, because measurement approach takes a long time to perform the experiments and it is hard to reuse results from existing works, since there is not an addressing for common research protocol to analyze the combining of the energy and security in IoT.

Therefore, the main aim of this research based on Systematic Literature Review (SLR) method is to comprehend the diversity of research protocols to investigate or compare the methodologies to evaluate security mechanisms with low energy consumption for IoT (including WSN). The main commitments of this study are highlighted as follows:

- Presenting a discussion of the research protocols (definition of a set of equipment, topology, traffic, parameters, metrics and other variables) that considered energy, security and sensors (IoT or WSN) in measurement approach.
- Presenting the weaknesses and highlighting among evaluations of the security mechanisms based on practical experiments.
- Designing recommendations to be addressing future research with energy, iot, security and measurement approach.

The organization of this systematic review is considered as follows. Section 2 presents the related works. The research methodology (SRL process) is clarified in Sect. 3. The discussion of the papers selected by SRL is described in Sect. 4, including the weaknesses, highlighting and recommendations to be addressing future research with energy, iot, security and measurement approach. Finally, the conclusion and future works are in Sect. 5.

2 Related Works

This section presents a summary of some characteristics of the secondary studies that described information about IoT, security and energy issues.

The paper [4] is a review about Edge Computing in terms of the definition, characteristics and architectures, considering IoT and security (no deep), but it does not include energy consumption.

In the paper [5], a survey about sensors to monitor healthcare is presented, considering security, energy consumption and others contexts. However, this study does not analyze the measurements that associate energy consumption and security.

The work [6] is a survey about Smart Grid (SG). This explains how solution for minimizing the wastage of electrical energy can be used with IoT and other information about SG in terms of applications, architectures, prototypes, big data and communication IoT and non-IoT for smart grid. However, this study does not analyze existed experiments with IoT devices considering security.

In terms of [7], this work describe about data aggregation to avoid the transmission of the duplicate data. It compared the protocol considering intelligent technique used, energy consumption, cost reduction, security, accuracy, organisational type and metrics. However the analyzed metrics, security and energy were not studied in terms of existed real evaluations.

Similarly to paper [6], the paper [8] addresses energy in the context of smart power. It reviews the development and implementation of smart power meters, including smart electricity meters, smart heat meters, and smart gas meters. However, this study does not analyze existed experiments with IoT devices considering security.

An in-depth research and analyzes of the security issues were presented by [9–11]. The paper [9] merger security and smart city, including a view of the taxonomia for security, while [10,11] associate WSN and security. However, both works did not analyze the studies in terms of parameters, metrics and other features that are presents in evaluations.

Therefore, this paper is the first study, using SLR method, that reviews the evaluation methods of security and energy in the IoT (including WSN). Briefly, Table 1 represents a summary of the related secondary studies (the systematic literature review, survey or review - no systematic). It is clear that none of the papers have used the SLR method for study IoT, energy and security. In Table 1, the paper with E+ contains study components (some comparative table or classification) of the energy, and S+ represents works that contains study components of the security. Therefore just one paper [7] contains some explicit information about security and energy, but the information in terms of measurement

Table 1. Secondary works in the combining of IoT, security and energy

Ref.	Review P. type	Year	Paper selection process	Measurement	Main topic	Security (S) Energy (E)	Covered years
[4]	Review	2019	Not clear	No	Edge computing	S-/E-	2015–2018
[5]	Survey	2010	Not clear	No	Healthcare	S-/E-	2003–2009
[6]	Survey	2019	Not clear	No	Smart grid	S+/E-	2011–2015
[7]	Survey	2013	Not clear	Partially	Data aggregation	S+/E+	2006–2011
[8]	Review	2016	Not clear	No	Smart energy	S-/E+	2007–2015
[9]	Survey	2019	Not clear	No	Smart city	S+/E-	2009–2018
[10]	Survey	2017	Not clear	No	WSN	S-/E-	2007–2016
[11]	Survey	2018	Not clear	No	WSN	S+/E-	2002–2017

is superficially described (only one table that does not present parameter, metric and others important information about evaluation). According to the existing secondary papers, the existing deficiencies propose that is important to do a comprehensive literature review to address these weaknesses as follows:

- The present studies do not provide in-deth study about measurements in IoT.
- Some studies do not evaluate the important association among security, energy and IoT devices.
- The structure of the presented studies does not have the systematic review and the paper selection method is not clear.

