Smart Homes Privacy Metrics

Nooredin (Noory) Etezady
netezady@unm.edu
Anderson School of Management
University of New Mexico
Albuquerque, NM, USA

Abstract

Internet of Things (IoT) has exponentially increased the collection of different types of consumer information through IoT sensors. IoT makes people's life more convenient and at the same time poses new challenges to privacy and security protection. Most consumers do not completely realize the potential privacy and security risks related to IoT. To make the matters worse, there is no standard metric for IoT and specifically for smart homes. There have been several calls by researchers for identification and development of new metrics to measure the level of privacy harm and security protection. In this paper a comprehensive literature review was conducted on privacy metrics for smart homes. The literature review identified three papers on smart homes privacy metrics. The metrics developed by these papers have their shortcomings and need to be further verified and tested.

Keywords: smart home, privacy, metric, IoT, Internet of Things

1. INTRODUCTION

Internet of Things (IoT) has exponentially increased the collection of consumers' information through device sensors. Although IoT makes people's life more convenient, at the same time it poses new challenges to privacy and security protection. Most consumers do not completely realize the potential privacy and security risks related to IoT (Choi, Lowey, & Wang, 2020).

Access control and cryptography for controlling privacy have been researched with strong results. These methods can be strong deterrents against outside adversaries. However, they do not provide privacy protection against those with access to the data (Dong, Ratliff, Cardenas, Ohlsson, & Sastry, 2018). For example, utility companies with access to energy consumption may be able to infer lifestyle information from usage patterns.

One of the prime factors for users' willingness to deploy smart technology is convenience. However, it appears that personal data tracking by these devices is not important to the users of these technology (Princi & Kramer, 2020). Choi et al. (2020) noted that many consumers have limited information on IoT and even the ones with enough information seldom protect their personal information because of the cognitive gap between the attitude and actual behavior.

Although IoT maximizes convenience, the unseen collection of data, usage, and sharing increase privacy concerns for IoT users (Aleisa & Renaud, 2017). IoT privacy and security problems intensify the demand for mechanisms to protect IoT privacy and security (Choi et al., 2020).

As Amar, Haddadi, and Mortier (2018) noted; users are usually oblivious to the kind of information they are divulging. The users' data patterns can be used for inference and the users cannot be expected to be aware of that. Zheng, Apthorpe, Chetty, and Feamser (2018) also stated that users need to be informed of the continuing data collection through IoT devices. In most cases, collection of some type of data might be harmless. However, specific household information can lead to compromising inferences. They also observed that for privacy protection, it is necessary to make it easier for the users to understand and control smart home data collection. Providing a way to easily configure privacy features would assist users with privacy protection. Privacy metrics will assist users in understanding the level of privacy protection of their devices and motivate them to configure their privacy features.

The contribution of this paper is to present and overview of the existing research on smart homes (IoT for homes) privacy metrics and to point out its shortcomings.

2. LITERATURE REVIEW

In general, research on identifying metrics for privacy has been scarce. Research by Liu and Terzi (2010) is one of the exceptions who developed a framework for computing privacy scores for online social networks users. There have been calls by several researchers for identifying privacy metrics (Bugeja, Jacobsson, & Davidsson, 2020 ; Vemou & Karyda, 2018; Haug, Lanza, & Gewald, 2021).

Research on IoT privacy metrics is also scarce. Choi et al. (2020) noted that many previous privacy scoring studies are on the context of social media. Therefore, the IoT vulnerabilities and new information types used in IoT are not considered.

Toch, Bettini, Shmueli, Radaelli, Lanzi, Riboni, and Lepri (2018) called for the identification and development of new metrics that measure the level of privacy harm and security protection of systems. These new metrics could help in the future development and regulation policies of cyber security systems.

