Differential Privacy Techniques for Cyber Physical Systems: A Survey

Muneeb Ul Hassan, Mubashir Husain Rehmani, *Senior Member, IEEE*, and Jinjun Chen

***Abstract*—Modern cyber physical systems (CPSs) has widely being used in our daily lives because of development of information and communication technologies (ICT). With the provision of CPSs, the security and privacy threats associated to these systems are also increasing. Passive attacks are being used by intruders to get access to private information of CPSs. In order to make CPSs data more secure, certain privacy preservation strategies such as encryption, and k-anonymity have been presented in the past. However, with the advances in CPSs architecture, these techniques also need certain modifications. Meanwhile, differential privacy emerged as an efficient technique to protect CPSs data privacy. In this paper, we present a comprehensive survey of differential privacy techniques for CPSs. In particular, we survey the application and implementation of differential privacy in four major applications of CPSs named as energy systems, transportation systems, healthcare and medical systems, and industrial Internet of things (IIoT). Furthermore, we present open issues, challenges, and future research direction for differential privacy techniques for CPSs. This survey can serve as basis for the development of modern differential privacy techniques to address various problems and data privacy scenarios of CPSs.**

***Index Terms*—Differential privacy, cyber physical systems (CPSs), smart grid (SG), health care systems, transportation systems, industrial Internet of Things (IIoT), privacy preservation.**

I. Introduction

PREVIOUSLY, embedded computers were used to control and monitor the physical processes via feedback loop control [1]. With the passage of time, integration of computation technologies with traditional embedded physical systems lead the foundation of new type of systems named as cyber physical systems (CPSs) [2]. The advances in CPSs have gathered considerable attention over the last ten years [3]. The major reason behind this stupendous attention is the dual nature of CPSs, via which they integrate the dynamic properties of embedded computers with those of information and communication technologies (ICT) [4]. Similarly, the merger of ICT and embedded systems spread to a number of physical domains of dynamic nature, including energy, transportation, healthcare, medical, industrial, and manufacturing systems [5]. Majority of CPSs are deployed in life support devices, critical infrastructures (CI), or are very vital to our everyday lives. Therefore, CPSs users expect them to be emancipated from every type of vulnerabilities. One of the critical issue in deployment of CPSs in real world is their privacy, as any type of information leakage can result in very serious consequences [6]. Particularly, the complex architecture of CPSs make it difficult to assess the privacy threats, and new privacy issues arises. It is also strenuous to trace, identify, examine, and eliminate privacy attacks that may target multiple components of CPSs such as real-time sensors, wearable health devices, industrial control systems, etc. [6]. Similarly, CPSs basically rely on diverse number of sensors and data centres containing very huge amount of personal and private data. For example, wearable devices of patients are continuously reporting their real-time data to consulting doctors [7]. However, if one does not use a strong privacy preservation scheme during this communication, then any adversary can try to hack this personal information and can use it for illegal benefits such as blackmailing, false information injection, etc. [8]. Therefore, there is a strong possibility of compromising the personal privacy of CPS users in the absence of proper privacy protection strategy [9].

Attacks on CPSs can be classified into passive (privacy oriented) or active (security oriented). The basic objective of passive attacks is to access a certain amount of private data being shared in the network, or to infer about any critical information from public dataset [5]. Many researchers proposed cryptographic techniques to preserve data privacy [13]–[15]. However, these cryptographic techniques are computationally expensive, because users' needs to maintain the set of encryption keys. Moreover, it becomes more difficult to ensure privacy in a situation when public sharing of data is required. Similarly, anonymization techniques such as k-anonymity [16] are also proposed by researchers to address privacy issues. However, these anonymization strategies do not guarantee complete level of protection from adversaries because the chances of re-identification increase if size of attributes in dataset increases [11]. An adversary trying to infer the data can match the non-anonymized data with anonymized data, which in turn will lead to privacy breach. Another important privacy scheme named as differential privacy was introduced in 2006 to overcome these privacy issues. Currently, the use of differential privacy is emerging as a future

Manuscript received September 8, 2018; revised April 19, 2019 and July 15, 2019; accepted September 21, 2019. Date of publication October 1, 2019; date of current version March 11, 2020. This work was supported in part by the Australian Research Council (ARC) under Project DP190101893, Project DP170100136, Project LP140100816, and Project LP180100758. *(Corresponding author: Mubashir Husain Rehmani.)*

M. Ul Hassan and J. Chen are with the Faculty of Science, Engineering and Technology, Swinburne University of Technology, Hawthorn, VIC 3122, Australia (e-mail: muneebmh1@gmail.com; jinjun.chen@gmail.com).

M. H. Rehmani is with the Department of Computer Science, Cork Institute of Technology, Cork T12 P928, Ireland (e-mail: mshrehmani@gmail.com).

Digital Object Identifier 10.1109/COMST.2019.2944748

TABLE I
COMPARISON OF PRIVACY PRESERVATION STRATEGIES ON THE BASIS OF METHOD, MERITS, WEAKNESSES, AND COMPUTATIONAL OVERHEAD

Privacy Name	Method to Protect Privacy	Merits (Advantages)	Weaknesses and Challenges	Computational Overhead
Encryption	Public and private keys are assigned to transmitted data that are used to decrypt data at receiving end	• Original data is not lost • Data becomes inaccessible to unauthorized users	• Computationally complex • Reduces system speed • Not Suitable for public databases	Very high [10]
Anonymization	Personal identifiable information (e.g. name, date of birth, passport number etc.) is removed before query evaluation	• Limits disclosure risks • Works with high dimensional data	• Original data is lost • 100% privacy is not guaranteed • Chances of re-identification exists in large data	High [11]
Differential Privacy (focus of this survey article)	Random noise is added using various mathematical algorithms, e.g. Laplace, Gaussian, etc.	• Low complexity • Original data is not lost • Privacy can be controlled according to need by varying privacy parameter	• Dimensionality curse • Reduction in data utility • Selecting desirable trade-off between privacy and accuracy is tough	Low [12]

of privacy [17]. Differential privacy protects statistical or real-time data by adding desirable amount of noise along with maintaining a healthy trade-off between privacy and accuracy. In differential privacy, user can control the level of privacy or indistinguishability, which in turn will lead to protection of maximum possible privacy for any particular individual in dataset. For example, the value of privacy parameter can be used to control trade-off between utility and privacy, it can either be 100% utility or 100% privacy depending upon the requirement of system. A detailed overview of these privacy preserving strategies along with their merits and demerits is presented in Table I.

Differential privacy has the capability to preserve large proportion of data from both, databases and real-time data [20]. Data perturbation is carried out in majority of differential privacy techniques. In data perturbation, amount of noise is calculated using differential privacy algorithms and this noise is further added to query data to make it secure and indistinguishable for observer. This perturbation has direct effect with the accuracy of data being reported. On the other hand, the more perturbed data ensures that privacy is strongly protected. Therefore, while using differential privacy, one needs to maintain an advantageous trade-off among accuracy and privacy. Due to this privacy and accuracy trade-off, utilizing differential privacy in CPSs is a challenging task, because various CPSs applications require accurate reporting of data, for example health care and medical systems. To efficiently use differential privacy techniques in CPSs, various techniques in energy systems, transportation systems, healthcare, machine learning, and industrial systems have been proposed in literature. The actual goal is to improve privacy level along with minimizing the trade-off with accuracy.

A. Motivation: Differential Privacy for Cyber Physical Systems

To date, various privacy preservation strategies have been proposed by researchers to overcome certain privacy threats. *Encryption* is one of the traditional privacy preserving technique used by majority of systems to protect the data from adversaries and unauthorized users [18], because it provides feature of data inaccessibility to unauthorized users. However, in modern CPSs, encryption can barely be applied, because of the sensors' limitation of computing capacity [10]. For example in public key cryptography also called as asymmetric cryptography, the generation, and distribution of public and private keys is a computationally complex task and cannot easily be carried out with small devices having limited resources [21]. Furthermore, various attacks, such as brute-force attack may be used by any vulnerability against the encrypted CPS data [22]. Similarly, in a network of multiple sensors, encryption strategies require the interconnection of every node for generation and transmission of private keys in the network. Therefore, if one node gets failed in a network of n number of nodes, then the decryption and collection of data from CPSs nodes becomes nearly impossible, because of missing keys in the network [10].

Another privacy preserving strategy used by researchers is *data anonymization* [23]. However, recent literature work indicates that privacy of anonymized data can easily be compromised. For example, De Montjoye *et al.* [24] collected and simply anonymized mobility data for 15 minutes of 1.5 million people. Even from this anonymized data, they identified a person with around 95% accuracy via four temporal points only. Furthermore, the weaknesses of simply anonymized data was confirmed further by a test carried out on credit card transactions [25], and researchers re-identified the individuals with 90% accuracy by using only four temporal points.

Existing privacy preservation schemes being used in CPSs pose serious challenges to users' privacy. Therefore, a perturbation technique that protects the private data with appropriate mechanism was the need. In 2006, Dwork proposed the concept of differential privacy as an efficient privacy preserving approach to obstruct adversaries from recovering data [26]. Similarly, a statistical differential privacy interpretation was developed by Wasserman in 2010 [27]. Continuing this research line, researchers proposed *membership privacy* [28] and *differential identifiability* [29] to address certain problems in differential privacy framework. In context of CPSs,

TABLE II
UTILITY-PRIVACY COMPARISON BETWEEN DIFFERENTIAL PRIVACY, ANONYMIZATION, AND ENCRYPTION

Privacy Technique	Major Constraint	Description
Anonymization	Limited privacy	Anonymization does not guarantee complete privacy as it is claimed that anonymized data is either protected or either usable, because chances of re-identification always exists in anonymization [11].
Encryption	Third-party privacy	Protects data from third-party intruders along with providing complete privacy, but privacy is not protected from observing analyst [18].
Differential Privacy	Utility-privacy trade-off	Deals with utility-privacy trade-off that can be controlled by data provider according to privacy requirement [19].

Zhu *et al.* [3] suggested the usage of differential privacy in advanced CPSs. Contrary to encryption, differential privacy provides a less complex, privacy preservation mechanism. The actual reason is that computational cost of differential privacy only comprises of noise computation using a pre-defined probability distribution. However, the nodes using encryption has to carry out certain tasks of generation, and distribution of keys along with encrypting and decrypting data. Therefore, the computational complexity of differential privacy is fairly low as compared to encryption. Furthermore, in differential privacy, CPSs users can control the level of privacy according to the need by varying noise addition parameter "ε". Unlike anonymization, original data of CPSs is not lost during query evaluation using differential privacy because data is protected using perturbation methodology. Various noise addition mechanisms of differential privacy provide strong privacy protection against numeric and non-numeric queries [30]. By keeping in view its tremendous benefits, mathematical and theoretical basis, and easy realization, differential privacy has been applied extensively in CPSs to preserve individual privacy [31].

B. Contributions of This Survey Article

While few previous survey articles have highlighted some specific aspects of differential privacy techniques in certain CPSs domains, to the best of our knowledge there is no comprehensive survey over the implementation and applications of differential privacy techniques in CPSs. In this paper, we survey state-of-the-art work on differential privacy techniques in CPSs scenarios. In summary, following contributions are made in the article:

- We review previous survey articles on differential privacy and highlight important features of them.
- We focus more on the presenting practical aspects of differential privacy in CPSs.
- We provide a thorough survey of differential privacy and its implementation in CPSs.
- We provide an extensive survey of applications of differential privacy in CPSs.
- We survey the work done over implementation of differential privacy in energy systems, transportation system, healthcare, and industrial IoT systems.
- We outline certain open issues, challenges, and possible future research direction for differential privacy based CPSs.

TABLE III
LIST OF ACRONYMS AND CORRESPONDING DEFINITIONS

Acronyms	Definitions
AMI	Advanced Metering Infrastructure
BLH	Battery Load Hiding
CI	Critical Infrastructure
CIDS	Collaborative Intrusion Detection Systems
CPS	Cyber Physical System
D2D	Device-to-Device
DSM	Demand Side Management
DSRC	Dedicated Short-Range Communication
EM	Exponential Mechanism
EV	Electric Vehicle
FHMM	Factorial Hidden Markov Model
HA	Hybrid Automation
HetVNET	Heterogeneous Vehicular Networks
ICS	Industrial Control Systems
ICT	Information and Communication Technologies
IIoT	Industrial Internet of Things
IoT	Internet of Things
IoV	Internet of Vehicle
ITS	Intelligent Transportation System
LM	Laplace Mechanism
LPWA	Low Power Wide Area
LTE	Long-Term Evolution
MAB	Multi-Armed Bandit
MANET	Mobile Ad-Hoc Networks
NCS	Networked Control System
NILM	Non-Intrusive Load Monitoring
PII	Personally Identifiable Information
PKC	Public Key Cryptography
RER	Renewable Energy Resource
SG	Smart Grid
UNB	Ultra Narrow Band
V2D	Vehicle-to-Device
V2V	Vehicle-to-Vehicle

C. Review of Related Survey Articles

Our present survey article on differential privacy in CPSs is distinct from all previous studies, as we extensively cover the area of differential privacy implementation in CPSs. There is a comprehensive literature of previous survey articles that has focus on differential privacy, and few of them focused over differential privacy in big data analysis. However, to the best of our knowledge, there is no prior detailed survey article that thoroughly addresses differential privacy strategies

TABLE IV
SUMMARY COMPARISON OF PREVIOUS SURVEY ARTICLES OF DIFFERENTIAL PRIVACY (DP) WITH THEIR APPLICATION SCENARIO, YEAR, MAJOR CONTRIBUTIONS, AND CONSIDERED FACTORS. ✔ INDICATES THAT THE TOPIC IS COVERED, ✗ INDICATES THAT THE TOPIC IS NOT COVERED, AND ✻ INDICATES THAT THE TOPIC IS PARTIALLY COVERED

Application Scenario	Ref No.	Year	Major Contribution	Considered Factors	Discussed CPSs
Mobile Sensing System	[19]	2017	A comprehensive survey on improvement of data utility	• Distribution • Optimization • Calibration • Transformation • Decomposition	✻
Social Networks	[32]	2011	A comprehensive survey over privacy techniques in social networks including differential privacy	• Privacy breaches • Anonymization in social networks	✻
	[33]	2014	A comprehensive survey of differential privacy in social networks is carried out and after that two differential privacy based *outlink privacy* and *partition privacy* standards are proposed	• Triangle count and distribution • Graph modelling	✻
Finite Precision Semantics	[34]	2016	A discussion about method of quantifying of data privacy by finite precision	• Computational error	✗
Sensitive Data Mining	[35]	2014	An investigation is done over learning base data release mechanism	• Loss function	✗
Mobile Recommender System	[36]	2016	An overview of privacy preserving algorithms including differential privacy is given by focusing on collection, generation, and storage in mobile recommender systems	• Privacy risks	✻
Statistical Databases	[37]	2008	A presentation of two basic techniques of differential privacy	• Learning theory • Statistical data inference	✗
	[38]	2012	An investigation and approach on individual experience cost as a function of privacy loss is proposed	• Privacy and accuracy trade-off	✗
	[39]	2017	An overview about differential privacy and its relevance with other data science topics	• Computational complexity • Cryptography • Theoretical computer science	✗
Communication in Big Data	[11]	2018	A comprehensive comparison of differential privacy with other privacy preservation approaches is carried out in scenario of big data from the perspective of communication	• Privacy attacks • Privacy risks in big data	✻
Miscellaneous	[40]	2016	Overview of differential privacy methods to chose accurate epsilon value for a better trade-off	• Epsilon value	✗
	[41]	2016	A detailed study on data clustering and privacy framework	• Cryptography • Data mining • Biometric privacy • Game theory	✗
	[42]	2017	Analysis over data publishing and data analysis using differential privacy	• Data release mechanism • Efficiency • Accuracy	✗
	[43]	2018	A comparison of differential privacy with other big data privacy schemes	• Execution time • Complexity • Data utility	✗
	[44]	2018	A survey on fundamental ideas of privacy budget and sensitivity in differential privacy	• Noise calculation mechanism • Fundamental architectures for differential privacy	✗
	[45]	2019	A detailed survey over integration of modern differential privacy algorithms with deep learning models	• Privacy attacks • Private data extraction • Deep learning layers	✗
	[46]	2019	In-depth analysis of more than 50 variants of differential privacy from perspective of methodology	• Privacy loss • Differential privacy definitions • Computational effect of variants	✗
Cyber Physical Systems	This Work	2018	An in-depth survey of differential privacy techniques in applications of cyber physical systems (energy, transportation, healthcare, medical, and industrial IoT systems)	• Privacy preservation • CPSs applications • Privacy attacks • Design mechanism • Technical challenges	✔

in CPSs. We categorize the previous survey literature work over differential privacy into seven major categories named as statistical databases, social networks, mobile sensing system, finite precision semantics, sensitive data mining, machine recommender systems, miscellaneous. The application scenario, major contribution and considered factors about these survey articles is presented in Table IV.

An extensive literature on differential privacy in context of salient privacy related features of differential privacy from context of data analytic, big data, and privacy budget is presented in [40]–[44]. The term big data refers to transmission, collection, storage, or usage of large amount of data collected from any source [47]. Yao *et al.* [40] discussed about different methods of calculation of accurate (ε) value to minimize privacy and accuracy trade-off. A brief analysis over data release mechanism, efficiency, and accuracy of differential privacy is presented in [42]. In [41], a detailed study on data clustering and privacy framework is presented

by focusing mainly over cryptography, data mining, biometric privacy, and game theory. A survey over comparison of execution time, complexity, and data utility of differential privacy with other privacy schemes of big data is given in [43]. While, Jain *et al.* [44] surveyed the fundamental ideas of sensitivity and privacy budget by focusing on fundamental architecture and noise calculation mechanism of differential privacy.

A comprehensive survey on improvement of data utility of differential privacy in mobile sensing systems is presented in [19]. The discussion in [32] covers the aspect of privacy breaches for differential privacy techniques including differential privacy in social networks. Similarly, in [33] authors carried out a comprehensive survey of differential privacy in social networks and then presented two privacy techniques *(outlink privacy and partition privacy)* based on the concept of differential privacy. A method of quantifying data privacy and reducing computational error by finite precision based differential privacy is discussed in [34].

The detailed investigation about sensitive data mining, loss function, and learning from data bases by focusing on differential privacy is carried out in [35]. Furthermore, the implementation of various privacy preserving algorithms of mobile recommender system is compared with differential privacy by Xu and Yan [36] in context of privacy risks. Studies on privacy preservation of statistical databases using differential privacy has been presented in [37]–[39]. Dwork [37], laid the foundation of differential privacy for statistical data inference and surveyed two basic techniques of differential privacy. Similarly, an investigation and approach on individual experience cost as a function of their privacy and accuracy trade-off is proposed in [38]. Furthermore, the comparison of differential privacy with other data science privacy strategies by focusing on computational complexity, and theoretical basis is carried out in [39]. The field of privacy preservation in big data from the perspective of communication is analysed by Wang *et al.* [11]. The paper presents the comparison of differential privacy with other privacy preservation approaches in context of framework and preserving technique. Furthermore, it also highlights certain privacy attacks that needs to be analysed in the mentioned privacy preserving approaches. A detailed discussion about the integration of differential privacy with various deep learning models is presented in [45]. The authors first discusses three aspects of deep learning models along with the possible privacy attacks. Afterwards, authors demonstrated the integration of differential privacy in these models from perspective of layer-wise implementation. Similarly, an in-depth technical analysis over extensions and variants of differential privacy is covered by authors in [46]. The paper presents dimension, axioms, and relation based analysis of 54 differential privacy variants and analysed them from the point-of-view of computational complexity, and privacy loss.

However, the privacy topics of all differential privacy surveys do not address the applications and implementation of differential privacy in CPSs from any perspective.

D. Article Structure

A list of acronyms that are used throughout our survey paper is presented in Table III. The remainder of this paper is organized as follows: Section II provides an overview of differential privacy and CPSs, while Section III surveys differential privacy techniques in energy systems. Section IV provides a detailed survey of privacy preservation of transportation systems using differential privacy. Section V surveys implementation of differential privacy in healthcare and medical systems. Similarly, Section VI surveys differential privacy approaches in industrial Internet of things systems. In Section VII, we outline certain open issues, challenges, and future research directions. Finally, Section VIII concludes the survey article.

II. Differential Privacy and Cyber Physical Systems: An Overview

Privacy can be defined as a method of protecting information that can be sensitive to any individual. The basic reason of privacy preservation is to prevent an intruder from learning more than minimum required information regarding any specific individual either in case of real-time or statistical data.

A. Privacy Attacks

Adversaries always try to attack crucial systems in order to get complete or partial access to information. In this section, certain privacy attacks closely related to CPSs and differential privacy are discussed.

1) Disclosure Attack: Disclosure attack is a traffic pattern analysis attack, and in this type of attack, adversary is able to recognize the defined set of receivers on the basis of observed traffic [48], [49]. Adversaries use this attack method to identify the specific receiver and compromise its communication. However, disclosure attacks are not easy to implement because they require a certain level of computational efficiency. This is because of fact that adversary has to scan the whole network several times in order to get accurate receivers' identity that makes it difficult to launch [50]. Still, in order to overcome this attack, the real-time information being communicated between sender and receiver needs to be protected; that even if adversary is able to compromise the receiver, he will not be able to judge the accurate information.

2) Linking Attack: The type of attacks in which external data is combined with anonymized or protected data in order to infer critical information is known as linking attack [51]. For example, two anonymized datasets are linked together having different types of data about same individuals; re-identification can easily be carried out using linking attack. In the age of big data, launching an effective linking attack can be quite easy for any adversary. Thus, even anonymized data is not safe, and it can be used to breach any individual privacy. Therefore, a privacy protection strategy to efficiently protect query evaluation over statistical data is required.

3) Differencing Attack: Direct queries about any individual are usually blocked during a query evaluation to avoid any privacy breach. For example, in a hospital database, queries

like "does Mark have diabetes" are restricted because such queries directly violate privacy of individuals. Instead of these, queries for aggregated results are usually allowed, for example "how many men in a specific region have diabetes". However, an adversary can submit multiple queries to get personal information about certain individual. For example, an intruder can first ask "How many individuals in the dataset have diabetes", and then it can submit query as "How many people in the diabetic dataset, not named Mark". Thus, by repeating such queries, adversary will be able to determine the diabetes status of Mark. This type of repetitive query evaluation attack is known as differencing attack [11]. A privacy mechanism that does not give 100% accurate output to adversary for such statistical queries is required to protect secret data of individuals.

4) Correlation Attack: In real-world data, strong correlation may exist such as shared relationships and family members share attributes in various social networking datasets. If an adversary tries correlation attack using similar datasets, then this existing correlation may lead to disclosure of more than expected information [52], [53]. An intruder having different anonymized datasets for comparison can obtain private information of individuals in datasets by performing correlation attack, thereby it directly violates the principles of privacy. For example, anonymized datasets of a hospital can be merged and correlated to find the presence of any specific disease in members of family. This certain type of attack is called as correlation attack, and adversaries can easily launch correlation attack to identify certain details if they have rich data about their targets. In order to prevent correlation attack, a privacy preserving mechanism with efficient data handling is required that reduces the risk of information leakage even in case of public query evaluation.

B. Differential Privacy

To date, most of work on privacy preservation is done in perspective of databases. This work can be categorized into two major domains; first domain involves the protection of complete data from database in which anonymization techniques play a major roles, and the second one involves development of a good theoretical framework on the basis of privacy requirement in which differential privacy came up as a viable solution. Anonymization techniques initiated from *k-anonymity*, to *l-diversity*, and then to *t-closeness* method [54]. Similarly, theoretical framework based differential privacy strategies are further divided into *differential identifiability* and *membership privacy* [41]. The detailed discussion about these derivatives is out of the scope of this article. However, detailed discussion about differential privacy and its integration in different CPSs domain is presented. In this section, classification, comparison, and application scenarios of differential privacy is discussed. The concept of differential privacy technique on the basis of probability model was first introduced by Dwork [26]. The model was totally independent of the prior knowledge of adversary [26], [55]. The aim of differential privacy is to make sure that the output result of any query should not reveal enough information about any individual that leads to its identification. The randomized algorithm $\Re$ of differential privacy ensures that the output values of query cannot be distinguished irrespective of absence or presence of a specific member in the database ß. This means, that query results of neighboring datasets are indiscernible by introducing some randomized value of noise [19]. This sums up the conclusion, that adversary will not be able to presume sensitive information of any dataset with confidence. Differential privacy can formally be defined on the basis of two neighboring databases ß and ß′ that differs from each other in only one single member.

Definition 1 (Neighboring Datasets): A randomized algorithmic function $\Re$ satisfies ε-differential privacy condition $\mathbb{P}_{\mathbb{R}}$ if for any two adjacent datasets ß and ß′, and for any sort of possible outcome $\xi \in Range(\Re)$, we get:

$$\mathbb{P}_{\mathbb{R}}[\Re(ß) \in \xi] \leq exp(\varepsilon) \times \mathbb{P}_{\mathbb{R}}[\Re(ß') \in \xi] \tag{1}$$

In above equation, $Range(\Re)$ is the range of resultant output function $\Re$. Similarly, "ε" is the epsilon privacy parameter, that determines the actual level of privacy for proposed mechanism. The lower value of ε is desired in order to have stronger privacy and vice versa [56].

Definition 2 (Global Sensitivity): The value of sensitivity actually determines the required amount of perturbation in differentially private mechanism. Similarly, the term global sensitivity works over the phenomenon of maximum possible difference between query outputs from two datasets differing with each other by only one element (also known as neighboring datasets). For a randomized query $f : ß \rightarrow \Re$, the value of global sensitivity Δf_{gs} can be found using the following formula [30]:

$$\Delta f_{gs} = \max_{ß,ß'} \left\| f(ß) - f(ß') \right\| \tag{2}$$

The basic noise addition mechanism for differential privacy is shown in Fig. 1. Discussion about differential privacy can be divided into two major branches; differential privacy existing methods, and noise addition mechanisms.

1) Differential Privacy Existing Methods: Differential privacy existing protocols can be divided into two major categories, one according to the perspective of differential privacy optimization, and other according to the perspective of datasets. The integration of differential privacy in any data can further be categorized on the basis of two categories: (*i*) *Distribution Optimization* [57]–[62], in this branch, the probability density function of differential privacy is optimized without taking in account the dataset. In these techniques, differential privacy is generally achieved by adding randomized noise calculated via Laplacian or Exponential mechanism. The probability distribution of these schemes is further partitioned into centralized and distributed schemes. (*ii*) *Sensitivity Calibration* [63]–[69], in these techniques, data utility is improved by calibrating the sensitivity value to an optimal state. The sensitivity is further smoothed and lowered in order to enhance the data utility. These two mentioned categories perturbs data on the basis of mentioned criteria, for example if one needs to preserve data according to a certain probability distribution, then it will use the first "distribution

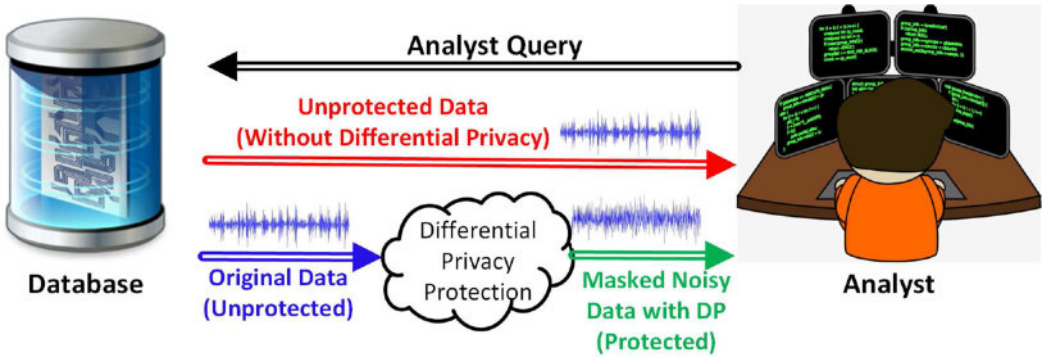

Fig. 1. Analyst query evaluation scenario explaining data output with Differential Privacy (DP) preservation (protected data) and without DP preservation (unprotected data).

optimization", or if one is interested to protect data according to its sensitivity value then "sensitivity calibration" is the most suitable option for that. However, these both types of integrations are also interlinked with each other in a manner that one can adjust both values at the same time to achieve desirable results. For example, a person wants to protect its data can use any probability distribution (such as Exponential, Laplacian, etc.) along with its required sensitivity value.

Similarly, the branch of differential privacy in perspective of dataset is also divided into two major subcategories: (*i*) *Synopsis of Original Databases and Datasets* [70]–[81]. In this method, the synopsis of datasets is built by applying various techniques of decomposition, transformation, or compression. The noise in these techniques is added in such a way that it minimizes rate of error and improves utility of data, along with satisfying ε-differential privacy value; (*ii*) *Correlation Exploitation* [63], [70] [82]–[84], in these proposed strategies of differential privacy, the correlation among attributes and data records is exploited to reduce the effect of noise and redundancy, that in return preserves data privacy more effectively.

2) Data Perturbation Mechanisms: In differential privacy, noise addition mechanism is referred as a way to protect data by perturbing it via pre-defined mechanisms. Three noise adding mechanisms are generally used in differential privacy approaches. They are named as Laplace mechanism (LM) [85], Gaussian mechanism [86], and Exponential mechanism (EM) [44]. The actual magnitude of added noise directly depends upon the global sensitivity and privacy budget [87]. Another term named as privacy bound do also contribute while noise addition in some circumstances. Generally, privacy bound is referred as privacy budget unless a specific bound is required [88].

a) Laplace mechanism: In Laplace mechanism, the noise is computed using the Laplacian function, and each coordinate of data is perturbed using the calculated Laplacian noise from LM distribution. The sensitivity of the differential privacy function determines the scale of noise being added.