3 Methodology

A systematic review according to [12] is a type of study conducted using a methodology that analyzes published articles as consequence the experiment to select works can be reproduced. This methodology is used to select the most relevant studies to, for example, identify similarities or contradictions between papers selected. This method can be conducted by manually process or by tools. For example, Start [13] is an example of a tool that can be used to produce a systematic review. This tool allows the importation of file with extension ".bib" that were exported from the electronic bases, allowing the management of a large number of articles to be classified in the three stages of the systematic review methodology: data planning; execution; and analysis. The first phase includes the formulation of research questions, definition of inclusion and exclusion criteria. The second phase is used to select relevant papers and to extract data that will analyzed in last phase. The third phase is executed to generate results of the graphics, tables and descriptions.

3.1 Research Questions (RQs)

In order to understand the evaluations of studies that merger energy, security and IoT, this SLR paper formulated eight question that will answers in last phase of the research:

1. How are the distribution of the research studies over the years?
2. Which domains are categorized the selected papers?
3. Do the experiments have a high level of reproducibility and precision?
4. What are the characteristics of the parameters (equipment, traffic types and others) most used to configure the measurement environment?
5. What are the most commonly used metrics?
6. What recommendations for future work that will conduct experiments in the field of IoT, energy and security?

3.2 Search Process

The objective of an SLR is to conduct a review of relevant studies in order to quantity of evidence existing to address the RQs. This method is rigorous and unbiased, allowing to be reproduce by other people. For this reason, it is important to define which are electronic bases were used to search the papers and to inform the inclusion and exclusion criteria to select the papers.

This study was based on the following electronic databases: IEEE Xplore, ACM digital library and Science Direct. Each electronic resources accepts different string format and, for this reason, the Fig. 1 shows the search string defined to retrieve information for each electronic resources.

ACM	(+"Internet of Things" +"energy" +"consumption" +"Security") (+"IoT" +"energy" +"consumption" +"Security") (+"Sensor Network" +"energy" +"consumption" +"Security") (+"WSN" +"energy" +"consumption" +"Security")
IEEE	((((("Internet of Things") AND energy) AND consumption) AND security) ((((("IoT") AND energy) AND consumption) AND security) ((((("Sensor Network") AND energy) AND consumption) AND security) ((((("WSN") AND energy) AND consumption) AND security)
Science Direct	"Internet of Things" AND "energy" AND "consumption" AND "Security" "IoT" AND "energy" AND "consumption" AND "Security" "Sensor Network" AND "energy" AND "consumption" AND "security" "WSN" AND "energy" AND "consumption" AND "security"

Fig. 1. Search strings

After the definition of the search string for each electronic base, this SLR identified 5671 papers. Therefore, the following inclusion (IC) and exclusion (EC) criteria were important to identified a viable number of papers to analyze:

- EC1: Works not written in English.
- EC2: Papers does not contain in the title or in the abstract the words in the context of security (security or secure or malicious or crypt or shared key or confidential or attack) and energy (energy or power consumption).
- EC3: Secondary studies (abstract or title contains the word review or survey).
- EC4: Duplicate articles.
- EC5: Secondary work identified after to read it, because relevant words (review or survey) were not in title or abstract.
- EC6: Incomplete work, because the paper has no value related to measurement experiments.
- EC7: Papers with irrelevant content, because after reading, they did not present measurement description in terms of the energy consumption and security.
- IC1: papers that were not excluded by EC1, EC2, EC3 and EC4.
- IC2: papers did not exclude by any of the exclusion criteria.

3.3 Studies Selection

In this SRL, the paper was selected in execution phase that was subdivided into two stages with support of the Start Tool, as follows:

- Stage 1: Analyze title and summary of all articles to confront them with the exclusion criteria (EC1, EC2, EC3 and EC4). The selected paper in this stage were classified by inclusion criteria IC1.
- Stage 2: Read all paper in order to exclude works by CE5, EC6 and EC7. The selected paper in this stage were classified by IC1 and IC2.

As a result, in stage 1, a total of 927 studies were selected and 4744 were excluded. In stage 2, the full text of each primary study included as IC1 was read to include as IC2 and to extract information related to RQs. The primary studies included in the final selection corresponded to the relevant papers that meet the RQs addressed by this SRL. It was excluded 855 papers and 72 relevant studies were identified from the 3 electronic bases.