Various researchers have suggested different ways to measure privacy. For example, Haug et al. (2021) stated that to measure privacy concerns one might need to utilize privacy risks as a proxy. Bugeja et al. (2020) presented a data sensitivity metric based on personal data exposure for smart connected homes. Dong et al. (2018) looked into the behavioral methods and noted that since it is not easy to convert a person's emotions and decision making about privacy into a mathematical object, the majority of existing behavioral methods can be useful. Using behavioral methods requires emphasis on a privacy level evaluation that closely follows either a person's privacy assessment or decision to reveal information. User studies research that employ this method will maintain their applicability to real-life applications.

Machine learning can also be utilized in privacy research. Liu, Ding, Shaham, Rahayu, Farokhi, and Lin (2021) noted that machine learning can be used as a powerful tool for privacy research from an attack as well as defense point of view.

There are several literature review papers on IoT and smart homes privacy concerns (Abdi, Zhan, Ramokapane, & Such, 2021; Aleisa & Renaud, 2017; Kulyk, Milanovic, & Pitt, 2020; Ogonji, Okeyo, & Wafula, 2020; Princi & Kramer, 2020; Yao, Basdeo, McDonough, & Wang, 2019). However, as of the date of this paper, no literature reviews on privacy metrics for smart homes were found.

This study is a literature review of privacy metrics for smart homes. The results of this study will help researchers to understand the current status of research on smart home privacy metrics and the need to develop privacy metrics for smart homes.

3. METHOD

To perform the literature review, the methodology developed by Pickering and Byrne (2014) was used in order to systematically analyze existing academic literature and produce a quantitative overview of smart-home privacy metrics. The benefit of this method is its facility for finding what the existing research covers and where the gaps are (Aleisa & Renaud, 2017). This method has been used by various researchers in the past (Aleisa & Renaud; Ogonji et al., 2020; Low-Choy, Riley, & Alston-Knox, 2017; Templier & Pare, 2018; Bergstrom, Van Winsen, & Henriqson, 2015).

The Pickering and Byrne (2014) methodology is a 15-stage process that starts with defining the topic, formulating research questions, identifying keywords, identifying and searching databases to evaluating key results and conclusions and finally revising paper till it is ready for submission.

For the literature review the following databases were searched for research papers and conference proceedings related to Home IoT privacy metric: Association of Information systems (AIS), ACM, IEEE Xplore, Elsevier ScienceDirect, ProQuest, Emerald Management, and Web of Science. Only research in English was considered. Considering that 70% of social science and 90% of natural science research is conducted in English the language bias may not be large (Pickering & Bryne, 2014).

A combination of the following keywords was used: Internet of Things, IoT, home, Smart Home, Privacy metric, and privacy measurement. The search was conducted up to and including the year 2022.

Databases	Number of Articles
ACM	10
AIS	10
Elsevier Science Direct	18 (The total was 41. Only 18 papers were relevant to IoT after reading the abstracts.)
Emerald Management	1
IEEE	13
ProQuest	16
Web of Science	1
Total:	69 (92 total)

Table 1: Search Databases 1

4. RESULTS

The search yielded 92 original peer-reviewed research papers. The abstract, methodology, and conclusion of these papers were reviewed to identify the ones addressing privacy for internet of things. There were 69 papers that discussed privacy specifically in the IoT domain. Research on IoT privacy was categorized among various IoT research areas as shown in table 2.

The top three area of IoT privacy research were Location Based Services (LBS) with 13 papers; followed by IoT privacy models, frameworks, and protocols with 12 papers; and healthcare with 5 papers. Since locations-based services are used by smart devices and applications (for example; smart phones, smart vehicles, and web applications) user privacy is a major concern, which is reflected by the number of research papers in that area. To implement privacy; privacy models, frameworks, and protocols are needed; which explains the high number of research papers on the topic. Healthcare data, such as patient data, needs to be safeguarded. Patients' privacy is also of prime concern shown by the number of research papers on healthcare privacy.

There has been less research on smart homes privacy as it is a relatively new area for IoT and of less importance compared to the top three. However, as indicated in table 2 by the low number of research papers on smart homes privacy, more research is needed on smart homes privacy. In general table 2 is a good indicator for the IoT privacy research areas that need attention.

