Differential Privacy Applied To Smart Mete rs: A Mapping Study

Jacob Marks
jacob.marks@student.runt.edu
New Mexico Tech
Socorro, NM, USA

Bran don Montano
brandon.montano@student.runt.edu
New Mexico Tech
Socorro, NM, USA

Jiw an Chong
jiwan.chong@student.nmt.edu
New Mexico Tech
Socorro, NM, USA

Manjusha Raavi
manjusha.raavi@student.runt.edu
New Mexico Tech
Socorro, NM, USA

Raisa Islam
raisa.islam@student.nmt.edu
New Mexico Tech
Socorro, NM, USA

Tomas Cerny
tomas.cerny@baylor.edu
Baylor University
Waco, TX, USA

Dongw an Shin
Dongwan.Shin@nmt.edu
New Mexico Tech
Socorro, NM, USA

ABSTRACT

Smart meters and the smart grid will allow utility companies and customers to monitor their electricity and utility usage in fine-grained detail instead of the previously common monthly or yearly measurements. With this fine-grained detail comes serious privacy concerns . One of the most promising solutions for measuring and preserving privacy loss is differential privacy. Both differential privacy and the smart grid are relatively young developments thatwill require more research before they can be confidently implemented worldw ide. With this systematic mapping study, we will provide an overview of the current literature and attempt to determine the future directions the research may take.

ACM Reference Format:
Jacob Marks, Brandon Montano, Jiwan Chong, Manjusha Raavi, RaisaIslam, Tomas Cerny, and Dongwan Shin. 2021. Differential Privacy Applied To Smart Meters: A Mapping Study . In The *36th ACMISIGAPP Symposium on Applied Computing (SAC '21), March 22- 26, 2021, Virtual Event, Republic of Korea.* ACM, New York, NY, USA, Article 4, 10 pages. https://doi.org/10.1145/3412841.3442360

1 INTRODUCTION

The smart grid is a term for a planned and partially implemented utility infrastructure which will allow electric companies to more carefully monitor electrical usage and helpoptimize the power grid [1). Smart meters and the smart grid will allow utility companies and customers to monitor their electricity and utility usage in fine-grained detail instead of the previously common monthly or yearly measurements. With this fine-grained detail comes serious privacy concerns. Giving third parties access to data could be extremely useful, but also possibly damaging to the smart meter users. Many proposed methods for preserving the privacy of smart meter data usedifferential privacy. Differential privacy is a mathematically rigorous method for determining and setting the privacyof a method [2). Both smart meters and differential privacy are relatively new, meaning there are many competing concepts, and it is difficult to determine the future direction of the research.

Even though smart meters only report electrical data and not exactly what is being used, it is still possibly to extract an incredible amount of information about the smart meter users just from their daily electrical data. Greveler et al. found that with measurements every 0.5 seconds they were able to identify what was being watched on television in that household [3]. Smart meters do not currently process data this quickly, but there are concerning implications about what can be learned from user data. Even without smart meters, non-intrusive load monitoring(NILM) techniques can detect what appliances are being used in a home [1, 3). Differential privacy is one of the most promising privacy preserving methods being applied to the smart grid [1, 4, 5). It offers measurable privacy with a lower computational complexity than cryptographic methods [1]. k-anonymity, another form of statistical privacy, does not work well for large scale smart grid data because "the chances of re-identification increase if size of attributes in dataset increases." [1].With many privacy preserving solutions, the data must still be released cautiously because of the possibility of differencing attacks [1, 6], however when differential privacy is successfully applied the aggregated data can be released without compromising any individual user'sprivacy [2]. Natively differential privacy requires a trusted data aggregator, but many applications of it to smart meters allow for an untrusted aggregator. Differential privacy adds noise to data in order to ensure its privacy, which leads to a difficult balance between the amount of privacy and the utility of the data.Knowing the best balance between privacy and utility, the right type of noise to add, and the trust model to use are all open questions.

To understand how researchers are trying to answer these questions literature reviews are needed. Though many surveys have been done on the topic of differential privacy applied to smart meters, the field is constantly changing and requires new research and

SAC'21, March 22-26 2021, Virtual Event, Republic of Korea

ACM ISBN 978-1-4503-8104-8/21/03...$15.00
https://doi.org/10.1145/3412841.3442360

surveys. To help better understand the current state of the literature and provide information for future reviews and work, we have performed a systemic mapping study. The goal of a mapping study, according to Brereton et al., is to "describe the kinds of research activity that have been undertaken relating to a research question." [7]. Rather than choosing only the research thatwe have seen previously, we develop repeatable methods to identify the best literature for answering our research questions. The research questions we have developed are intended to help us understand the distribution of various topics and methods in the literature, and determine the possible future direction of the research. Our research questions are:

- (RQl) What are differential privacy-preserving methods/tools/strategies/techniques applied to smart meters, and what is their distribution in the literature?
- (RQ2) What subjects, or topics, have been addressed in the research for differential privacy in the smart grid, and what is their distribution in the literature?
- (RQ3) What datasets are used to study differential privacy applied to smart meters?
- (RQ4) Wha t is the future direction in the research of applying differential privacy to smart meters?

Diane Cooper states that mapping studies are "basedon the conceptthat published articles not only represent findings but, indirectly, represent activity related to the finding" [8]. With this mapping study, we aim to discover linkages between modern differentially private methods and better understand the future direction when applying these methods to the smart grid.

In Section 2 we will introduce differential privacy, and the smart grid. Section 3 covers our methods of research and our reasons for using these methods. Our results and a discussion of those results is in Section 4. Finally we offer our conclusions in Section 5.

2 BACKGROUN D AND RELATED WORK

Smart grids and smart meters are getting more and more popular, and it is envisioned that they will be widely used in the near future. With smart meters, even collecting data every 10 minutes, a vast amount ofdata is beingproduced and monitored. Thisdetailed level willallow utility companies to billcustomers dependingon the time ofday and usage per reading. This could encourage people to adjust their usage depending upon availability. Alongside billing, smart meters are expected to be used for many other possible purposes. Data could be released for research, services to help customers monitor their appliance and utility usage, as well as control power distribution within the smart grid. The smart grid can be used for many useful things, but it also brings security concerns. The fine-grained data collected by smart meters could be used to reveal a wealth of information about the meter owner. Using fine-grained smart meter data, researchers have been able to discover many private details about a household, including their economic status, the occupancy of the house [1], or even what they' re watching on television[3].

A tempting solution to privacy problems is anonymization. If the identity of each smart meter is obscured it can seem like this solves the problem. However, research has found that even with anonymization it can be possible to identify someone's identity from their anonymized data using a linking attack [6].