4 Results

This section presents and discusses the answers to six RQs in Sect. 3.1 considering the results obtained in the analysis of the 72 papers that were included in the study.

4.1 RQ1: How Are the Distribution of the Research Studies of the Measurement in IoT over the Years?

The studies found in this review are in a time period between 2006 and 2019. However, this studies extracted paper until on June 2019, for this reason the Fig. 2(a) shows the number of included papers by year of publication and it does show 2019. Thirty papers published before 2015 were included, since the inclusion and exclusion criteria placed no bar upon the year of publication. From 2016, it was possible to identify and include at least six paper with explicit IoT for each year. This indicates that the area has become more mature from 2016.

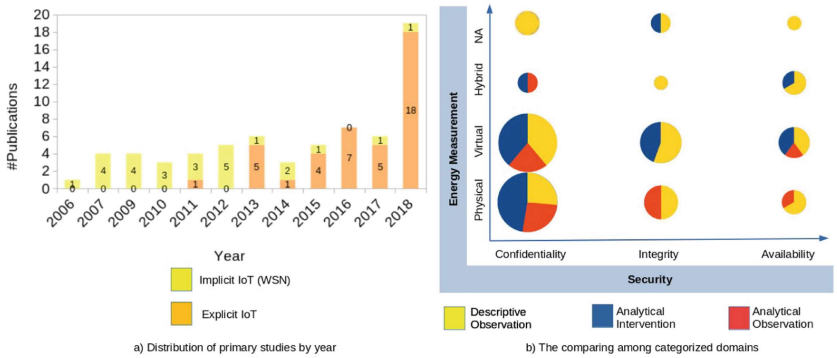


Fig. 2. Distribution of results

4.2 RQ2: Which Domains Are Categorized the Selected Papers?

The papers were categorized in three main types of domains in order to study IoT: information security, energy measurement and research feature. The information security was subdivided in Confidentiality (paper contains information of the mechanisms to avoid the extraction or monitoring of the information for unauthorised users), Integrity (works has studies about technical to avoid the modification or changing of the information and system setting for instance unauthorized access to sensitive information) and Availability (articles presents information to avoid the system close and unavailable for authorized users). The energy is the classification in terms of mechanism used to extract the energy consumption of security approach for IoT. This domain was splitted in Virtual (the measurement of the energy is based on some software or mathematical model), Physical (some real tool was used to identify the energy consumption), Hybrid (the energy is identified using the approach based on Virtual and Physical domains) and NA (the paper did not describe how to reach the energy results).

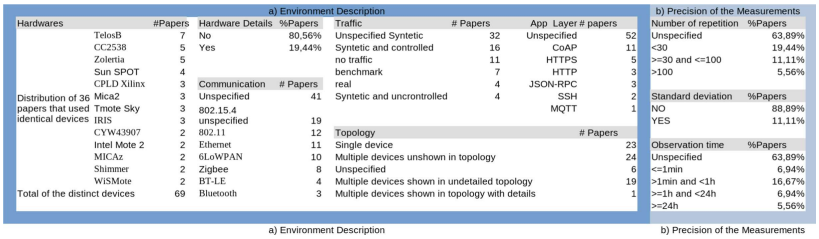
The research type was separated in three types of experimental studies: analytical intervention, analytical observation and descriptive observation. The analytical intervention are works that contain a proposal analyzed against other existing proposals in order to prove hypotheses regarding this new proposal. Analytical observation are studies that perform the analysis of experiments to compare two or more existing solutions to prove hypotheses. Descriptive observation are articles that investigate events through experiments that will generate hypotheses or when a proposal was not analyzed against other existing work.

The results in Fig. 2(b) show that no experiments with physical measurement were found in order to describe analytical intervention in terms of availability and integrity. Moreover, there are few experiments considering availability. On the other hand, there is a large number of research related to analytical intervention in the confidentiality subarea of the information security. In terms of energy measurement, most articles are classified at the virtual level. That is, few studies actually measured the energy consumption with real equipment (oscilloscope, voltage meter, etc.).