Various aspects of privacy were addressed by the reviewed research papers. Some researchers investigated personal data privacy for any system that obtains personal data. One such example is Amar et al. (2018) that studied personal data privacy for any system that data consumers use to obtain personal data. They suggested implementing personal data privacy for producers of data using cheap hardware at the source of data. Other researchers like Dong et al. (2018) investigated the tradeoff between stringent data privacy rules and usefulness of the obtained data for consumers of that data.

IoT Area	Number of Papers
Camera Glass	1
Crowdsourcing	2
Cyber-physical Systems	3
Data (utility & privacy)	1
Data – Car	1
Data – Personal	3
Healthcare	5
IoT & privacy models, frameworks, and protocols	12
Location Based Services (LBS)	13
Machine Learning	1
Mobile Analytics on IoT Devices	1
Mobile applications used in smart homes & IoT devices	1
Mobile participatory sensing*	1
Network Monitoring (IoT)	1
Privacy labeling	1
Privacy preserving solutions	1
Smart Cities - Crowdsensing	1
Smart Communities	1
Smart Devices	1
Smart Devices – mobility management	1
Smart Energy Management Systems	1
Smart Grid	3
Smart Home	3
Smart Home - Speakers	2
Smart Meter	2
Value Creation in IoT (Digital Platform) Eco-system	1
Vehicles	4
Wearables	1
Total	69

Table 2: IoT Privacy Research Categories

*In table 2, mobile participatory sensing refers to the sensing, processing, and storage resources in mobile phones that is used to obtain insight about the participants and their environment through various applications (Christin, 2016).

To identify research that specifically addressed privacy metrics; the introduction, methodology, and conclusion of the 69 research papers in table 2 were read carefully. In some cases, the whole paper was read. Eighteen research papers were identified that discussed privacy metrics in IoT. These research papers are listed in table 3 in Appendix A. The findings from table 3 are discussed in the next section.

5. FINDINGS

The privacy metrics, models, or frameworks that were discussed or developed in the reviewed papers were mostly based on one or more of three main privacy metrics. These privacy metrics included differential privacy, k-anonymity, and entropy and have been used by various researchers in the past.

Differential privacy was first introduced and used in statistic databases. It is a rigorous mathematical definition of privacy. Differential privacy was inspired by Dalenius (1977) that "nothing about an individual should be learnable from the database that cannot be learned without access to the database" (Dwork, 2006). In simple terms, differential privacy introduces noise into a dataset so that personal information cannot be identified when statistical analysis is performed on the dataset.

As Dong et al. (2018) noted, the most popular privacy metric is differential privacy. However, differential privacy for many practical applications requires a particular structure of uncertainty. Its use is not clear in a dynamic system when the sampling rate is adjusted (Dong, et al.).

k-Anonymity is a widely adopted method for preserving privacy that was introduced for the database community by Sweeney (2002). K-anonymity is based on hiding sensitive information by introducing k-1 dummies so that the adversary will be unable to recognize the actual information.

Entropy was first introduced by Serjantov and Denezis (2002) to measure the degree of uncertainty in an anonymous set. Entropy privacy metric refers to the uncertainty in a random variable. Entropy is the measure of anonymity in a set (Babaghayou, Labraoui, Abba Ari, Lagraa, & Ferrag, 2020). A lower entropy translates into a lower privacy protection level (Alaradi and Innab, 2019). Entropy is used in Location Based Services (LBS) to measure the uncertainty degree of a location belonging to a user (Sun, Chen, Hu, Qian, & Hassan, 2017).

Cyber-physical Systems

To protect user's privacy in smart cyber-physical systems Chaaya, Barhamgi, Chbeir, Arnould, & Benslimane (2019) proposed Privacy Oracle. Privacy Oracle is a context-aware semantic reasoning system, providing users with a dynamic overview of their privacy risks as their context changes. When users are aware of the direct and indirect privacy risks, they can take the proper steps to protect their privacy.