2.1 Statistical Approaches

An alternative to simple anonymization is applying an algorithm to the dataset that provides better privacy guarantees. The broad goalof statistical privacy is to apply an algorithm on a dataset such that "sensitive information about the individuals that constitute the data set"[5] are not revealed. One common method of statistical privacy is k-anonymity. k-anonymity is a privacy requirement which requires that for every person in a dataset, there are $k - 1$ people whose data is indistinguishable from that person's data [5, 9).

Differential privacy, introduced in 2006 by Dwork et al. [2], is a type of statistical privacy. Considering situations where the utility company may not be trusted, or situations which require fast solutions, differen tial privacy is one of the most promising. Differential privacy is the promise that whether or not your data appears in a dataset, it is improbable that anyone will be able to tell. The probability that someone will be able to detect your presence in the dataset (or lack of presence) is related to a value £, which defines how differentiallyprivate the algorithm is. The formal definition of differential privacy can be seen in Equation 1, where A is an algorithm that is only differentially private if, "for all data sets D1 and Dz, where D1 and *Dz* differ in at most a single user, and for all subsets of possible answers SI: *Range(A)"* [4], Equation 1 is true. Acs et al., state "the modification of any single user's data in the dataset (including its removal or addition) changes the probability of any output only up to a multiplicative factor e<." [4].

$$P(A(Dt) \in S) :-::; e£ \cdot P(A(Dz) \in S) \quad (1)$$

Differential privacy can be applied to any domain which has large datasets where the privacy of the users needs to be protected from any party looking at the processed data. Yang et al. cover the use of differential privacy to protect social network data, data from Netflix users , and even genomic data [10].Others have applied differential privacy to sparsedatasets [11], or less common problems like the unlimited auction problem [12]. Many differentially private solutions for internet of things devices can also be applied to the smart grid, and viceversa [1]. The advantage to this is that many of the sources we have looked at in this paper can be applied to other domains. Four papers we read explicitly discussed applying their method to other domains besides the smart grid in the future.

2.2 Cry ptographic Approaches

Some popular privacy preserving methods use cryptographic approaches. Encrypting the data can prevent third parties from intercepting the data. It can also be encrypted while in storage, or before sending to legitimate third parties. This privacy goal is a fundamentally different one from the goal of statistical privacy: protecting data from interception before processing, instead of protecting user privacy after processing. Ashgar et al. note that both these forms of privacy are complementary, not opposing [5]. Twenty of the fifty five papers we have looked at in this mapping study usecryptographic methods alongside differential privacy.

Though cryptographic and statistical methods can be used together, many approaches only use cryptography. Some of the most common cryptographic methods applied to smart meter privacy are homomorphic encryption (13, 14], symmetric DC-Nets (4, 15], and asymmetric DC-Nets [13]. All of these solutions require key sharing, which can beproblematic depending on the scale of the smart grid [5].

3 METHODS

For a systematic mapping study, our methods of finding valid sources must be carefully planned and rationalized. Our intention is not to discuss only the research we are familiar with but also to find a wider range of applied research.

In order to get a feeling for the current state and future direction of differential privacy applied to the smart grid, we need a set of research questions. The questions need to be broad enough that we can find answers in all of our sources. We have identified four research questions that can help us determine the state of the literature:

- (RQl) What are differential privacy-preserving methods/tools/strategies/techniques applied to smart meters, and what is their distribution in the literature?
- (RQ2) What subjects, or topics, have been addressed in the research for differential privacy in the smart grid, and what is their distribution in the literature?
- (RQ3) What datasets are used to study differential privacy applied to smart meters?
- (RQ4) What is thefuture direction in the research of applying differential privacy to smart meters?

In order to find valid sources that answer these questions, we used the search stringin Tab. 1. The phrases "differential privacy" and either "smart meter" or "smart grid" must be found within the abstract of the paper. Our intention is to filter out many of the papers that may mention a topic without being explicitly about that topic. The rest of the search stringis used to ensure each paper answers at least one of our questions. The search string does not guarantee good results, but it can help to filter out invalid sources.

Table 1: Search String

Search String
("Abstract":·differential privacy")
AND
("Abstract":"smart meter•· **OR** "Abstract ":"smar t grid"")
AND
(data• **OR** attack **OR** threat **OR** identification **OR**
security **OR** "user control " **OR** "third party" **OR** battery)

With our search string, the next important question is where to get our sources from. We have chosen IEEE Xplore [16], ACM Digital Library [17], and Elsevier ScienceDirect [18] as our main search engines. We chose these due to their importance in computer science literature. On top of these three search engines, we also collected sources from Differential Privacy Techniques for Cyber-Physical Systems: A Survey [1]. This is a recent survey of privacy-preserving solutions for the smart grid that hasa large section on differential privacy. Our intention is to gain a more broad selection of applicable literature that we may not find using our limited set of search engines by including these additional sources.

Our search string may help filter out some sources that would not help answer our questions, but we need a more explicit method of deciding which sources to keep and exclude from each search engine. For inclusion, we have two criteria: the article must relate to differential privacy, and the article must relate to the smart grid and smart meters. For exclusion, we have three criteria: the article is not written in English, the article is a repeated result from another search engine, or we cannot gain access to the article.

Our research questions needed ways in which we could fully evaluate each source fairly. We first read through the sources and created a collection of simpler questions that could help us characterize the methods used and the subjectscovered. The first question for methods is "Which noise method is used for differential privacy?". This categorical question helps us understand which noise methods are most common and possibly use more research. Our remaining questions for methods and subjects are all true or false questions. For methods, these are:"Was a variation on differential privacy used?", "Were cryptographic techniques implemented?" "Was a performance evaluation done?" "Did this method use a trusted aggregator?", "Did this method use an untrusted aggregator?" and "Was a battery needed for this method?". For subjects and topics covered for research question two, we asked the following true or false questions: "Was fault tolerance discussed?","Was the scalability of the method discussed?" "Was monetary cost a subject?", "Were attacks on the system covered?" "Was user control over their privacy a pointof discussion?". Research question three is a simple categorical question of which datasets were used if any. Research question four is more difficult. To aid us, we took quotes from each source expressing their intentions for future research. With these quotes we then categorized them into the following categories: "User Control", "Attacks", "Cost", "Scalability","Utility","Privacy", "Non-Smartgrid", "Prototype", "Experiment", "Performance", and "Other"."Other" covers the intended future research that was individual to that work and not repeated in other sources. For the other categories, these will bediscussed in Section 4.4.

4 RESULTS

Using our search string we found 40 results from IEEE Xplore [16], 3 results from ACM Digital Library [17], 7 results from Elsevier ScienceDirect [18], and 12 results from Differen tial Privacy Techniques for Cyber-PhysicalSystems: A Survey [l].Coming to a total of 64 results. After filtering by our exclusion criteria, we were left with 58articles. Filtering with our inclusion criteria resulted in 55 remaining articles.