4.3 RQ3: Do the Experiments Have a High Level of Reproducibility and Precision?

Reproducibility is the combination observed when different operators measure the same part multiple times using the same meter (hardware) under the same conditions (environment configuration).

So, the experimental research should describe the environment in high detail of the hardware and parameters used in the configurations in order to ensure a high level of reproducibility (the same evaluation results or results with very little degree of difference). Moreover, it is important, because the measurement with real devices is very costly and, therefore, evaluating new solutions should avoid the cost of remeasuring new studies already evaluated.



a) Environment Description

Hardwares		#Papers
Distribution of 36 papers that used identical devices	TelosB	7
	CC2538	5
	Zolertia	5
	Sun SPOT	4
	CPLD Xilinx	3
	Mica2	3
	Tmote Sky	3
	IRIS	3
	CYW43907	2
	Intel Mote 2	2
	MICAz	2
	Shimmer	2
	WiSMote	2
Total of the distinct devices		69

Hardware Details	%Papers
No	80,56%
Yes	19,44%

Communication	# Papers
Unspecified	41
802.15.4 unspecified	19
802.11	12
Ethernet	11
6LoWPAN	10
Zigbee	8
BT-LE	4
Bluetooth	3

Traffic	# Papers
Unspecified Syntetic	32
Syntetic and controlled	16
no traffic	11
benchmark	7
real	4
Syntetic and uncrontrolled	4

App. Layer	# papers
Unspecified	52
CoAP	11
HTTPS	5
HTTP	3
JSON-RPC	3
SSH	2
MQTT	1

Topology	# Papers
Single device	23
Multiple devices unshown in topology	24
Unspecified	6
Multiple devices shown in undetailed topology	19
Multiple devices shown in topology with details	1

b) Precision of the Measurements

Number of repetition	%Papers
Unspecified	63,89%
<30	19,44%
>=30 and <=100	11,11%
>100	5,56%

Standard deviation	%Papers
NO	88,89%
YES	11,11%

Observation time	%Papers
Unspecified	63,89%
<=1min	6,94%
>1min and <1h	16,67%
>=1h and <24h	6,94%
>=24h	5,56%

a) Environment Description b) Precision of the Measurements

Fig. 3. Comparing the selected papers (environment and precision)

However, the Fig. 3(a) shows that only 19.44% of the selected papers in this SRL provide details on specifying all hardware used.

In addition, there are a large number of papers that did not specify important items in IoT solutions. 41 papers did not inform the communication technology used and 19 did not report the type of 802.15.4 technology used. This technology can be used with different types of routing that influences energy consumption, so it is extremely important to detail the information.

Although it is possible to build an IoT solution without using an application layer protocol standard, 52 articles have not been explicit. There is also a lot of work that does not specify the topology and traffic used. Moreover, 69 distincts devices (including different versions, for example, Raspberry pi is different from Raspberry pi 3) were used by 72 selected papers.

An example of the importance of richness of detail is the description of traffic in the experiment. When studying the delay of communication without bottlenecks is not important, controlled synthetic traffic should be used. The uncontrolled synthetic traffic allows the use of sending many messages in order to stress the equipment, for example, it can be used to calculate throughput. When using a brenchmark, it provides a high degree of data reliability because it will be synthetic traffic that can be more easily reproduced. Real traffic is important for an observation survey to make assumptions about, but it is not appropriate to evaluate a new proposal, as it will probably not be possible to reproduce this fact from the past.

The precision refers to the closeness between repeated measurements on same experimental design. It is related to the number of repetitions and standard deviation. For example, [14] informs that "standard" values for the number of repeated runs is usually 30 or 50, with occasional recommendations of using 100 or more, because the higher the number of measurement repetitions has as result the lower the standard deviation and the greater the accuracy of the mean value of the obtained results.

However, the Fig. 3(b) shows low precision in existing experimental researches in security for IoT. Several papers unspecified standard deviation, time observation and number of repetition. Moreover, small number of article realized experimental with adequate values to obtain precision results.

4.4 RQ4: What Are the Characteristics of the Parameters Most Used to Configure the Measurement Environment?

Controlled variables are also known as adjusted parameters before making an observation in the experiment. This SRL found 72 selected papers and identified two main parameters (controlled variables) in Fig. 4 to evaluate low-power security for the IoT: hardware feature and security key size.