Location Based Services (LBS)

Compromised location servers, which store users' activities information, can use inference attacks to track the users' real location and obtain personal and sensitive user information. Alaradi and Innab (2019) proposed Location Based Services protection method to guarantee location privacy by enhancing the previously employed method of using dummy locations. Dummy locations surround the real location to impede recognition of the real location among the dummies by the server. Alaradi and Innab employed entropy privacy metric.

Set of Anonymity Size (SAS) "refers to the indistinguishability of a target vehicle in comparing to other vehicles in the same context." (Babaghayou et al., 2020). Babaghayou et al. surveyed the Vehicular Ad-hoc Networks (VANETS) privacy protection strategies that use pseudonyms in place of individual real identities and changing them often to protect the privacy of users. They reviewed various location based privacy metrics for VANETS, including SAS, entropy, the degree of anonymity, adversary's success rate, maximum tracking time, and statistics on pseudonym change. Babaghayou, Labraoui, Abba Ari, Ferrag, Maglaras, and Janicke (2021) used a location privacy metric called traceability. Traceability is defined "as the correctness of an adversary to build the target vehicle's traces using eavesdropped beacons" (Babaghayou et al., 2021).

Bin, Lei, and Guoyin (2019) proposed a mathematically rigorous method for LBS privacy protection called Ɛ-sensitive correlation privacy protection scheme which provides correlation indistinguishable to the location data. Entropy is used in Ɛ-sensitive correlation privacy protection.

IoT

Consumer-disclosed information is classified by previous research into six information types, which include demographic; contact; vehicle; lifestyle, interests, and activities data; financial and economic data; and financial and credit data. Examples of financial and economic data include estimated income and home value. Examples of financial and credit data are credit score, loan, and credit card data. The new type of data that is captured by IoT includes consumers' behavioral tendencies, real-time locations, and schedules, which can be subject to ill use (Choi et al., 2020).

To protect private information of IoT users, Choi et al. (2020) proposed a design framework to evaluate and quantify IoT privacy security risks (PSR) that is associated with IoT adoption. PSR scores are used to assess IoT Privacy and Security Risks (PSR). PSR scores are determined by the collective consideration of consumers' IoT information types, weight impact factors, and personal capabilities. Their work contributes to increasing user awareness of PSRs and thereby minimizing the cognitive gap that is the possible cause of consumers' paradoxical behaviors when it comes to protecting their privacy. The limitation of the proposed approach is that the direct impact of cognitive gap between the attitude and actual behavior is not easily measurable. In addition, PSR scores can be subjective until there are sufficient PSR scores to compare individuals to populations. And finally, the individuals' personalities and experiences change in different cultures which affects risks associated with different information types (Choi et al.).

Dong et al. (2018) introduced inferential privacy metric for IoT that takes into consideration data quality and its utility to the collectors of data. Inferential privacy metric is the probability that an adversary can correctly infer private information from public observations. However, in practice, determining the required distributions is not trivial (p. 9).

Tavakolan and Faridi (2020) presented a model for describing and applying privacy-aware policies in IoT devices. They suggested dividing general privacy policies into four main metric categories of obligation, disclosure, collection, and selectivity that could be used to build a descriptive model of privacy aware policy on IoT devices. These general categories can be further expanded into more metric subcategories. The proposed model needs to be evaluated and tested practically.

Smart Energy Management Systems

Ukil, Bandyopadhyay, and Pal (2015) proposed a privacy management method for smart energy applications. The proposed approach automatically detects, measures, and preserves privacy for smart meter data before sharing it with third parties. The user will also be alerted when there is a possibility for privacy breaches of the shareable data. The proposed method requires a facilitation tool or device to perform the necessary analysis and computation on data.

Smart Homes

Bugeja et al. (2020) classified smart connected home systems into a four-tiered classification of app-based accessors, watchers, location harvesters, and listeners. An equation was then presented to calculate the data sensitivity score of smart home systems. Data type (e.g., Image, audio, position), privacy parameter (e.g., data type sensitivity, location sensitivity, and data accessibility) were used in the equation to calculate data sensitivity score. It is possible to include other parameters such as data retention time and trust in a manufacturer to measure data sensitivity. The proposed data sensitivity metric needs to be analyzed and validated. A metric will also be needed for grading the calculated data sensitivity.