Almostall of the sources we found are proposing new methods or building upon older methods to protect smart meter users' privacy. Though we did not intend to focus on this type of research solely, it fits well with our research questions and has offered an interesting insight into the literature's current state.

As seen in Fig. 1, the publication dates of our sources go back to 2011 and cover all years up to 2020. The majority of the sources are after 2015, giving us a most recent snapshot of the literature.

Table 2:Methods Covered in Sources.

Methods	Count	Percentage	Sources
Differential Privacy Variation	7	12.7%	(19, 20, 21, 22, 23, 24, 25)
Cryptographic Techniques	20	36.4%	(26, 27, 28, 20, 21, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 23, 39, 40, 4, 41)
Performance Evaluation	39	70.9%	(19, 26, 27, 28, 42, 43, 20, 44, 21, 29, 30, 45, 31, 32, 33, 35, 36, 46, 38, 39, 47) (48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 40, 58, 59, 4, 25, 60, 41, 61)
Trusted Aggregator	23	41.8%	[62, 26, 28, 42, 43, 44, 21, 30, 63, 45, 31, 34, 35, 36, 37, 38, 23, 49, 40, 59) (64, 60, 41]
Untrusted Aggregator	21	38.2%	[65, 66, 19, 67, 27, 20, 29, 32, 68, 33, 34, 36, 37, 39, 48, 51, 56, 59, 4, 24, 25)
Trust Not Specified	15	27.3%	(69, 70, 22, 71, 46, 47, 50, 72, 52, 53, 54, 55, 57, 58, 61)
Battery-based Load Hiding	7	12.7%	[67, 63, 71, 33, 58, 59, 24)

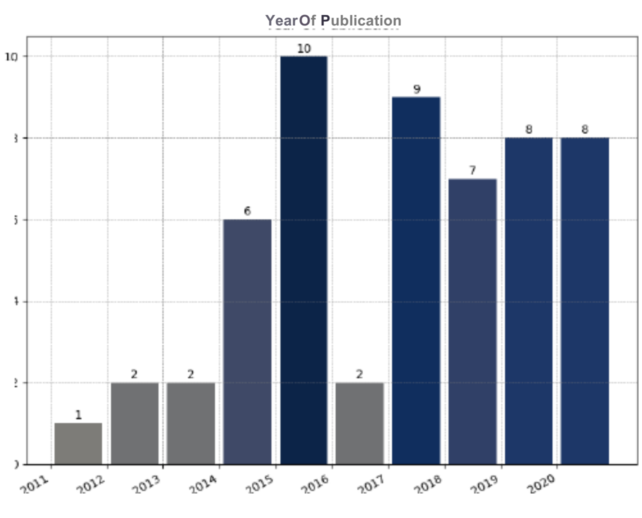

Figure 1: Year of publication.

4.1 Research Question 1

In Tab. 2, we can see some of the methods used by our sources and how common those methods are. Some interesting observations are the low number of differential privacyvariations and the number of battery-based load hiding (BLH) methods. Creating modifications to differential privacy is challenging, and there is still agreat deal of research to be done without making modifications. Battery-based methods of privacy preservation are a topic in need of further research. Many researchers are concerned about the cost of putting a large rechargeable battery in every smart meter, and they are also unsure whether differential privacy can truly be preserved. In terms of cost, Barbosa et al. stipulate that the batteries required for a single meter could cost $1000 and only last for two years [56), malting them a far from the low-cost solution. Almost 40% of our sources use cryptographic techniques in their methods. Depending on the privacy model being implemented, this can beinvaluable to prevent smart meter data from being read before it reaches an aggregator. By far, the most common aspect of our sources, implemented by over 70%, is some form of performance evaluation. Though any new research into these topics is valuable, being able to compare their performance will help to understand their utility in the real world. Fifteen of our sources did not clearly specify what model of trust they havedecided to use for their data aggregator. Of the 40 sources that did specify there is a nearly even split implementing trusted and untrusted aggregators. Several sources created methods that could be used with trusted or untrusted aggregators (36, 37, 59).

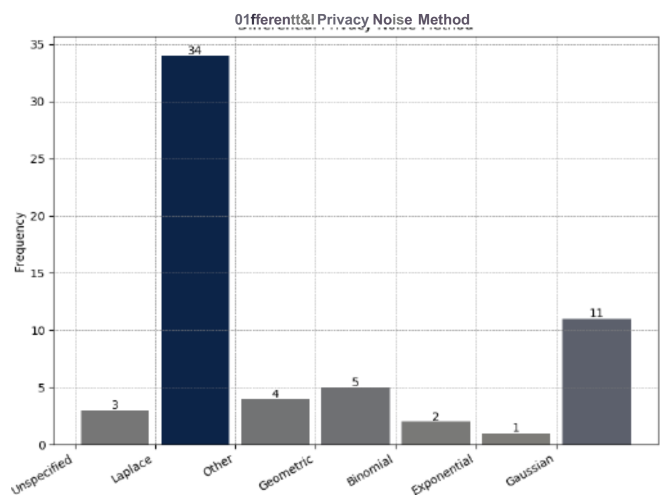

Figure 2: Noise method used for differential privacy.

The distribution of noise methods used for differential privacy in our sources can be seen in Fig. 2. In three of our sources, the noise method wasnot clearly stated.The four sourcesin the "Other" category all use noise methods of their own devising (41, 25, 45, 19]. The vast majority ofour sources draw from the Laplace distribution to add noise to their data. This is likely the most common because in Dwork et al.'s [2] paper introducing differential privacy, they used the Laplace distribution. Many sources likely use this distribution because of the precedent and not because it is the only distribution they could use for their method.

4.2 Research Question 2

Tab. 3 shows the subjects and topics covered in our sources. The subject of attacks is covered by over 60% of our sources. This is a topic that will need constant research to truly provide privacy for consumers. There are many different kinds of attacks that could damage the privacy of smart meter customers. The first of which is linkage attacks. Even if someone's data is anonymized, if an attacker finds another set of data which includes that person's data, the attacker may be able to perform a linkage attack to identify the person's anonymized data. Differential privacy makes linkage attacks infeasible because the data is not completely accurate [1, 2]. Differencing attacks are where an attacker uses multiple queries to a dataset to find out personal information about an individual [6]. Each individual question may not damage a person's privacy, but combined they can reveal personal information. The goalofdifferential privacy is to make the aggregated data from a dataset appear the same regardless of whether an individual is in the dataset, this makes differencing attacks almost impossible [1]. Non-intrusive load monitoring (NTIM) attacks use the electricity usage of a household over time to try and determine what appliances are being used, and from that learn the occupancy and schedules of the household. This can partly be addressed by encrypting the smart meter's data, however an honest-but-curious controller could still learn this information. Liao et al. propose a peak-time load balancing mechanism to prevent an adversary from learning any private information about individual households [20]. Though differential privacy prevents many of these attacks by decreasing the accuracy of the data, there are some concerns that differential privacy could introduce new issues. Allowing a utility company to view the complete data from each smart meter can helpwith detecting integrity attacks where an attacker has compromised a smart meter and is sending false information. Giraldo et al. have concerns that an attacker could take advantage of noisy differentially private data to doa stealthy integrity attack that hasbeen hidden by the noise in the data [66].To be widely adopted, all of the subjects in our table will need research- an interesting topic which relatively few of our sources covered is the topic of user control. Users could customize many aspects of their smart meter service, including their privacy, but this is a topic that is not very well understood. Users could have control of their privacy by selecting an ε value, but according to Hassan et al., despite differential privacy "being mathematically sound, still there is no rigorous method that explains choosing and generation of the optimalvalue of e.•[1].