In a given dataset ß, function $\Re$, and the global sensitivity δf_s, the randomized algorithm $\mathring{A}$ in Eq. (3) satisfies ε-differential privacy parameter, if the calculated noise value complies with the actual value of Laplace distribution; which is, $noise \sim Lap(\delta f_s/\varepsilon)$. LM is generally used in case of numerical output results [85].

$$\mathring{A} = \Re(ß) + Lap(\delta f_s/\varepsilon). \tag{3}$$

b) Exponential mechanism: A method to implement differential privacy in case of non-numerical outputs is Exponential mechanism. Exponential mechanism was specifically developed for certain conditions in which the best response was required to be picked. In a given dataset ß, $l \in Ł$ denotes the possible answer, in a score function $u : ß \times Ł \rightarrow Ł$; and a randomized algorithm $\mathring{A}$ selects a probability based answer, then the given randomized algorithm $\mathring{A}$ will satisfy the ε-differential privacy according to Eq. (4) [44].

$$\mathring{A}(ß, u) = l : |\mathbb{P}_{\mathbb{R}}[l \in Ł] \infty exp(\varepsilon u(ß, l)/2\Delta u) \tag{4}$$

In the above presented equation, Δu denotes the sensitivity of exponential score function. The value of Δu varies according to the requirement of user.

For example, Table V discusses an example of exponential mechanism, in which we take the value of sensitivity $\Delta u = 1$, and the dataset of medical records is evaluated on the basis of different epsilon values. The third column of table shows that when ε is taken as 0, then the mechanism can uniformly pick any option from all five options because the probability of selection of all possible outcomes becomes the same. Hence, it guarantees 100% privacy, but the utility is minimum. Similarly, in case of $\varepsilon = 0.1$, Headache has the maximum probability of being picked from the samples and Dehydration has minimum probability. Although, the gap between values is not very large, thus the value of $\varepsilon = 0.1$ can provide a considerable level of privacy. Finally, when $\varepsilon = 1$, the gap of probability between Headache and Dehydration is very significant which indicates a very high utility value, but the level of privacy reduces via considerable amount.

c) Gaussian mechanism: Gaussian mechanism is another essential block that is currently being used in implementation of differential privacy algorithms. Similar to Laplace mechanism, noise in Gaussian mechanism is calculated using normal (Gaussian) distribution [56], [86]. In a query function *f*, let value of ε be between 0 and 1, then the output for Gaussian perturbation σ will be as follows:

$$\sigma = \frac{\Delta_2 f}{\varepsilon}\sqrt{2log(1.25/\varepsilon)}. \tag{5}$$

TABLE V
MEDICAL RECORD BASED DEMONSTRATION OF EXPONENTIAL MECHANISM OF DIFFERENTIAL PRIVACY. THE TABLE SHOWS THE TRADE-OFF BETWEEN PRIVACY AND UTILITY SUCH THAT 0.2 AT $\varepsilon = 0$ DEMONSTRATES THAT THERE ARE 20% CHANCES OF THAT SPECIFIC ANSWER BEING PICKED WHICH MEANS 100% PRIVACY, AND 0.72 IN $\varepsilon = 1$ DEMONSTRATES THE CHANCES FOR HEADACHE ARE 72%, WHICH MEANS MINIMUM PRIVACY

Analyst Query	**No. of Applicant**	ε **= 0**	ε **= 0.1**	ε **= 1**
Cough	32	0.2	0.275	0.2675
Asthma	18	0.2	0.136	2.4 x 10^{-4}
Cholesterol	24	0.2	0.185	4.9 x 10^{-3}
Dehydration	12	0.2	0.101	1.2 x 10^{-5}
Headache	34	0.2	0.303	0.727

Composition Theorem [89]: In addition to noise addition mechanisms, differential privacy also has two composition theorems, which can be defined formally as follows:

Theorem 1 (Sequential Composition): The basic concept of sequential composition theorem states that if we have n-algorithms that are differentially private individually, and we want to feed results of first algorithm to second one, and so on, without sacrificing the complete privacy of output results. Then, sequential composition theorem allows such operations. Sequential composition theorem is usually beneficial for algorithms involving multiple iterations over same dataset.

Proof: A mechanism M($\mathcal{B}$) follows $n\varepsilon$-sequential composition differential privacy theorem if it obeys following property.

Let $\mathcal{B}_1 \& \mathcal{B}_2$ be two neighboring datasets then:

$$\begin{aligned} Pr[M(\mathcal{B}_1) = x_n] &= Pr[M_1(\mathcal{B}_1) = x_1] Pr[M_2(\mathcal{B}_1; x_1) = x_2] \cdots \\ &\quad \times Pr[M_n(\mathcal{B}_1; x_1, \ldots, x_{n-1}) = x_n] \\ &\leq exp(n\varepsilon) \prod_{k=1}^{n} Pr[M_k(\mathcal{B}_2; x_1, \ldots, x_{k-1}) = x_k] \\ &= exp(n\varepsilon) Pr[M(\mathcal{B}_2) = x_n]. \end{aligned}$$

■

Theorem 2 (Parallel Composition): Parallel composition applied in a condition when there is a single dataset which is further partitioned into n disjoint subsets. Privacy bound can be improved when queries are applied to disjoint subset of data. Primarily, if we partition input records into disjoint sets that are independent of actual data, then ultimate privacy guarantee of differential privacy depends only over worst guarantees of each differential privacy analysis subjected to data, not the sum.

Proof: A mechanism M($\mathcal{B}$) follows parallel composition differential privacy theorem if it obeys following property.

Let $\mathcal{B}_1 \& \mathcal{B}_2$ be two neighboring datasets then:

$$\begin{aligned} Pr[M(\mathcal{B}_1) = x_n] &= \prod_{k=1}^{n} Pr[M_k(\mathcal{B}_2; x_1, \ldots, x_{k-1}) = x_k] \\ &\leq exp(\varepsilon) Pr[M_L(\mathcal{B}_2; x_1, \ldots, x_L) = x_L] \\ &\quad \times \prod_{k \neq L}^{n} Pr[M_L(\mathcal{B}_1; x_1, \ldots, x_{k-1}) = x_L] \\ &= exp(\varepsilon) Pr[M(\mathcal{B}_2) = x_n]. \end{aligned}$$

■

C. Technical Challenges in Application of Differential Privacy

Although the basic privacy preservation concept of differential privacy is not much complex and most of the techniques require only data perturbation, but its implementation in certain applications faces numerous technical challenges. In this section, we highlight few challenges that researchers and industries do face while implementing differential privacy in emerging applications. A graphical illustration of some technical challenges in application of differential privacy in different scenario is presented in Fig. 2.

1) Sensitivity: Differential privacy was actually introduced to maintain the level of indistinguishability between certain cases, e.g., the presence or absence of record of some specific individual in dataset. In practical datasets, statistical queries are evaluated with low sensitivity using differential privacy [90]. For example, any random value *x* may be 1, or may even be 10,000,000 in a statistical record, thus, its domain will be $x \in [1, 10^7]$. A malicious administrator submits a query to aggregate all values of *x* such as *SUM*(*x*) which also involve the sensitive value of a participant. In this case, differential privacy algorithm calculates and adds Laplace noise in accordance to its standard deviation that will be directly proportional to range 10^7. In such cases, noise potentially hides the useful information and does not let intruders to know the exact sensitive protected value of individual participant. However, high value of sensitivity in a differential privacy algorithm will lead to undesirable loss of utility in various queries related to aggregation. Therefore, in order to maintain a certain utility level, privacy is relaxed by service providers or individuals and a degree of information is allowed to get leaked [11]. For example, a case in which an adversary is able to estimate salary of a certain participant in a certain range is better than the case in which adversary will not be able to infer any participant salary while performing statistical analysis. In this way, relaxation in differential privacy algorithms allow highly private output but along with privacy loss. That is why trade-off is always there that needs to be maintained between utility and privacy. Several emerging services and applications are using diverse sensitivities [91]–[93]. Therefore, it is still a challenge for researchers to propose optimal algorithms which overcome the privacy-utility trade-off by using optimal sensitivity value in the most efficient way.

2) Choosing Epsilon Value: Despite of being mathematically sound, still there is no rigorous method that explains

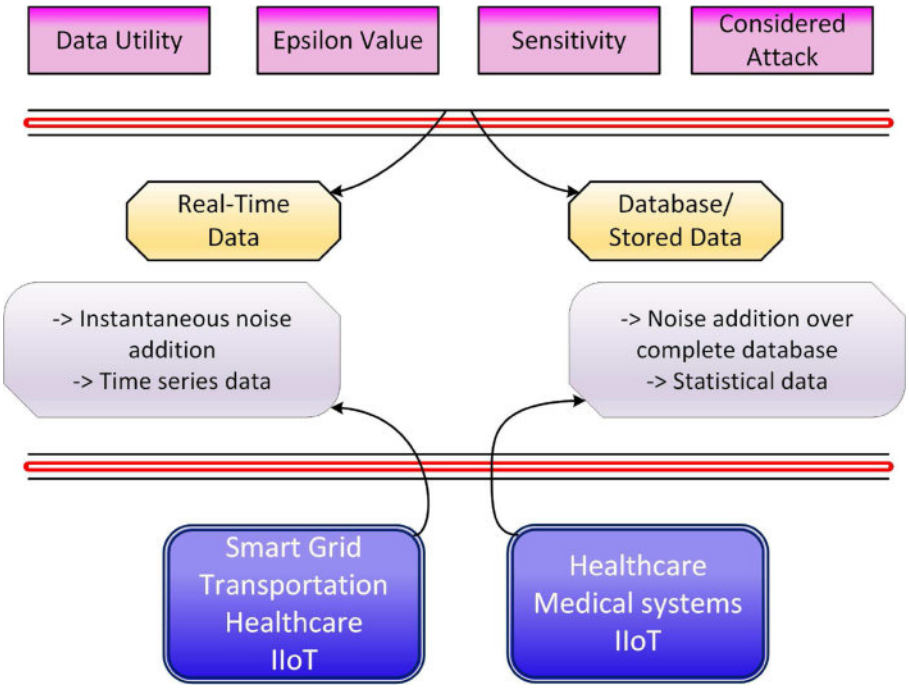

Fig. 2. Differential privacy implementation in cyber physical systems can broadly be classified into two scenarios (real-time data and stored data), however both the categories face some similar technical challenges such as selection of value of epsilon, sensitivity, data utility, and attack protection.

choosing and generation of optimal value of ε. Epsilon parameter serves to be one of the most important factor in controlling the trade-off between utility and privacy [94]. A smaller value of ε indicates quite high level of noise in the mechanism; thus, adversary will not be able to attack individual privacy. However, this high value of ε results in loss of utility or accuracy in output data. Therefore, choosing the optimal value of ε in various practical scenarios is a challenging task and is not completely addressed by researchers yet. In literature, certain researches have been carried out to find most optimal value of ε. In [37], [94]–[98], various approaches have been proposed to calculate optimal ε value on the basis of certain criteria such as success probability, largest affordable value, etc. However, choosing an accurate ε is still a considerable technical challenge for researchers.

3) Data Correlation: Strong coupling correlation often exhibits in real-world datasets, and certain records can be correlated with each other; that results in disclosure of information [99]. For instance, differential privacy assures that modifying, adding, or removing any individuals' record from a set of data will have no effect over aggregated data. However, presence of data correlation can benefit adversary by providing information that may help to infer private data of any specific individual. For example, in case of any social networks data, the presence of any specific disease in a specific family, and adjacent spatio-temporal location continuity can help the adversary to infer private individual information; this directly violates differential privacy definition. In [63], [100], [101], researchers developed model-based approaches, based over sensitivity weights, correlation degree, and correlated sensitivity to overcome this issue. Similarly, transformation-based approaches working over principle of transformation of actual correlated data to independent data while maintaining key information have also been proposed by researchers in [72], [74], [102]–[104]. However, experimental results evaluated that model-based approaches do not cover all aspects of correlation, and transformation-based approaches actually damages the correlated data up to some extent [11]. Therefore, overcoming correlation in differential privacy algorithm is currently among few biggest challenges for differential privacy researchers.

D. Effect of Differential Perturbation Over Analyst and Adversary

Differential privacy mechanism ensures that the privacy of user gets protected from adversary, and in order to do so, it perturbs data using various differential mechanisms. However, choice of sensitivity and epsilon value play an important role in determining the trade-off between accuracy and privacy. One important factor that differential privacy ensures is that the adversary will not be able to judge with confidence about presence or absence of any individual in a dataset. In order to analyse it, let's imagine two datasets D and D' differing with each other by just one record. If an adversary makes a query "F" on both presented datasets, then there is a very high probability that adversary will get same result "R" in both cases. On the basis of this result, the adversary will not be able to differentiate that a specific person "X" is present or absent in the dataset. However, on the other hand, a genuine analyst who wants to analyse the data in a legitimate way and do not have any intention to intrude into details of any specific individual will not feel much difference in the results. In this manner, differential privacy ensures that the output result should not

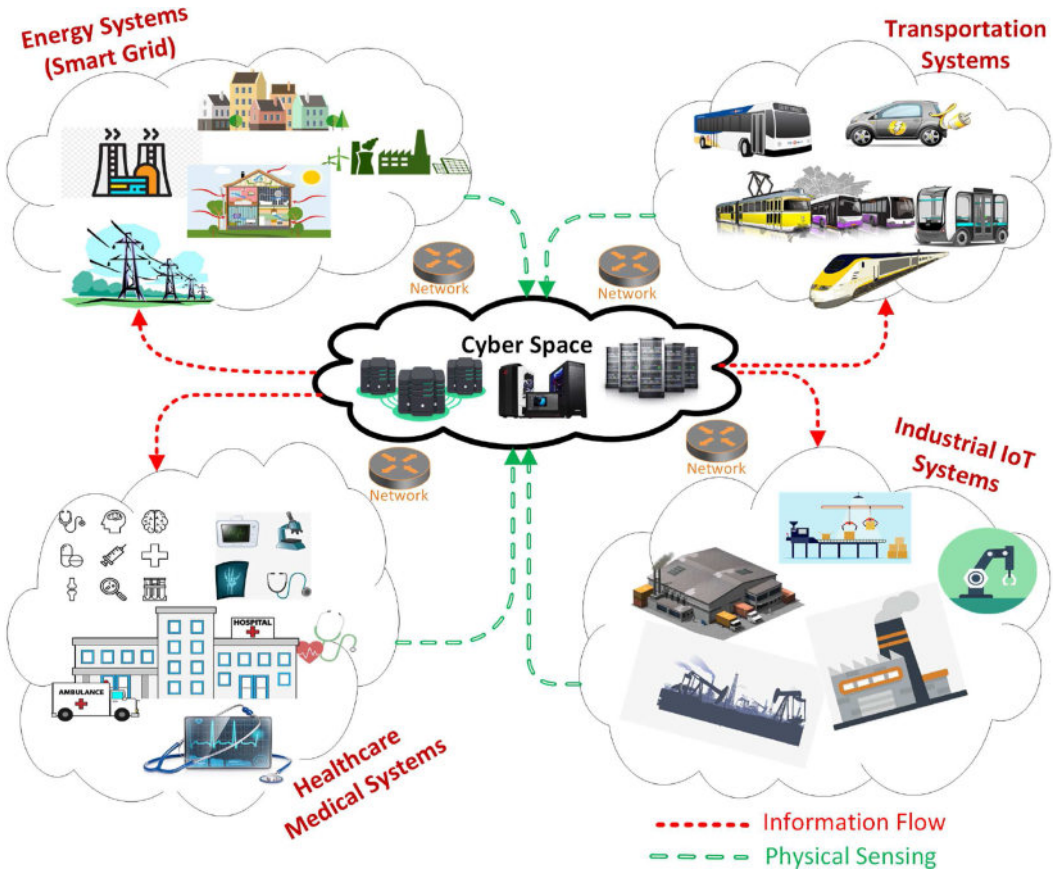

Fig. 3. Application Scenarios of cyber physical systems describing the information flow and physical sensing between cyber space and connected physical devices.

disclose too much statistical information about any specific individual of that dataset.

E. Comparison Between Differential Privacy and Information-Theoretic Privacy

In recent years, another modern privacy preservation strategy named as "information-theoretic privacy" is being used by researchers to protect users' data which is emerged from information-theoretic flow security. Similar to differential privacy, information-theoretic privacy do also work over preserving the private information by using statistical and analytical tools by leveraging the concept of data disclosure [109], [110]. Information-theoretic privacy quantifies and characterises confidentiality of query evaluation and limits the probability of disclosure of secret information using certain entropy based techniques such as Shannon entropy [107], [108]. Where Shannon entropy can be termed as average rate via which the information is generated by an available data source. Formally, Shannon entropy is defined as a negative log function of the product of probabilities of bunch of independent events [111]. Another important concept in information-theoretic privacy mechanism is mutual information which is referred as a parameter that signifies the relation between two random variables within dataset [106]. For example, within a dataset, the amount of information that a variable "A" can provide about variable "B" is termed to be its mutual information parameter. Similarly, this parameter will be zero if these variables are totally independent and irrelevant of each other. This parameter also serves as a foundation of many information theoretic approaches and researches are being carried out actively to enhance this parameter to an optimal level in order to provide maximum privacy guarantee.

In order to compare information theoretic privacy with differential privacy, first we need to consider their theoretical bounds and strength. Firstly, differential privacy works over the phenomenon of noise addition which depends upon ε and Δ factor that are referred as privacy parameter and sensitivity respectively. However, contrary to differential privacy, information theoretic privacy mechanisms are controlled by entropy based mechanisms that controls the level of indistinguishability for quantitative analysis [105]. Furthermore, differential privacy guarantees privacy of user and by only providing analytical proof for private answer of query. However, information theoretic privacy protects data by varying the difficulty of guessing the correct answer which can also be termed as leakage [112]. Finally, in order to compare privacy strength, certain researches have showed that differential privacy is a stronger privacy guarantee as it implies bound on Shannon mutual information and this bound approach value of "0" as the privacy controlling parameter ε approaches

TABLE VI
COMPARISON OF DIFFERENTIAL PRIVACY AND INFORMATION THEORETIC PRIVACY FROM TECHNICAL PERSPECTIVE

Privacy Factor	Differential Privacy	Information-Theoretic Privacy
Privacy Bound	Privacy bound controlled by e^{ε} sensitivity and Δ factor [20]	Privacy bound controlled by entropy mechanism (such as Shannon entropy) [105]
Privacy Guarantee	Provides guarantee for users' privacy [19]	Characterises confidentiality property of program [106]
Privacy Definition	Can be added by adding appropriate random noise [57]	It limits the probability of inferring secret information via entropy [107]
Privacy Strength	Differential privacy is termed as a stronger privacy as it implies bound on mutual information [108]	Restricts the probability of guessing but does not have bound over differential privacy mechanism [108]

"0". (A detailed discussion about this is elaborated by Alvim *et al.* [108].) Contrary to this, information theoretic privacy does not impose any bound over any parameter of differential privacy. Keeping in view all the discussion it can be summarized that both information theoretic privacy and differential privacy provides strong privacy guarantee to their respective usage application and both have their advantages and limitations that can be adjusted according to requirement. A detailed technical comparison between information theoretic privacy and differential privacy is given in Table VI. Moreover, since information theoretic privacy is in itself a huge topic, therefore, in this paper, we only focused on differential privacy. However, interested readers can further understand information-theoretic privacy from the following references [107], [110], [113]–[115].

F. Cyber Physical Systems

In 1946, first computer was invented to perform ballistic calculations [116]. With the passage of time, the position of computers got strengthened in various close loop controls around different physical systems. From this motivation, in 1973, the first computer which was capable of real-time computations was developed [117], which addressed the problem of scheduling multiple tasks so that every job gets completed before the deadline. Since then, the interest initiated in CPSs, though the actual name invented quite late. In the late 90's, the interest between interaction of physical and computational systems nourished when industries started modelling physical plants using differential equations which was named as hybrid systems [118].

In the meantime, another path named networks was also leading towards this area from the origin of Internet and cellular telephony [119]. This field of network control paved its way with the development of Smart Dust Project in 1998 [120], in which the nodes connected with the network can bring information regarding the physical environment around the devices. This evolutionary path initiated from communication, computation, and network control merged into a broader domain called as *networked* CPS [118]. Another path that have traces in the present CPSs is control system, which paved its path towards modern CPSs by invention of digital control approximately 50 years ago [118]. Around 2006, the researchers working in hybrid systems, control systems, and real-time systems devised the name *Cyber Physical Systems* to describe the systems incorporating cyber and physical worlds. Currently, the modern CPSs that we see all around us are basically the merger of communication, computing, and control technologies.

In the modern world, CPSs are closely linked with certainly every field of life including healthcare, energy, automotive, civil infrastructure, transportation, and industry. The information is being generated, sensed, and transmitted from all these technologies, and is being stored in certain databases and servers [121], [122]. Securing this transmission and data sensing gives birth to another critical domain of privacy and security in CPSs. In this section, we will be discussing system architectures, and applications of CPSs. While the privacy of CPSs and implementation of differential privacy will be discussed in Section II-G.

1) System Architectures: Generally, CPSs architectures consists of two major functional components [123]: (*i*) *Advanced Connectivity*, in which the real-time data transmission and reception is taking part between physical world and cyber space; and (*ii*) *Intelligent Data Management*, in which computational, and analytical capabilities are developed that is the core part of cyber space. Researchers have divided CPSs into certain models on the basis of their architecture. In this section, we review three major architectures of CPSs.

a) Networked control systems (NCS): The mediation of communication network between computing and physical devices is one of the major attribute of modern CPSs, and these types of control systems are called as networked control systems (NCSs) [118]. In NCSs, the control signals from devices and feedback signals from output can be exchanged in between system components. Owning this communication network based control, NCSs have many benefits as compared to traditional control systems. NCSs eliminate the use of unnecessary wires, they are less complex, cost friendly in designing and implementation, and can be upgraded or modified without major reformations in the basic structure [124]. On the other hand, NCSs do also have certain issues as well. The major issues NCSs face are: reduction of network traffic load due to sampling [125]–[127], network induced delays [128], packet dropout phenomenon [129], and quantization errors [130].

b) Hybrid systems: Systems which work on the switching phenomenon between multiple operation modes are known as switching systems. Similarly, the framework of CPSs that

is able to capture both, transitions between various continuous and discrete states over time is known as hybrid automation (HA) [118]. HA is generally used to model the complex dynamic nature of CPSs via several mathematical and computational formalisms [131], [132].

c) Distributed hybrid systems: These types of systems are quite complex, because they involve the differential equations based dynamic, discrete models, and real-time communication and computation technologies [118]. These types of systems are basically the composition and combination of several cyber and physical systems. Researchers are working in proving correctness of these systems by developing certain systematic methods and compositional frameworks.

2) Applications of CPSs: The research spectrum of CPSs is quite broad and it is hard to limit CPSs to few selected domains. CPSs are present in approximately every phase of life, from our homes to offices, and from our public life to personal life. The applications of CPSs with respect to information transmission and physical sensing is shown in Fig. 3. In this section, we discuss few benefits that CPSs research is providing and can provide in some selective application areas.

a) Energy systems (smart grid): Traditional energy systems can be summed up into generation, transmission, and distribution of electricity. But the modern energy systems named as *smart grids* are a combination of energy and ICT. Smart grid is said to be next generation infrastructure that will be capable of managing all our energy, and environmental needs, by providing us un-interrupted, cost-effective, and environment friendly electricity [133]. The production, transmission, and distribution efficiency of electric system can be optimized by using real-time measurements, analysis, and sensing techniques. Moreover, cyber and physical interactions are playing a vital role in advancement of efficient smart grid, and various new technologies, and certain methods are being developed to facilitate smart grid users. Few of them are real-time pricing, demand response, load forecasting, real-time load monitoring, etc. [134].

b) Transportation systems: Intelligent transportation systems (ITSs) is one of the emerging field of CPSs. In ITSs, development of traffic systems, vehicles, mass transit, and other similar factors are being addressed in order to enhance efficiency, congestion, sustainability, and safety [118]. A new terminology named as Internet of Vehicles (IoV) is introduced by researchers, in which every vehicle travelling in a certain radius will be connected with each other via device-to-device (D2D) and vehicle-to-vehicle (V2V) communication [135]. By using these capabilities, intelligent vehicles can aid the drivers or can even drive intelligently by sensing, estimating, and monitoring their surrounding circumstances and conditions. Moreover, the electric vehicles (EV) that are considered to be future of cars are being made fully intelligent, autonomous, and environmental friendly. ITSs are considered to be future of transportation systems and CPSs technologies are playing a vital role in practical implementation of this system in our daily life.

c) Healthcare and medical systems: Healthcare and medical systems are considered to be one of the most sensitive systems because they are directly linked with the wellbeing of people connected to them. Similarly, the evolutionary technologies of CPSs being implemented in healthcare systems are making them efficient, reliable, and intelligent. Healthcare systems generally contain wearable body sensors, OT (operation theatre) equipment, and physiological hardware devices. In modern era, these devices are made smart by connecting them with Internet and naming these things as e-Health. Wireless sensors are also being implanted in majority of these devices for real-time monitoring, but wireless devices have their own limitations and constraints [118]. Similarly, real-time response and user personal data protection are few major issues of these devices that are currently being observed and improved by medical researchers and biomedical engineers.

d) Industrial Internet of Things (IIoT): With the evolution of fourth generation of industry (Industry 4.0), the industrial systems are becoming smarter day by day. This term of Industrial Internet of Things (IIoT) flourished when researchers started integrating concepts of Internet of Things (IoT) with the environment of industrial control systems (ICS) [136]. The rise of IIoT is expected to enhance the process optimization, workers safety, factory management, etc. [137]. At the same time, the practical implementation of IIoT in industries is facing certain difficulties, e.g., developing efficient communication protocols, security and privacy issues of massive datasets, and formulation of efficient design patterns [138]. Researchers on the other hand are also focusing over the merger of various technologies such as edge computing, fog computing, and cloud computing with IIoT to make these systems more advance and autonomous.

G. Motivation of Using Differential Privacy in CPSs

Differential privacy has the potential to provide substantial amount of privacy to majority of application of CPSs and it may be a good choice where critical or public information needs to be preserved [139]. Similarly, integration of differential privacy with modern CPSs has emerged as a hot-topic not only in academic field but it is also paving its paths in industry [140]. Most of CPSs applications are real-time, that generates large amount of data named as big data. In order to handle and protect transmission, communication, and storage of this big data of CPSs, a strong privacy preservation approach such as differential privacy is required. In this subsection, we provide few of the major stimulating causes for applying differential privacy in CPSs:

- Various privacy techniques, such as encryption, k-anonymity, l-diversity, and t-closeness have been proposed for big data. At the same time, certain applications of CPSs are also being evaluated over these privacy techniques. However, differential privacy is one of the most suitable option to preserve privacy because it does not degrade systems' speed as compared to other techniques because of the light-weight nature of algorithms of differential privacy [43]. For example, in encryption, generation and distribution of

public and private cryptographic keys in the network becomes a hectic task and if one node in the network of "n" nodes gets failed then the aggregation of data becomes impossible due to missing distributed keys in that network [141]. Similarly, anonymizing complete dataset that contains millions of records is not feasible option for certain service provides because of limited computational capacity. Furthermore, in order to keep original records, the database companies have to store both datasets along with; one anonymized dataset for query evaluation, and one original dataset for their internal use. However, differential privacy eradicates both of the mentioned issues as it only protects data at run time by using basic low-complex algorithms which require calculations using Laplacian, exponential, and Gaussian distributions.

- Differential privacy provides enough quantitative theoretical basis which provides researchers an exact information that how much statistical CPSs data is safe to release along with what amount of accuracy [39].
- The original data of CPSs applications is very critical and the owner of data cannot take risk of losing that data. Therefore, in differential privacy preservation, the original dataset remains the same and is not modified at all. Irrespective of k-anonymity, l-diversity, or t-closeness schemes, where original values of data are manipulated to preserve identity [142]–[144].
- Differential privacy perturbs data by adding noise in such a way that the preserved CPSs statistical or real-time data can still be used by analysts according to their required needs [43], [140].
- Differential privacy provides substantial protection even in distributed CPSs environment, irrespective of other privacy preservation schemes that cannot provide efficient results because of correlation issues among attributes [145].
- Most of the encryption strategies used by real-time devices are computationally complex and need the generation of private encrypted keys at every node. But differential privacy provides a light-weight solution to preserve privacy for CPSs devices as compared to computationally complex encryption schemes as it only perturbs the data with certain calculated amount of noise [146], [147].
- If the list of queries is large in any CPSs database, traditional differential privacy suffers from utility loss, however integration of modern machine learning and deep learning algorithms with differential privacy is turning out to be a feasible solution. Researches have proved that differential privacy integrated with state-of-the-art machine learning and deep learning algorithms can effectively meet the demands of listing, perturbing, and query evaluation in large databases [3].
- In social CPSs, differential privacy provides both *node privacy* and *edge privacy*, by protecting individual information and any specific relationship information respectively [33].

H. Design Requirements of Differential Privacy in CPSs Applications

Differential privacy is a light-weight privacy preservation strategy that does not require complex hardware to run upon [12]. However, design and efficiency requirements vary in different applications of CPSs. Moreover, the optimality of differentially private mechanism also varies according to the application requirement. For example, in some cases the optimal solution will be complete preservation of privacy, however in some cases providing a certain level of utility can be termed as an optimal solution. Similarly, one cannot determine any definition of optimal solution of differential privacy, therefore researchers working in differential privacy of use the term "approximate optimal solution" while referring towards the most suitable solution according to requirement. Moving towards applications of CPSs, in context of smart grid, devices enabling differential privacy usually deal with communication of time-series data from one destination to another (mainly from smart meter to grid utility and vice versa). Therefore, point-wise privacy is generally considered in most of smart grid applications. Similarly, the most common attack in energy systems is non-intrusive load monitoring (NILM) attack, whose purpose is to identify the routine and appliance usage of smart home users [161]. Therefore, implementation of differential privacy techniques in smart grid usually consider overcoming these attacks. The aim of implementation of differential privacy strategies in energy systems is to provide a cost-effective medium level privacy protection by considering a healthy trade-off between accuracy and privacy [165]. Moving further to transportation systems, the V2V and D2D communication also requires a privacy strategy to ensure time-series data protection at a specific instant of time without delay. The major task in ITSs is to protect the real-time location data co-ordinates that are being transmitted between different vehicles and devices in the network. This type of communication is vulnerable to correlation attacks, in which the correlation between real-world data may reveal more than expected information [145], [166]. Therefore, most of differential privacy techniques being implemented over ITSs consider overcoming this attack in order to provide secure real-time location transmission. Another important aspect to consider in ITSs implementation is timeliness, the privacy schemes should not be complex enough to cause delays during protection. Therefore, this aspect cannot be neglected while designing ITSs privacy algorithms.