Daubert, Wiesmaier, and Kikiras (2015) proposed a model that linked information, privacy and trust. The model was based on privacy dimensions and trust dimensions. Privacy dimensions included identity privacy, location privacy, footprint privacy (such as preferred language and operating system), and query privacy (e.g., the fact that a query is made on weather). Trust dimensions included trust in device, processing, connection, and system.

Kennedy, Li, Wang, Liu, Wang, and Sun (2019) proposed a new privacy metric for voice command fingerprinting attacks against smart-home speakers called semantic distance that used natural language processing to measure the privacy leakage. A voice command fingerprinting attack takes advantage of the fact that every voice command and its response, although encrypted, possess a unique traffic pattern because of packet length, direction, order, etc. (Kennedy et al., 2019). The semantic distance metric uses accuracy, which is the effectiveness of a voice command fingerprinting attack, and semantic distance. Semantic distance refers to the fact that two similar voice commands are not exactly the same, for example "what is the weather" and "what is the weather tomorrow?". Semantic distance is used as a metric to measure privacy leakage in addition to accuracy.

6. CONCLUSION

With the progressive advancement of technology, Internet of Things (IoT) has exponentially increased the collection of numerous consumers' information through IoT sensors. IoT makes people's life more convenient and at the same time it confronts them with new challenges to privacy and security protection. Research shows that most consumers do not completely realize the potential privacy and security risks related to IoT (Choi et al., 2020).

There is no standard metric for smart homes. Several researchers have called for identification and development of new metrics to measure the level of privacy harm and security protection (Bugeja et al., 2020; Toch et al., 2018; Haug et al., 2021; Vemou & Karyda, 2018). Development of new metrics could also help in the future development and regulation policies of cyber security systems.

In this paper a comprehensive literature review was conducted on privacy metrics for smart homes. The literature review identified three papers on smart homes privacy metrics. The metrics developed by these papers have their shortcomings and need to be further verified and tested.

Considering the dearth of research on IoT and smart home privacy, future researchers need to focus on identifying and developing new metrics for IoT and smart homes as a step toward user privacy protection.

7. REFERENCES

Abdi, N., Zhan, X., Ramokapane, K. M., & Such, J. (2021). Privacy norms for smart home personal assistants. *Proceedings of the ACM CHI Conference, Yokohama*, 14 pages.

Alaradi, S., & Innab, N. (2019). Ensuring privacy protection in location-based services through integration of cache and dummies*. International Journal of Advanced Computer Science and Applications (IJACSA). 10*(2), 88-100.

Aleisa, N., & Renaud, K. (2017). Privacy of the Internet of Things: A systematic literature review. *Proceedings of the 50th Hawaii International Conference on Systems Sciences*, 5947-5956.

Amar, Y., Haddadi, H., & Mortier, R. (2018). An Information-Theoretic Approach to Time-Series Data Privacy. *Proceedings of InW-P2DS'18: 1stWorkshop on Privacy by Design in Distributed Systems, April 23–26, 2018, Porto, Portugal. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3195258.3195261*

Babaghayou, M., Labraoui, N., Abba Ari, A. A., Lagraa, N., Ferrag, M. A. (2020). Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: a survey. *Journal of Information Security and Applications. 55* (2020) 102618, 1-17.

Babaghayou, M., Labraoui, N., Abba Ari, A. A., Ferrag, M. A., Maglaras, L., & Janicke, H. (2021). WHISPER: A location privacy-preserving scheme using transmission range changing for Internet of Vehicles. *Sensors, 21*,2443,1-21.

Bansal, G., & Nah, F. (2020). Measuring privacy concerns with government surveillance and right-to-be-forgotten in nomological net of trust and willingness-to-share. *Proceedings of American Conference on Infor, M., mation Systems*, 1-10. 31.