4.3 Research Question 3

Datasets were not used by 16 of our sources, but the distribution of the remaining 39 can be seen in Fig. 3.

The majority of datasets used were in the "Other" category or were synthetic. The "Other" category consisted of datasets that were only used by that source and not by any others. The synthetic datasets were individual to each source as well and not repeated. The remaining datasets are real-world datasets that were used by multiple sources. The least used dataset was the MERL dataset created by Mitsubishi Electric Research Labs [73). This dataset is motion sensor data designed for machine learning purposes. It is not smart grid-relatedand so was only used by two sources. The second most commonly used dataset, used by three sources, is the UCI Knowledge Discovery in Databases Archive [74). This is a collectionof datasets covering a wide variety of applications. Once again, these datasets are designed primarily with machine learning applications in mind and are used by few sources. The next dataset is the SMART" dataset hosted by the University of Massachusetts

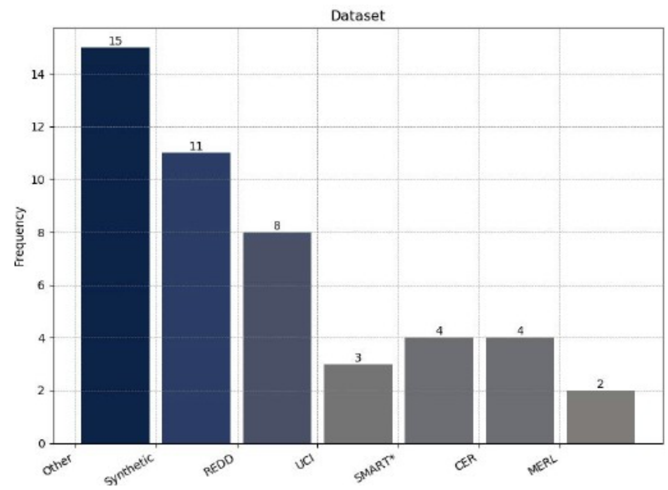

Figure 3: Dataset used for research.

[75]. This dataset has been updated as recently as 2019 and covers home energy consumption. As of 2019, this dataset contains data from over 400 homes, including energy meter data This dataset is far more applicable to smart grid applications, which likely explains why four of our sources used it. Also, four ofour sources are usedby the Commission for Energy Regulation (CER) datase t from the Irish SocialScience Data Archive [76]. This dataset includes smart meter data from over 5000 homes and businesses in Ireland. The data was collected between 2009 and 2010 but is still extremely useful for testing new smart meter privacy methods. The most commonly used real-world dataset in our sources was the REDD datase t from MIT [77).This dataset covers 10 homes, with 268 monitors, over 119 days. This data adds up to over a terabyte, which the authors' state is "the largestpublicly available data set for disaggregation with the true loads of each house identified" [77). This quantity of data being publicly available makes it a good choice for smart meter research. As smart meter data becomes more fine-grained, the datasets researchers used will have to adapt.

4.4 Research Question 4

In Fig. 4 we show the different goals stated for future research in our sources.

The "User Control" category is the goal to provide users with more control over their privacy."Attacks" covers all the researchers who intend to research different types of attacks and how to cope with them. "Cost" is fairly self-explanatory and covers research into the smart grid'svarious monetary costs. The "Utility" category is for researchers who want to improve data utility after adding noise for differential privacy. "Scalability"is the need for scalable systems. The "Privacy" category is for further researchinto improving the privacy preservation of users. Researchers who intend to prototype physical systems are in the "Prototype" category."Non-SmartGrid" covers all the researchers who intend to apply their methods to applications other than the smart grid. "Experiment" is the need for further experiments in the research. Finally, the "Performance"

Table 3: Subjects Covered in Sources.

Subjects	Count	Percentage	Sources
Fault Tolerance	14	25.5%	(26, 27, 29, 30, 31, 32, 33, 35, 39, 48, 49, 51, 56, 4]
Scalability	19	34.5%	(19, 69, 43, 20, 29, 30, 68, 33, 34, 35, 36, 37, 38, 39, 50, 56, 57, 25, 64)
Cost	21	38.2%	(62, 19, 67, 28, 30, 63, 45, 71, 68, 33, 35, 38, 39, 48, 49, 56, 57, 59, 4, 24, 41]
Attacks	34	61.8%	(66, 19, 26, 67, 27, 43, 20, 44, 70, 21, 30, 63, 45, 31, 32, 71, 33, 35, 46, 38, 39, 48, 49, 52, 54, 55] [56, 57, 40, 58, 4, 25, 60, 41]
User Control	9	16.4%	(62, 68, 35, 50, 51, 56, 57, 58, 41]

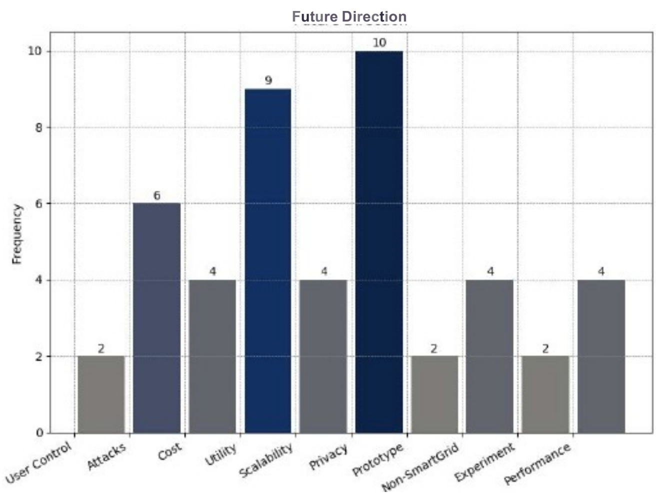

Figure 4: Author intentions for future research.

category covers the need to research and improve the performance of various methods.