In healthcare and medical systems, the most important design requirement is to provide extremely high level privacy along with maximum accuracy, because these systems are directly linked with lives of patients and concerned people. That is why there is no chance of considering any less that optimal trade-off between accuracy and privacy [167]. Similarly, because of presence of both type of (statistical and time-series) data in these systems, differential privacy mechanisms need to consider instantaneous and global privacy both for real-time reporting, and query evaluation mechanisms respectively. Finally, in case of industrial IoT systems, high level privacy is required to secure statistical and time-series

TABLE VII
DESIGN REQUIREMENTS OF DIFFERENTIAL PRIVACY IN APPLICATIONS OF CYBER PHYSICAL SYSTEMS

Application Name	Level of Privacy Required	Data Types	Sensitivity Calibration	Common Attacks	Considered Factors	3^{rd} Party Aggregation
Smart Grid	Medium	Time-Series	Instance / Point-wise sensitivity	• Non-intrusive load monitoring (NILM) attacks	Cost effectiveness	Yes
Transportation Systems	Medium	Time-Series	Instance / Point-wise sensitivity	• Correlation attacks	Timeliness	Yes
Healthcare & Medical Systems	Extremely High	Time-Series and Statistical	Instantaneous sensitivity and global sensitivity	• Inference attacks	Data accuracy	No
Industrial Internet of Things	High	Time-Series and Statistical	Instantaneous sensitivity and global sensitivity	• Stealthy attacks	Secure communication	No

TABLE VIII
MILESTONES ACHIEVED IN DIFFERENTIAL PRIVACY FROM PERSPECTIVE OF CYBER PHYSICAL SYSTEMS

2006	[26] C. Dwork proposed the concept of differential privacy to obstruct adversaries from recovering private data.
2011	[148] G. Acs for first time integrated differential privacy with private smart metering data.
2013	[149] F. Kargl implemented differential privacy with policy enforcement framework to protect transportation data.
2014	[150] J. Zhao introduced the concept of integration of battery load balancing with differential privacy protection.
2015	[151] H. Li developed private partition algorithm for electronic health record protection using differential privacy.
2015	[152] N. Mohamed used differential privacy to protect cancer database from SQL queries.
2015	[153] S. Han used concept of join differential privacy to protect real-time data reported by EVs.
2015	[154] M. Savi conducted experiment to protect smart metering data by using Gaussian white & colored noise.
2016	[155] G. Rodriguez worked over integration of differential privacy & k-anonymity for industrial systems.
2017	[156] G. Eibl proposed the notion of pointwise differential privacy for smart metering real-time data.
2017	[157] H. Zhai carried out differentially private auction to protect EV identities from swap stations during bidding.
2017	[158] Y. Shi protected railway freight data using apriori and differential privacy algorithm.
2017	[159] J. Zhang examined use of differential privacy in real-time health data via adaptive sampling.
2017	[160] Y. Wang presented the use of differential privacy to protect privacy of linear distributed control systems.
2018	[161] H. Cao carried out private differentially private aggregation of smart grid over fog nodes.
2018	[162] T. Zhang proposed differentially private machine learning approach for vehicular networks
2018	[163] L. Raisaro presented the use of encryption in combination with differential privacy for genomic & clinical data.
2018	[164] L. Ni designed a differentially private algorithm for scanning in multi-core data clustering in industrial database systems.

industrial data. Various IIoT systems are vulnerable to stealthy attacks that may cause certain privacy harms such as false data injection [168]. Differential privacy strategies in IIoT systems needs to overcome such stealthy attacks in order to make these systems resilient from adversary interference. Use case scenarios after integration of differential privacy in CPSs applications is presented in Fig. 4. Similarly, taxonomy diagram of differential privacy from CPS perspective is given in Table VIII. The detailed design requirements of differential privacy implementation in different CPSs applications is presented in Table VII.

III. DIFFERENTIAL PRIVACY IN ENERGY SYSTEMS (SMART GRID)

The term smart grid (SG) is traditionally used for electrical grid which is the enhanced version of power grid of 20th century [169]. Traditional forms of power grids are generally used to perform basic tasks of transmitting energy from generating station to customers. On the other hand, modern power grid or SG uses bidirectional flow of information and electricity [170]. This bidirectional communication in SG is usually carried out using modern communication technologies, such as ZigBee, Bluetooth, wireless LAN, powerline communication, optical networks, and cognitive radio communication [171]. Because of this two-way flow of information and electricity, smart grid outperforms traditional energy grid by delivering energy in more efficient ways and by tackling large number of drawbacks of traditional power grid [169].

Along with the benefits of SG, the efficient way of communication and SG data storage also paved the path towards certain security and privacy issues [172]. For instance, leakage of real-time energy reading of SG user can become a serious threat towards that individual's personal life [173], [174]. Moreover, certain non-intrusive load monitoring (NILM) techniques have been designed to know exact appliance usage of any specific home during specific interval of time [175]. Hart introduced the concept of NILM for the first time which further lead to the development of modern NILM techniques we have nowadays [176]. NILM is referred as a technique to determine every minute detail about energy consumed inside the targeted area, e.g., usage of any specific appliance in a certain time slot can be extracted using such NILM techniques [177]. Furthermore, the key steps included in NILM techniques can be termed as event detection, feature extraction, and load identification. Since 2010, researchers are actively

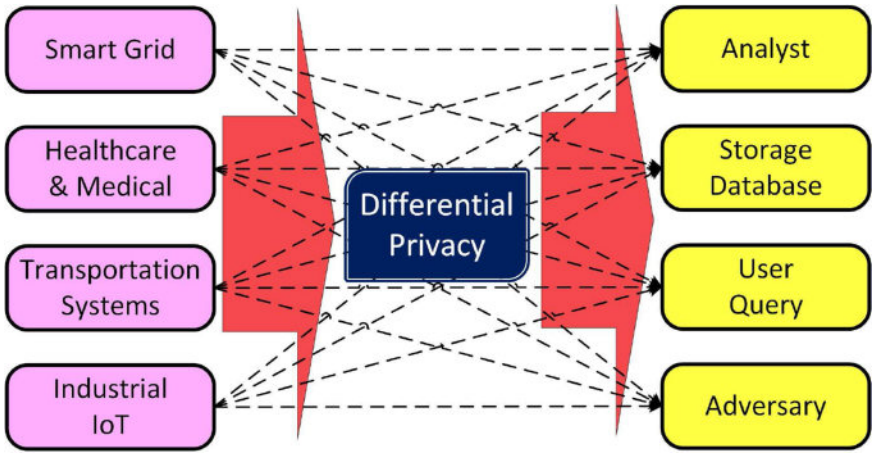

Fig. 4. Use case scenarios of differential privacy in applications of cyber physical systems such data analysing by analyst, storage databases, user query evaluation, and adversary query request.

working to develop more advanced NILM techniques to extract every minute detail from load data. However, getting exact usage pattern of smart home appliances can cause certain privacy concerns for people living inside the house. For instance, any intruder can detect the routine of residents and can plan a theft, or advertising companies can do targeted advertisements by detecting the missing appliance in home. Therefore, the privacy protection of SG users has always been the most crucial point among researchers working over SG. Majority of smart grid scenarios come under real-time data monitoring because smart grid devices are transmitting real-time data after a specific interval and therefore point-wise differential privacy protection is normally used to protect user's privacy in these scenarios. In order to protect this critical data, researchers have proposed numerous techniques to overcome privacy issues in SG. Here, benefits and trends of differential privacy in SG have been discussed. We divide differential privacy implementation in energy systems into three subclasses named as grid demand response, grid load monitoring, and grid data collection using fog computing, as illustrated in Fig. 5. Furthermore, the detailed taxonomy of energy systems is given in Table IX and Fig. 6. In this section, we discuss four major scenarios of SG over which researchers have applied differential privacy.

A. Grid Demand Response

One of the important goal of SG is to make energy use more efficient [178]. While, in order to obtain energy efficiency, management of volatile energy demands using scalable information is very important. The term demand side management (DSM) covers all aspects of demand response according to customer needs. DSM is quite important in operational cost reduction, elimination of blackouts, and reduction in emission of CO_2 [179]. Generally, smart meter data is used for calculation of demand response. Contrary to this, if any intruder gets the high resolution demand response data, then this data can be used for various monitoring and unethical purposes [180]. Therefore, this data requires protection in order to secure individual private information [181]. As discussed in the prior section, the real-time data is protected using data perturbation strategy of differential privacy. But the calculation of demand response from this perturbed data is actual problem that arises. To resolve this problem, Barbosa *et al.* [10] masked the data using Laplacian noise and after that worked over demand response calculation by dealing with individual appliance data. Similarly, they also evaluated two types of privacy attacks and showed that differential privacy is an optimal solution to overcome privacy risks. Therefore, the proposed differential privacy scheme efficiently protects demand response data by perturbing required features.

B. Smart Buildings

Recent facts and figures showed that more than 54% of population of world is living in modern cities and urban areas, and it is predicted that by 2050 this ratio will reach up to 66% [191]. This rapid increase in urban population has raised certain social, economic, organizational, and technical issues, which can be a harmful threat to economical and environmental situation of these areas. In order to overcome such situation, majority of governments are taking steps towards development and integration of "smart" concepts in all possible domains. Similarly, the concept of "smart city" refers to implification of all possible available resources and technologies in a coordinated and intelligent manner with an aim to develop more sustainable and habitable urban centers [192], [193]. One important sub block that requires considerable attention in such advancements are smart buildings. The concept of smart building refers to a modern building/home that is capable of performing measuring, controlling, monitoring, and optimizing operations without any external support. Smart buildings can further be classified into commercial and residential homes in which latest communication technologies are integrated to make them more suitable to live. Modern ICT technologies play an important role in such automation by providing a platform to carry out such real-time operations. The data stream from such smart buildings can be analysed to carry out certain automation tasks in order to make

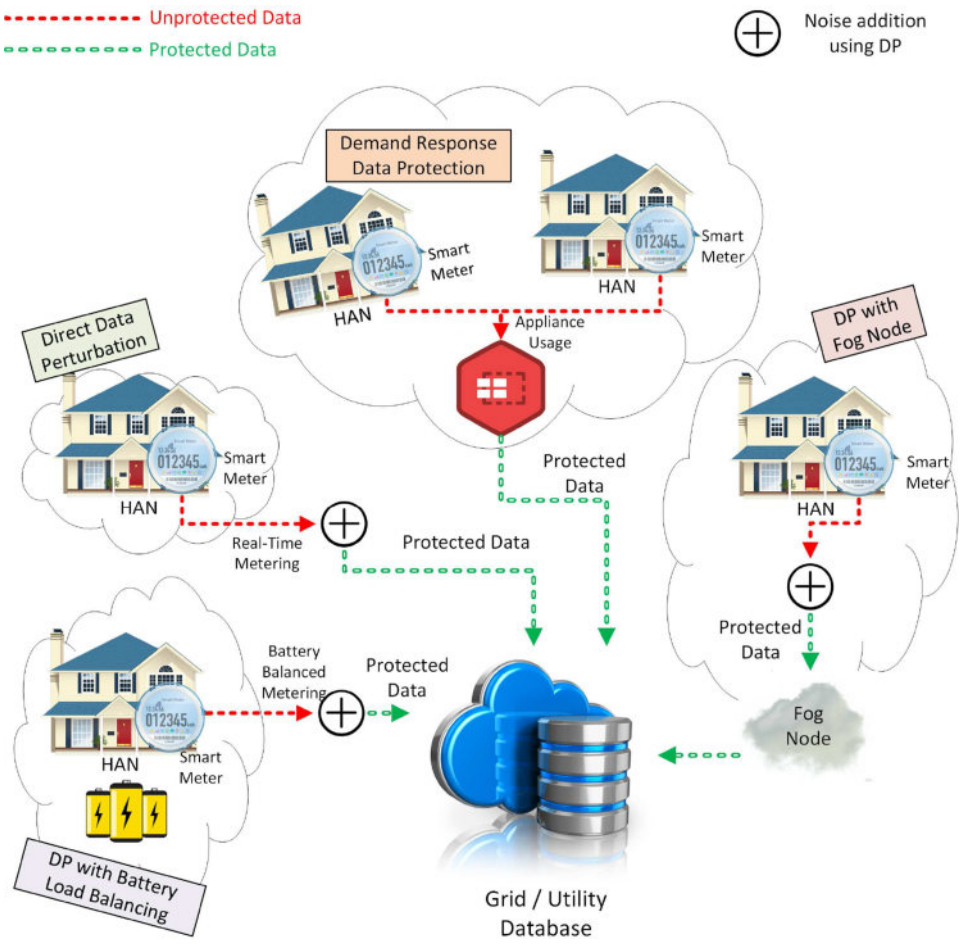

Fig. 5. Illustration of organization of differential privacy (DP) implementation in energy systems into four scenarios: direct data perturbation, battery load balancing, demand response protection, and DP with fog node. When DP is incorporated into these scenarios, real-time smart metering data of smart meter users is protected and the data stored by database can be used for query evaluation.

the city smart [194]. For example, smart buildings can regulate their own heating and lighting based on the presence or absence of habitants [195], can monitor the quality and structural health of their own [196], and can make use of intelligent and smart appliance in order to automate daily tasks [197]. In order to summarize, it can be said that multiple number of sensors, actuators, and controllers installed in a smart building work together to provide a comfortable, and energy efficient living to its habitants. Despite of all these advantages, smart buildings are not 100% perfect and are prone to many security and privacy threats. Many service providers, involved parties, and third parties dealing with smart buildings at different stages have access to plenty of private data which can further be used to infer into personal information of its users [198]. The data that can be used to attack privacy can be categorised into four sources: published data, observable data, leaked data, and repurposed data. The adversaries can use one of these four types of data to infer into personal life of habitants of smart buildings, which in turn can cause severe implications if not protected on time [199]. One of the prospective method to preserve privacy of such data is to integrate differential privacy protection before storage or transmission of data. In this section, we discuss the integration of differential privacy in two major scenarios of smart buildings.

1) Sensors Data Stream: One important feature of smart building is that they produce real-time environmental data from sensors in order to make effective predictions and calculations. However, leakage of this data can cause severe issues towards privacy of that building [200]. In order to overcome this issue, integration of differential privacy with data of sensors before transmission came up as a viable solution. The authors in [189] proposed PeGaSus mechanism that incorporates differential privacy over monitoring of real-time sensors' data. Proposed technique use the concept of perturbing, grouping, and then smoothing of data to protect sensors streaming. The authors further worked over differential privacy based query evaluation for hierarchical streams. In order to evaluate the performance of their proposed strategy, the authors performed experiment over data from 4000 access points collected over a period of 6 months. Similarly, the authors preserved event monitoring, hierarchical aggregation, and different query responses by using differential privacy perturbation. The proposed strategy was over sensors streaming, however to make it more relevant to smart city and smart buildings, the authors presented a next step of this

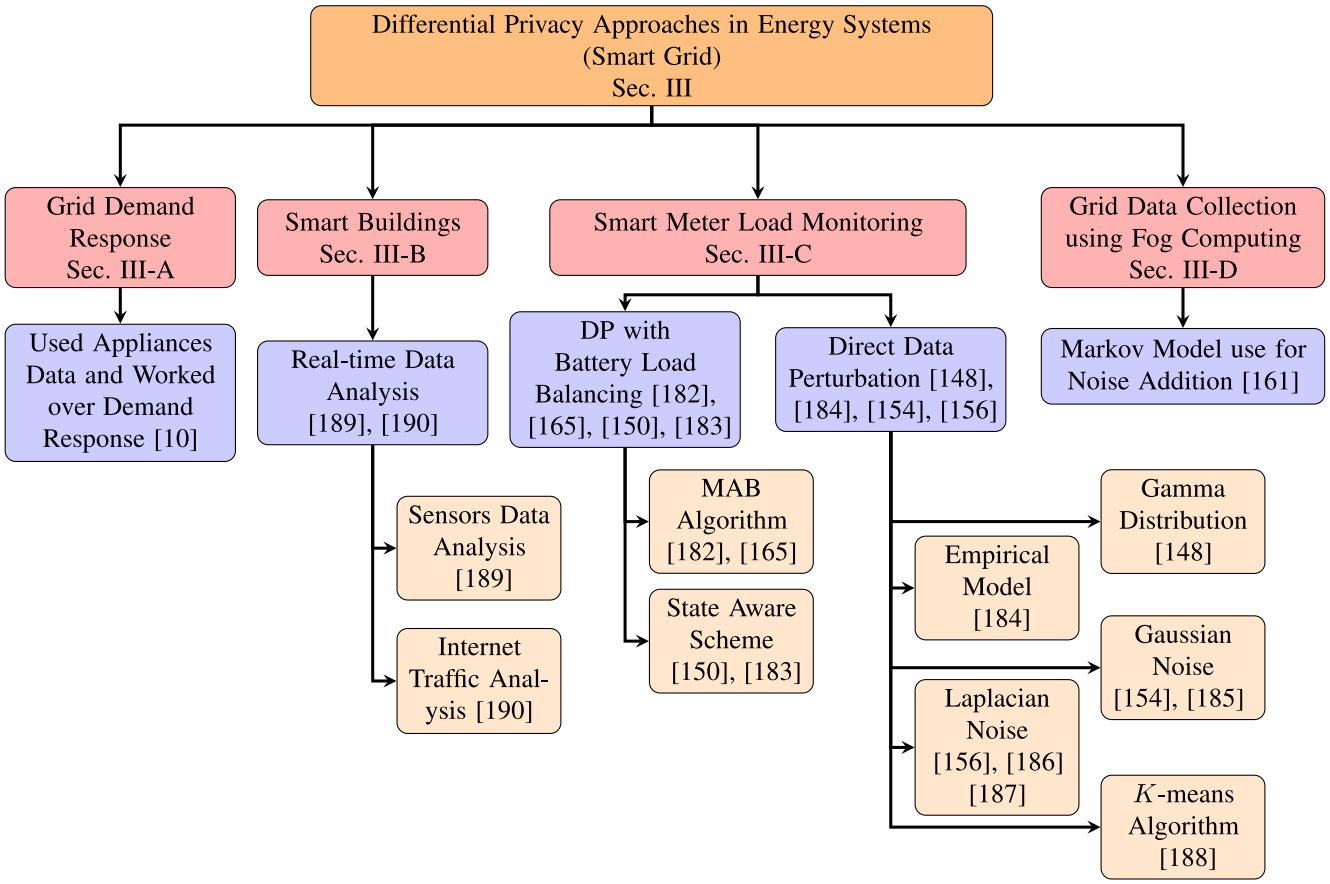

Fig. 6. The differential privacy approaches implemented in energy systems (smart grid) can be mainly classified into real-time data monitoring, demand response, and combination with fog computing.

work in [201]. In [201], the authors evaluated PeGaSus on real-world IoT scenarios for smart buildings and developed a tested and differential privacy engine for data stream. The authors concluded that the presented differential privacy based methodology successfully preserve sensors' streaming privacy for smart building scenarios.

2) Home Traffic Analysis: As discussed earlier in this section, residential smart buildings constitute an important part of network of smart buildings. Residential smart buildings also known as smart homes are capable of monitoring and controlling their energy and data flow and these smart homes combine to form a communication known as smart community [202]. In smart homes, majority of devices are connected to the Internet for monitoring and controlling purposes, this connectivity helps to take timely decisions via automating tasks. However, on the other hand this connectivity also raises certain threats that can be exploited by adversaries to carry out cyber-attacks on these homes and their residents. One such issue is highlighted by Liu *et al.* [190], the authors stated that the Internet traffic from smart homes can cause leakage of private information. Furthermore, authors claimed that even cryptographic tools cannot protect data privacy because of effective machine learning algorithms used by adversaries. To tackle this issue, authors proposed a differentially private traffic obfuscation framework for smart homes in a smart community network. The authors proposed utility-aware and exponential differential privacy mechanism for gateway selection of Internet traffic. From this work, authors ensured that accumulated data from such traffic ensure unlinkability and enhance privacy along with reduction in network resource consumption. The authors modelled this mechanism design as a linear optimization problem and proposed a differentially private strategy to overcome all mentioned issues. Finally, the authors carried out extensive simulation work to show that their algorithm enhanced privacy and reduced delay in a smart community network. Keeping in view this discussion, it is not hard to claim that differential privacy serves as a viable solution to protect privacy of smart homes.

C. Smart Meter Load Monitoring

One of the biggest hurdle in the implementation of SG is the privacy concerns of SG users [182], [193]. The smart meters are connected with each other and the main electricity grid utility via strong communication network and they constitute to make a complex network named as advanced metering infrastructure (AMI). Smart meters send their energy utilization information to SG utility after a specific interval of time (e.g., 10 minutes), and if any adversary gets access to these reported readings, then this data can leak sensitive information of smart meter user [176], [203]. This can lead to various threatening consequences; for instance, any burglar

TABLE IX
COMPARATIVE VIEW OF DIFFERENTIAL PRIVACY TECHNIQUES IN ENERGY SYSTEMS (SMART GRID) WITH THEIR SPECIFIC TECHNIQUE, OPTIMIZED PARAMETERS, PRIVACY CRITERION, SCENARIO, AND EXPERIMENTAL PLATFORM

Main Category	Ref No.	Year	Privacy Mechanism	Technique of DP Used	Enhancement due to Differential Privacy	Privacy Criterion	Platform Used	Scenario	Time Complexity
Smart Meter Load Monitoring	[148]	2011	DREAM (Differentially private Smart Metering)	Perturbed noise using Gamma distribution and encryption is used for aggregation	• Reduced cluster error • Preserved appliances multiple slot privacy	ε-differential privacy	Electricity Trace Simulator	Real-time	$O(n)$
	[184]	2014	Light weight privacy for smart metering data	Random masking value generated using Empirical model and error value	• Masked residential and industrial load profiles	ln-mechanism privacy	N/A	Real-time	$O(n^2)$
	[150]	2014	Multitasking - BLH - Exp3	Context aware battery load hiding strategy	• Enhanced mutual information sharing • Optimized event detection accuracy	(ε, δ)-differential privacy	N/A	Real-time	$O(log\ n)$
	[183]	2015	Stateless and stateful privacy protection schemes	Proposed relaxed differential privacy strategy by adjusting noise distribution along with battery capacity	• Mutual information sharing optimized in differential capacities of battery	(ε, δ)-differential privacy	N/A	Real-time	–
	[154]	2015	Precision-Privacy trade-off data perturbation technique for Smart Metering	White and colored Gaussian noise used for data perturbation	• Enhanced aggregated data privacy	ε-differential privacy	N/A	Real-time	–
	[182]	2017	Differential privacy battery supported meter reading	Differential privacy concept is used in conjunction with battery, and multi-armed bandit (MAB) algorithm	• Reduces extra cost • Reduces mutual information sharing	(ε, δ)-differential privacy	N/A	Real-time	–
	[165]	2017	Cost friendly differential privacy (CDP) scheme	Differential privacy with battery load balancing and MAB algorithm	• Optimized prices in both static and dynamic metering environment • Reduces mutual information sharing	(ε, δ)-differential privacy	N/A	Real-time	$O(log\ n)$
	[156]	2017	Differential privacy for real smart metering data	Point-wise differential privacy with Laplacian noise is used	Enhanced privacy and smoothing of signal	ε-differential privacy	N/A	Real-time	–
	[186]	2018	Differential privacy based distributed load balancing for smart grid	3ε based differential privacy using Laplacian noise	Optimized efficiency, and fine grained reporting without trusted third party	ε-differential privacy	Arduino micro-controller	Real-time	$O(kn)$
	[185]	2018	Differentially private crypto-system based smart metering	Perturbation and encryption based aggregation algorithm integrated with task assigning algorithm is used to protect user privacy	• Blocked filtering attack • Prevented true value attack	(ε, δ)-differential privacy	N/A	Real-time	–
	[187]	2018	HIDE (Differential privacy for smart micro-grid architecture)	Privacy preserving data publishing differential privacy using greedy algorithm and Markov assumptions	• Privacy-utility trade-off is minimized • Max query, count query, and average query is enhanced	(ε, δ)-differential privacy	N/A	Real-time	–
	[188]	2018	Data clustering using differential privacy for intelligent electrical IoT	K-means data clustering algorithm is combined with traditional differential privacy	• Enhanced F-score • Enhanced clustering privacy	ε-differential privacy	Java	Real-time	$O(n)$
Smart Buildings	[189]	2017	Differential privacy based monitoring of real-time sensors' data	Perturbing, grouping, & smoothing based differential privacy applied over sensors' streaming	• Protected stream query privacy • Protected sensors' event monitoring	ε-differential privacy	N/A	Real-time	-
	[190]	2018	Differentially privacy private traffic obfuscation framework for smart community	Utility-aware & exponential differential privacy mechanism for gateway selection	• Ensure unlinkability in Internet traffic • Reduction in network resource consumption	(ε, δ)-differential privacy	N/A	Real-time	$O(n^2M)$
Grid Demand Response	[10]	2017	Differential privacy strategy to protect appliance usage in smart metering	Data masking using random Laplacian noise	• Enhances real-time data privacy • Improved utility performance by demand response calculation	ε-differential privacy	Simulators[2] in C	Real-time	$O(1)$
Grid Data Collection using Fog Computing	[161]	2018	Differentially private data disclosure in smart grid	Factorial Hidden Markov Model (FHMM) is used to implement differential privacy	• Enhanced F-1 score • Optimized kullback leibler divergence	ε-differential privacy	NILMTK	Real-time	$O(km)$

can detect the occupancy or un-occupancy schedule of a house before attempting any burglary, similarly, potential targets can be selected by vendors to market their campaigns [154]. Therefore, certain standardization bodies [204], [205] and smart meter users require a privacy-friendly and secure framework for real-time monitoring of SG data that provides useful

data to SG utility by keeping in view the confidentiality and privacy of users.

Extensive amount of literature is presented on smart meter data aggregation using encryption technologies, so that only the SG utility knows the exact usage information of users [206]–[209]. However, various implementations showed that encryption is hard to apply over real-time smart metering data because of the requirement of high computational capacity [141]. Another obstacle in application of encryption is the necessity of cooperation between all smart meters, because all smart meters have to exchange distributed keys and in case of failure of even a single smart meter, faults may arise in the whole network [10]. Another popular privacy approach to protect smart metering data is anonymization [210]. One approach discussed the idea of hiding individual privacy by providing two different identities, one for billing and other for monitoring purpose [210]. Similarly, the transmission of data using low-frequency and high-frequency ID is also proposed in the literature. However, this data can further be mined, and identification can be carried out using the anonymized data. This certain piece of information can further be classified to a specific group of people in order to deduce their average behaviours [211].

Therefore, protecting real-time data by adding desired amount of noise is one of the most desirable approach to transmit data without compromising privacy [212]. Implementing differential privacy in order to protect real-time data has been employed by various researchers in the past on the basis of different SG scenarios, and different ways of addition of noise in the data. It can be classified into two major categories. One method is protection of real-time smart meter data by combining the advantages of differential privacy and battery load balancing, while the second one is direct perturbation of data using differential privacy, as shown in Fig. 6.

1) Differential Privacy With Battery Load Balancing: An effective way to protect smart meter data privacy is to balance the load by using an external battery, this technique is also known as battery load hiding (BLH). But there are few major downsides of using direct BLH mechanisms that cannot be disregarded. For example, BLH techniques do lack theoretical discussion, as they are usually evaluated in context of their relative entry, regression, and clustering classification [150]. However, there is no proved evidence to show their relevance directly to privacy protection. Therefore, in order to measure the exact protection and accuracy of privacy mechanisms, researchers used BLH schemes with differential privacy protection. In [182], the authors proposed a differential privacy based smart meter reading mechanism by perturbing the data without violating the limitations of battery. The authors worked over parameters of noise distribution and also combined multi-armed bandit (MAB) algorithm to further decrease the battery cost. The proposed techniques in [165] enhanced the privacy loss in a battery based differential privacy scenario. Furthermore, the authors worked over reduction of cost under both dynamic and static pricing environment, and formulated two cost friendly approaches. The study in [150] analysed previous BLH techniques by identifying their shortcomings, and then proposed a multitasking-BLH algorithm that successfully enhances the constraints of traditional BLH algorithms by optimizing event detection accuracy. The authors in [183] first analysed the theoretical and practical challenges of differential privacy in BLH mechanisms, and then proposed stateless and stateful differential privacy BLH mechanisms in order to optimize mutual information sharing in different capacities of battery.

2) Direct Data Perturbation: To protect smart meter user privacy, perturbing real-time smart metering data has been adopted by many researchers. Noise dimensioning is the most important factor to consider while perturbing the data directly. The correct amount of noise according to the scenario requirement makes differential privacy schemes more useful [154]. Choice of noise addition parameter ε cannot be neglected in this discussion, because it determines the level of privacy. Therefore, a vast amount of literature argues over choosing the most efficient ε value [213]. Another parameter which is important to consider while selecting differential privacy for smart metering data is sensitivity. Generally, differential privacy techniques have been applied over counting data according to time-series [74]. In counting data, the sensitivity parameter is generally taken as 1, while smart metering data cannot be depicted as counting data and the value of global sensitivity is not known, therefore the sensitivity cannot be directly taken same as of counting data [156].

In [148], real-time smart metering data is perturbed using Gamma distribution, and in order to make the aggregation secure, the authors used encrypted aggregation strategy. Furthermore, the proposed strategy reduced cluster errors in a SG scenario, and preserved appliance multiple slot privacy. The simulations of this proposed technique is performed using electricity trace simulator. The authors in [184] proposed a light weight differential privacy approach that generated a random masking value based upon empirical model and error value. Analysis is carried out in the paper after masking residential and industrial profiles with differential privacy approach. Savi *et al.* [154] first analytically derived ε parameter to satisfy privacy guarantee in data aggregation, and then perturbed the data using Gaussian white and colored noise. They aggregated the data from different smart meters and at the end concluded that Gaussian colored noise provides a desirable level of privacy protection. Similarly in [185], authors proposed a differentially private crypto-system based smart metering approach to preserve users privacy. In order to make perturbation more efficient and secure, the authors merged Gaussian noise based perturbation with task assigning algorithm and encryption. Furthermore, the authors analysed two privacy attacks named as filtering and time value attack and claimed that their proposed strategy efficiently protects smart meter users' privacy.