Beker, I., Posner, R., Islam, T., Ekblom, P., Borrion, H., McGuire, M., & Li, S. (2021). Privacy in transport? Exploring perceptions of location privacy through user segmentation. *Proceedings of the 54th Hawaii International Conference on Systems Sciences.* 5347-5356. URI:https://hdl.handle.net/10125/71270. 978-0-9981331-4-0

Bergstrom, J., Van Winsen, & R., Henriqson, E. (2015). On the rationale of resilience in the domain of safety: a literature review. *Reliability Engineering & System Safety, 14*, 131-141.

Bin, W., Lei, Z., & Guoyin, Z (2019). A novel ε-sensitive correlation indistinguishable scheme for publishing location data. *PLoS ONE, 14*(12), 1-17.

Bugeja, J., Jacobsson, A., &Davidsson, P. (2020). Is your home becoming a spy? A data-centered analysis and classification of smart connected home systems. *Proceedings of the 10th International Conference on the Internet of Things (IoT 2020), Malmo, Sweden.* ACM, New York, USA, 8 pages.

Chaaya, K. B., Barhamgi, M., Chbeir, R., Arnould, P., & Benslimane, D. (2019). Context-aware system for dynamic privacy risk inference, Application to smart IoT environments. *Future Generation Computer Systems. 101*, (2019),1096-1111.

Choi, D., Lowry, P. B., & Wang, G. A. (2020). The design of personal privacy and security risk scores for minimizing consumers' cognitive gaps in IoT settings. *Proceedings of the 53rd Hawaii International Conference on Systems Sciences.* 5076-5085.

Christin, D. (2016). Privacy in mobile participatory sensing: Current trends and future challenges. *The Journal of Systems and Software 116*(2016), 57-68.

Dalenius, T. (1977). Towards a methodology for statistical disclosure control. *Statistik Tidskrift 15*, pp. 429–222.

Daubert, J., Wiesmaier, A., & Kikiras, P. (2015). A view on privacy & trust in IoT. Proceedings of IEEE ICC 2015 - Workshop on Security and Privacy for Internet of Things and Cyber-Physical Systems. 2665-2670

Dong, R., Ratliff, L. J., Cárdenas, A. A., Ohlsson, H., & Sastry, S. S. (2018). Quantifying the Utility–Privacy Tradeoff in the Internet of Things. *ACM Trans. Cyber-Phys. Syst. 2, 2, Article 8 (May 2018), 28 pages. https://doi.org/10.1145/3185511*

Du, Y., Cai, G., Zhang, X., Liu, T., & Jiang, J. (2019). An efficient dummy-based location privacy-preserving scheme for Internet of Things services. *Information 2019, 10*, 278. 1-15.

Dwork, C. (2006). Differential privacy. *Proceedings of the International Colloquium on Automata, Languages and Programming*. Springer, 1–12.

Haug, M., Lanza, J., & Gewald, H. (2021). Only if it affects me! The influence of privacy on different adoption phases. *Proceedings of the Forty-Second International Conference on Information Systems (ICIS 2021), Austin.*10. 1-17.

Kennedy, S., Li, H., Wang, C., Liu, H., Wang, B., & Sun, W. (2019). I can hear your Alexa: Voice command fingerprinting on smart home speakers. *Proceedings of 2019 IEEE Conference on Communications and Network Security (CNS)*. 232-240.

Kulyk, O., Milanovic, K., & Pitt, J. (2020). Does my smart device provider care about my privacy? Investigating trust factors and user attitudes in IoT systems. *Proceedings of the 11th Nordic Conference on Human-Computer Interaction (NordiCHI '20)*, Tallinn, Estonia, 12 pages.

Li, T., He, X., Jiang, S., & Liu, J. (2022). A survey of privacy-preserving offloading methods in mobile-edge computing. *Journal of Network and Computer Applications, 203*, 103395, 1-28.

Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F., & Lin, Z. (2021). When machine learning meets privacy: A survey and outlook. *ACM Computing Surveys, 54*(2), Article 31, 1-36. https://doi.org/10.1145/3436755

Liu, K., Terzi, E. (2010). A framework for computing the privacy score of users in online social networks. *ACM Transactions Knowledge Discovery from Data 5*(1), article 6, 1-30.