By far, the most common categories for future research are the "Utility" and "Privacy" categories . This likely indicates that the future direction of the research will be focused on improving the utility, and privacy, of their methods.Most researchers who statethe need for research into one also state the need for research into the other. This reflects the difficult balance between fully protecting the users with useless data, or having completely accurate data with no privacy. The next most common is "Attacks." Research into attacks and how to cope with them will always need to be done. Without strategies for protecting user data from attacks, users can never truly be private.

4.5 Connections And Correlations

After finding the resultsfor our research questions, we were curious if there were any connections between the various methods used and subjects covered. To help try and answer this, we created a correlation matrix seen in Fig. 5. Most of the correlations are not of note. As expected, using a trusted aggregator or an untrusted aggregator have a negative correlation because usually, only one or the other is used. Though many of these correlations are difficult to interpret , there are a few that stand out. First is the correlation between battery usage and cost. When using a battery method, the topic of cost is a natural discussion point because of the serious concerns about the battery's cost.

In an effort to better understand how different methods and subjects are connected, we created Tab. 4. In this table, for each method, we find every source for which that method is used. For those sources, we then find the fraction which implements each subject. Next, we subtract the total fraction of each subject. This process can be seen in Equation 2 below. We then represent the final outcome as a percentage in the table. The final result shows how much more, or less, likely each subject is to be discussed depending on which methods are used. The most interesting value in the table can be seen on the battery row in the cost column. This cell shows how much more likely researchers were to discuss cost if they used a battery-based load hiding method. Researchers were 48% more likely to do so. This could also be seen in our correlation matrix but is much more pronounced here because this table is unidirectional.

$$\frac{RowAndColumnTrueCount}{RowTrueCount} \quad \frac{ColumnTrueCount}{Total} \qquad (2)$$

5 CONCLUSION

In thismapping study, we analyzed 55 papers on differential privacy applied to the smart grid in an attempt to provide a broad overview of the current literature on the subject and determine the future directions the research might take.In order to provide this overview we asked four research questions of each source. What methods were used, what subjects were covered, what datasets were used, and what is the future direction of the research? We identified common methods and subjects in the literature and provided an overview of their distribution within the sources.We also identified the most common datasets used by our sources. Determining the futuredirection of the research is a much more difficult task.Though we can' t determine the best direction the research can take, we were able to categorize some possible future research that each paper discussed. A large challenge with differential privacy is the balance between data utility and the privacy of users. These concerns are the most commonly suggested future research among our sources. Another aspect of preserving privacy is being able to protect users from attacks. Attacks and how to copewith them are among the most common subjects covered in our sources and one of the top concerns for future research.

ACKNOWLEDGE

This work was partially supported at the Secure Computing Laboratory at New Mexico Tech by the grant from the National Science Foundation (1757207).

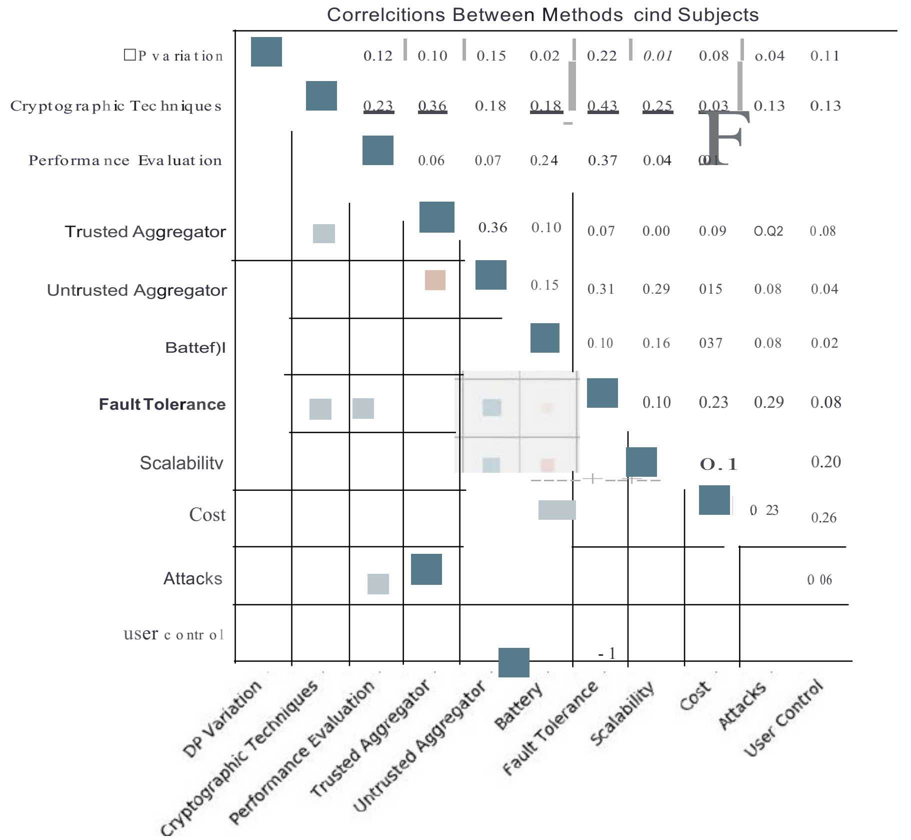

Figure 5: **Correlations between the different methods and subjects.**

Table 4: If **method is used, how much more likely is subject?**

		Fault Tolerance	Scalability	Cost	Attacks	User Control
DP Variation	->	-25%	+8%	-10%	-5%	-16%
Cryptographic Techniques	->	+25%	+15%	+2%	+8%	-6%
Performance Evaluation	->	+10%	+1%	0%	+13%	+2%
Trusted Aggregator	->	-4%	0%	+5%	-1%	-3%
Untrusted Aggregator	->	+17%	+18%	+9%	-5%	-2%
Battery	->	-11%	-20%	**+48%**	+10%	-2%

REFERENCES

[1] M. U. Hassan, M. H. Rehmani, and].Chen. Differential privacy techniques for cyber physicalsystems: a survey. *IEEE Communications Surveys Tutortals:1- 1,* 2019.1ssN: 2373 -745X .

[2] C. Dwork, F. Mcsherry, K. Nissim, and A. Smith. Calibrating noise to sensitivity in private data analysis. In S. Halevi and T. Rabin, editors. Redacted by D. Hutchison, T. Kanade, J. Kittler, J.M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, 0. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, and

G. Weiku m , *Theory of Cryptography.* Volume 3876, pages 265- 284. Springer BerlinHeidelberg, Berlin,Heidelberg, 2006.ISBN: 978-3-540-32731-8 978-3-540-32732-5. Series Title: Lecture Notes in Computer Science.

[3] U. Greveler, P. Glosekotter , B. Justus , and D. Loehr. Multimedia content identificationthrough smart meter power usage profiles:8, 2012.