In [156], authors analysed the trade-off of privacy and accuracy for real-time smart metering data and proved that differential privacy can be applied over real-time data and suitable advantages can be achieved using this approach. The authors further proposed the notion of point-wise privacy stating that the requirements of differential privacy in real-time data are different from differential privacy in statistical

databases. Taking another step ahead, the authors in [186] proposed 3ε-differential privacy approach and analysed the outcomes using Arduino micro-controller. The practical output results showed that differential privacy optimized the efficiency value, and provided fine grained data reporting using Arduino even without need of any trusted third party. In [187], HIDE mechanism is proposed to address problem of privacy-utility trade-off in smart micro-grid scenario. The authors enhanced max query, count query, and average query along with using greedy algorithm, Markov assumption model, and Laplace noise for differential privacy. Contrary to traditional differential privacy approaches, authors in [188] introduced the concept of secure and private data clustering in intelligent energy systems using differential privacy. The authors proposed a light-weight secure clustering algorithm and tested the algorithm over different ε values to optimize performance and privacy-utility trade-off accordingly.

D. Grid Data Collection Using Fog Computing

Data collected from smart meters is usually aggregated and stored in data centres operating on cloud computing. During the transmission and storage, data may encounter delay and can decrease the response time. In order to overcome these issues, fog computing came up as a practical solution. Fog computing can be defined as a computing paradigm which was introduced to overcome burdens of data centers in traditional cloud technology. With time, fog computing emerged as a most viable solution to provide support to latency sensitive, geographically distributed, QoS aware applications of IoT [214]. However, recent researches demonstrate privacy and security as the most important challenges for fog-computing based IoT applications. As fog computing nodes are not completely trusted and are vulnerable to certain threats and adversaries [215]. Therefore, protecting privacy of data being communicated from fog-nodes is important. For example, what if a fog node aggregating the smart meter data gets compromised. To answer this question, researchers suggested usage of differential privacy along with fog computing in SG systems, to maintain the efficiency and privacy of data [147], [161]. One of the differential privacy approach considering fog computing in SG scenario has been implemented by Cao *et al.* [161]. The authors proposed factorial hidden Markov model (FHMM) based differential privacy approach to aggregate data in fog nodes. Authors claimed that the proposed technique protects fog nodes data from any sort of NILM strategies. Furthermore, the given technique improved F-1 score [216] along with optimizing kullback leibler divergence in fog computing scenario. Energy consumption of every appliance is perturbed with a noise generated by FHMM, and the data is transmitted to fog node for storage purpose. Thus, this protected data can further be transmitted to analysts or the control centres to carry out certain DSM operations.

E. Summary and Lessons Learnt

The integration of ICT technologies in energy systems have paved the path for modern, intelligent, and secure energy, collectively named as SG [133]. However, plenty of issues still needs to be resolved, and the most important of them is securing users' private data to maximum extent. On the other hand, utility also requires smart meter data for certain calculations, such as demand response, load forecasting, etc. Researchers have proposed various strategies to overcome security and privacy issues of SG, including, encryption, battery load balancing, anonymization, and differential privacy. However, from above discussion, we can say that differential privacy provides a suitable solution to majority of SG scenarios. For example, when differential privacy is used with battery load hiding, it proves to be the backbone of mathematical analysis for BLH strategies. Similarly, the use of differential privacy in direct data perturbation showed that it also provides privacy protection at a specific instant of time by perturbing the instantaneous value of measured reading. Correspondingly, differential privacy incorporated with smart buildings can efficiently preserve sensors' and the Internet traffic data.

Demand response calculation strategies do also require a specific level of privacy preservation to protect personal predicted data of users. Therefore, differential privacy comes up as a viable solution to protect demands response data. Likewise, along with privacy protection, efficiency, and speed is also required. Therefore, the integration of differential privacy with fog computing paved the way for future secure energy systems. However, there are certain field of smart grid that still needs to be preserved using differential privacy. For instance, fault information and transmitting information needs to be preserved, in order to make it private from any intruder that needs to attack any specific damaged area. Similarly, load profiling information and meteorological data also needs critical attention in context of privacy. Moreover, preserving billing information along with maintaining dynamic pricing policy needs to be addressed in different SG scenarios. Furthermore, preserving the identity of buyer and seller using differential privacy must be considered for buying and auction of renewable energy resources (RERs) applications. Similarly, firmware updates for smart meters needs to be carefully considered to protect the leakage of any specific software component of smart meters.

IV. Differential Privacy in Transportation Systems

Transportation systems are advancing day by day, and the major purpose behind all these advancements is to provide improved services for riders and drivers in the system [220]–[222]. Since the beginning of 1970s, ITSs have been developing in various forms and are now considered to be the future of transportation systems [223]. ITSs incorporate a large number of advanced technologies such as data transmission technologies, intelligent control technologies, and electronic sensing technologies into traditional transportation systems [224]. In ITSs, every kind of transport (e.g., cars, trains, buses, etc.) is equipped with multiple wireless devices that are generating data for vehicle-to-device (V2D) and vehicle-to-vehicle (V2V) communications [225]. ITSs communication is usually carried out using certain modern technologies, such as mobile ad hoc network

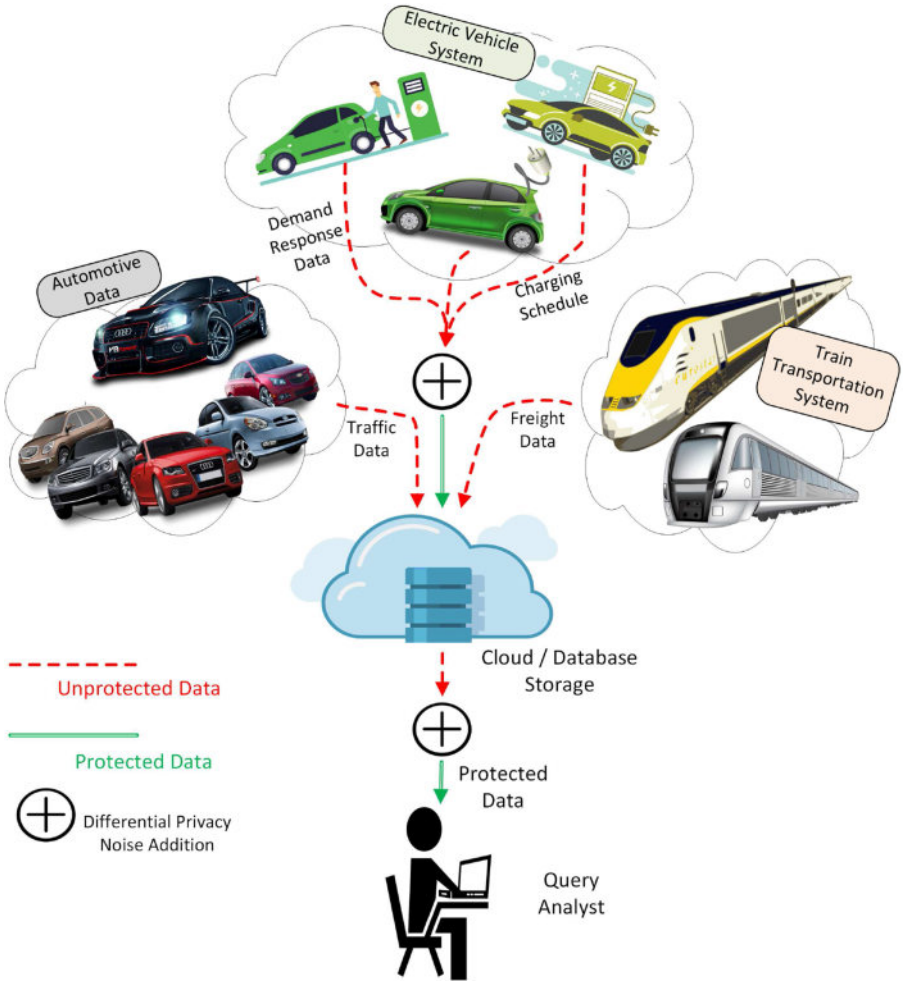

Fig. 7. Illustration of organization of differential privacy (DP) implementation in transportation systems into three scenarios: electric vehicle, automotive data, and train transportation system. When DP is incorporated into these scenarios, automotive, demand response, charging schedule, and train systems data of transportation systems is protected and the data stored by database can be used for query evaluation.

(MANET), IEEE 1609 or dedicated short-range communication (DSRC), cognitive radio, and heterogeneous vehicular networks (HetVNET) [226], [227]. The participants of ITSs periodically share their vehicular information to communicate with other users in the network. This effective and accurate data is also used by various sources, in order to provide better and reliable services for ITSs [228], [229]. Most of these V2V and V2D communication schemes rely on trustworthiness of sources receiving or aggregating their data [230].

However, the communication and storage of ITSs data is prone to many attacks and adversaries. For instance, an attacker can record the transmitted messages of any vehicle and can re-use these messages to get access to certain resources like compromising toll services, etc. Similarly, any false accident warning can be transmitted from a compromised vehicular network to block traffic from a certain highway. Moreover, the identity of a train, vehicle, or bus can be impersonated and can be used for unethical causes [231]. Therefore, the privacy of ITSs data needs to be considered before implementing ITSs in our daily lives [162]. Many privacy protection strategies have been implemented in the past to consider different scenarios of modern transportation systems. In this section, we divide differential privacy implementation in transportation systems into three subclasses named as railways freight networks, vehicular networks, and automotive manufacturer data, as illustrated in Fig. 7. The taxonomy diagram for differential privacy in transportation systems is given in Fig. 8, and the summary table of literature work of differential privacy in transportation systems is provided in Table X.

A. Railways Freight Network

Railways are considered as one of the most important mean of freight transportation in the world. The arrival of technology of big data in the railway freight system has brought various opportunities along with some challenges [232]. Because of involvement of big data analytics technology, customers' requirements, timeliness, and efficiency can be achieved in railways. However, this evolution also comes up with certain privacy and security risks. One of the major issue in the way of achieving efficiency through big data is data privacy and confidentiality [233]. Privacy risks can arise in the way of sharing and communication of information, any adversary can try to attack the shared data and can get restricted freight

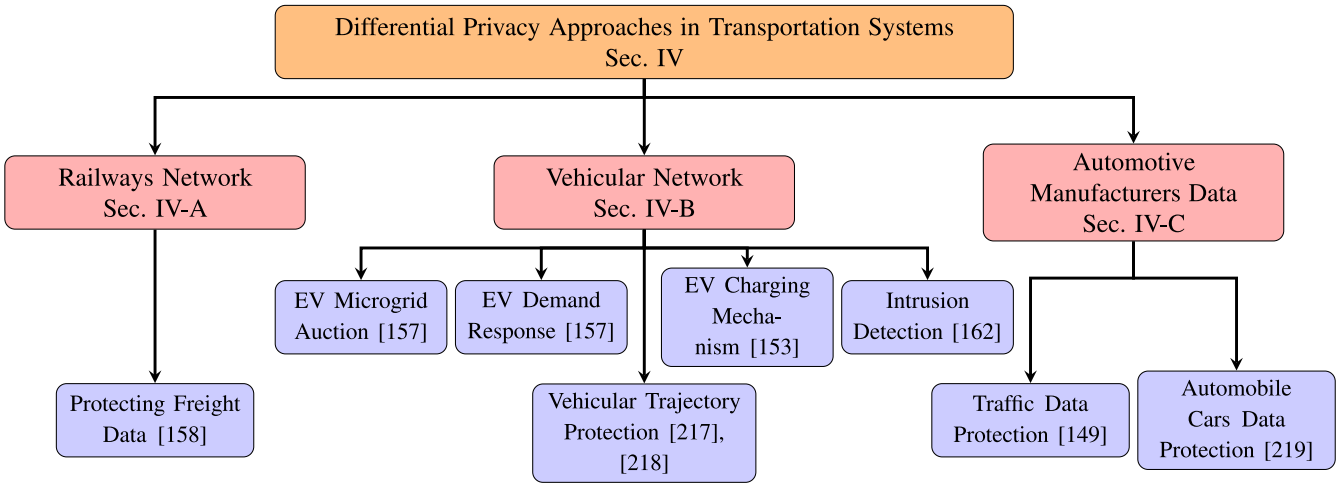

Fig. 8. The differential privacy approaches implemented transportation systems can be divided into railways network, vehicular network and automotive manufacturer's data privacy techniques.

information. This leakage of data can be hazardous to one's personal privacy. Very few researches are carried out so far in order to protect privacy of railway freight systems [158]. Previously researchers worked over proposing of game model to protect freight data. However, the proposed models only proved to be a macro solution, and no specific implementation was carried out. Since, railway networks deal with the passenger's data stored in their databases and this data is further used to calculate the commute rate, hourly, daily, weekly, and monthly travel rates. Therefore, statistical differential privacy is applied to such scenarios.

Similarly, in order to prevent leakage of private information of citizens, Shi *et al.* [158] proposed a differential privacy based correlation approach for railway freight systems. In [158], the authors first sliced the original service data to an optimal length, and then used apriori and differential privacy algorithm to introduce Laplace noise in the datasets of candidates. By following this method, they ensured that customer's information is protected even if any adversary is successful in getting access to the background knowledge. Therefore, in context of railway networks, differential privacy strategies prove to be viable and efficient because they provide suitable solution without being computationally complex.

B. Vehicular Networks

Modern vehicular networks made it possible for drivers or vehicles to communicate with surrounding vehicles or drives. In this way, vehicle is aware of its surroundings environment, which considerably improves on-boards services, and road traffic safety [234]. For instance, the vehicles in a specific area can detect or expect dangerous situations in their way that may cause severe damages such as collisions or accidents. As a consequence, the vehicles can take intelligent decisions in order to prevent themselves from such incidents [235]. Although, this real-time information may also be exploited by any attacker or adversary for unauthorized tracking of vehicles' location [236]. Generally, wireless medium is used for V2V and V2D communication that can easily be compromised, and broadcasts can easily be eavesdropped by a passive adversary. This unethical eavesdropping data can be a serious threat to someone's personal privacy. For instance, getting the information about the frequency of visits to a certain hospital can raise many doubts about the health of driver. Moreover, the life of driver can be put at a risky situation if the adversary eavesdropping the broadcast is a criminal [225], [237]. Similarly, information about charging/discharging of EV and, auction information for EV in microgrids also needs to be protected, in order to prevent adversaries from monitoring the daily routine of EV users [157]. We have divided the privacy protection in vehicular networks into two subcategories; protection of EVs auction and charging information, and preserving privacy of intrusion detection systems of vehicular networks.

1) EV Auction and Charging Protection: As discussed earlier, the privacy protection of communication between EVs is an important issue that is currently being addressed by many researchers. Similarly, the auction phenomenon of EVs while selling or buying energy also needs specific attention. In context of flexible storage, EVs can benefit demand response functionalities of energy grids. Particularly, EVs are designed in such a way that they can be charged in low electricity and in the time of need they can be discharged or can sell their energy to other EVs or SG [238]. Recently, swap stations are being introduced for charging of EVs. By using swap station technology, EVs charging speed is improved greatly [239]. Various efforts have been put in by researchers on scheduling the charging of EVs from swap stations [240]. Similarly, the discharging EVs sale out their surplus electricity to other EVs or smart homes and this trading is carried out using an auction process. This auction is usually a game-theoretic process in which selling price and incentives are determined after collecting bids and asks from buyers and sellers respectively [241]. However, the charging, discharging, auction, and demand response data of EVs needs to be preserved even from swap stations, because making this data public sacrifices the individual privacy of EVs [157]. Wireless sensor networks and cloud computing is the general medium used for

TABLE X
COMPARATIVE VIEW OF DIFFERENTIAL PRIVACY TECHNIQUES IN TRANSPORTATION SYSTEMS WITH THEIR SPECIFIC TECHNIQUE, OPTIMIZED PARAMETERS, PRIVACY CRITERION, SCENARIO, AND EXPERIMENTAL PLATFORM

Main Category	Ref No.	Year	Privacy Mechanism	Technique of DP Used	Enhancement due to Differential Privacy	Privacy Criterion	Platform Used	Scenario	Time Complexity
Vehicular Network	[153]	2015	EV Charging truthful mechanism via differential privacy	Used exponential differential privacy along with drawing random vector from distribution	• Enhanced truthfulness of privacy mechanism	(ε, δ)-differential privacy	N/A	Statistical Database	–
	[157]	2017	ExPO: Exponential based privacy preserving online auction	Exponential differential privacy is used	• Demand response • Improved peak load along with privacy preservation	ε-differential privacy	MATLAB	Real-time	–
	[217]	2017	Differentially private vehicular trajectory protection algorithm	Exponential differential privacy in collaboration with trajectory partition & clustering algorithm is used	• Protected information loss • Enhanced data utility & efficiency	(ε, δ)-differential privacy	SUMO	Real-time	–
	[162]	2018	Machine learning based collaborative intrusion detection (PML - CIDS) to preserve privacy	Machine learning based differential privacy approach with dual variable perturbation	• Enhancement of empirical risk	(ε, δ)-differential privacy	N/A	Statistical Database	–
	[218]	2019	Private real-time vehicular trajectory data release	Laplacian perturbation & Kalman filter based position protection for dynamically sampled data	• Enhanced accuracy • Reduced error rate • Enhanced data availability	ε-differential privacy	MATLAB	Real-time	$O(m^2)$
Railways Network	[158]	2017	Railway freight data correlation analysis using differential privacy	Laplacian noise is added using Apriori algorithm	• Improved privacy in freight data mining	ε-differential privacy	N/A	Statistical Database	–
Automobile Data	[149]	2013	Differential privacy in intelligent transportation system (ITS)	Smooth sensitivity using Laplacian perturbation	• Preserved floating car data (FCD) in traffic data centres	ε-differential privacy	N/A	Real-time	–
	[219]	2017	Differential Privacy scheme in automotive Industry	Laplace, exponential, and randomized mechanisms are discussed	• Protected personal identifiable information (PII)	(ε, Δ)-differential privacy	N/A	Statistical Database	–

communication and storage between EVs and swap stations. Therefore, it is easy for any passive adversary to eavesdrop the information being transmitted [242].

Researches have been done in order to protect the auction privacy of EVs, few researchers suggested the use of cryptography to protect auction privacy [243]. Due to computational complexity and communication overhead, the performance of cryptographic strategies decreases. However, the privacy protection mechanism of differential privacy emerged as one of the optimal solution to preserve individual privacy of auction based strategies of EVs [244]. One of the most significant work in implementation of differential privacy in EV auction is carried out by Zhai *et al.* [157]. The authors used exponential based differential privacy to protect private information of EV owner from being compromised by adversary. They used auctioneer to maximize social welfare of market by

matching sellers and buyers. The demand response calculated after using the given scheme improved the peak load requirement without compromising the privacy of EV users. Another noteworthy work in order to protect charging schedule of EVs via differential privacy is carried out by Han *et al.* [153]. The authors used the idea of joint differential privacy to limit power and involvement of users at the time of reporting their specifications for Online auction. The proposed strategy ensured that even if any EV misreport its specifications to mediator or swap station, it will not get much benefit from it, that in turn will lead to truthfulness. Moreover, differential privacy can provide secure bidding in conjunction with energy auction scenario of EVs by successfully controlling the information and only displaying the minimum required information. Thus, differential privacy easily surpasses other privacy preservation strategies in context of EVs data protection.

2) Vehicle Trajectory Protection: In modern world it is predicted that every vehicle will be connected to Internet and every vehicle will be sharing its real-time information with the network in order to develop a seamless traffic and transportation system. However, this real-time reporting do also raises certain issues and vehicular trajectory leakage is most crucial among them. These trajectories can be used to predict behaviour of passengers that may further lead to leakage of personal life routine of that individual [245]–[247]. This data can further be supplied to certain corporation and companies that may exploit this location data for their business purposes such as carpooling companies [248]. Researches are being carried out to overcome this issue in the most efficient way in which the individual will be able to share its real-time location along with preserving its private information. One such effort is carried out in [217], the authors developed a differentially private vehicular trajectory protection algorithm in which they explored and integrated exponential differential privacy protection with trajectory partition and clustering algorithm. Furthermore, the authors worked over preserving information loss along with enhancing efficiency and data utility of differentially private algorithm. Similarly, another work which protects real-time user location is carried out by Ma *et al.* [218]. The authors first adopted dynamic sampling strategy in order to process real-time location data, and further used Kalman filter to ensure data availability. Afterwards, the authors used Laplacian perturbation of differential privacy to protect user data. By doing so, authors ensured that the protected data provides enough utility along preserving it from malicious adversaries. The output results presented by authors ensured that the privacy and data availability increased as compared to similar approaches.

3) Privacy of Intrusion Detection Systems: Intrusion detection systems play a vital role to mitigate threats of vehicular networks by detection adversarial behaviour using signature based and/or anomaly based approaches [249]. An advanced architecture of intrusion detection systems is collaborative intrusion detection systems (CIDS), that enable nodes to share the detected knowledge about attacks, and in return increase detection accuracy [250]. CIDS enable the EVs to utilize labelled dataset of other vehicles; that speeds up the training process for each EV without burdening the EVs storage capacity. Moreover, the workload is also distributed among all EVs by sharing the laborious task of collecting labelling data. Data communication between EVs is not completely secure and can cause serious privacy threats to training data because of distributed environment. If any adversary is able to successfully extract the private information of EVs, then it can maliciously pretend to be some EV in the network which can observe its surrounding vehicles or it can also observe and manipulate the outcomes of learning process [162]. Therefore, a privacy preserving mechanism for intrusion detection systems in EVs is important. In order to protect this real-time CIDS data, Zhang and Zhu [162] proposed a differential privacy based machine learning CIDS approach that enhances empirical risk in the network by making the data private via dual variable perturbation. The authors in the paper first captured the privacy notation and then worked over dynamic differential privacy for data perturbation in machine learning scenario. Furthermore, the detection accuracy, design, and privacy-security trade-offs of CIDS in context of differential privacy are also considered and enhanced by the authors. From above discussion, it can be concluded that sharing data between modern electric vehicles can be made more secure and private using differential privacy strategies.

C. Automotive and Manufacturer Data

As discussed earlier, the data from connected vehicles is prone to many security and privacy risks. When it comes to EVs, this problem of privacy protection needs to be tackled and solved by the manufacturing companies in order to maintain trust of drivers. One of the major aspect that manufacturers are considering the most is confidentiality of personally identifiable information (PII) [219]. A common notion while working with privacy protection of PII is to remove the data that is linked with PII, such as names, tracking numbers, etc. However due to lack of any exact technical definition, it is surprisingly difficult to define and identify perfect PII [251]. Moreover, Gao *et al.* [252] demonstrated that the speed of driving can be combined with road maps in order to trace the exact location of vehicle. Furthermore, Tockar [253] showed that anonymized cab data of NYC combined with public data, revealed sufficient information to detect celebrities and passengers that made visits to sensitive places within the city. By keeping in view the above discussion, we can say that it is also the responsibility of smart car manufacturers to keep the point of view of privacy in mind while designing modern cars.

One of the most promising privacy technique that can be implemented by manufactures to preserve privacy of individuals without damaging the original data is differential privacy [219]. Boes *et al.* proposed the application of differential privacy for real-time automotive data. Furthermore, the authors discussed various types of noises (e.g., Laplace, exponential, and randomized mechanism) that can be used to perturb data according to manufacturer's requirement. The authors in [149] integrated differential privacy with policy-enforcement framework in order to protect floating car data

storage in traffic data centres. Moreover, they provided specific guidelines to ensure the specific privacy guarantee along with providing efficient data accuracy. Thus, differential privacy can prove to be a viable solution to solve certain privacy leakage problems according to manufacturer's point of view. As differential privacy efficiently adds noise in desirable PII, so users' travelling in vehicles have control over the information they are sharing and that is how they can control their privacy according to the need.

D. Summary and Lessons Learnt

Network of connected devices in transportation system ensures reliable service, but it also comes up with certain privacy and security related issues. A major issue being faced in ITSs is privacy leakage of individual identity of EV users. The adversary can compromise a communication channel by the help of passive attacks. Therefore, proper privacy preservation of data being transmitted throughout the network should be maintained. Researchers proposed differential privacy as one of the optimal solution to overcome these real-time and database privacy issues. But still plenty of issues in transportation system needs to be resolved.

An important application of transportation systems is modern EVs, which improve reliability, safety, and security in every perspective [254]. These EVs can be charged at low power and can be used in case of power shortage or failure via discharge process [255]. However, this modernization comes up with certain privacy issues. For instance, the real-time location, battery status, and charging/discharging schedule reveal a large number of personal information of EV users. Therefore, the most successful approach presented by researchers to prevent this privacy leakage is differential privacy. The above discussion mainly focuses over two major aspects of EVs; charging/discharging protection, and protection of intrusion detection strategies. It is found out that by considering the advantages of differential privacy in EVs, we can publicise the data of EV without worrying about the privacy of individuals.

The privacy control according to Manufacturers' point of view is also discussed in this section along with specifically mentioning the protection of PII in modern vehicles. Because certain experiments have been conducted by researchers in which they combined two anonymized datasets and successfully achieved the precise information about individual activities. However, if we preserve the data using differential privacy, then the anomaly will not be able to break in to the privacy. Similarly, differential privacy is also implemented in railways freight network to protect customers' information for data mining.

However, many fields of transportation system still need consideration in order to protect them from anomalies, first and foremost of them is device-to-device (D2D) communication. Whenever, devices in a transportation networks are communicating, they are sharing a considerable amount of personal data that can be a threat to someone's privacy in case of an attack. Therefore, research efforts to protect D2D via differential privacy needs to be made. Furthermore, securing the storage of big data of ITSs also needs more attention in order to remove any sort of confusion or privacy concern from minds of ITSs users or customers. Similarly, live traffic information also needs to be preserved in order to disrupt any adversary from tracking the lifestyle of any EV user. Moreover, researchers need to focus about enhancement and protection of privacy in V2V communication as well, because a large number of V2V applications may have crucial significances in case of privacy leakage.

V. Differential Privacy in Healthcare and Medical Systems

One of the most attractive application of connecting cyber and physical world is healthcare and medical systems [256]. This connection has a great potential in CPSs, and it gives rise to many healthcare applications such as real-time health monitoring, fitness programs, remote health monitoring, and elderly care. Medication and treatment from distant places or homes is another potential application of this connection [257]. Similarly, storage of health records using big data, and performing data analytic surveys for better diagnosing of disease at early stage is also under development phase. Therefore, the healthcare and medical systems are considered to be one of the core part of CPSs. These modern healthcare systems surpass traditional healthcare systems by improving time, cost, and quality of life. Furthermore, the modernization of these systems provides efficient scheduling of finite resources by assuring their most efficient use.

One major issue to consider in healthcare systems is the timely measurement and diagnosis of critical factors for treatment of disease. In majority of cases, the late diagnosis leads to dangerous chronic diseases, certain advanced cancer stages, or even death in some cases [258]. Another important factor to consider in healthcare and medical CPSs practical implementation is its privacy preservation, because even a minor privacy threat can risk someone's life [259]. Majority of these healthcare and medical devices are connected via wireless networks for data reporting and transmission [260]. This timely measurement and reporting requires seamless communication infrastructure. Generally in healthcare CPSs, 4G long-term evolution (LTE), ultra-narrow band (UNB), ingenu, and low power wide area (LPWA) technologies are used to carry out communication [261]. These technologies transmit real-time health data by causing minimum delays. The medical data contains specific patterns for real-time or e-health monitored data, and these patterns should be protected with certain privacy control because they are directly linked with someone's personal life. For instance, date of appointment from a specific doctor, health insurance ending date, a specific glucose level in the body, diagnosis of any specific disease, etc. If any intruder gets access to this real-time data, then it can directly or indirectly have an effect on the life of the patient.

Researchers have proposed many privacy protection techniques in the past for various applications of healthcare and medical systems. For example, encryption, and data perturbation for real-time data, key-agreement, and anonymization for e-health data sets, etc. However, in this section we divide

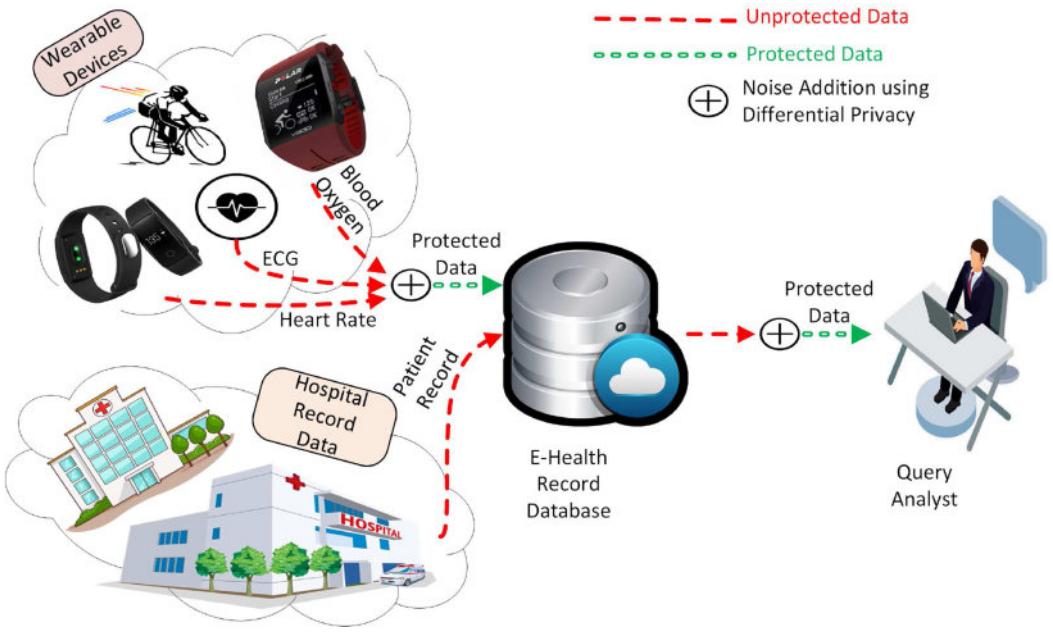

Fig. 9. Illustration of organization of differential privacy (DP) implementation in healthcare and medical systems into two scenarios: wearable devices, and hospital record database. When DP is incorporated into these scenarios, heart rate, ECG, blood oxygen level, and patient record data of healthcare and medical systems is protected and the data stored by database can be used for query evaluation.