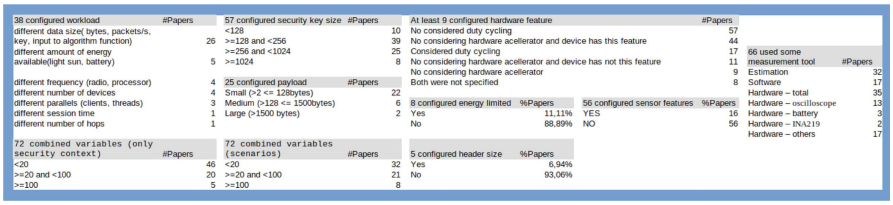


Fig. 4. Variables to configure the experimental research

In terms of hardware feature, 105 papers configured the environment considering the hardware accelerator active and disabled. However, 15% from papers did not consider this variable, although it was possible. In terms of the security key size, this variable was configured considering values between 128 and 1024 bits.

In overview, 90% from selected papers did not consider sensor features (a kind of hardware in IoT) to configure the experimental. Considering one graph result for each scenario setting, 79% from selected articles presented less than four graphics and 90% from publication had less three security as controlled variable.

4.5 RQ5: What Are the Most Commonly Used Metrics?

Metrics are variables dependent on the parameters that were set to perform the experiment. This SRL identified two main metrics in Fig. 5: energy as metric analized by 72 papers and time is another metric referencied by 57 papers.

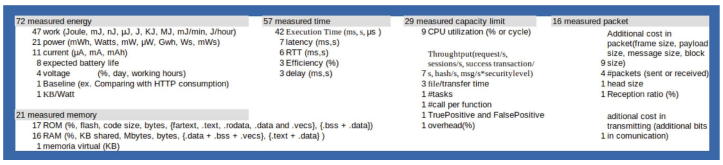


Fig. 5. Metrics to measure the experimental research

Selected articles were related to low-power security for the IoT. This explains the 100% of the articles with the energy as the metric. However, several energy measurement methods have been found and presented in Fig. 5.

So, future work on security, energy and IoT should at least measure time execution and energy in terms of the power consumption and current. New papers with these metrics can be more easily compared to existing results from older works.

4.6 RQ6: What Recommendations for Future Work that Will Conduct Experiments in the Field of IoT, Energy and Security?

This section presents a summary about recommendations for new experimental research in context of the security, energy and IoT that are enumerated in following:

- In terms of gaps, future researches must execute experiments that analyze availability in security, because there are practically no papers in this approach.
- In view of reproducibility and precision of the results, regardless of the security area in IoT, the description of new studies must reference a datasheet of each hardware used in research, to inform application layer, communication technology and traffic used in research to allow for high level of the reproducibility, as this will provide hardware details for future reproductive of the research. Moreover, it is very important to present the figure with information of the location of the hardware in experimental environment, to describe the standard deviation, to have at least 100 as the number of repetition and 100 s as time of observation.
- Considering configurable parameters in the evaluations, new papers should to use at least hardware feature (with and without accelerator and duty cycling) and security key size between 128 and 1024 bits. However, the articles could be comparable with major number of paper if new experimental researches consider also the following parameters: payload size, packets per seconds and heard size (with and without compression). In terms of the energy measurement, the authors should use at least one estimate model for energy, even when to use a tool to measure energy, because, when they present both results (estimating and real values), the article will provide information in a way that will be more easily compared with other articles, as most measure energy consumption through an estimate generated by a modeling.
- Taking account the metric types, new papers must use energy (power consumption and current) and time (execution) as main metrics. Additional the throughput in Msg/s, payload size and memory should be used if the authors would like that their works can be compared with more existing papers. Other option is to amplify the capacity of the paper to be compared with other publication is when the article to explore the variation of metrics for energy described in Fig. 4.

5 Conclusion

The presented results of this SLR aimed at investigating the characteristics of measurements in context of IoT, energy and security. This review has helped to understand the current state-of-the-art in methodologies to real experiments, and also to identify research gaps and future directions. After analyzing each measurement, they are classified according to their aims and the way they work. Thus, this SLR proposed three classification schemes: (i) by energy measurement type, (ii) by security, and (iii) by research type. Also, it has identified the main characteristics of the measurements (reproducibility, precision of the results, parameter used to configure the experiments and metrics).