Low-Choy, S., Riley, T., Alston-Knox, C. (2017). Using Bayesian statistical modelling as a bridge between quantitative and qualitative analyses: illustrated via analysis of an online teaching tool. Educational Media International 54(4), 317-359.

Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of Internet of Things. Computer Science Review, 38(2020), 100312, 1-19.

Pickering, C., & Byrne, J. (2014). The benefits of publishing systematic quantitative literature reviews for PhD candidates and other early-career researchers, *Higher Education Research & Development,* 33:3, 534-548, DOI: 10.1080/07294360.2013.841651

Princi, E., & Kramer, N. C. (2020). I spy with my little sensor eye – effect of data-tracking and convenience on the intention to use smart technology. *Proceedings of the 53rd Hawaii International Conference on System Sciences,* 1391-1400.

Serjantov, A., Danezis, G. (2002). Towards an information theoretic metric for anonymity. *In Privacy Enhancing Technologies*; LNCS 2482, Springer-Verlag Berlin Heidelberg 2003; pp. 41–53.

Sun, Y., Chen, M., Hu, L., Qian, Y., & Hassan, M. M. (2017). ASA: Against statistical attacks for privacy-aware users in location based service. *Future Generation Computer Systems. 70* (2017) 48-58.

Sweeney, L. (2002). k-anonymity: a model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10*(5), pp. 557–570.

Tavakolan, M., Faridi, I. A. (2020). Applying privacy-aware policies in IoT Devices using privacy metric. *International Conference on Communications, Computing, Cybersecurity, and informatics (CCCI)*. 978-1-7281-7315-3/20/

Templier, M., Paré, G. (2018) Transparency in literature reviews: an assessment of reporting practices across review types and genres in top IS journals. *European Journal of Information Systems 27*(5), 503-550.

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. *ACM Comput. Surv. 51(2)*, Article 36, 1-27.

Ukil, A., Bandyopadhyay, S., & Pal, A. (2015). Privacy for IoT: Involuntary privacy enablement for smart energy systems. *Proceedings of ICC 2015 SAC - Internet of Things.* 536-541.

Vemou, K., & Karyda, M. (2018). An evaluation framework for privacy impact assessment methods. *Proceedings of the Mediterranean Conference on Information Systems (MCIS 2018),* 5. 1-10.

Wang, D., Ren, J., Wang, Z., Zhang, Y., & Shen, X. (2022). PrivStream: A privacy-preserving inference framework on IoT streaming Data at the edge. *Information Fusion, 80* (2022). 282-294.

Wang, J., Tian, L., Huang, Y., Yang, D., & Gao, H. (2018). Achieving the optimal k-anonymity for content privacy in interactive cyberphysical systems. *Security and Communication Networks. 2018*. Article ID 7963163. 1-15.

Yao, Y., Basdeo, J. R., McDonough, O. R., & Wang, Y. (2019). Privacy perceptions and designs of bystanders in smart homes. *Proceedings of ACM Human-Computer Interaction, 3*(59), 1-24.

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of Hum.-Comput. Interact.* 2, CSCW, Article 200, 20 pages.

Zhang, B., Liu, C. H., Lu, J., Song, Z., Ren, Z., & Ma, J. (2016). Privacy-preserving QoI-aware participant coordination for mobile crowdsourcing. *Computer Networks, 101*, 29-41.