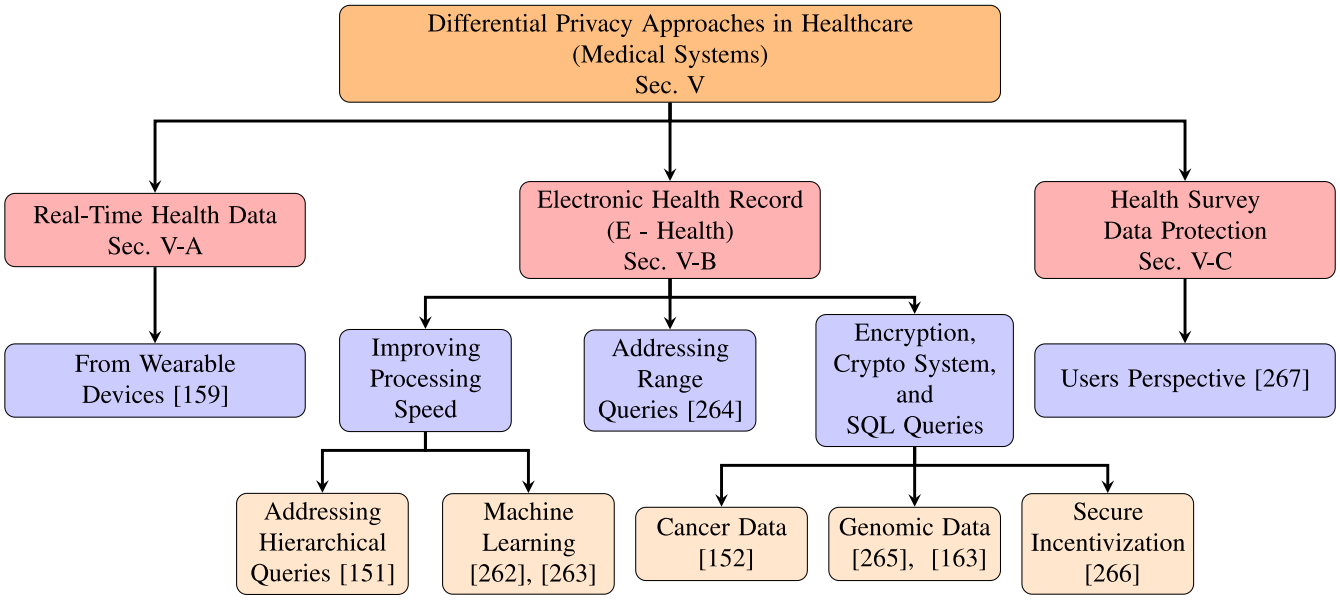

Fig. 10. The differential privacy approaches implemented health care and medical systems can be categorized into real-time health data, electronic health data, and survey data record strategies.

differential privacy implementation in healthcare and medical systems into three subcategories named as real-time health data, electronic health record, and health survey data protection, as illustrated in Fig. 9. The taxonomy diagram for differential privacy in healthcare and medical systems is given in Fig. 10, and the summary table of literature work of differential privacy in healthcare and medical systems is provided in Table XI.

A. Real-Time Health Data

With the rapid expansion of wireless devices in our daily lives, the way we deal with our health is also changing. Real-time health data is being reported to doctors or databases to keep track of user behaviour and activities [159]. For example, data of heart rate, sleep conditions, blood pressure, walk steps can be shared with doctor, hospital, or with insurance companies. However, the disclosure of unnecessary data can lead to severe privacy concerns [268]. While sharing the health data two things are generally considered as first priority, *(i)* utility (usefulness of data) and *(ii)* privacy (disclosure of less than a certain privacy budget). One of the major source of real-time health data are wearable medical devices; that can be defined as non-invasive, and autonomous devices designed to perform any specific medial function such as health data

TABLE XI
COMPARATIVE VIEW OF DIFFERENTIAL PRIVACY TECHNIQUES IN HEALTH AND MEDICAL SYSTEMS WITH THEIR SPECIFIC TECHNIQUE, OPTIMIZED PARAMETERS, PRIVACY CRITERION, SCENARIO, AND EXPERIMENTAL PLATFORM

Main Category	Ref No.	Year	Privacy Mechanism	Technique of DP Used	Enhancement due to Differential Privacy	Privacy Criterion	Platform Used	Scenario	Time Complexity
Real-time Health Data	[159]	2017	Real-time health data releasing scheme (Re-Dpoctor)	Data perturbation is used along with adaptive sampling and filtering	• Mean absolute error and mean relative errors are enhanced	(ε, δ)-differential privacy	PIP Controller	Real-time	$O(n)$
Electronic Health Record Privacy	[151]	2015	Efficient E-health data release	Heuristic hierarchical query method and private partition algorithm proposed for DP	• Enhanced time, overhead, and query error	(ε, Δ)-differential privacy	N/A	Statistical Database	$O(n)$
	[152]	2015	Private and Secure management of databases of health care database	Used Laplace mechanism for data privacy	• Reduced computational overhead	(ε, Δ)-differential privacy	Prototype in Java16 using Big Integer	Statistical Database	$O(Nlog^2N)$
	[264]	2017	Health data differential privacy algorithm for range queries	Partitioning by data and work load are implemented with use of Laplacian noise	• Optimized error rate of queries	ε-differential privacy	N/A	Statistical Database	–
	[163]	2018	MedCo (Privacy preservation of genomic and distributed clinical data)	Encryption in combination with differential privacy is used to secure and preserve sensitive data	• Enhanced i2b2 database privacy • Optimized runtime, and network over head	ε-differential privacy	Postgre-SQL	Statistical Database	–
	[265]	2018	Genomic data privacy protection	Protecting encrypted data using differential privacy and two step decryption	• Enhanced execution time • preserved secret keys leakage in dual decryption	ε-differential privacy	NFLib	Statistical Database	–
	[263]	2018	End-to-end differentially private deep learning health record protection	Differentially private stochastic gradient descent based deep learning method	• Enhanced training accuracy • Improved computational cost	(ε, δ)-differential privacy	N/A	Statistical Database	–
	[262]	2019	Differentially private data clustering (EDPDCS) framework for medical data	K-means clustering based differentially private machine learning over MapReduce	• Optimized privacy allocation budget • Improved learning accuracy	(ε, δ)-differential privacy	Hadoop	Statistical Database	–
	[266]	2019	Secure E-Health data aggregation with fair incentives	Combined local differential privacy with Boneh-Goh-Nissim crypto system & Shamir's secret sharing	• Improved key generation overhead • Aggregation privacy	ε-differential privacy	Java (JPBC library)	Real-time	$O(\sqrt{t})$
Health Survey Data Protection	[267]	2018	Privacy-Utility trade-off in health record systems	K-Anonymity and random data perturbation discussed	• Discussed and improved survey data according to users perspective	-	N/A	Statistical Database	–

monitoring [269]. Vital signs of patients such as blood pressure, heart rate, body fat, blood oxygen level, and respiration are constantly being measured and monitored to be aware of any upcoming undesirable situations. Similarly, athletes also use such wearable medical devices in order to measure their calorie burn, pace, heart rate, and speed during exercise and report it to their coaches. This data contains specific patterns, which may provide critical information about any individuals' health life. However, if this personal data of any patient or athlete gets stolen by any adversary, then the respective individual may face severe health circumstances.

Several methods including encryption [270], limitation and participation restrictions (privacy by design) [271] have been proposed by researchers to preserve this crucial data. But none of the proposed method ensures complete privacy protection, because encryption protocols are computationally complex, and the restriction methods have loophole regarding definition of exact PII. However, differential privacy emerged out to be one of the possible and most viable solution to protect real-time wearable medical devices data. Zhang *et al.* [159] proposed *Re-DPoctor* scheme to provide budget allocation and adaptive sampling using differential privacy. The proposed

strategy satisfies all conditions of differential privacy and reduces mean relative error and mean absolute error of the transmitted data. Moreover, the authors used proportional-integral-plus (PIP) controller and compared utility and privacy trade-off by applying differential privacy over real-time health data. Keeping in view the above discussion, it can be seen that differential privacy can provide a healthy trade-off between privacy and accuracy for real-time health data. As the mathematical models of differential privacy can efficiently be used for data protection by adding desired value of noise, therefore including differential privacy approach in wearable devices can preserve PII to maximum extent. Thus, we can conclude that data perturbation using differential privacy is the most suitable solution, if someone wants to preserve their personal privacy for real-time healthcare and medical systems.

B. E-Health Records

Over the past decade, the trend of hospitals adopting electronic way of storing patient records has increased dramatically [272]. This specific mechanism named as e-health mechanism [273] integrates advanced ICT features, such as electronic storage, and data outsourcing. This health data contains PII, such as date of birth, presence of any specific disease, medical symptoms, weekly or monthly heart rate, blood pressure level, etc. Data stored in PII datasets is extremely sensitive and should not be disclosed to anyone else except the patient and doctor. Typically, these datasets are protected using obscuring or anonymizing methods during data preparation and cleaning. In obscuring, identifiers such as the quasi identifiers, key identifiers, and certain other types of sensitive and personal data identifiers are masked, after that a separate and protected dataset is prepared for mining [274], [275]. However, these cleaned and protected datasets can easily expose certain PII when they are analysed and mixed with different other feature sets [276]. Another valuable scheme used to preserve the confidentiality of e-health data is encryption. In this scheme, the data is protected using public and private generated keys. But the major challenge in encryption is to make sure the confidentiality of encrypted data while allowing query execution over it [152]. Keeping in view all these points, the most suitable scheme that comes up to protect e-health data is differential privacy.

Using differential privacy data perturbation algorithm, one can publicize e-health data for query execution without compromising any sort of privacy [277]. Similarly, majority of differential privacy algorithms do not have high computational complexity. Therefore, differential privacy can be implemented in basic level e-health databases. Furthermore, e-health records purely deal with statistical data preservation because these health records are further used by various organizations and hospitals to enquire and predict about status of patient. Therefore, statistical differential privacy is usually applied to such electronic health records. Researches have been carried out till now in order to implement differential privacy in various e-health databases for query execution. Li *et al.* [151] first developed a heuristic hierarchical query method, and then proposed a private partition algorithm for differential privacy in order to enhance time, overhead and query error. Similarly, the authors in [263] worked over end-to-end differential privacy based deep learning approach to enhance training accuracy and efficiency. The authors proposed a private stochastic gradient descent based deep learning approach that preserves privacy via efficiently perturbing the clinical data. To secure it further, the authors integrated this differential privacy strategy with cryptographic encryption. Authors claimed that their developed mechanism is private, secure, and efficient as it efficiently protects privacy and security along with reducing computational cost. Another work over preserving privacy while enhancing learning accuracy is carried by authors in [262], the authors proposed a differential privacy based data clustering algorithm that works over k-means clustering and protects private data by integrating differential privacy with machine learning. Furthermore, the presented framework operated over Hadoop and efficiently optimize privacy allocation budget along with improving learning accuracy. Similarly, the authors in [264] preserved privacy using Laplacian noise and worked over data partitioning and work load for optimization of error rate of queries. Furthermore, Mohammed *et al.* [152] used the Laplace noise of differential privacy to enhance data privacy by performing experiments over cancer patient's data. The authors reduced the computational overhead by developing a lightweight framework that supports complex data mining tasks and a variety of SQL queries. The field of genomic data record protection is explored by researchers in [163], [265]. In [163], authors preserved the privacy of genomic and distributed clinical data by first encrypting the data and then perturbing it using differential noise mechanism. Furthermore, they worked over informatics for integrating biology and bedside (i2b2) framework, and enhanced its privacy along with reducing the network overhead. Similarly, the authors in [265] also preserved genomic data privacy by using traditional differential privacy approach and two way decryption method to save it from any attacker. The authors enhanced privacy and execution time of i2b2 framework in electronic genomic data records. Moreover, the authors in [266] developed a differentially private aggregation strategy which aggregated health devices data and do also provides timely incentives to its users. The proposed strategy combined differential privacy, Boneh-Goh-Nissim crypto system, and Shamir's secret sharing to enhance both the security and privacy of users. The model is developed using JPBC library of java and it ensures the reduction of computational overhead. Therefore, the proposed strategy is more suitable for health IoT devices that have limited computational capacity. As differential privacy was first designed for statistical databases, therefore the mathematical models of differential privacy perfectly fits healthcare and medical system databases, and this data can easily be secured from intruders using differential privacy perturbation. Keeping in view all the above discussion, we can conclude that differential privacy applied in e-health databases provides a desirable solution to protect privacy during query execution.

C. User Perspective for Health Survey Data Protection

As discussed in the above section, sometime the access of databases is given to certain companies and media cells to conduct surveys or query executions in order to learn more about a particular disease or to solve any specific problem. For instance, medical data and patient symptoms data can be used by mobile recommender systems to suggest a medication having less side effects [278]. Certain therapies can be suggested by recommender system, that matches best with the dispositions of patient [279], [280]. However, these benefits come with a trade-off of privacy. For example, if the query conducting media cell becomes an adversary or get compromised. It can then try to infer in to the personal details of patients, in such cases it is responsibility of data providers to protect users' data before publicising it for any survey. The major question here arises, how to choose correct and desirable level of privacy without compromising over the benefits. The purpose of this section is to provide users' perspective over applying privacy in health domain for their personal data. Especially the perspective of a common person towards privacy-precision trade-off of differential privacy.

In [267], authors analysed the users' perspective over two different privacy preservation schemes; k-anonymity [281], and differential privacy [26]. The authors presented the point of view of common people to give their data towards future health care and for commercial purposes. The experimental results showed that users' perspective towards their confidentially of data was quite strict if the data was about to be given for a commercial use. While the patients showed reluctance while providing the same data for scientific use. Furthermore, people showed various reservations for anonymization strategies because of the examples that privacy can be breached even after anonymization. However, differential privacy seemed suitable for users upon its idea of preserving privacy by data perturbation and by providing a privacy-precision trade-off. But the most confusing question for users was; how exactly data perturbation protects the privacy? Furthermore, users felt comfortable being the part of large crowd while applying differential privacy to their dataset. By keeping in view all these points, we can conclude that differential privacy used with large datasets is fairly optimal strategy to protect data according to users' perspective.

D. Summary and Lessons Learnt

The new wave of modernizing and digitalizing medical devices and records has seen an exponential growth over the past decade and medical devices are being connected with each other and other databases via wireless networks. This replacement of old system to digitalized medical systems has paved the path to several privacy and security issues [282]. The actual concern is that medical devices data contains certain PII, such as name, address, heartrate, blood pressure level, symptoms of any disease, certain medical test outcome, etc. This data can be used by malicious attackers to target a specific person, blackmail them, steal their money, and so on [283]. However, we cannot deny the importance of this digitalized data as well, because doctors and hospitals require this data to overcome any severe consequences within time [282]. Therefore, a certain level of privacy is required by the medical systems to utilize the data efficiently without risking it.

One important application of healthcare and medical systems is real-time data monitoring from certain medical equipment that are used as wearable devices such as smart watches, heart rate sensors, etc. This data contains specific patterns that can be used to judge personal information about any individual. However, this data cannot directly be perturbed because it should be useful for the required observer, e.g., physician, coach, and hospital administration. Certain techniques to protect this data is proposed by researchers, but the most suitable technique to provide efficient results is differential privacy. Differential privacy perturbs the data in such a way that even if any intruders compromises the real-time data, still it will not be able to get the useful information. However, this field is just under consideration and researchers are working to provide efficient ways to protect this real-time data without reducing data efficiency.

Another important application of health care data is data mining for early detection of diseases by viewing symptoms. Query execution is carried out by medical companies or hospitals to know better about early symptoms regarding any disease, or to perform statistical analysis of data. However, protecting the privacy during this query execution is a challenging task. But after the introduction of differential privacy in 2006 for statistical databases, the healthcare and medical data is also being protected using the applications of differential privacy. Still, a lot of work needs to be carried out in future. For instance, the artificially intelligent algorithms are being introduced to provide useful results in health databases without compromising the privacy.

The protection of healthcare and medical systems using differential privacy has been carried out by many scientists and researchers, however a large number of applications of healthcare systems still needs a considerable attention. For instance, introduction of machine learning in healthcare system is the new trend. Similarly, differential privacy can be incorporated with machine learning algorithms in order to ensure complete privacy of health data. Furthermore, the body sensors or wearable devices are becoming smaller in size with passage of time. Therefore, light-weight and less complex differential privacy algorithms are required to fit in to such devices. To sum up, differential privacy is a vital solution for healthcare and medical systems, but still a lot of efforts are required to address all applications of healthcare and medical system.

VI. Differential Privacy in Industrial Internet of Things

The term IoT was first introduced to address unique identifiable interoperable objects connected with a wireless technology named as radio-frequency identification (RFID) [287]. This concept of IoT shifted gradually from RFID to Internet. However, with the rapid advancement of IoT technologies, modern Internet has taken over the world in every aspect. Physical layer of IoT devices are connected with each other using Internet protocol (IP) to form an IoT system [288].

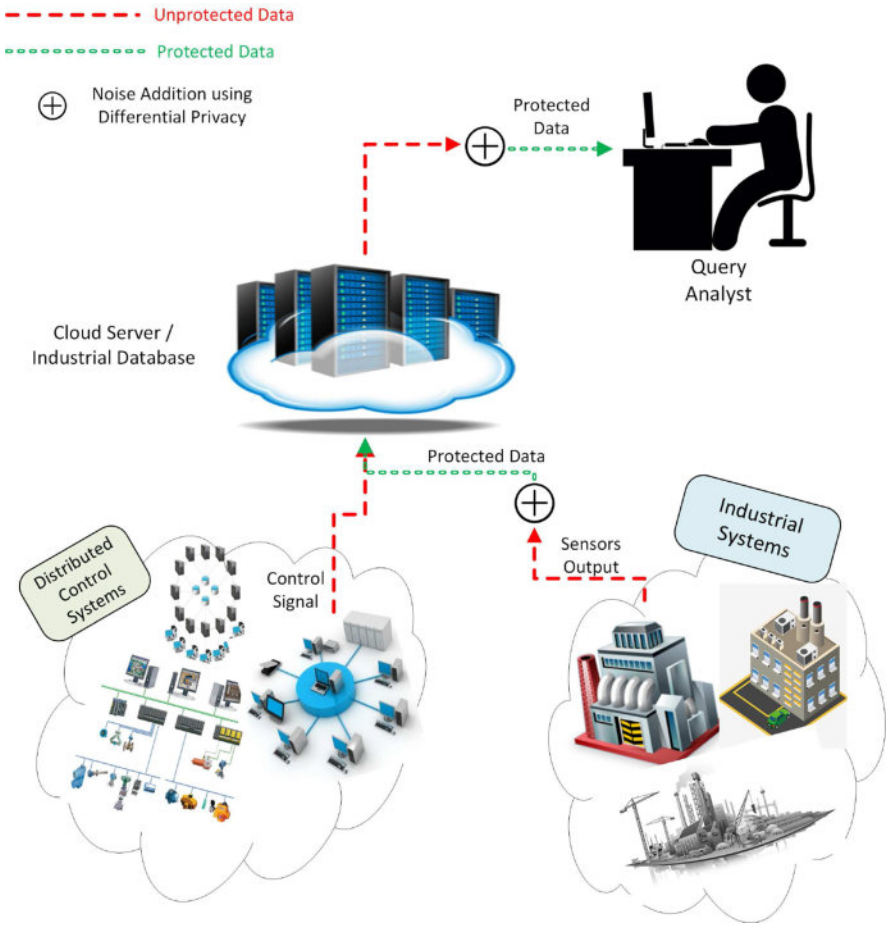

Fig. 11. Illustration of organization of differential privacy (DP) implementation in industrial Internet of thing (IIoT) systems into two scenarios: distributed control, and industrial systems. When DP is incorporated into these scenarios, industrial sensors data and distributed control signals of IIoT systems is protected and the data stored by database can be used for query evaluation.

The trend of using IoT technologies in industries is exponentially increasing because of its effectiveness [289], [290]. However, standard CPSs communication systems does not cope with IIoT systems because modern IIoT systems have certain extra requirements such as hostile environment operation, predictable throughput, maintenance by some other than communication specialists, and extremely low downtown [291]. The two most common IIoT communication systems include Fieldbus, and supervisory control and data acquisition (SCADA) [292]. Large number of projects related to food industry, agriculture, security surveillance, and other similar fields have been conducted using IIoT technologies. As IIoT technologies are being used extensively in a large number of industrial projects, there are various commercial and political interests in it [293]. Because of those interests, the intruders always try to launch targeted attacks to obtain maximum possible data from IIoT systems and databases in order to damage that specific industry.

Keeping in view all these points, it can be said that it is very important to protect the privacy of IIoT systems. A large number of privacy preservation technologies for IoT have been recently discussed in [294]–[297], but most of them focuses over basic IoT systems privacy preservation. However, the privacy of industrial systems differs from that of general IoT systems because critical decisions without time delays needs to be made in IIoT devices. Few researches proposed limit release [298], data distortion [299], and data encryption [300], [301] as a solution to preserve IIoT privacy, but with constant observation it can be seen that their advantages are limited and they cannot be implied broadly over every IIoT system.

Differential privacy is a new standard to preserve the privacy if IIoT systems. Differential privacy defines a detailed attack model, reduces privacy risks for data disclosure, and ensure data availability at same time of query or decision [164], [302]. On the basis of privacy preservation using differential privacy, IIoT systems can be further divided into three subcategories; industrial systems, distributed control systems, and industrial database systems, as illustrated in Fig. 11. In this section, we discuss the implementation of differential privacy in these IIoT systems. The detailed taxonomy of differential privacy implementation in IIoT systems is presented in Table XII and Fig. 12.

A. *Industrial Systems*

The rapid development of ICT technologies also changed the perspective of controlling traditional industrial devices.

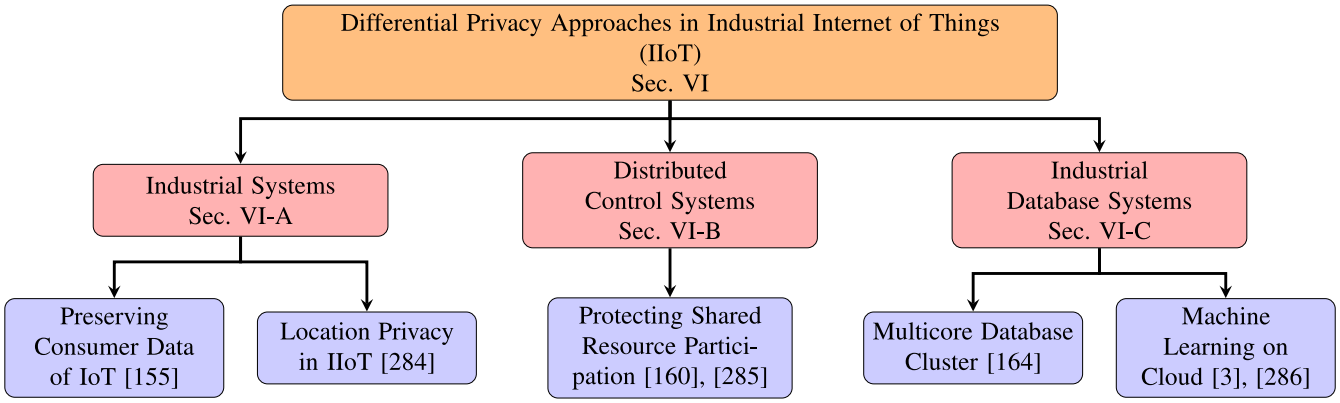

Fig. 12. The differential privacy approaches implemented industrial Internet of things (IIoT) can be classified into industrial systems, distributed control systems, and industrial database systems.

Similarly, merger of IoT, and ICT with traditional industry have revolutionized these systems and a new era of "Fourth Industrial Revolution" is on its way [303]. Modern trends of IoT, and ICT are greatly influencing automation of industrial devices and higher degree of inter-connection among devices is being achieved using these technologies [304]. In industry 4.0, almost every sort of communication will happen via wireless medium, therefore researchers are working over implementation of modern ways of communications (e.g., 5G) in industrial devices and sensors. The communication between these sensors and devices needs to be secured because these sensors and devices generate a large amount of safety-critical and privacy-sensitive data. Safe and secure operation of this data needs to be ensured for smooth running of industry [305]. Generally, the privacy threats of IIoT systems [306] can be classified into two subcategories; based on preserving data and over preserving of location. Traditional approaches used to preserve data and location privacy are anonymity [307] fuzzification technology [284].

However, because of multiple data fusion, and techniques of re-identification of anonymized data, these techniques do not show very considerable outcomes in IIoT system. Therefore, differential privacy appeared as one of the most suitable solution to communicate this data from sensors to required devices without compromising the integrity and privacy. Researches are being carried out over implementation of differential privacy in different scenarios of industrial automation. Similarly, the authors in [155] improved data privacy by implementing differential privacy with k-anonymity. The authors used the traditional concept of differential privacy, integrated it with k-anonymity and enhances anonymization of data, their preserved data can be aggregated and transmitted without risking the privacy component. However, the authors in [284] considered the factor of preserving location of industrial sensors using differential privacy. The authors first demonstrated that extracting location of IIoT sensors can prove to be a serious threat to industry and later on authors provided the solution by merging differential privacy with these sensors. In [284], MATLAB and PyCharm are used to implement tree node accessing frequency model with Laplacian noise perturbation to enhance data utility timeliness. The authors firmly believe, in order to protect location and data privacy of industrial systems, differential privacy is an optimal solution in context of accuracy and timeliness. By keeping in view the above discussion regarding industrial automated systems privacy, and considering the effectiveness of dynamic nature of differential privacy strategies, it can be said that differential privacy can efficiently preserve privacy when applied with industrial systems.

B. Distributed Control Systems

In recent years, the interest in advancement of distributed control systems has increased exponentially in industrial domain [308]. These types of systems involve cooperation of all connected devices in order to take intelligent decisions on the basis of input data. This control is generally achieved using emergent behaviour of various autonomous, simple and cooperative agents/devices [309]. On one hand, the real-time sensing and sharing of this information provides large number of benefits, and on other hand, if any attacker gets access to this information then it can cause serious issues. For instance, halting or even destroying of industrial machines [310]. Therefore, preserving crucial information of modern distributed control systems is very important for their complete implementation in industrial sector. Different approaches to overcome privacy issues of these autonomous distributed control systems have been proposed by researchers such as encryption, and k-anonymity. But the most promising approach to protect the privacy without losing the originality of data of these systems is differential privacy.

In case of linear distributed systems, differential privacy can easily preserve real-time continuously varying data from distributed linear devices by using the metric method presented in [311]. The authors in [160] used this metric based method of differential privacy and perturbed the data using random Laplacian noise. By following this pattern, the authors minimized entropy of system along with increasing the privacy of data being communicated between devices. Similarly, the authors in [285] defined inherent differential privacy for systems based on feedback-control. The authors calculated

TABLE XII
COMPARATIVE VIEW OF DIFFERENTIAL PRIVACY TECHNIQUES IN INDUSTRIAL INTERNET OF THINGS WITH THEIR SPECIFIC TECHNIQUE, OPTIMIZED PARAMETERS, PRIVACY CRITERION, SCENARIO, AND EXPERIMENTAL PLATFORM

Main Category	Ref No.	Year	Privacy Mechanism	Technique of DP Used	Enhancement due to Differential Privacy	Privacy Criterion	Platform Used	Scenario	Time Complexity
Industrial Systems	[155]	2016	Differential privacy for IoT	k-anonymity with traditional differential privacy is used	• Enhanced anonymization	ε-differential privacy	N/A	Real-time	–
	[284]	2017	Location privacy for IIoT using Differential privacy	Tree node accessing frequency model is used with Laplacian noise	• Maximize data utility and timeliness	(ε, δ)-differential privacy	MATLAB and PyCharm	Real-time	–
Distributed Control Systems	[160]	2017	Differential privacy in linear distributed control systems	Randomized Laplacian noise is used in distributed systems data	• Entropy minimization	(ε, Δ)-differential privacy	N/A	Real-time	$O(T^3/N_{\varepsilon^2})$
	[285]	2017	Differential privacy mechanism for feedback control systems	Minimum required Gaussian noise is calculated	• Improved privacy, performance, and attack resiliency	(ε, δ)-differential privacy	N/A	Real-time	–
Industrial Database Systems	[164]	2018	Differential privacy for multicore DB scan clustering (DP-MCDBScan)	Random Laplacian noise is used with data clustering	• Improved efficiency, accuracy and privacy of network data	ε-differential privacy	MATLAB	Statistical Database	–
	[286]	2018	Preserving Multiple data-providers privacy via differential privacy mechanism	Perturbation is added to cipher text after encrypting Laplacian noise	• Multiple-providers data is preserved	ε-differential privacy	MAGMA and Java Simulator	Real-time	–
	[3]	2018	Differential privacy model machine learning mechanism in CPS using prediction model	Machine learning model publishing is used with traditional differential privacy	• Mean absolute error is enhanced	ε-differential privacy	N/A	Real-time	–

the minimum amount of Gaussian noise that is required to ensure privacy of system. Furthermore, the provided mechanism improves performance, privacy, and attack resiliency of system. Both of the proposed methodologies showed that data perturbation technique of differential privacy can preserve this real-time floating data between control devices. Thus, by viewing the nature and privacy requirements of distributed control systems data, we can say that differential privacy provides is the best light-weight approach to preserve real-time data privacy in distributed control systems.

C. Industrial Database Systems

Advances in IoT systems coupled with social networks are providing more intelligent and comprehensive services in our daily life [312]–[315]. These systems generate large proportion of data that is stored usually in cloud servers or databases. Certain functions in these social IoT systems are carried out via predefined interfaces using the stored big data [316]–[318]. The data is continuously being shared between clients and servers, and during this process, any information can be leaked if the data is not preserved properly. This in return can generate huge security and privacy threats to the databases of all social systems, because the individual privacy can easily be compromised during communication and query evaluation [9]. Large number of current researches proposed cryptographic encryption to preserve the privacy of social IoT systems [13], [15]. However, certain number of keys needs to be maintained in cryptographic schemes that makes it impossible to implement in databases where data needs to be shared with public or query evaluation. To overcome these issues, Dwork proposed the idea of differential privacy for statistical database [26]. Nevertheless, because of advancements in machine learning algorithms and multiple query releases in datasets, the traditional differential privacy cannot be used in social IoT systems [319].

In order to tackle the problems of traditional differential privacy approaches in social IoT systems, many researchers proposed different ways to overcome it. In [164], Ni *et al.* proposed a powerful differential privacy approach using the combination of random Laplacian noise and data clustering technology using MATLAB simulator. Furthermore, as compared to traditional privacy protection approaches, the authors improved efficiency, accuracy, and overall network data privacy. A step ahead of the pack, the authors in [286] proposed a scheme to preserve multiple data-providers privacy using differential privacy. Instead of data providers, the noise is added via cloud server in this scheme. To further preserve confidentiality, the authors also encrypted the data using double decryption algorithm in combination with differential privacy. Zhu *et al.* [3] worked over implementation of machine learning

along with differential privacy for efficient query evaluation. The authors reduced mean absolute error and preserved privacy of data using prediction model. To sum up, databases of social IoT systems needs to be preserved from cyber-attacks. Therefore, modern differential privacy approaches provide efficient privacy protection from all vulnerabilities along with enhanced query evaluation and providing support for machine learning algorithms.