[4] G. Acs and C. Castelluccia. I have a DREAM! (DiffeRentially privatE smArt metering). In T. Filler, T. Pevny, S. Craver, and A. Ker, editors, *Information Hiding.* Volume 6958, pages 118- 132. Springer Berlin Heidelberg Berlin, Heidelberg, 2011. ISBN978-3-642-24177-2 978-3-642-24178-9.

[5] M. R. Asghar, G. Dan, D.Miorandi, and I. Chlarntac. Smart meter data privacy: a survey. *IEEE Communications Surveys & Tutorials,* 19(4):2820- 2835, 2017. ISSN1553-877X.

[6] T. Wan g, Z. Zheng , M. H. Rehmani, S. Yao, and Z. Huo. Privacy preservation in big data from the communication perspective- a survey. *IEEE Communications Surveys Tutorials,* 21(1):753- 778, 2019. ISSN: 1553 -87 7X. Conference Name: IEEE Communications Surveys Tutorials.

[7] P. Brereton, B. A. Kitchenharn, D. Budgen, M. Turner, and M. Khalil. Lessons from applying the systematic literature review process within the software engineering domain. *Journal of Systems and Software,* 80(4):571- 583, Apr. 2007. ISSN: 01641212.

[8] I. D. Cooper. What is a "mappingstudy?". *Journal of the Medical Library Association: JMLA,* 104(1):76- 78, Jan. 2016. ISSN: 1536 -5050 .

[9] L. Sweeney. K-ANONYMITY: a MODEL FOR PROTECTING PRIVACY. *International Journal ofUncertainty,Fuzziness and Knowledge--Based Systems,* lo(5):557- 570, Oct. 2002. ISSN: 0218 -4885 , 1793 -6411.

[1 0] Y. Yang, Z. Zhang , G. Miklau, M. Winslett, and X. Xiao. Differential privacy in data publication and analysis. In *Proceedings of the 2012 international conference on Management of Data - SIGMOD12.*the 2012 international conference, page601, Scottsdale, Arizona, USA. ACM Press, 2012, ISBN: 978-1-4503-1247-9.

[11] G. Cormode , M. Procopiuc , D. Srivastava , and T. T. L. Tran . Differentially private publication of sparse data. In *In International Conference on Database Theory (!CDT,* 2012.

[12] F. McSherry and K. Talwar. Mechanism design via differential privacy:10.

[13] F. Borges de Oliveira. *On Prlvac-y-Preservlng Protocols for Smart Metering Systems.*Springer International Publishing, Cham, 2017. ISBN: 978-3-319-40717-3 978-3-319-40718-0.

[14]] Z. Erkin and G. Tsudik. Private computation of spatial and tempo- ral power consumption with smart meters. In F. Bao, P. Samarati, and J.Zhou, editors, *Applied Cryptography and Network Security,* pages 561-577, Berlin, Heidelberg. Springer Berlin Heidelberg, 2012. ISBN: 978-3-642-31284-7,

[15] K.Kursawe G. Danezis, and M.Kohlweiss. Privacy -friendly aggregation for the smart-grid. In S.Fischer-Hubner and N.Hopper, editors, *Privacy Enhancing Technologies,* pages 175- 191, Berlin, Heidelberg. Springer Berlin Heidelberg, 2011. ISBN: 978-3-642-22263-4.

[16] IEEE xplore. URL: https://ieeexploreieee.org/Xplore/home.jsp (visitedon 09/11/2020).

[17] ACM digital library. URL: https://dl.acm.org/(visited on 09/13/2020).

[18] ScienceDirect.com|science, health and medical journals , full text articles and books. URL: https://www.sciencedirect.com(visited on 09/13/2020).

[19] R. Pal, P. Hui, and V.Prasanna. Privacy engineering for the smart micro-grid. *IEEE Transactions on Knowledge and Data Engineering,* 31(5):965- 980, May 201,9 ISSN: 1558-2191.

[20]] X. Liao, P. Srinivasan , D. Formby, and R. A. Beyah. Di-PriDA: differ- entially private distributed load balancing control for the smart grid. *IEEE Transactions on Dependable and Secure Com puting,* 16(6):1026-1039, Nov. 2019. ISSN: 1941 -0018.

[21] X. Liao , D . Formby , C. Day , and R. A . Beyah. Towards secure metering data analysis via distributed differential privacy. In *2014 44th Annual IEEFIIFIP Internat ional Conference on Dependable* Systems *and Networks.* 2014 44thAnnual IEEE/IFIP International Conference on Dependable Systems and Networks, pages 780- 785, June 2014. ISSN: 2158-3927.

[22] F. Farokhi. Temporally discounted differential privacy for evolving datasets on an infinite horizon. In *2020 ACM/IEEE 11th InternationalConference onCyber-Phystcal Systems(JCC PS).* 2020ACM/IEEE 11th International Conference on Cyber-Physical Syste!IlS (ICCPS), pages 1- 8, Apr. 2020 ISSN 2642-9500

[23] G. Barthe, G. Danezis, B. Gregoire, C. Kunz, and S. Zanella-Beguelin. Verified computational differential privacy with applications to smart metering. In *2013IEEE 26th Computer Security Foundations Symposium.* 2013IEEE 26th Computer Security Foundations Symposium, pages 287- 301, June 2013. ISSN: 2377-5459.

[24] Z. Zhang , Z. Qin , L. Zhu , W. Jiang , C. Xu, and bibinitperiod K Ren. Toward practical differential privacy in smart grid with capacity-limited rechargeable batteries. *arXiv:1507.03000 [cs],*July 22, 2015.

[25] M. Sav i, C. Rottondi , and G. Verticale. Evaluation of the precision-privacy tradeoff of data perturbation for smart metering. *IEEE Transactions on Smart Grid,*6(5):2409- 2416, Sept. 2015. ISSN: 1949 -3061 .

[26] H. Bao and R. Lu. DDPFT: secure data aggregation scheme with differential privacy and fault tolerance.In *2015 IEEE International Conference on Communications(ICC).* 2015 IEEE International Conference on Communications (ICC), pages 7240- 7245, June 2015 ISSN1938-1883.

[27] J. Ni, K. Zhang , K. Alharbi,X. Lin, N.Zhang, and X.S.Shen.Differentially private smart metering with fault tolerance and range-based filtering. *IEEE Transactions on Smart Grtd,*8(5):2483- 2493, Sept. 2017. ISSN: 1949 -3061.

[28] J.Wang, X. Zhang, H. Zhang, H. Lin, H. Tode, M. Pan,and Z.Han. Data-driven optinlization for utility providers with differential privacy of users' energy profile. In *2018 IEEE Global Commun ications Conference (GLOBECOM).* 2018 IEEE Global Communications Conference (GLOBECOM, pages 1- 6, Dec. 2018. ISSN: 2576-6813.