The results of this SLR suggest that there is a predominance of real experiments which use estimation model to inform energy consumption of security approaches for IoT and a lower number of paper executed real measurement of energy consumption. This SLR encourages researches to continually execute real experiment in new IoT devices, because experiments with real devices contain important information to be used by energy consumption model. Moreover, it was possible to find gaps in availability research for IoT (subarea from information security).

In this direction, the results achieved in this study can be used as a guide for researches to identify which parameters and metrics best fit for new articles can be more broadly compared to existing publications. In addition, the problems of reproducibility and precision in selected papers from this SRL were identified.

References

1. Lazarescu, M.T.: Wireless sensor networks for the Internet of Things: barriers and synergies, pp. 155–186. Springer, Cham (2017)
2. Elshrkawey, M., Elsherif, S.M., Wahed, M.E.: An enhancement approach for reducing the energy consumption in wireless sensor networks. J. King Saud Univ. Comput. Inf. Sci. **30**(2), 259–267 (2018). https://doi.org/10.1016/j.jksuci.2017.04.002
3. Menezes, A.H.S., Kelvin, R.M.d.O., Oliveira, L.P., Oliveira, P.J.d.S.: IoT environment to train service dogs. In: 2017 IEEE First Summer School on Smart Cities (S3C), pp. 137–140, August 2017. https://doi.org/10.1109/S3C.2017.8501386
4. Sittón-Candanedo, I., Alonso, R.S., Corchado, J.M., Rodríguez-González, S., Casado-Vara, R.: A review of edge computing reference architectures and a new global edge proposal. Future Gener. Comput. Syst. **99**, 278–294 (2019). https://doi.org/10.1016/j.future.2019.04.016
5. Alemdar, H., Ersoy, C.: Wireless sensor networks for healthcare: a survey. Comput. Netw. **54**(15), 2688–2710 (2010). https://doi.org/10.1016/j.comnet.2010.05.003
6. Saleem, Y., Crespi, N., Rehmani, M.H., Copeland, R.: Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions. IEEE Access **7**, 62962–63003 (2019). https://doi.org/10.1109/ACCESS.2019.2913984
7. Dhasian, H.R., Balasubramanian, P.: Survey of data aggregation techniques using soft computing in wireless sensor networks. IET Inf. Secur. **7**(4), 336–342 (2013). https://doi.org/10.1049/iet-ifs.2012.0292

8. Sun, Q., Li, H., Ma, Z., Wang, C., Campillo, J., Zhang, Q., Wallin, F., Guo, J.: A comprehensive review of smart energy meters in intelligent energy networks. IEEE Internet Things J. **3**(4), 464–479 (2016). https://doi.org/10.1109/JIOT.2015.2512325
9. Sookhak, M., Tang, H., He, Y., Yu, F.R.: Security and privacy of smart cities: a survey, research issues and challenges. IEEE Commun. Surv. Tutor. **21**, 1718–1743 (2019). https://doi.org/10.1109/COMST.2018.2867288
10. Kantharaju, H.C., Murthy, K.N.N.: A survey on enhancing system performance of wireless sensor network by secure assemblage based data delivery. In: 2017 International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT), pp. 289–296, March 2017. https://doi.org/10.1109/ICRAECT.2017.55
11. Karakaya, A., Akleylek, S.: A survey on security threats and authentication approaches in wireless sensor networks. In: 2018 6th International Symposium on Digital Forensic and Security (ISDFS), pp. 1–4, March 2018. https://doi.org/10.1109/ISDFS.2018.8355381
12. Ravindran, V., Subramanian, S.: Systematic reviews and meta-analysis demystified. Indian J. Rheumatol. **10** (2015). https://doi.org/10.1016/j.injr.2015.04.003
13. Fabbri, S., Silva, C., Hernandes, E., Octaviano, F., Di Thommazo, A., Belgamo, A.: Improvements in the start tool to better support the systematic review process. In: Proceedings of the 20th International Conference on Evaluation and Assessment in Software Engineering, EASE 2016, pp. 21:1–21:5. ACM, New York (2016). https://doi.org/10.1145/2915970.2916013
14. Campelo, F., Takahashi, F.: Sample size estimation for power and accuracy in the experimental comparison of algorithms. J. Heuristics **25**(2), 305–338 (2019). https://doi.org/10.1007/s10732-018-9396-7