D. Summary and Lessons Learnt

The development of IoT technology has paved paths for many future applications, one of the most important among them is the involvement of IoT in industry. Modern industrial devices are equipped with sensors that are communicating with each other in real-time to take crucial control decisions. However, leakage of this real-time information can cause severe privacy threats to the machinery or individuals associated with it [320]. For instance, an unmanned steel mill was halted and destroyed using cyber-attacks in Germany by disrupting and manipulating the control mechanism [310]. Therefore, a certain privacy level for IIoT systems is required in order to operate smoothly. Industrial systems are one of the major aspects of IIoT, these systems include large industrial machines that are communicating with each other using sensors in real-time. With the introduction of fourth generation of industry, these systems are developing very rapidly, and a large amount of data is being transmitted every second from one device to another. However, protecting the privacy of these real-time systems by focusing on data and location privacy of these sensors and devices is the actual challenge at the moment [321]. Differential privacy came out as an optimal solution to protect the privacy up to a certain extent without compromising the usefulness of data. Till now, differential privacy preserved the data integrity during data aggregation and data transmission of industrial systems. Nevertheless, a large of fields of industrial systems still needs to be preserved. For example, extensive efforts are required to secure the industrial and offices automation control.

Another important application similar to industrial systems is distributed control systems. In these systems, intelligent decision is taken on the basis of feedback or input data. Therefore, this input data needs to be protected before transmitting it to system, because if any intruders gets access to the input or feedback then disastrous results can be seen. For example, in Iran in 2008, a centrifuge is sabotages at a uranium enrichment plant [310]. Therefore, preserving input privacy is very crucial for such systems. Several techniques related to differential privacy have been presented by researchers to protect privacy without losing the originality of data. However, certain fields such as handling of big data of such systems still needs to be explored. Similarly, finding the most efficient trade-off between accuracy and privacy is also a challenge for industrial researchers.

Furthermore, the crucial data of IIoT systems is usually stored in cloud or large databases. These databases holders usually allow companies to perform query execution over them in order to conduct surveys and other statistical tasks. However, if the company or utility becomes a hacker then the sensitive data of users can be leaked. For instance, the database of any social network contains a large amount of personal information whose privacy needs to be ensured before allowing companies to perform query execution. To cope up with this privacy challenge, data scientists apply data perturbation using differential privacy in these databases before allowing any company to perform query evaluation. This data perturbation allows different companies to execute query evaluation without risking users' data. Although, there are many fields that still needs to be explored by researchers. One important application is the implementation of privacy protection in data mining and machine learning systems to make the artificially intelligent systems more secure. Another future domain to protect is buying/auction of industrial products. For example, buyers do not want to disclose their identity to sellers and similarly sellers do not want to disclose their identity to buyers. To sum up, differential privacy actively played the role to protect privacy of industrial systems. However, certain number of domains still needs to be protected and efforts needs to be made over these domains to make secure and reliable further generation IIoT systems.

VII. Open Issues, Challenges, and Future Research Directions

Currently, differential privacy implementation in cyber physical systems is facing a large number of challenges, because of dynamic nature of CPSs. In this section, we discuss few challenges, open issues, and future research directions for implementation of differential privacy in CPSs.

A. Energy Systems Issues and Research Directions

Smart grid is the future of energy systems, because it incorporates capabilities of both; traditional energy systems and modern information and communication technologies. However, there are certain applications of smart grid that still need considerable attention in context of user privacy. In this section, we discuss such applications of smart grid in which differential privacy can improve the privacy preservation in an exceptional way.

1) Billing With Dynamic Pricing: One of the biggest benefit of smart metering is accurate calculation of bills within a dynamic pricing environment [322]. This pricing strategy requires detailed energy consumption information, which on other hand may leak private information of smart meter users. Therefore, implementing differential privacy along with accurate dynamic pricing billing is a challenge for researchers. In recent year, many researches focused over dynamic private billing using differential privacy protection [323]. The trade-off between accuracy and privacy of real-time data reporting is the biggest hurdle in implementation of differential privacy in smart meters. Many researchers are working and developing efficient algorithms to overcome this trade-off to a maximum level. Still, there is a large room that requires to be filled in order to preserve privacy along with dynamic consumption reporting for dynamic billing.

2) Auction of Micro-Grid Energy Resources: The demand of renewable energy is increasing due to rising costs of traditional fossil fuel based energy. Most of these energy resources such as small wind turbines, and solar panels will be deployed in smart homes [133]. Energy consumption of each house is different, therefore, some smart homes may use all their produced energy while others may still have excessive energy left that is not of their use. Smart homes can then auction this excessive energy to other buyers, they can auction this energy and buyers purchase it according to their need [324]. However, during this process, buyer and seller usually do not want to disclose their identity to each other. Therefore, preservation of this information is very crucial for smooth running of auction mechanism in smart grid [187]. Few proposed researches considered micro-grid in EV scenario, but the specific application of auction in RERs based smart home is still not addressed in the literature. In order to secure this mechanism, techniques of differential privacy need to be proposed.

3) Firmware Updates: Smart meters usually operate over an installed firmware that determines every functionality of them. Generally, this firmware is developed by smart meter vendors who usually update them to improve functionality or to remove any detected bug. Similarly, utility companies sometimes do also require firmware updates in case of any change among pricing or laws [324]. Since the firmware update file is proprietary, therefore it needs to be communicated to smart meters in a secure and private manner. Furthermore, sometimes update is required for only certain group of smart meters instead of all, in which utility requires case access control. However, to protect this firmware file, certain security and privacy based mechanisms are required. Till now, researchers only proposed security based approaches to overcome this problem. However, privacy requirement cannot be neglected in this application. We believe that incorporation of differential privacy scheme with other security schemes such as encryption can provide optimal results in this scenario.

4) Resource Constrained Micro-Grids: In order to get a cost-effective supply and power management alternative in remote areas, micro-grid resource constrained architectures are the optimal solution [325]. To minimize operational cost, certain lossy networks are used to carry out communication between these resource constrained architectures. However, these lossy networks are prone to many adversaries and privacy attacks because of their unreliable nature [326]. This loss of privacy can provoke various crimes, such as energy theft etc. Existing data preservation strategies cannot directly be applied to these lossy networks because these algorithms do not cope-up with cost requirements in rural areas. As per our point of view, light-weight differential privacy can mitigate these privacy risks and provide a larger control over power management, distribution and anonymization [326]. Therefore, researches need to carry out in privacy preservation of resource constrained micro-grids using differential privacy techniques.

B. Transportation Systems Issues and Research Directions

Smart transportation system is the need of a smart city. Therefore, governments are trying to improve the quality of transportation systems day by day. Along with the enhancement in quality and rapid communication between vehicles, certain security and privacy issues arises that need to be tackled along with quality enhancement. In this section, we discuss two major applications that require considerable attention in context of privacy preservation.

1) Live Traffic Information: In order to overcome delays due to congestion, live traffic information is generally used by route planning applications [327]. These applications consider live feed from connected cars, connected mobile devices, smart signals, and public transport to plan the shortest and less congested path for drivers. This is an advantageous feature that saves time of drivers, but on the other side of coin, it can cause serious threats to location privacy of connected devices and cars. If the network is unprotected, then any intruder can hack the system of these applications and may have access to the live location tracking of connected cars. Therefore, it is important to protect location privacy before reporting it to route planning applications. Differential privacy can provide real-time location privacy by perturbing location or identity in order to preserve drivers' privacy. Therefore, this field of ITSs has a lot potential and it needs to be explored in future.

2) Vehicle-to-Vehicle (V2V) Communication: With the exponential development of wireless communication technologies, vehicular ad-hoc networks, and V2V communication have become progressively popular. Certain services such as VoIP, Web browsing, and video conferencing have been carried out with help of these networks and V2V communication [328]. In recent years, certain privacy and security issues of V2V communication has arisen. These issues have attracted attention from both academia and industries. Encryption is considered to be the most famous strategy to secure communication between two vehicles, but it also comes with certain faults and loopholes. Therefore, in order to preserve privacy in communication among two vehicles, differential privacy can be an optimal solution. Future researches should consider integrating differential privacy with different V2V communication scenarios.

C. Healthcare and Medical Systems Issues and Research Directions

The trend of connecting cyber and physical worlds in healthcare and medical system has increased tremendously. However, this connection comes up with certain issues that needs to be resolved before its successful implementation in daily lives. In this section, we discuss few applications of healthcare systems in which differential privacy can be applied to get advantageous results.

1) Body Sensors Data: With the advancement in wireless technologies, the trend of using body sensors for medical purposes is also increasing dramatically. These sensors (i.e., heart rate sensor, and body temperature sensors) monitor your real-time readings and report them to your physician or trainer [329]. Although, this information cannot directly be transmitted to required person without protecting it from adversaries. Encryption is one of the solution for this type of

application, but it is computationally complex. On the other hand, differential privacy based real-time reporting of data can be a light weight solution to solve this particular problem. The technique presented by Zhang *et al.* [159] is a great step towards implementing differential privacy in real-time health data sensing and reporting. Still this field has a lot of room and needs to be explored further. For instance, the real challenge is implementing differential privacy noise addition mechanism in low memory devices such as small micro-controllers. We believe that modern differential privacy algorithms can enhance this field and can produce optimal results in real-time health data reporting.

2) Elderly Home Sensor Network: Retirement homes or elderly homes do also need considerable attention because the people living in there require full time care and attention. Therefore, many healthcare devices are placed in these homes for monitoring and diagnostic purposes [330]. However, along with monitoring, these devices also need considerable privacy protection, because even a small loophole in privacy can cause severe circumstances [331]. The whole elderly home network can be protected using differential privacy techniques in the devices. The potential applications of differential privacy in elderly homes can be protecting electronic patient records [332], that contains all useful information, identity, and medical records of people living in that home.

D. Industrial Internet of Things Systems Issues and Research Directions

The advancements in industry is highly influenced by modern IoT technologies. As IoT is taking over industry by providing autonomous control, efficient data storage, and reliable communication, although it also comes up with risk of attacks related to security and privacy of industry. Few past events occurred in industries showed that these advanced technologies can be targeted, hackers can get access to private industrial data. These malicious adversaries can also control machinery or can even destroy industrial systems. Therefore, certain IIoT fields need to be secured first for smooth running of IoT systems in industry.

1) Industrial Big Data Trading (Auction): One major issue in applications of big data in industry is to handle auction of products or services. Trusted third-party platforms are generally used to carry out auction between buyer and seller. However, fully trusting third party platform is difficult because of many reasons, including insider adversaries, cyber threats, and platform insecurities [333]. We believe that, in order to address this issue of privacy protection in third-party platforms, differential privacy is a suitable solution. Because of strong mathematical modelling background, differential privacy can provide a desirable level of privacy in auction scenario of big data in industries.

E. Other Issues and Research Directions

1) Big Data: The horizon of big data is not only limited to CPSs, this covers almost every aspect of human life ranging from schools to offices and from farming to industry. In this section, we will be discussing particularly about some future directions and challenges regarding implementation of differential privacy in certain big data applications. We believe that as the data is increasing, differential privacy based algorithms are also becoming advanced and more responsive. However, there are certain challenges that still need to be addressed for big data.

a) Intuitive privacy definition: In context of differential privacy itself, one of the major challenge is defining the exact privacy. Even after establishing of mathematical proofs and strict privacy model, differential privacy lacks in giving an intuitive definition of privacy according to big data. Thus, finding a more intuitive definition of privacy in accordance with big data analytics is still a challenge for data scientists [19].

b) Composition theorem: As we discussed earlier (see Section II-B2), that composition theorem plays an active role in designing of algorithm, and allocation of privacy budget. However, existing methods of deciding privacy budget using composition theorem are not optimal [334]. Therefore, optimal computation of composition of differential privacy in big data analytics is still an unsolved challenge. Similarly, in the domain of big data, maintaining privacy protection along with issue of dimensionality because of large data volume and computation overhead is a big challenge for researchers [335], [336].

In context of future research directions, few novel approaches based on the principal of differential privacy such as local privacy [337], concentrated privacy [338], w-event privacy [339], and Bayesian differential privacy [101] have very large scope in big data applications. For instance, dealing with time-series data publishing, w-event privacy provides an optimal balance between *event-level* and *user-level* privacy [340]. As for future work, researches should focus on handling the privacy for large data volumes and designing of optimal privacy budget for different notions of differential privacy.

2) Machine Learning: The actual purpose of any machine learning algorithm is to extract beneficial information from given data. However, preserving individual privacy along with extracting data is one of the most challenging task of future machine learning algorithms [341]. For example, if one is analysing sensitive medical data, then first it needs to be made sure privacy is preserved properly, and query evaluation can be performed [342]. To tackle this issue, researchers have started working over merging differential privacy data perturbation technique with machine learning algorithms [35], [343], [344]. Future research directions in this field needs to examine the merger of efficient differential privacy data preservation techniques with complex machine learning algorithms.

3) Cloud Computing: Huge amount of data generated through ubiquitous communication among smart devices paved the path towards a reliable and secure storage named as cloud computing [345]–[347]. Furthermore, cloud computing emerged as a new computing paradigm and business model that enables on-demand supply of storage and computational resources. However, outsourcing this data to any third party can cause certain privacy issues [348]. These

privacy risks are generally caused due to information redundancy in big data from different sources, multi-tenancy, and ubiquitous access features of platforms of cloud computing [349]. Traditional method of protecting cloud privacy is to store encrypted data over cloud platform, and data owners must download and decrypt the data locally to be sent for processing [350]. However, with the increase in size of data, it is becoming hard for data owners to afford this computationally complex approach [351]. Differential privacy is now emerging as a new practical approach to overcome these privacy issues of cloud computing scenario. Researchers have started work towards privacy preservation of cloud computing data using differential privacy. Privacy of certain cloud applications such as big graphs [351], multi-agent programs [352], blockchain-based cloud [353], and scalable processing platforms [349] have been enhanced via modern differential privacy algorithms. We believe that this field has a large potential and light-weight differential privacy algorithms can revolutionize privacy standards of cloud computing.

4) Wireless Edge Computing: Along with increase in smart devices, edge computing has now become a mainstream while dealing with wireless communication scenario. Wireless edge computing provides broad benefits according to aspects of mining and analysing data, and intelligently perceiving the information of location [354]. These wireless edge computing networks contain large amount of private data that cannot be sent directly for data prediction and processing. Therefore, protecting important features of wireless edge computing needs to be made sure before any sort of query evaluation. In order to tackle this situation, researchers are proposing differential privacy based strategies as an optimal solution [355], [356]. Keeping in view all this discussion, it can be said that modern differential privacy algorithms can enhance wireless edge computing, and these algorithms should be explored and presented in future.

5) Blockchain Technology: In the past few years, blockchain emerged as one of the novel distributed strategy that allows the secure storage of transactions, or any other type of data without need of any predefined centralized data authority [357], [358]. The notion of blockchain was tightly coupled with Bitcoin for some time, but now it has been adopted widely in many applications, e.g., healthcare, finances, and logistics [359]–[361]. The feature of public accessibility without any centralized authority made it famous among its users, but on the other hand it also raised certain security and privacy issues in it. Because of inadequacy of existing blockchain protocols [362], most of the blockchain users are worried about their transaction privacy. To overcome this issue, researchers are proposing certain privacy schemes on the basis of identity, anonymity, and perturbation [363]–[365]. Researchers are enhancing data perturbation strategies by making them artificially intelligent using machine learning algorithm. We believe that, modern differential privacy algorithms in conjunction with blockchain can eradicate the issue of privacy loss even in case of public query evaluation. Because of mathematical background and light-weight privacy model, differential privacy can preserve transactions and other data storage in blockchain technology. Therefore, researchers should focus on integration of these two modern world technologies to achieve efficient results.

6) Game Theory: Game theory addresses issues in which multiple participants compete with each other having contradictory goals or incentives [322], [366]. Similarly, in order to enhance administrators' decision making, game theory can be used to analyse large number of possible scenarios before taking the most appropriate action such as smart grid energy trading [367]. Security and privacy is also an important aspect of game theory algorithms. As we discussed earlier in context of differential privacy, that trade-off between privacy and utility is a critical issue being considered at the moment (see Section II-B1). This trade-off between privacy and utility is being evolved further into a game problem. Researchers have now started developing modern differential privacy approaches by efficiently handling utility-privacy trade-off with help of game theory based algorithms [368], [369]. We believe that game theory based differential privacy techniques can be used to handle privacy of certain differential privacy and CPSs applications. Therefore, researches in this field need to be carried out in future.

VIII. Conclusion

With the advancement in information and communication technologies (ICT), cyber physical systems (CPSs) have become an essential part of our lives, ranging from our homes to industries and from offices to hospitals. However, this advancement comes up with certain security and privacy risks attached to it. Various privacy attacks are carried out in CPSs to access critical data or information from private or public datasets. One of the most optimal solution to overcome these privacy hazards is preserving data by noise addition using differential privacy perturbation mechanisms. In this article, we have presented a detailed and up-to-date survey of implementation of differential privacy techniques in various CPSs applications. We have comprehensively covered all dimensions and aspects of differential privacy implementation in major CPSs domains. Integration of differential privacy in four application scenarios of CPSs, named as energy systems, transportation systems, healthcare and medical systems, and industrial systems is presented in the paper. Within energy systems, we surveyed privacy protection of demand response data, real-time data, and fog computing communication systems using differential privacy. Similarly, in transportation systems, we covered the aspect of privacy preservation with help of differential privacy in railway networks, vehicular networks, and automotive manufactures databases. Moreover, in healthcare and medical systems, we surveyed differential privacy approaches in real-time health data, and e-health databases. Furthermore, according to industrial point of view, we presented implementation of differential privacy techniques in industrial, distributed control systems, and industrial database systems. We then concluded the survey article by highlighting challenges, open issues, and future research directions in differential privacy techniques for CPSs.

REFERENCES

[1] C. Yu, S. Jing, and X. Li, "An architecture of cyber physical system based on service," in *Proc. IEEE Int. Conf. Comput. Sci. Service Syst. (CSSS)*, Nanjing, China, 2012, pp. 1409–1412.

[2] E. A. Lee, "Cyber physical systems: Design challenges," in *Proc. 11th IEEE Symp. Object Orient. Real Time Distrib. Comput. (ISORC)*, Orlando, FL, USA, 2008, pp. 363–369.

[3] T. Zhu, P. Xiong, G. Li, W. Zhou, and P. S. Yu, "Differentially private model publishing in cyber physical systems," *Future Gener. Comput. Syst.*, to be published.

[4] J. Shi, J. Wan, H. Yan, and H. Suo, "A survey of cyber-physical systems," in *Proc. IEEE Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Nanjing, China, 2011, pp. 1–6.

[5] J. Giraldo, E. Sarkar, A. A. Cardenas, M. Maniatakos, and M. Kantarcioglu, "Security and privacy in cyber-physical systems: A survey of surveys," *IEEE Des. Test.*, vol. 34, no. 4, pp. 7–17, Aug. 2017.

[6] Q. Xu, P. Ren, H. Song, and Q. Du, "Security-aware waveforms for enhancing wireless communications privacy in cyber-physical systems via multipath receptions," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1924–1933, Dec. 2017.

[7] M. Gowtham and S. S. Ahila, "Privacy enhanced data communication protocol for wireless body area network," in *Proc. 4th IEEE Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, 2017, pp. 1–5.

[8] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 51–58, Feb. 2010.

[9] Z. Wang, H. Chen, Q. Cao, H. Qi, Z. Wang, and Q. Wang, "Achieving location error tolerant barrier coverage for wireless sensor networks," *Comput. Netw.*, vol. 112, pp. 314–328, Jan. 2017.

[10] P. Barbosa, A. Brito, and H. Almeida, "A technique to provide differential privacy for appliance usage in smart metering," *Inf. Sci.*, vols. 370–371, pp. 355–367, Nov. 2016.

[11] T. Wang, Z. Zheng, M. H. Rehmani, S. Yao, and Z. Huo, "Privacy preservation in big data from the communication perspective—A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 753–778, 1st Quart., 2019.

[12] Y. Shen and H. Jin, "Privacy-preserving personalized recommendation: An instance-based approach via differential privacy," in *Proc. IEEE Int. Conf. Data Min. (ICDM)*, Shenzhen, China, 2014, pp. 540–549.

[13] L. Chen *et al.*, "Robustness, security and privacy in location-based services for future IoT: A survey," *IEEE Access*, vol. 5, pp. 8956–8977, 2017.

[14] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. H. G. Wang, and S. W. Baik, "Secure surveillance framework for IoT systems using probabilistic image encryption," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3679–3689, Aug. 2018.

[15] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang, and J. Han, "When intrusion detection meets blockchain technology: A review," *IEEE Access*, vol. 6, pp. 10179–10188, 2018.

[16] L. Sweeney, "k-anonymity: A model for protecting privacy," *Int. J. Uncertainty Fuzziness Knowl. Based Syst.*, vol. 10, no. 5, pp. 557–570, 2002.

[17] C. Dwork, "A firm foundation for private data analysis," *Commun. ACM*, vol. 54, no. 1, pp. 86–95, 2011.

[18] R. Lu, H. Zhu, X. Liu, J. K. Liu, and J. Shao, "Toward efficient and privacy-preserving computing in big data era," *IEEE Netw.*, vol. 28, no. 4, pp. 46–50, Jul./Aug. 2014.

[19] X. Yang, T. Wang, X. Ren, and W. Yu, "Survey on improving data utility in differentially private sequential data publishing," *IEEE Trans. Big Data*, to be published.

[20] Y. Cao, M. Yoshikawa, Y. Xiao, and L. Xiong, "Quantifying differential privacy in continuous data release under temporal correlations," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 7, pp. 1281–1295, Jul. 2019.

[21] K.-A. Shim, "A survey of public-key cryptographic primitives in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 577–601, 1st Quart., 2016.

[22] K. Apostol, *Brute-force Attack*. 2012.

[23] M. E. Skarkala, M. Maragoudakis, S. Gritzalis, L. Mitrou, H. Toivonen, and P. Moen, "Privacy preservation by k-anonymization of weighted social networks," in *Proc. IEEE Comput. Soc. Int. Conf. Adv. Soc. Netw. Anal. Min. (ASONAM)*, 2012, pp. 423–428.

[24] Y.-A. De Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: The privacy bounds of human mobility," *Sci. Rep.*, vol. 3, p. 1376, Mar. 2013.

[25] Y.-A. De Montjoye, L. Radaelli, V. K. Singh, and A. Pentland, "Unique in the shopping mall: On the reidentifiability of credit card metadata," *Science*, vol. 347, no. 6221, pp. 536–539, 2015.

[26] C. Dwork, "Differential privacy," in *Proc. 33rd Int. Conf. Automata Lang. Program. (ICALP) Vol. II*, 2006, pp. 1–12.

[27] L. Wasserman and S. Zhou, "A statistical framework for differential privacy," *J. Amer. Stat. Assoc.*, vol. 105, no. 489, pp. 375–389, 2010.

[28] N. Li, W. Qardaji, D. Su, Y. Wu, and W. Yang, "Membership privacy: A unifying framework for privacy definitions," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, Berlin, Germany, 2013, pp. 889–900.

[29] J. Lee and C. Clifton, "Differential identifiability," in *Proc. 18th ACM SIGKDD Int. Conf. Knowl. Disc. Data Min.*, Beijing, China, 2012, pp. 1041–1049.

[30] T. Zhu, G. Li, W. Zhou, and P. S. Yu, *Preliminary of Differential Privacy*. Cham, Switzerland: Springer Int., 2017, pp. 7–16. [Online]. Available: https://doi.org/10.1007/978-3-319-62004-6_2

[31] H. Zhang, Y. Shu, P. Cheng, and J. Chen, "Privacy and performance trade-off in cyber-physical systems," *IEEE Netw.*, vol. 30, no. 2, pp. 62–66, Mar./Apr. 2016.

[32] E. Zheleva and L. Getoor, "Privacy in social networks: A survey," in *Social Network Data Analytics*. Boston, MA, USA: Springer, 2011, pp. 277–306.

[33] C. Task and C. Clifton, "What should we protect? Defining differential privacy for social network analysis," in *State of the Art Applications of Social Network Analysis*. Cham, Switzerland: Springer, 2014, pp. 139–161.

[34] I. Gazeau, D. Miller, and C. Palamidessi, "Preserving differential privacy under finite-precision semantics," *Theor. Comput. Sci.*, vol. 655, pp. 92–108, Dec. 2016.

[35] Z. Ji, Z. C. Lipton, and C. Elkan, "Differential privacy and machine learning: A survey and review," *arXiv preprint arXiv:1412.7584*, 2014.

[36] K. Xu and Z. Yan, "Privacy protection in mobile recommender systems: A survey," in *Proc. Int. Conf. Security Privacy Anonymity Comput. Commun. Stor.*, 2016, pp. 305–318.

[37] C. Dwork, "Differential privacy: A survey of results," in *Proc. Int. Conf. Theory Appl. Models Comput.*, 2008, pp. 1–19.

[38] K. Ligett and A. Roth, "Take it or leave it: Running a survey when privacy comes at a cost," in *Proc. Int. Workshop Internet Netw. Econ.*, 2012, pp. 378–391.

[39] S. Vadhan, "The complexity of differential privacy," in *Tutorials on the Foundations of Cryptography*. Cham, Switzerland: Springer, 2017, pp. 347–450.

[40] X. Yao, X. Zhou, and J. Ma, "Differential privacy of big data: An overview," in *Proc. IEEE 2nd Int. Conf. Big Data Security Cloud (BigDataSecurity)*, New York, NY, USA, 2016, pp. 7–12.

[41] S. Yu, "Big privacy: Challenges and opportunities of privacy study in the age of big data," *IEEE Access*, vol. 4, pp. 2751–2763, 2016.

[42] T. Zhu, G. Li, W. Zhou, and P. S. Yu, "Differentially private data publishing and analysis: A survey," *IEEE Trans. Knowl. Data Eng.*, vol. 29, no. 8, pp. 1619–1638, Aug. 2017.

[43] S. H. Begum and F. Nausheen, "A comparative analysis of differential privacy vs other privacy mechanisms for big data," in *Proc. IEEE 2nd Int. Conf. Inventive Syst. Control (ICISC)*, 2018, pp. 512–516.

[44] P. Jain, M. Gyanchandani, and N. Khare, "Differential privacy: Its technological prescriptive using big data," *J. Big Data*, vol. 5, no. 1, p. 15, 2018.

[45] J. Zhao, Y. Chen, and W. Zhang, "Differential privacy preservation in deep learning: Challenges, opportunities and solutions," *IEEE Access*, vol. 7, pp. 48901–48911, 2019.

[46] D. Desfontaines and B. Pejó, "SoK: Differential privacies," *arXiv preprint arXiv:1906.01337*, 2019.

[47] D. Lv and S. Zhu, "Achieving correlated differential privacy of big data publication," *Comput. Security*, vol. 82, pp. 184–195, May 2019.

[48] D. Agrawal and D. Kesdogan, "Measuring anonymity: The disclosure attack," *IEEE Security Privacy*, vol. 1, no. 6, pp. 27–34, Nov./Dec. 2003.

[49] R. Boussada, M. E. Elhdhili, and L. A. Saidane, "A survey on privacy: Terminology, mechanisms and attacks," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Agadir, Morocco, 2016, pp. 1–7.

[50] S. Gambs, M.-O. Killijian, and M. N. del Prado Cortez, "De-anonymization attack on geolocated data," *J. Comput. Syst. Sci.*, vol. 80, no. 8, pp. 1597–1614, 2014.

[51] G. Danezis, "Statistical disclosure attacks," in *Proc. IFIP Int. Inf. Security Conf.*, 2003, pp. 421–426.

[52] X. Zhou, S. D. Wolthusen, C. Busch, and A. Kuijper, "Feature correlation attack on biometric privacy protection schemes," in *Proc. IEEE 5th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. (IIH-MSP)*, Kyoto, Japan, 2009, pp. 1061–1065.

[53] F. Li, B. Luo, P. Liu, A. C. Squicciarini, D. Lee, and C.-H. Chu, "Defending against attribute-correlation attacks in privacy-aware information brokering," in *Proc. Int. Conf. Collaborative Comput. Netw. Appl. Worksharing*, 2008, pp. 100–112.

[54] B. C. M. Fung, K. Wang, R. Chen, and P. S. Yu, "Privacy-preserving data publishing: A survey of recent developments," *ACM Comput. Surveys*, vol. 42, no. 4, pp. 1–53, Jun. 2010.

[55] F. McSherry and K. Talwar, "Mechanism design via differential privacy," in *Proc. 48th Annu. IEEE Symp. Found. Comput. Sci. (FOCS)*, Providence, RI, USA, 2007, pp. 94–103.

[56] F. Liu, "Generalized Gaussian mechanism for differential privacy," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 4, pp. 747–756, Apr. 2019.

[57] Q. Geng and P. Viswanath, "The optimal noise-adding mechanism in differential privacy," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 925–951, Feb. 2016.

[58] F. Eigner, A. Kate, M. Maffei, F. Pampaloni, and I. Pryvalov, "Differentially private data aggregation with optimal utility," in *Proc. 30th ACM Annu. Comput. Security Appl. Conf.*, New Orleans, LA, USA, 2014, pp. 316–325.

[59] Q. Geng and P. Viswanath, "The optimal mechanism in differential privacy," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Honolulu, HI, USA, 2014, pp. 2371–2375.

[60] J. Soria-Comas and J. Domingo-Ferrer, "Optimal data-independent noise for differential privacy," *Inf. Sci.*, vol. 250, pp. 200–214, Nov. 2013.

[61] A. Ghosh, T. Roughgarden, and M. Sundararajan, "Universally utility-maximizing privacy mechanisms," *SIAM J. Comput.*, vol. 41, no. 6, pp. 1673–1693, 2012.

[62] M. Gupte and M. Sundararajan, "Universally optimal privacy mechanisms for minimax agents," in *Proc. 29th ACM SIGMOD-SIGACT-SIGART Symp. Principles Database Syst.*, Indianapolis, IN, USA, 2010, pp. 135–146.