[29] L. Lyu, Y. W. Law , J.Jin , and M. Palaniswami. Privacy-preserving aggregation ofsmart metering via transformation and encryption. In *2017IEEETrustcom/BlgDataSFIICESS.* 2017IEEETrustco m/BigDataSE/ICESS pages 472- 479, Aug. 2017. ISSN: 2324-9013.

[30] H. Bao and R. Lu. A new differentially private data aggregation with fault tolerance for smart grid communications. *IEEE Internet of Thtngs Journa* 2(3):248- 258, June 2015. 1ssN: 2327-4662.

[31] M Lu, Z. Shi, R.Lu, R.Sun, and X.S. Shen. PPPA: a practical privacy-preserving aggregation scheme for smart grid communications.In *2013IEEEICTC International Conference on Communicationstn China (!CCC).* 2013 IEEE/CIC International Conference on Communications in China (ICCC), pages 692- 697, Aug. 2013. ISSN: 2377-8644.

[32] Z. Shi , R.Sun , R. Lu, L. Chen,]. Chen, andX.Sherman Shen. Diverse grouping-basedaggregation protocol with error detection for smart grid communications. *IEEE Transacttons on Smart Grid,* 6(6):2856-2868, Nov 2015. ISSN: 1949 -3061.

[33] J.Won, C. Y. T. Ma, D. K. Y. Yau, and N. S. V. Rao. Privacy-assured aggregation protocol for smart metering: a proactive fault-toleran t approacli. *IEEE/ACM Transactions onNetworking,* 24(3):1661- 1674, June 2016, ISSN: 1558 -2566.

[34] J. Le Ny and G.J. Pappas. Differentially private filtering. In *2012 IEEE 51st IEEE Conference on Decision and Control (CDC).* 2012 IEEE 51st

IEEE Conference on Decision and Control (CDC), pages 3398- 3403, Dec. 2012. ISSN: 0743-1546.

[35] 0. Samuel, N. Javaid, M. Awais, Z. Ahmed, M. Imran, and M. Guizani. A blockchain model for fair data sharing in deregulated smart grids. In *2019 IEEE Global Communications Conference (GLOBECOM)*. 2019 IEEE Global Communications Conference (GLOBECOM), pages 1- 7, Dec. 2019. ISSN: 2576-6813.

[36] J. Le Ny and G. J. Pappas. Differentially private filtering. *IEEE Transactions on Automatic Contra* 59(2):341- 354, Feb. 2014. ISSN: 1558-2523.

[37] J. Le Ny and G.J. Pappas. Differentially private kalman filtering. In *201250th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. 2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton), pages 1618-1625, Oct. 2012.

[38] A. Paverd, A. Martin, and I. Brown. Privacy-enhanced bi-directional communication in the smart grid using trusted computing. In *2014 IEEE International Conference on Smart Grid Communications (SmarlGridComm)*. 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm}, pages 872- 877, Nov. 2014.

[39] L. Lyu, K. Nandakumar, B. Rubinstein, J. Jin, J. Bedo, and M. Palaniswami. PPFA: privacy preserving fog-enabled aggregation in smart grid *IEEE Transactions on Industrial Informatics,* 14(8):3733- 3744, Aug. 2018. ISSN: 1941-0050.

[40] H. *Ye, J.* Liu, W. Wang, P. Li, T. Li, and]. Li. Secure and efficient outsourcing differential privacy data release scheme in cyber- physical system. *Future Generation Computer Systems,* 108:1314- 1323, July 2020. ISSN: 0167739X.

[41] J. Liu, C. Zhang, and Y. Fang. EPIC: a differential privacy framework to defend smart homes against internet traffic analysis. *IEEE* Internet *of Things Journa* 5(2):1206- 1217, Apr. 2018. 1ssN: 2327-4662.

[42] Z. Lv, L. Wang, Z. Guan,]. Wu, X. Du, H. Zhao, and M. Guizani. An optimizing and differentially private clustering algorithm for mixed data in SDN-based smart grid *IEEE Access*, 7:45773 - 45782, 2019. ISSN: 2169-3536.

[43] W. Chen, A. Zhou, P. Zhou, L. Gao, S. Ji, and D. Wu. A privacy-preserving online learning approach for incentive-based demand response in smart grid. *IEEE Systems Journa* 13(4):4208- 4218, Dec. 2019. ISSN: 1937-9234.

[44] D. Li, Q. Yang, W. Yu, D. An, Y. Zhang, and W. Zhao. Towards differential privacy-based online double auction for smart grid. *IEEE Transactions on Information Forensics and Security,* 15:971- 986, 2020. ISSN 1556-6021.

[45] H. Cao, S. Liu, L. Wu, and Z. Guan. SCRAPPOR: an efficient privacy-preserving algorithm baseon sparse coding for information-centric IoT. *IEEE Access*, 6:63143 - 63154, 2018. ISSN:2169-3536.

[46] E. Ustundag Soykan, Z. Bilgin, M.A. Ersoy and E. Tomur. Differentially private deeplearning for load forecasting on smart grid. In *2019 IEEE Globecom Workshops (GC Wkshps)*. 2019 IEEE Globecom Workshops (GCWkshps), pages 1- 6, Dec. 2019.

[47] J. Le Ny and M. Mohammady. Differentially private MIMO filtering for event streams. *IEEE Transactions on Automatic Contra* 63(1):145-157, Jan. 2018. ISSN: 1558-2523.

[48] A. Gohar, F. Shafik, F. Duerr, K. Rothermel, and A. E!Mougy. Privacy-preservation mechanisms for smart energy metering devices based on differential privacy. In *2019 IEEE Wireless Communications and Networking Conference Workshop (WCNCW)*. 2019 IEEE Wireless Communications and Networking Conference Workshop (WCNCW}, pages 1- 6, Apr. 2019.

[49] M. U. Hassan, M. H. Rehmani, and J. Chen. Differentially private dynamic pricing for efficient demand response in smart grid. In *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*. ICC 2020 - 2020 IEEE In ternational Conference on Communications (ICC), pages 1- 6, June 2020. ISSN: 1938-1883.

[50] A. Karapetyan, S. K. Azman, and Z. Aung. Assessing the privacy cost in centralized event-based demand response for microgrids. In *2017 IEEE Trustcom!BlgDataSFIICESS.* 2017 IEEE Trustcom/BigDataSE/ICESS, pages 494- 501, Aug. 2017. ISSN: 2324-9013.

[51] H. Sandberg, G. Dan, and R. Thobaben. Differentially private state estimation in distribution networks with smart meters. In *2015 54th IEEE Conference on Decision and Control (CDC)*. 2015 54th IEEE Conference on Decision and Control (CDC), pages 4492- 4498, Dec. 2015.