APPENDIX A
Table 3

Research Authors	Category	Privacy Metric	Privacy Method	Publisher
Zhang, Liu, Lu, Song, Ren, & Ma (2016)	Crowdsourcing - IoT Mobile Crowdsourcing	Entropy	Privacy-preserving participant coordination mechanism is proposed to achieve optimal Quality of Information (QoI) for sensing tasks and protect the participants' location privacy.	Elsevier
Wang, Tian, Huang, Yang, & Gao (2018)	Cyber physical systems	entropy and differential privacy	Proposed and used theoretical multilayer Alignment (MLA) algorithm to establish k-anonymity based mechanism for preserving privacy and to achieve content privacy	Prorequest
Chaaya, Barhamgi, Chbeir, Arnould, & Benslimane (2019)	Cyber physical systems	Privacy risk	Privacy Oracle - a context aware semantic reasoning system	Elsevier
Dong, Ratliff, Cardenas, Ohlsson, & Sastry, (2018)	Data - utility & privacy in IoT and smart grid	Inferential privacy	Inferential privacy	ACM
Babaghayou, Labraoui, Abba Ari, Ferrag, Maglaras, & Janicke. (2021)	Internet of Vehicles	location privacy metric called traceability.	WHISPER – A privacy preserving scheme based on reducing the transmission range while sending the safety beacons	Prorequest
Babaghayou, Labraoui, Abba Ari, Lagraa, & Ferrag (2020).	Internet of Vehicles - Vehicular ad-hoc networks (VANETS)	Reviewed LBS privacy metrics: SAS, entropy, the degree of anonymity, adversary's success rate, maximum tracking time, statistics of pseudonym change	Literature Review - A survey of various privacy protections based on pseudonym change strategies	Elsevier
Li, He, Jiang, & Liu (2022)	IoT	Privacy metrics for offloading: privacy entropy, task sensitivity, secrecy rate, secrecy outage probability, location privacy loss, and differential privacy	Literature review - Review paper on Edge Servers & wireless Transmissions (offloading).	Elsevier
Tavakolan & Faridi (2020)	IoT - A model for applying user preferences	Four main categories of obligation, disclosure, collection, and selectivity.	Users prioritize a set of extendable privacy policies by assigning weights to the	IEEE

Research Authors	Category	Privacy Metric	Privacy Method	Publisher
			policies. The proposed method is used to apply user’s preferences within the privacy aware policies in IoT devices.	
Wang, Ren, Wang, Zhang, & Shen (2022)	IoT - Privacy preserving IoT streaming data analytical Framework (theoretical), based on edge computing	Sensitive inferences accuracy. Identity and gender recognition were defined as sensitive inferences.	It uses a deep learning model to filter sensitive information and combines with differential privacy to stop the untrusted edge server from making inferences from the IoT streaming data.	Elsevier
Choi, Lowry, & Wang (2020)	IoT - framework	Framework – The framework is grounded in cognitive dissonance theory and information processing theory.	A design framework for evaluating and quantifying IoT privacy security risks associated to IoT adoption	AIS
Alaradi & Innab (2019)	LBS (Location Based Services)	entropy	Location privacy protection called Safe Cycle Based Approach (SCBA)	Prorequest
Bin, Lei, & Guoyin (2019)	LBS	entropy	Ɛ -sensitive correlation privacy protection	Prorequest
Sun, Chen, Hu, Qian, & Hassan (2017)	LBS	entropy	Entropy is used to devise methods to defend two attacks to LBS.	Elsevier
Du, Cai, Zhang, Liu, & Jiang (2019)	LBS	Entropy is used to measure the degree of privacy preservation for an anonymous set.	Entropy is used is used to measure the uncertainty of recognizing the user’s location in a dummy location set.	Prorequest
Ukil, Bandyopadhyay, & Pal (2015)	Smart Energy Management Systems	Proposed a model called Dynamic Privacy Analyzer	The proposed dynamic privacy analyzer for smart meters uses estimation of privacy disclosure risk through analytical framework.	IEEE
Bugeja, Jacobsson, and Davidsson (2020)	Smart Home	Based on data sensitivity score	Based on data sensitivity score	ACM
Daubert, Wiesmaier, & Kikiras (2015)	Smart Home	Trust - Trust is used as a scalar metric and mapped to privacy, sensitivity, and personally	A model to link information, privacy and trust.	IEEE

Research Authors	Category	Privacy Metric	Privacy Method	Publisher
		identifiable information.		
Kennedy, Li, Wang, Liu, Wang, & Sun (2019)	Smart Home - speakers	Semantic distance	Accuracy and semantic distance are used	IEEE

Table 3: Research on IoT Privacy Metric