[63] T. Zhu, P. Xiong, G. Li, and W. Zhou, "Correlated differential privacy: Hiding information in non-IID data set," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 2, pp. 229–242, Feb. 2015.

[64] Y. Xiao and L. Xiong, "Protecting locations with differential privacy under temporal correlations," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Security*, Denver, CO, USA, 2015, pp. 1298–1309.

[65] G. Kellaris and S. Papadopoulos, "Practical differential privacy via grouping and smoothing," *Proc. VLDB Endow.*, vol. 6, no. 5, pp. 301–312, 2013.

[66] X. Xiao, G. Bender, M. Hay, and J. Gehrke, "iReduct: Differential privacy with reduced relative errors," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, Athens, Greece, 2011, pp. 229–240.

[67] K. Nissim, S. Raskhodnikova, and A. Smith, "Smooth sensitivity and sampling in private data analysis," in *Proc. 39th Annu. ACM Symp. Theory Comput.*, San Diego, CA, USA, 2007, pp. 75–84.

[68] W.-Y. Day and N. Li, "Differentially private publishing of high-dimensional data using sensitivity control," in *Proc. 10th ACM Symp. Inf. Comput. Commun. Security*, 2015, pp. 451–462.

[69] A. Inan, M. E. Gursoy, and Y. Saygin, "Sensitivity analysis for non-interactive differential privacy: Bounds and efficient algorithms," *IEEE Trans. Depend. Secure Comput.*, to be published.

[70] G. Cormode, C. Procopiuc, D. Srivastava, E. Shen, and T. Yu, "Differentially private spatial decompositions," in *Proc. IEEE 28th Int. Conf. Data Eng. (ICDE)*, 2012, pp. 20–31.

[71] G. Acs, C. Castelluccia, and R. Chen, "Differentially private histogram publishing through lossy compression," in *Proc. IEEE 12th Int. Conf. Data Min.*, Brussels, Belgium, 2012, pp. 1–10.

[72] X. Xiao, G. Wang, and J. Gehrke, "Differential privacy via wavelet transforms," *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 8, pp. 1200–1214, Aug. 2011.

[73] Y. D. Li, Z. Zhang, M. Winslett, and Y. Yang, "Compressive mechanism: Utilizing sparse representation in differential privacy," in *Proc. 10th Annu. ACM Workshop Privacy Electron. Soc.*, Chicago, IL, USA, 2011, pp. 177–182.

[74] V. Rastogi and S. Nath, "Differentially private aggregation of distributed time-series with transformation and encryption," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, Indianapolis, IN, USA, 2010, pp. 735–746.

[75] S. Papadimitriou, F. Li, G. Kollios, and P. S. Yu, "Time series compressibility and privacy," in *Proc. 33rd Int. Conf. Very Large Data Bases*, Vienna, Austria, 2007, pp. 459–470.

[76] X. Yang, X. Ren, J. Lin, and W. Yu, "On binary decomposition based privacy-preserving aggregation schemes in real-time monitoring systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 10, pp. 2967–2983, Oct. 2016.

[77] J. Hua, Y. Gao, and S. Zhong, "Differentially private publication of general time-serial trajectory data," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, 2015, pp. 549–557.

[78] W. Qardaji, W. Yang, and N. Li, "Differentially private grids for geospatial data," in *Proc. IEEE 29th Int. Conf. Data Eng. (ICDE)*, Brisbane, QLD, Australia, 2013, pp. 757–768.

[79] R. Chen, N. Mohammed, B. C. Fung, B. C. Desai, and L. Xiong, "Publishing set-valued data via differential privacy," *Proc. VLDB Endow.*, vol. 4, no. 11, pp. 1087–1098, 2011.

[80] R. Chen, B. C. M. Fung, B. C. Desai, and N. M. Sossou, "Differentially private transit data publication: A case study on the montreal transportation system," in *Proc. 18th ACM SIGKDD Int. Conf. Knowl. Disc. Data Min.*, 2012, pp. 213–221.

[81] R. Chen, G. Acs, and C. Castelluccia, "Differentially private sequential data publication via variable-length n-grams," in *Proc. ACM Conf. Comput. Commun. Security*, Raleigh, NC, USA, 2012, pp. 638–649.

[82] H. Li, L. Xiong, X. Jiang, and J. Liu, "Differentially private histogram publication for dynamic datasets: An adaptive sampling approach," in *Proc. 24th ACM Int. Conf. Inf. Knowl. Manag.*, Melbourne, VIC, Australia, 2015, pp. 1001–1010.

[83] L. Fan and L. Xiong, "An adaptive approach to real-time aggregate monitoring with differential privacy," *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 9, pp. 2094–2106, Sep. 2014.

[84] L. Fan, L. Bonomi, L. Xiong, and V. Sunderam, "Monitoring Web browsing behavior with differential privacy," in *ACM Proc. 23rd Int. Conf. World Wide Web*, 2014, pp. 177–188.

[85] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends® Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, 2014.

[86] B. Balle and Y.-X. Wang, "Improving the Gaussian mechanism for differential privacy: Analytical calibration and optimal denoising," *arXiv preprint arXiv:1805.06530*, 2018.

[87] A. Machanavajjhala, X. He, and M. Hay, "Differential privacy in the wild: A tutorial on current practices & open challenges," in *Proc. ACM Int. Conf. Manag. Data*, 2017, pp. 1727–1730.

[88] Z. Lu and H. Shen, "A new lower bound of privacy budget for distributed differential privacy," in *Proc. 18th Int. Conf. Parallel Distrib. Comput. Appl. Technol. (PDCAT)*, 2017, pp. 25–32.

[89] F. D. McSherry, "Privacy integrated queries: An extensible platform for privacy-preserving data analysis," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, Providence, RI, USA, 2009, pp. 19–30.

[90] J. Soria-Comas, J. Domingo-Ferrer, D. Sánchez, and D. Megías, "Individual differential privacy: A utility-preserving formulation of differential privacy guarantees," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1418–1429, Jun. 2017.

[91] E. ElSalamouny and S. Gambs, "Differential privacy models for location-based services," *Trans. Data Privacy*, vol. 9, no. 1, pp. 15–48, 2016.

[92] X. He, G. Cormode, A. Machanavajjhala, C. M. Procopiuc, and D. Srivastava, "DPT: Differentially private trajectory synthesis using hierarchical reference systems," *Proc. VLDB Endow.*, vol. 8, no. 11, pp. 1154–1165, 2015.

[93] Q. Xiao, R. Chen, and K.-L. Tan, "Differentially private network data release via structural inference," in *Proc. 20th ACM SIGKDD Int. Conf. Knowl. Disc. Data Min.*, New York, NY, USA, 2014, pp. 911–920.

[94] J. Hsu *et al.*, "Differential privacy: An economic method for choosing epsilon," in *Proc. IEEE 27th Comput. Security Found. Symp. (CSF)*, 2014, pp. 398–410.

[95] J. Lee and C. Clifton, "How much is enough? Choosing ε for differential privacy," in *Proc. Int. Conf. Inf. Security*, 2011, pp. 325–340.

[96] L. K. Fleischer and Y.-H. Lyu, "Approximately optimal auctions for selling privacy when costs are correlated with data," in *Proc. 13th ACM Conf. Electron. Commerce*, Valencia, Spain, 2012, pp. 568–585.

[97] P. Dandekar, N. Fawaz, and S. Ioannidis, "Privacy auctions for recommender systems," *ACM Trans. Econ. Comput.*, vol. 2, no. 3, p. 12, 2014.

[98] C. Li, D. Y. Li, G. Miklau, and D. Suciu, "A theory of pricing private data," *ACM Trans. Database Syst.*, vol. 39, no. 4, p. 34, 2014.

[99] C. Han and K. Wang, "Sensitive disclosures under differential privacy guarantees," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, New York, NY, USA, 2015, pp. 110–117.

[100] E. Shen and T. Yu, "Mining frequent graph patterns with differential privacy," in *Proc. 19th ACM SIGKDD Int. Conf. Knowl. Disc. Data Min.*, Chicago, IL, USA, 2013, pp. 545–553.

[101] B. Yang, I. Sato, and H. Nakagawa, "Bayesian differential privacy on correlated data," in *Proc. ACM SIGMOD Int. Conf. Manag. Data*, Melbourne, VIC, Australia, 2015, pp. 747–762.

[102] X. Xiao, "Differentially private data release: Improving utility with wavelets and Bayesian networks," in *Proc. Asia–Pac. Web Conf.*, 2014, pp. 25–35.

[103] W. Jiang, C. Xie, and Z. Zhang, "Wishart mechanism for differentially private principal components analysis," in *Proc. AAAI*, 2016, pp. 1730–1736.

[104] C. Dwork, K. Talwar, A. Thakurta, and L. Zhang, "Analyze gauss: optimal bounds for privacy-preserving principal component analysis," in *Proc. 46th Annu. ACM Symp. Theory Comput.*, New York, NY, USA, 2014, pp. 11–20.

[105] G. Barthe and B. Kopf, "Information-theoretic bounds for differentially private mechanisms," in *Proc. 24th IEEE Comput. Security Found. Symp.*, 2011, pp. 191–204.

[106] G. Giaconi, D. Gündüz, and H. V. Poor, "Smart meter privacy with renewable energy and an energy storage device," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 129–142, Jan. 2018.

[107] N. Zhang and W. Zhao, "Privacy-preserving OLAP: An information-theoretic approach," *IEEE Trans. Knowl. Data Eng.*, vol. 23, no. 1, pp. 122–138, Jan. 2011.

[108] M. S. Alvim, K. Chatzikokolakis, P. Degano, and C. Palamidessi, "Differential privacy versus quantitative information flow," *arXiv preprint arXiv:1012.4250*, 2010.

[109] L. Sankar, S. R. Rajagopalan, S. Mohajer, and H. V. Poor, "Smart meter privacy: A theoretical framework," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 837–846, Jun. 2013.

[110] S. Li, A. Khisti, and A. Mahajan, "Information-theoretic privacy for smart metering systems with a rechargeable battery," *IEEE Trans. Inf. Theory*, vol. 64, no. 5, pp. 3679–3695, May 2018.

[111] P. D. Beale and R. K. Pathria, *Statistical Mechanics*. Amsterdam, The Netherlands: Elsevier, 2011.

[112] C. Cachin, "Entropy measures and unconditional security in cryptography," Ph.D. dissertation, ETH Zurich, Zürich, Switzerland, 1997.

[113] S. Asoodeh, F. Alajaji, and T. Linder, "Notes on information-theoretic privacy," in *Proc. IEEE 52nd Annu. Allerton Conf. Commun. Control Comput. (Allerton)*, Monticello, IL, USA, 2014, pp. 1272–1278.

[114] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "An information-theoretic approach to privacy," in *Proc. IEEE 48th Annu. Allerton Conf. Commun. Control Comput. (Allerton)*, 2010, pp. 1220–1227.

[115] M. Bezzi, "An information theoretic approach for privacy metrics," *Trans. Data Privacy*, vol. 3, no. 3, pp. 199–215, 2010.

[116] J. Eckert and J. Mauchly. (1946). *Outline of Plans for Development of Electronic Computers*. [Online]. Available: http://archive.computerhistory.org/resources/access/text/2010/08/102660910-05-01-acc

[117] C. L. Liu and J. W. Layland, "Scheduling algorithms for multiprogramming in a hard-real-time environment," *J. ACM*, vol. 20, no. 1, pp. 46–61, 1973.

[118] K.-D. Kim and P. R. Kumar, "Cyber-physical systems: A perspective at the centennial," *Proc. IEEE*, vol. 100, pp. 1287–1308, May 2012.

[119] B. M. Leiner *et al.*, "A brief history of the Internet," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 5, pp. 22–31, 2009.

[120] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next century challenges: Mobile networking for 'smart dust,"' in *Proc. 5th Annu. ACM/IEEE Int. Conf. Mobile Comput. Netw.*, Seattle, WA, USA, 1999, pp. 271–278.

[121] G.-G. Wang, X. Cai, Z. Cui, G. Min, and J. Chen, "High performance computing for cyber physical social systems by using evolutionary multi-objective optimization algorithm," *IEEE Trans. Emerg. Topics Comput.*, to be published.

[122] Z. Cui, B. Sun, G. Wang, Y. Xue, and J. Chen, "A novel oriented cuckoo search algorithm to improve DV-Hop performance for cyber-physical systems," *J. Parallel Distrib. Comput.*, vol. 103, pp. 42–52, May 2017.

[123] J. Lee, B. Bagheri, and H.-A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manuf. Lett.*, vol. 3, pp. 18–23, Jan. 2015.

[124] X.-M. Zhang, Q.-L. Han, and Y.-L. Wang, "A brief survey of recent results on control and filtering for networked systems," in *Proc. 12th IEEE World Congr. Intell. Control Autom. (WCICA)*, Guilin, China, 2016, pp. 64–69.

[125] P. Tabuada, "Event-triggered real-time scheduling of stabilizing control tasks," *IEEE Trans. Autom. Control*, vol. 52, no. 9, pp. 1680–1685, Sep. 2007.

[126] J. Lunze and D. Lehmann, "A state-feedback approach to event-based control," *Automatica*, vol. 46, no. 1, pp. 211–215, 2010.

[127] X. Wang and M. D. Lemmon, "Self-triggered feedback control systems with finite-gain L2 stability," *IEEE Trans. Autom. Control*, vol. 54, no. 3, pp. 452–467, Mar. 2009.

[128] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proc. IEEE*, vol. 95, no. 1, pp. 138–162, Jan. 2007.

[129] J. Xiong and J. Lam, "Stabilization of networked control systems with a logic ZOH," *IEEE Trans. Autom. Control*, vol. 54, no. 2, pp. 358–363, Feb. 2009.

[130] D. Nesic and D. Liberzon, "A unified framework for design and analysis of networked and quantized control systems," *IEEE Trans. Autom. Control*, vol. 54, no. 4, pp. 732–747, Apr. 2009.

[131] N. Lynch, R. Segala, F. Vaandrager, and H. B. Weinberg, "Hybrid I/O automata," in *Proc. Int. Hybrid Syst. Workshop*, 1995, pp. 496–510.

[132] A. Platzer, *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*. Heidelberg, Germany: Springer, 2010.

[133] M. H. Rehmani, M. Reisslein, A. Rachedi, M. Erol-Kantarci, and M. Radenkovic, "Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies," *IEEE Trans. Ind. Informat.*, vol. 14, no. 7, pp. 2814–2825, Jul. 2018.

[134] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 446–464, 1st Quart., 2017.

[135] Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, "V2X access technologies: Regulation, research, and remaining challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1858–1877, 3rd Quart., 2018.

[136] L. Da Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[137] Z. Cui *et al.*, "A pigeon-inspired optimization algorithm for many-objective optimization problems," *Sci. China Inf. Sci.*, vol. 62, no. 7, Jan. 2019, Art. no. 70212. [Online]. Available: https://doi.org/10.1007/s11432–018-9729–5

[138] G. Bloom, B. Alsulami, E. Nwafor, and I. C. Bertolotti, "Design patterns for the Industrial Internet of Things," in *Proc. 14th IEEE Int. Workshop Factory Commun. Syst. (WFCS)*, 2018, pp. 1–10.

[139] X. Hu *et al.*, "Differential privacy in telco big data platform," *Proc. VLDB Endow.*, vol. 8, no. 12, pp. 1692–1703, 2015.

[140] H. Ye, J. Liu, W. Wang, P. Li, T. Li, and J. Li, "Secure and efficient outsourcing differential privacy data release scheme in cyber–physical system," *Future Gener. Comput. Syst.*, to be published.

[141] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in *Proc. 3rd ACM Workshop Cloud Comput. Security*, 2011, pp. 113–124.

[142] P. Jain, M. Gyanchandani, and N. Khare, "Big data privacy: A technological perspective and review," *J. Big Data*, vol. 3, no. 1, p. 25, 2016.

[143] A. Gosain and N. Chugh, "Privacy preservation in big data," *Int. J. Comput. Appl.*, vol. 100, no. 17, pp. 44–47, 2014.

[144] A. S. Thanamani, "Comparison and analysis of anonymization techniques for preserving privacy in big data," *Adv. Comput. Sci. Technol.*, vol. 10, no. 2, pp. 247–253, 2017.

[145] R. Chen, B. C. M. Fung, P. S. Yu, and B. C. Desai, "Correlated network data publication via differential privacy," *Int. J. Very Large Data Bases (VLDB)*, vol. 23, no. 4, pp. 653–676, 2014.

[146] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[147] C. Xu, J. Ren, D. Zhang, and Y. Zhang, "Distilling at the edge: A local differential privacy obfuscation framework for IoT data analytics," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 20–25, Aug. 2018.

[148] G. Ács and C. Castelluccia, "I have a DREAM! (Differentially private smart metering)," in *Proc. Int. Workshop Inf. Hiding*, 2011, pp. 118–132.

[149] F. Kargl, A. Friedman, and R. Boreli, "Differential privacy in intelligent transportation systems," in *Proc. 6th ACM Conf. Security Privacy Wireless Mobile Netw.*, 2013, pp. 107–112.

[150] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *Proc. IEEE INFOCOM*, 2014, pp. 504–512.

[151] H. Li, Y. Dai, and X. Lin, "Efficient e-health data release with consistency guarantee under differential privacy," in *Proc. IEEE 17th Int. Conf. E-Health Netw. Appl. Services (HealthCom)*, 2015, pp. 602–608.

[152] N. Mohammed, S. Barouti, D. Alhadidi, and R. Chen, "Secure and private management of healthcare databases for data mining," in *Proc. IEEE 28th Int. Symp. Comput. Based Med. Syst. (CBMS)*, 2015, pp. 191–196.

[153] S. Han, U. Topcu, and G. J. Pappas, "An approximately truthful mechanism for electric vehicle charging via joint differential privacy," in *Proc. IEEE Amer. Control Conf. (ACC)*, 2015, pp. 2469–2475.

[154] M. Savi, C. Rottondi, and G. Verticale, "Evaluation of the precision-privacy tradeoff of data perturbation for smart metering," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2409–2416, Sep. 2015.

[155] C. R. G. Rodríguez and S. E. G. Barrantes, "Using differential privacy for the Internet of Things," in *IFIP International Summer School on Privacy and Identity Management*. Cham, Switzerland: Springer, 2016, pp. 201–211.

[156] G. Eibl and D. Engel, "Differential privacy for real smart metering data," *Comput. Sci. Res. Develop.*, vol. 32, nos. 1–2, pp. 173–182, 2017.

[157] H. Zhai, S. Chen, and D. An, "ExPO: Exponential-based privacy preserving online auction for electric vehicles demand response in microgrid," in *Proc. IEEE 13th Int. Conf. Semantics Knowl. Grids (SKG)*, 2017, pp. 126–131.

[158] Y. Shi, C. Piao, and L. Zheng, "Differential-privacy-based correlation analysis in railway freight service applications," in *Proc. IEEE Int. Conf. Cyber Enabled Distrib. Comput. Knowl. Disc. (CyberC)*, 2017, pp. 35–39.

[159] J. Zhang, X. Liang, Z. Zhang, S. He, and Z. Shi, "Re-DPoctor: Real-time health data releasing with w-day differential privacy," *arXiv preprint arXiv:1711.00232*, 2017.

[160] Y. Wang, Z. Huang, S. Mitra, and G. E. Dullerud, "Differential privacy in linear distributed control systems: Entropy minimizing mechanisms and performance tradeoffs," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 118–130, Mar. 2017.

[161] 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," in *Concurrency and Computation: Practice and Experience*, Wiley, 2018, Art. no. e4528.

[162] T. Zhang and Q. Zhu, "Distributed privacy-preserving collaborative intrusion detection systems for VANETs," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 4, no. 1, pp. 148–161, Mar. 2018.

[163] J. L. Raisaro *et al.*, "MedCo: Enabling secure and privacy-preserving exploration of distributed clinical and genomic data," *IEEE/ACM Trans. Comput. Biol. Bioinformat.*, vol. 16, no. 4, pp. 1328–1341, Jul./Aug. 2019.

[164] L. Ni, C. Li, H. Liu, A. G. Bourgeois, and J. Yu, "Differential private preservation multi-core DBScan clustering for network user data," *Procedia Comput. Sci.*, vol. 129, pp. 257–262, 2018.

[165] 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 Trans. Smart Grid*, vol. 8, no. 2, pp. 619–626, Mar. 2017.

[166] D. Kifer and A. Machanavajjhala, "Pufferfish: A framework for mathematical privacy definitions," *ACM Trans. Database Syst.*, vol. 39, no. 1, p. 3, 2014.

[167] F. K. Dankar and K. El Emam, "Practicing differential privacy in health care: A review," *Trans. Data Privacy*, vol. 6, no. 1, pp. 35–67, 2013.

[168] R. Zhang and P. Venkitasubramaniam, "Stealthy control signal attacks in linear quadratic Gaussian control systems: Detectability reward tradeoff," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1555–1570, Jul. 2017.

[169] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, 4th Quart., 2012.

[170] H. Liang, A. K. Tamang, W. Zhuang, and X. S. Shen, "Stochastic information management in smart grid," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1746–1770, 3rd Quart., 2014.

[171] A. A. Khan, M. H. Rehmani, and M. Reisslein, "Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 860–898, 1st Quart., 2016.

[172] J. Lopez, J. E. Rubio, and C. Alcaraz, "A resilient architecture for the smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3745–3753, Aug. 2018.

[173] S. Finster and I. Baumgart, "Privacy-aware smart metering: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1088–1101, 2nd Quart., 2015.

[174] S. Desai, R. Alhadad, N. Chilamkurti, and A. Mahmood, "A survey of privacy preserving schemes in IoE enabled smart grid advanced metering infrastructure," *Cluster Comput.*, vol. 22, no. 1, pp. 43–69, 2019.

[175] S. Welikala, C. Dinesh, M. P. B. Ekanayake, R. I. Godaliyadda, and J. Ekanayake, "Incorporating appliance usage patterns for non-intrusive load monitoring and load forecasting," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 448–461, Jan. 2017.

[176] G. W. Hart, "Nonintrusive appliance load monitoring," *Proc. IEEE*, vol. 80, no. 12, pp. 1870–1891, Dec. 1992.

[177] E. J. Aladesanmi and K. A. Folly, "Overview of non-intrusive load monitoring and identification techniques," *IFAC PapersOnLine*, vol. 48, no. 30, pp. 415–420, 2015.

[178] G. W. Arnold, "Challenges and opportunities in smart grid: A position article," *Proc. IEEE*, vol. 99, no. 6, pp. 922–927, Jun. 2011.

[179] J. S. Vardakas, N. Zorba, and C. V. Verikoukis, "A survey on demand response programs in smart grids: Pricing methods and optimization algorithms," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 152–178, 1st Quart., 2015.

[180] R. Anderson and S. Fuloria, "Who controls the off switch?" in *Proc. 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010, pp. 96–101.

[181] P. Gope and B. Sikdar, "An efficient data aggregation scheme for privacy-friendly dynamic pricing-based billing and demand-response management in smart grids," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3126–3135, Aug. 2018.

[182] 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 *Proc. IEEE 25th Int. Symp. Qual. Service (IWQoS)*, 2017, pp. 1–9.

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

[184] P. Barbosa, A. Brito, H. Almeida, and S. Clauß, "Lightweight privacy for smart metering data by adding noise," in *Proc. 29th Annu. ACM Symp. Appl. Comput.*, 2014, pp. 531–538.

[185] U. B. Baloglu and Y. Demir, "Lightweight privacy-preserving data aggregation scheme for smart grid metering infrastructure protection," *Int. J. Crit. Infrastruct. Protect.*, vol. 22, pp. 16–24, Sep. 2018.

[186] X. Liao, P. Srinivasan, D. Formby, and A. R. Beyah, "Di-PriDA: Differentially private distributed load balancing control for the smart grid," *IEEE Trans. Depend. Secure Comput.*, to be published.

[187] R. Pal, P. Hui, and V. K. Prasanna, "On optimal privacy engineering for the smart micro-grid," *IEEE Trans. Knowl. Data Eng.*, to be published.

[188] J. Xiong *et al.*, "Enhancing privacy and availability for data clustering in intelligent electrical service of IoT," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1530–1540, Apr. 2019.

[189] Y. Chen, A. Machanavajjhala, M. Hay, and G. Miklau, "PeGaSus: Data-adaptive differentially private stream processing," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2017, pp. 1375–1388.

[190] J. Liu, C. Zhang, and Y. Fang, "EPIC: A differential privacy framework to defend smart homes against Internet traffic analysis," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1206–1217, Apr. 2018.

[191] M. Sookhak, H. Tang, Y. He, and F. R. Yu, "Security and privacy of smart cities: A survey, research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1718–1743, 2nd Quart., 2019.

[192] J. M. Barrionuevo, P. Berrone, and J. E. Ricart, "Smart cities, sustainable progress," *IESE Insight*, vol. 14, no. 14, pp. 50–57, 2012.

[193] J. Xie *et al.*, "A survey of blockchain technology applied to smart cities: Research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019.

[194] "Smart buildings enable smart cities [Online]," 2016.

[195] A. Ståhlbröst, A. Sällström, and D. Hollosi, "Audio monitoring in smart cities: An information privacy perspective," 2014.

[196] A. W. Burange and H. D. Misalkar, "Review of Internet of Things in development of smart cities with data management & privacy," in *Proc. IEEE Int. Conf. Adv. Comput. Eng. Appl.*, 2015, pp. 189–195.

[197] A. Bartoli, J. Hernández-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Security and privacy in your smart city," in *Proc. Barcelona Smart Cities Congr.*, vol. 292, 2011, pp. 1–6.

[198] P. Pappachan *et al.*, "Towards privacy-aware smart buildings: Capturing, communicating, and enforcing privacy policies and preferences," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, 2017, pp. 193–198.

[199] D. Eckhoff and I. Wagner, "Privacy in the smart city—Applications, technologies, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 489–516, 1st Quart., 2018.

[200] R. Jia, R. Dong, S. S. Sastry, and C. J. Sapnos, "Privacy-enhanced architecture for occupancy-based HVAC control," in *Proc. ACM/IEEE 8th Int. Conf. Cyber Phys. Syst. (ICCPS)*, 2017, pp. 177–186.

[201] S. Ghayyur *et al.*, "IoT-detective: Analyzing IoT data under differential privacy," in *Proc. Int. Conf. Manag. Data*, 2018, pp. 1725–1728.

[202] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: An Internet of Things application," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 68–75, Nov. 2011.

[203] C. Laughman *et al.*, "Power signature analysis," *IEEE Power Energy Mag.*, vol. 1, no. 2, pp. 56–63, Mar./Apr. 2003.

[204] A. Lee, "Guidelines for smart grid cyber security," NIST, Gaithersburg, MD, USA, Rep. 7628, 2010.

[205] H. Kreutzmann, S. Vollmer, N. Tekampe, and A. Abromeit, "Protection profile for the gateway of a smart metering system," *German Federal Office for Information Security*, 2011.

[206] M. Jawurek, F. Kerschbaum, and G. Danezis, *SoK: Privacy Technologies for Smart Grids—A Survey of Options*, Microsoft Res., Cambridge, U.K., 2012.

[207] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, and F. Pérez-González, "Privacy-preserving data aggregation in smart metering systems: An overview," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 75–86, Mar. 2013.

[208] G. Danezis, C. Fournet, M. Kohlweiss, and S. Zanella-Béguelin, "Smart meter aggregation via secret-sharing," in *Proc. 1st ACM Workshop Smart Energy Grid Security*, 2013, pp. 75–80.

[209] C. Rottondi, G. Verticale, and A. Capone, "Privacy-preserving smart metering with multiple data consumers," *Comput. Netw.*, vol. 57, no. 7, pp. 1699–1713, 2013.

[210] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, 2010, pp. 238–243.

[211] T. Baumeister, *Literature Review on Smart Grid Cyber Security*, Collaborative Softw. Develop. Lab., Univ. Hawaii, Honolulu, HI, USA, 2010.

[212] L. Fan and L. Xiong, "Real-time aggregate monitoring with differential privacy," in *Proc. 21st ACM Int. Conf. Inf. Knowl. Manag.*, 2012, pp. 2169–2173.

[213] C. Clifton and T. Tassa, "On syntactic anonymity and differential privacy," in *Proc. IEEE 29th Int. Conf. Data Eng. Workshops (ICDEW)*, 2013, pp. 88–93.

[214] M. Mukherjee, L. Shu, and D. Wang, "Survey of fog computing: Fundamental, network applications, and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1826–1857, 3rd Quart., 2018.

[215] J. Ni, K. Zhang, X. Lin, and X. S. Shen, "Securing fog computing for Internet of Things applications: Challenges and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 601–628, 1st Quart., 2018.

[216] K. D. Anderson, M. E. Bergés, A. Ocneanu, D. Benitez, and J. M. F. Moura, "Event detection for non intrusive load monitoring," in *Proc. IEEE 38th Annu. Conf. Ind. Electron. Soc. (IECON)*, 2012, pp. 3312–3317.

[217] Z. Zhou, Y. Qiao, L. Zhu, J. Guan, Y. Liu, and C. Xu, "Differential privacy-guaranteed trajectory community identification over vehicle ad-hoc networks," *Internet Technol. Lett.*, vol. 1, no. 3, 2018.

[218] Z. Ma, T. Zhang, X. Liu, X. Li, and K. Ren, "Real-time privacy-preserving data release over vehicle trajectory," *IEEE Trans. Veh. Technol.*, vol. 86, no. 8, pp. 8091–8102, Aug. 2019.

[219] B. Nelson and T. Olovsson, "Introducing differential privacy to the automotive domain: Opportunities and challenges," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, 2017, pp. 1–7.

[220] S.-H. An, B.-H. Lee, and D.-R. Shin, "A survey of intelligent transportation systems," in *Proc. IEEE 3rd Int. Conf. Comput. Intell. Commun. Syst. Netw.*, 2011, pp. 332–337.

[221] N.-E. El Faouzi, H. Leung, and A. Kurian, "Data fusion in intelligent transportation systems: Progress and challenges—A survey," *Inf. Fusion*, vol. 12, no. 1, pp. 4–10, 2011.

[222] J. Zhang, F.-Y. Wang, K. Wang, W.-H. Lin, X. Xu, and C. Chen, "Data-driven intelligent transportation systems: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1624–1639, Dec. 2011.

[223] L. Zhu, F. R. Yu, Y. Wang, B. Ning, and T. Tang, "Big data analytics in intelligent transportation systems: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 1, pp. 383–398, Jan. 2019.