[52] J. Le Ny and M. Mohammady. Differentially private MIMO filtering for event streams and spatio-temporal monitoring. In *53rd IEEE Conference on Decision and Control* 53rd IEEE Conference on Decision and Control, pages 2148- 2153, Dec. 2014. ISSN: 0191-2216.

[53] H. Wang and C. Wu. Understanding differential privacy in non-intrusive load monitoring. In *Proceedings of the Eleventh ACM International Conference on Future Energy Systems.* e-Energy '20: The Eleventh ACM International Conference on Future Energy Systems, pages 401- 403, Virtual Event Australia. ACM, June 12, 2020. ISBN: 978-1-4503-8009-6.

[54] L. Fan and H. Jin. A practical framework for privacy-preserving data analytics. In *Proceedings of the 24th International Conference on World Wide Web- WWW '15.* the 24th International Conference, pages 311-321, Florence, Italy. ACM Press, 2015. ISBN: 978-1-4503-3469-3.

[55] M. Ul Hassan, M. H. Rehmani, R. Kotagiri,]. Zhang, and]. Chen Differential privacy for renewable energy resources based smart metering. *Journal of Parallel and Distributed Com puting,* 131:69- 80, Sept. 2019. ISSN: 07437315.

[56] P. Barbosa, A. Brito, and H. Almeida. A technique to provide differential privacy for appliance usage in smart metering. *Information Sciences,* 370-371:355- 367, Nov. 2016. 1ssN: 00200255.

[57] T. Asikis and E. Pournaras. Optimization of privacy-utility trade-offs under informational self-determination. *Future Generation Computer Systems,* 109:488- 499, Aug. 2020. ISSN: 0167739X.

[58] F. Laforet, E. Buchmann, and K. Bohm. Individual privacy constraints on time-series data. *Information Systems,* 54:74- 91, Dec. 2015. ISSN: 03064379.

[59] M. Zellner, T. T. De Rubira, G. Hug, and M. Zeilinger. Distributed differentially private model predictive control for energy storage. *lFAC-PapersOnLlne* 50(1):12464- 12470, July 2017. ISSN 24058963.

[60] *J.* Xiong,]. Ren, L. Chen, Z. Yao, M. Lin, D. Wu, and B. Niu. Enhancing privacy and availability for data clustering in intelligent electrical service of IoT. *IEEE Internet of Things Journa* 6(2):1530- 1540, Apr. 2019. ISSN: 2327-4662.

[61] H. Cao, S. Liu, L. Wu, Z. Guan, and X. Du. Achieving differential privacy against non-intrusive load monitoring in smart grid: a fog computing approach. *Concurrency Computat Prad F.xper,* 31(22), Nov. 25, 2019. ISSN: 1532-0626, 1532-0634.

[62] A. Yassine, A. A. Nazari Shirehjini, and S. Shirmohammadi. Smart meters big data: game theoretic model for fair datasharing in deregulated smart grids. *IEEE Access*, 3:2743 - 2754, 2015. ISSN: 2169-3536.

[63] Z. Zhang, W. Cao, Z. Qin, L. Zhu, Z. Yu, and K. Ren. When privacy meets economics: enabling differentially-private battery-supported meter reporting in smart grid. In *2017 IEEFIACM 25th International Symposium on Quality of* Service *(IWQoS)*. 2017 IEEE/ACM 25th International Symposium on Quality of Service (IWQoS), pages 1- 9, June 2017.

[64] G. Eibl and D. Engel. Differential privacy for realsmart metering data. *Comput Set Res* Dev, 32(1):173- 182, Mar. 2017. ISSN 1865-2034, 1865-2042.

[65] L. Xiong. Harnessing personal data from internet of things: privacy enhancing dynamic information monitoring. In *2015 International Conference on Collaboration Technologies and Systems(CTS)*. 2015 International Conference on Collaboration Technologies and Systems (CTS), pages 37- 37, June 2015.

[66] J.Giraldo , A. A. Cardenas, and M. Kantarcioglu. Security vs. privacy: how integrity attacks can be masked by the noise of differential privacy. In *2017 American Control Conference (ACC).* 2017 American Control Conference (ACC), pages 1679-1684, May 2017. ISSN: 2378-5861.

[67] J.Zh ao, T.Jung, Y.Wang , and X. Li.Achieving differential privacy of data disclosure in the smart grid. In *IEEEINFOCOM 2014 - IEEE Conference on Computer Communications*.IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, pages 504-512, Apr. 2014. ISSN: 0743-166X.

[68] Z. Yang, P. Cheng, and]. Chen. Differential-privacy preserving optimal power flow in smart grid. *Transmission Distribution IET Generation,* 11(15):3853 - 3861, 2017. ISSN: 1751-8695.

[69] M. Saravanan,A. M. Thoufeeq, S.Akshaya, and V.Jayasre Manchari. Exploring new privacy approaches in a scalable classification framework.In *2014 International Conference on Data Science and Advanced Analytics (DSAA).* 2014 International Conference on Data Science and Advanced Analytics (DSAA,) pages 209- 215,Oct. 2014.

[70] L. Ou, Z. Qin,S. Liao, T. Li,and D. Zhang. Singular spectrum analysis for local differen tial priva cy of classifications in the smart grid. *IEEE Internet of Things Journal,* 7(6):5246- 5255, June 2020. ISSN: 2327-4662.

[71] Z. Zhang, Z. Qin, L. Zhu, J. Weng, and K. Ren. Cost-friendly differential privacy for smart meters: exploiting the dual roles of the noise. *IEEE Transactions onSmart Grid,* 8(2):619- 626, Mar. 2017. ISSN: 1949-3061.

[72] Y. Kawano and M. Cao. Design of privacy-preserving dynamic controllers. *IEEE Transactions on Automatic Contro* 65(9):386-33878, Sept. 2020. ISSN: 1558-2523.

[73] C. R. Wren, Y. A. Ivanov, D. Leigh, and J. Westhues. The MERL motion detector dataset. In *Proceedings of the* 2007 *workshop on Massive datasets - MD '07*.the 2007 workshop , pages 10- 14, Nagoya, Japan . ACM Press, 2007. ISBN: 978-1-59593-871-8.

[74] UCI KDD archive. URL: https://kdd.ics.uci.edu (visited on 09/25/2020.)

[75] Smart - UMass trace repository. URL: http:// traces.es.umass.edu/ index.php/Smart/Smart (visited on 09/ 25/2020).

[76] I. S. S. D. Archive. Home, irish social science data archive. Irish Social Science Data Archive. URL: https:/ / www.ucd.ie/ issda/ data/commissionforenergyregulationcer / (visited on 09/25/2020). Publisher: IrishSocial Science Data Archive.

[77] J.Z. Kolter and M. J.Johnson. REDD: a public data set for energy disaggregation research:6.