[224] L. Qi, "Research on intelligent transportation system technologies and applications," in *Proc. IEEE Workshop Power Electron. Intell. Transport. Syst. (PEITS)*, 2008, pp. 529–531.

[225] D. Eckhoff, R. German, C. Sommer, F. Dressler, and T. Gansen, "SlotSwap: Strong and affordable location privacy in intelligent transportation systems," *IEEE Commun. Mag.*, vol. 49, no. 11, pp. 126–133, Nov. 2011.

[226] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2377–2396, 4th Quart., 2015.

[227] A. Nshimiyimana, D. Agrawal, and W. Arif, "Comprehensive survey of V2V communication for 4G mobile and wireless technology," in *Proc. IEEE Int. Conf. Wireless Commun. Signal Process. Netw. (WiSPNET)*, 2016, pp. 1722–1726.

[228] Q. Shi and M. Abdel-Aty, "Big data applications in real-time traffic operation and safety monitoring and improvement on urban expressways," *Transport. Res. C Emerg. Technol.*, vol. 58, pp. 380–394, Sep. 2015.

[229] N. Mohamed and J. Al-Jaroodi, "Real-time big data analytics: Applications and challenges," in *Proc. IEEE Int. Conf. High Perform. Comput. Simulat. (HPCS)*, 2014, pp. 305–310.

[230] C. Gosman, C. Dobre, and F. Pop, "Privacy-preserving data aggregation in intelligent transportation systems," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM)*, 2017, pp. 1059–1064.

[231] A.-S. K. Pathan, *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*. Boca Raton, FL, USA: CRC Press, 2016.

[232] A. Thaduri, D. Galar, and U. Kumar, "Railway assets: A potential domain for big data analytics," *Procedia Comput. Sci.*, vol. 53, pp. 457–467, 2015.

[233] F. Ghofrani, Q. He, R. M. P. Goverde, and X. Liu, "Recent applications of big data analytics in railway transportation systems: A survey," *Transp. Res. C Emerg. Technol.*, vol. 90, pp. 226–246, May 2018.

[234] J. Guo, B. Song, Y. He, F. R. Yu, and M. Sookhak, "A survey on compressed sensing in vehicular infotainment systems," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2662–2680, 4th Quart., 2017.

[235] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 770–790, 1st Quart., 2018.

[236] K. Emara, W. Woerndl, and J. H. Schlichter, "Vehicle tracking using vehicular network beacons," in *Proc. IEEE 14th Int. Symp. Workshops World Wireless Mobile Multimedia Netw. (WoWMoM)*, 2013, pp. 1–6.

[237] D. Eckhoff, "Privacy and surveillance: Concerns about a future transportation system," in *Proc. 1st GI/ITG KuVS Fachgespräch Inter Veh. Commun. (FG-IVC)*, 2013, p. 15.

[238] U. K. Madawala and D. J. Thrimawithana, "A bidirectional inductive power interface for electric vehicles in V2G systems," *IEEE Trans. Ind. Electron.*, vol. 58, no. 10, pp. 4789–4796, Oct. 2011.

[239] D. T. Hoang, P. Wang, D. Niyato, and E. Hossain, "Charging and discharging of plug-in electric vehicles (PEVS) in vehicle-to-grid (V2G) systems: A cyber insurance-based model," *IEEE Access*, vol. 5, pp. 732–754, 2017.

[240] W. Wei, F. Liu, and S. Mei, "Charging strategies of EV aggregator under renewable generation and congestion: A normalized Nash equilibrium approach," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1630–1641, May 2016.

[241] M. Zeng, S. Leng, S. Maharjan, S. Gjessing, and J. He, "An incentivized auction-based group-selling approach for demand response management in V2G systems," *IEEE Trans. Ind. Informat.*, vol. 11, no. 6, pp. 1554–1563, Dec. 2015.

[242] M. Naor, B. Pinkas, and R. Sumner, "Privacy preserving auctions and mechanism design," in *Proc. 1st ACM Conf. Electron. Commerce*, 1999, pp. 129–139.

[243] M. Pan, J. Sun, and Y. Fang, "Purging the back-room dealing: Secure spectrum auction leveraging Paillier cryptosystem," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 4, pp. 866–876, Apr. 2011.

[244] Q. Xiang, L. Kong, X. Liu, J. Xu, and W. Wang, "Auc2Reserve: A differentially private auction for electric vehicle fast charging reservation," in *Proc. IEEE 22nd Int. Conf. Embedded Real Time Comput. Syst. Appl. (RTCSA)*, 2016, pp. 85–94.

[245] K. Al-Hussaeni, B. C. M. Fung, F. Iqbal, G. G. Dagher, and E. G. Park, "SafePath: Differentially-private publishing of passenger trajectories in transportation systems," *Comput. Netw.*, vol. 143, pp. 126–139, Oct. 2018.

[246] X. Ma, J. Ma, H. Li, Q. Jiang, and S. Gao, "AGENT: An adaptive geo-indistinguishable mechanism for continuous location-based service," *Peer-to-Peer Netw. Appl.*, vol. 11, no. 3, pp. 473–485, 2018.

[247] C. Xu, L. Zhu, Y. Liu, J. Guan, and S. Yu, "DP-LTOD: Differential privacy latent trajectory community discovering services over location-based social networks," *IEEE Trans. Services Comput.*, to be published.

[248] A. Machanavajjhala and X. He, "Analyzing your location data with provable privacy guarantees," in *Handbook of Mobile Data Privacy*. Cham, Switzerland: Springer, 2018, pp. 97–127.

[249] W. Zhang, R. Rao, G. Cao, and G. Kesidis, "Secure routing in ad hoc networks and a related intrusion detection problem," in *Proc. MILCOM*, vol. 2, 2003, pp. 735–740.

[250] T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks," in *Wireless Network Security*. Boston, MA, USA: Springer, 2007, pp. 159–180.

[251] A. Narayanan and V. Shmatikov, "Myths and fallacies of 'personally identifiable information,"' *Commun. ACM*, vol. 53, no. 6, pp. 24–26, 2010.

[252] X. Gao, B. Firner, S. Sugrim, V. Kaiser-Pendergrast, Y. Yang, and J. Lindqvist, "Elastic pathing: Your speed is enough to track you," in *Proc. ACM Int. Joint Conf. Pervasive Ubiquitous Comput. (UbiComp)*, 2014, pp. 975–986.

[253] A. Tockar, "Riding with the stars: Passenger privacy in the NYC taxicab dataset," Neustar Res., Sterling, VA, USA, 2014.

[254] Q. Wang, X. Liu, J. Du, and F. Kong, "Smart charging for electric vehicles: A survey from the algorithmic perspective," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1500–1517, 2nd Quart., 2016.

[255] Y. Zhang, J. Li, D. Zheng, P. Li, and Y. Tian, "Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice," *J. Netw. Comput. Appl.*, vol. 122, pp. 50–60, Nov. 2018.

[256] Z. Pang, "Technologies and architectures of the Internet-of-Things (IoT) for health and well-being," Ph.D. dissertation, Electron. Comput. Syst., KTH Roy. Inst. Technol., Stockholm, Sweden, 2013.

[257] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[258] A. Rizwan *et al.*, "A review on the role of nano-communication in future healthcare systems: A big data analytics perspective," *IEEE Access*, vol. 6, pp. 41903–41920, 2018.

[259] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving fusion of IoT and big data for e-Health," *Future Gener. Comput. Syst.*, vol. 86, pp. 1437–1455, Sep. 2018.

[260] N. Sharma and R. Bhatt, "Privacy preservation in WSN for healthcare application," *Procedia Comput. Sci.*, vol. 132, pp. 1243–1252, 2018.

[261] M. M. Alam, H. Malik, M. I. Khan, T. Pardy, A. Kuusik, and Y. L. Moullec, "A survey on the roles of communication technologies in IoT-based personalized healthcare applications," *IEEE Access*, vol. 6, pp. 36611–36631, 2018.

[262] Z. Guan, Z. Lv, X. Du, L. Wu, and M. Guizani, "Achieving data utility-privacy tradeoff in Internet of medical things: A machine learning approach," *Future Gener. Comput. Syst.*, vol. 98, pp. 60–68, Sep. 2019.

[263] B. K. Beaulieu-Jones, W. Yuan, S. G. Finlayson, and Z. S. Wu, "Privacy-preserving distributed deep learning for clinical data," *arXiv preprint arXiv:1812.01484*, 2018.

[264] A. Alnemari, C. J. Romanowski, and R. K. Raj, "An adaptive differential privacy algorithm for range queries over healthcare data," in *Proc. IEEE Int. Conf. Healthcare Informat. (ICHI)*, 2017, pp. 397–402.

[265] J. L. Raisaro *et al.*, "Protecting privacy and security of genomic data in i2b2 with homomorphic encryption and differential privacy," *IEEE/ACM Trans. Comput. Biol. Bioinformat.*, vol. 15, no. 5, pp. 1413–1426, Sep. 2018.

[266] W. Tang, J. Ren, K. Deng, and Y. Zhang, "Secure data aggregation of lightweight e-Healthcare IoT devices with fair incentives," *IEEE Internet Things J.*, to be published.

[267] A. C. Valdez and M. Ziefle, "The users' perspective on the privacy-utility trade-offs in health recommender systems," *Int. J. Human–Comput. Studies*, vol. 121, pp. 108–121, Jan. 2019.

[268] J. Lane and C. Schur, "Balancing access to health data and privacy: A review of the issues and approaches for the future," *Health Services Res.*, vol. 45, pp. 1456–1467, Aug. 2010.

[269] D. Hemapriya, P. Viswanath, V. Mithra, S. Nagalakshmi, and G. Umarani, "Wearable medical devices—Design challenges and issues," in *Proc. IEEE Int. Conf. Innov. Green Energy Healthcare Technol. (IGEHT)*, 2017, pp. 1–6.

[270] W. J. Long and W. Lin, "An authentication protocol for wearable medical devices," in *Proc. 13th IEEE Int. Conf. Expo Emerg. Technol. Smarter World (CEWIT)*, 2017, pp. 1–5.

[271] A. Cavoukian, A. Fisher, S. Killen, and D. A. Hoffman, "Remote home health care technologies: How to ensure privacy? Build it in: Privacy by design," *Identity Inf. Soc.*, vol. 3, no. 2, pp. 363–378, 2010.

[272] B. Shickel, P. Tighe, A. Bihorac, and P. Rashidi, "Deep EHR: A survey of recent advances in deep learning techniques for electronic health record (EHR) analysis," *arXiv preprint arXiv:1706.03446*, 2017.

[273] T. Sahama, L. Simpson, and B. Lane, "Security and privacy in eHealth: Is it possible?" in *Proc. IEEE 15th Int. Conf. e-Health Netw. Appl. Services (Healthcom)*, 2013, pp. 249–253.

[274] R. Agrawal and R. Srikant, "Privacy-preserving data mining," *ACM SIGMOD Rec.*, vol. 29, no. 2, pp. 439–450, 2000.

[275] X. Jiang, S. Cheng, and L. Ohno-Machado, "Quantifying fine-grained privacy risk and representativeness in medical data," in *Proc. ACM Workshop Data Min. Med. Healthcare*, 2011, pp. 64–67.

[276] P. Shi, L. Xiong, and B. C. M. Fung, "Anonymizing data with quasi-sensitive attribute values," in *Proc. 19th ACM Int. Conf. Inf. Knowl. Manag.*, 2010, pp. 1389–1392.

[277] S. Sharma, K. Chen, and A. P. Sheth, "Toward practical privacy-preserving analytics for IoT and cloud-based healthcare systems," *IEEE Internet Comput.*, vol. 22, no. 2, pp. 42–51, May 2018.

[278] W. Zhang, H. Zou, L. Luo, Q. Liu, W. Wu, and W. Xiao, "Predicting potential side effects of drugs by recommender methods and ensemble learning," *Neurocomputing*, vol. 173, pp. 979–987, Jan. 2016.

[279] Q. Zhang, G. Zhang, J. Lu, and D. Wu, "A framework of hybrid recommender system for personalized clinical prescription," in *Proc. IEEE 10th Int. Conf. Intell. Syst. Knowl. Eng. (ISKE)*, 2015, pp. 189–195.

[280] B. Esteban, Á. Tejeda-Lorente, C. Porcel, M. Arroyo, and E. Herrera-Viedma, "TPLUFIB-WEB: A fuzzy linguistic Web system to help in the treatment of low back pain problems," *Knowl. Based Syst.*, vol. 67, pp. 429–438, Sep. 2014.

[281] R. J. Bayardo and R. Agrawal, "Data privacy through optimal k-anonymization," in *Proc. IEEE 21st Int. Conf. Data Eng. (ICDE)*, 2005, pp. 217–228.

[282] B. Yüksel, A. Küpçü, and Ö. Özkasap, "Research issues for privacy and security of electronic health services," *Future Gener. Comput. Syst.*, vol. 68, pp. 1–13, Mar. 2017.

[283] G. Fimiani, "Supporting privacy in a cloud-based health information system by means of fuzzy conditional identity-based proxy re-encryption (FCI-PRE)," in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, May 2018, pp. 569–572.

[284] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3628–3636, Aug. 2017.

[285] J. Giraldo, A. Cardenas, and M. Kantarcioglu, "Security and privacy trade-offs in CPS by leveraging inherent differential privacy," in *Proc. IEEE Conf. Control Technol. Appl. (CCTA)*, 2017, pp. 1313–1318.

[286] P. Li, T. Li, H. Ye, J. Li, X. Chen, and Y. Xiang, "Privacy-preserving machine learning with multiple data providers," *Future Gener. Comput. Syst.*, vol. 87, pp. 341–350, Oct. 2018.

[287] K. Ashton. (Jun. 2009). *Internet of Things RFID Journal*. [Online]. Available: http://www.rfidjournal.com/articles/view?4986

[288] F. Javed, M. K. Afzal, M. Sharif, and B.-S. Kim, "Internet of Things (IoT) operating systems support, networking technologies, applications, and challenges: A comparative review," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2062–2100, 3rd Quart., 2018.

[289] Y. Li, M. Hou, H. Liu, and Y. Liu, "Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things," *Inf. Technol. Manag.*, vol. 13, no. 4, pp. 205–216, 2012.

[290] K. R. Sollins, "IoT big data security and privacy vs. innovation," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1628–1635, Apr. 2019.

[291] L. M. Thompson, *Industrial Data Communications*. Research Triangle Park, NC, USA: ISA, 2007.

[292] H. Li, A. D. Dimitrovski, J. B. Song, Z. Han, and L. Qian, "Communication infrastructure design in cyber physical systems with applications in smart grids: A hybrid system framework," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1689–1708, 3rd Quart., 2014.

[293] X. Lu, Q. Li, Z. Qu, and P. Hui, "Privacy information security classification study in Internet of Things," in *Proc. IEEE Int. Conf. Identification Inf. Knowl. Internet Things (IIKI)*, 2014, pp. 162–165.

[294] C. M. Medaglia and A. Serbanati, "An overview of privacy and security issues in the Internet of Things," in *The Internet of Things*. New York, NY, USA: Springer, 2010, pp. 389–395.

[295] P. De Leusse, P. Periorellis, T. Dimitrakos, and S. K. Nair, "Self managed security cell, a security model for the Internet of Things and services," in *Proc. 1st Int. Conf. Adv. Future Internet*, 2009, pp. 47–52.

[296] B. Shen and Y. Liu, "Privacy and security in the exploitation of Internet of Things," *J. Dialectics Nat.*, vol. 33, no. 6, pp. 77–83, 2011.

[297] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "Data security and privacy in cloud computing," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 7, 2014, Art. no. 190903.

[298] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," *Int. J. Uncertainty Fuzziness Knowl. Syst.*, vol. 10, no. 5, pp. 571–588, 2002.

[299] Y. Saygin, V. S. Verykios, and A. K. Elmagarmid, "Privacy preserving association rule mining," in *Proc. IEEE 12th Int. Workshop Res. Issues Data Eng. Eng. E-Commerce E-Bus. Syst. (RIDE-2EC)*, 2002, pp. 151–158.

[300] A. C.-C. Yao, "How to generate and exchange secrets," in *Proc. IEEE 27th Annu. Symp. Found. Comput. Sci.*, 1986, pp. 162–167.

[301] C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu, "Tools for privacy preserving distributed data mining," *ACM SIGKDD Explor. Newslett.*, vol. 4, no. 2, pp. 28–34, 2002.

[302] V. Tudor, V. Gulisano, M. Almgren, and M. Papatriantafilou, "BES: Differentially private event aggregation for large-scale IoT-based systems," *Future Gener. Comput. Syst.*, to be published.

[303] L. Bassi, "Industry 4.0: Hope, hype or revolution?" in *Proc. IEEE 3rd Int. Forum Res. Technol. Soc. Ind. (RTSI)*, 2017, pp. 1–6.

[304] M. Wollschlaeger, T. Sauter, and J. Jasperneite, "The future of industrial communication: Automation networks in the era of the Internet of Things and industry 4.0," *Ind. Electron. Mag.*, vol. 11, no. 1, pp. 17–27, Mar. 2017.

[305] Z. Lv, H. Song, P. Basanta-Val, A. Steed, and M. Jo, "Next-generation big data analytics: State of the art, challenges, and future research topics," *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 1891–1899, Aug. 2017.

[306] F. Xiao, L.-T. Sha, Z.-P. Yuan, and R.-C. Wang, "VulHunter: A discovery for unknown bugs based on analysis for known patches in industry Internet of Things," *IEEE Trans. Emerg. Topics Comput.*, to be published.

[307] C. Yin, S. Zhang, J. Xi, and J. Wang, "An improved anonymity model for big data security based on clustering algorithm," *Concurrency Comput. Pract. Exp.*, vol. 29, no. 7, 2017, Art. no. e3902.

[308] R. W. Brennan, "Toward real-time distributed intelligent control: A survey of research themes and applications," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 37, no. 5, pp. 744–765, Sep. 2007.

[309] H. Parunak, "Autonomous agent architectures: A non-technical introduction," Ind. Technol. Inst., Colombo, Sri Lanka, Rep., 1993.

[310] K. Zetter. (Jan. 2015). *A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever, Wired*. [Online]. Available: http://www.wired.com/2015/01/german-steel-mill-hack-destruction

[311] K. Chatzikokolakis, M. E. Andrés, N. E. Bordenabe, and C. Palamidessi, "Broadening the scope of differential privacy using metrics," in *Proc. Int. Symp. Privacy Enhanc. Technol. Symp.*, 2013, pp. 82–102.

[312] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, "A privacy preserving communication protocol for IoT applications in smart homes," in *Proc. IEEE Int. Conf. Identification Inf. Knowl. Internet Things (IIKI)*, 2016, pp. 519–524.

[313] R. Li, T. Song, N. Capurso, J. Yu, J. Couture, and X. Cheng, "IoT applications on secure smart shopping system," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1945–1954, Dec. 2017.

[314] T. Song, N. Capurso, X. Cheng, J. Yu, B. Chen, and W. Zhao, "Enhancing GPS with lane-level navigation to facilitate highway driving," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 4579–4591, Jun. 2017.

[315] Y. Liang, Z. Cai, Q. Han, and Y. Li, "Location privacy leakage through sensory data," *Security Commun. Netw.*, vol. 2017, Aug. 2017, Art. no. 7576307.

[316] H.-J. Yim, D. Seo, H. Jung, M.-K. Back, I. Kim, and K.-C. Lee, "Description and classification for facilitating interoperability of heterogeneous data/events/services in the Internet of Things," *Neurocomputing*, vol. 256, pp. 13–22, Sep. 2017.

[317] Z. Cui, Y. Cao, X. Cai, J. Cai, and J. Chen, "Optimal LEACH protocol with modified bat algorithm for big data sensing systems in Internet of Things," *J. Parallel Distrib. Comput.*, vol. 132, pp. 217–229, Oct. 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0743731517303453

[318] Z. Song, Y. Sun, J. Wan, L. Huang, Y. Xu, and C.-H. Hsu, "Exploring robustness management of social Internet of Things for customization manufacturing," *Future Gener. Comput. Syst.*, vol. 92, pp. 846–856, Mar. 2019.

[319] C. Li and G. Miklau, "Optimal error of query sets under the differentially-private matrix mechanism," in *Proc. 16th ACM Int. Conf. Database Theory*, 2013, pp. 272–283.

[320] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial Internet of Things," in *Proc. 52nd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, 2015, pp. 1–6.

[321] J. Sathishkumar and D. R. Patel, "Enhanced location privacy algorithm for wireless sensor network in Internet of Things," in *Proc. IEEE Int. Conf. Internet Things Appl. (IOTA)*, 2016, pp. 208–212.

[322] D. Alahakoon and X. Yu, "Smart electricity meter data intelligence for future energy systems: A survey," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 425–436, Feb. 2016.

[323] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtáč, "Smart meter data privacy: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2820–2835, 4th Quart., 2017.

[324] D. Li, Q. Yang, W. Yu, D. An, X. Yang, and W. Zhao, "A strategy-proof privacy-preserving double auction mechanism for electrical vehicles demand response in microgrids," in *Proc. IEEE 36th Int. Perform. Comput. Commun. Conf. (IPCCC)*, 2017, pp. 1–8.

[325] A. V. D. M. Kayem, C. Meinel, and S. D. Wolthusen, "A smart microgrid architecture for resource constrained environments," in *Proc. IEEE 31st Int. Conf. Adv. Inf. Netw. Appl. (AINA)*, 2017, pp. 857–864.

[326] P. L. Ambassa, A. V. D. M. Kayem, S. D. Wolthusen, and C. Meinel, "Privacy risks in resource constrained smart micro-grids," in *Proc. IEEE 32nd Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, May 2018, pp. 527–532.

[327] M. Gohar, M. Muzammal, and A. U. Rahman, "SMART TSS: Defining transportation system behavior using big data analytics in smart cities," *Sustain. Cities Soc.*, vol. 41, pp. 114–119, Aug. 2018.

[328] M.-C. Chuang and J.-F. Lee, "PPAS: A privacy preservation authentication scheme for vehicle-to-infrastructure communication networks," in *Proc. IEEE Int. Conf. Consum. Electron. Commun. Netw. (CECNet)*, 2011, pp. 1509–1512.

[329] S. Purri, T. Choudhury, N. Kashyap, and P. Kumar, "Specialization of IoT applications in health care industries," in *Proc. IEEE Int. Conf. Big Data Anal. Comput. Intell. (ICBDAC)*, 2017, pp. 252–256.

[330] L. Patrono, P. Primiceri, P. Rametta, I. Sergi, and P. Visconti, "An innovative approach for monitoring elderly behavior by detecting home appliance's usage," in *Proc. 25th IEEE Int. Conf. Softw. Telecommun. Comput. Netw. (SoftCOM)*, 2017, pp. 1–7.

[331] V. S. Alagar, K. Periyasamy, and K. Wan, "Privacy and security for patient-centric elderly health care," in *Proc. IEEE 19th Int. Conf. e-Health Netw. Appl. Services (Healthcom)*, 2017, pp. 1–6.

[332] Policy Engagement Network, "Electronic health privacy and security in developing countries and humanitarian operations," Protecting Med. Inf. eHealth Projects, London School Econ. Political Sci., London, U.K., Rep., pp. 1–28, 2010.

[333] W. Gao, W. Yu, F. Liang, W. G. Hatcher, and C. Lu, "Privacy-preserving auction for big data trading using homomorphic encryption," *IEEE Trans. Netw. Sci. Eng.*, to be published.

[334] J. Murtagh and S. Vadhan, "The complexity of computing the optimal composition of differential privacy," in *Proc. Theory Cryptography Conf.*, 2016, pp. 157–175.

[335] J. Zhang, G. Cormode, C. M. Procopiuc, D. Srivastava, and X. Xiao, "PrivBayes: Private data release via Bayesian networks," *ACM Trans. Database Syst.*, vol. 42, no. 4, pp. 1–41, Oct. 2017. [Online]. Available: http://doi.acm.org/10.1145/3134428

[336] R. Chen, Q. Xiao, Y. Zhang, and J. Xu, "Differentially private high-dimensional data publication via sampling-based inference," in *Proc. 21st ACM SIGKDD Int. Conf. Knowl. Disc. Data Min.*, 2015, pp. 129–138.

[337] P. Kairouz, K. Bonawitz, and D. Ramage, "Discrete distribution estimation under local privacy," *arXiv preprint arXiv:1602.07387*, 2016.

[338] C. Dwork and G. N. Rothblum, "Concentrated differential privacy," *arXiv preprint arXiv:1603.01887*, 2016.

[339] G. Kellaris, S. Papadopoulos, X. Xiao, and D. Papadias, "Differentially private event sequences over infinite streams," *Proc. VLDB Endow.*, vol. 7, no. 12, pp. 1155–1166, 2014.

[340] C. Dwork, M. Naor, T. Pitassi, and G. N. Rothblum, "Differential privacy under continual observation," in *Proc. 42nd ACM Symp. Theory Comput.*, 2010, pp. 715–724.

[341] Z. Cui, F. Xue, X. Cai, Y. Cao, G.-G. Wang, and J. Chen, "Detection of malicious code variants based on deep learning," *IEEE Trans. Ind. Informat.*, vol. 14, no. 7, pp. 3187–3196, Jul. 2018.

[342] C. Elkan, "Preserving privacy in data mining via importance weighting," in *Proc. Int. Workshop Privacy Security Issues Data Min. Mach. Learn.*, 2010, pp. 15–21.

[343] M. Senekane, M. Mafu, and B. M. Taele, "Privacy-preserving quantum machine learning using differential privacy," in *Proc. IEEE AFRICON*, 2017, pp. 1432–1435.

[344] X. Ma, J. Ma, S. Gao, and Q. Yao, "APDL: A practical privacy-preserving deep learning model for smart devices," in *Proc. Int. Conf. Mobile Ad Hoc Sensor Netw.*, 2017, pp. 377–390.

[345] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Gener. Comput. Syst.*, vol. 25, no. 6, pp. 599–616, 2009.
[346] Y. Li, H. Yu, B. Song, and J. Chen, "Image encryption based on a single-round dictionary and chaotic sequences in cloud computing," *Concurrency Comput. Pract. Exp.*, Mar. 2019, Art. no. e5182.
[347] Z. Sanaei, S. Abolfazli, A. Gani, and R. Buyya, "Heterogeneity in mobile cloud computing: Taxonomy and open challenges," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 369–392, 4th Quart., 2014.
[348] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 2, pp. 843–859, 2nd Quart., 2013.
[349] X. Zhang *et al.*, "MRMondrian: Scalable multidimensional anonymisation for big data privacy preservation," *IEEE Trans. Big Data* to be published.
[350] M. Zhang, H. Wang, Z. Cui, and J. Chen, "Hybrid multi-objective cuckoo search with dynamical local search," *Memetic Comput.*, vol. 10, no. 2, pp. 199–208, 2018.
[351] S. Sharma, J. Powers, and K. Chen, "PrivateGraph: Privacy-preserving spectral analysis of encrypted graphs in the cloud," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 5, pp. 981–995, May 2018.
[352] M. T. Hale and M. Egerstedt, "Cloud-enabled differentially private multi-agent optimization with constraints," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 4, pp. 1693–1706, Dec. 2018.
[353] M. Yang, A. Margheri, R. Hu, and V. Sassone, "Differentially private data sharing in a cloud federation with blockchain," *IEEE Cloud Comput.*, vol. 5, no. 6, pp. 69–79, Nov./Dec. 2018.
[354] L. Kong, D. Zhang, Z. He, Q. Xiang, J. Wan, and M. Tao, "Embracing big data with compressive sensing: A green approach in industrial wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 10, pp. 53–59, Oct. 2016.
[355] M. Du, K. Wang, Z. Xia, and Y. Zhang, "Differential privacy preserving of training model in wireless big data with edge computing," *IEEE Trans. Big Data*. to be published.
[356] M. Du, K. Wang, X. Liu, S. Guo, and Y. Zhang, "A differential privacy-based query model for sustainable fog data centers," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 2, pp. 145–155, Apr.–Jun. 2019.
[357] G. Karame and S. Capkun, "Blockchain security and privacy," *IEEE Security Privacy*, vol. 16, no. 4, pp. 11–12, Jul./Aug. 2018.
[358] F. Gao, L. Zhu, M. Shen, K. Sharif, Z. Wan, and K. Ren, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Netw.*, vol. 32, no. 6, pp. 184–192, Nov./Dec. 2018.
[359] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing: Challenges and applications," *arXiv preprint arXiv:1711.05938*, 2017.
[360] M. Banerjee, J. Lee, and K.-K. R. Choo, "A blockchain future for Internet of Things security: A position paper," *Digit. Commun. Netw.*, vol. 4, no. 3, pp. 149–160, 2018.
[361] A. Alnemari *et al.*, "Protecting infrastructure data via enhanced access control, blockchain and differential privacy," in *Proc. Int. Conf. Crit. Infrastruct. Protect.*, 2018, pp. 113–125.
[362] R. Henry, A. Herzberg, and A. Kate, "Blockchain access privacy: Challenges and directions," *IEEE Security Privacy*, vol. 16, no. 4, pp. 38–45, Jul./Aug. 2018.
[363] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Security Privacy Workshops (SPW)*, 2015, pp. 180–184.
[364] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Gener. Comput. Syst.*, vol. 97, pp. 512–529, Aug. 2019.
[365] H. Halpin and M. Piekarska, "Introduction to security and privacy on the blockchain," in *Proc. IEEE Eur. Symp. Security Privacy Workshops (EuroS&PW)*, 2017, pp. 1–3.
[366] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 472–486, 1st Quart., 2013.
[367] M. Pilz and L. Al-Fagih, "Recent advances in local energy trading in the smart grid based on game–theoretic approaches," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1363–1371, Mar. 2019.
[368] X. Wu, T. Wu, M. Khan, Q. Ni, and W. Dou, "Game theory based correlated privacy preserving analysis in big data," *IEEE Trans. Big Data*, to be published.
[369] L. Xu, C. Jiang, Y. Qian, J. Li, Y. Zhao, and Y. Ren, "Privacy-accuracy trade-off in differentially-private distributed classification: A game theoretical approach," *IEEE Trans. Big Data*, to be published.

Muneeb Ul Hassan received the bachelor's degree in electrical engineering from the COMSATS Institute of Information Technology, Wah Cantt, Pakistan, in 2017. He is currently pursuing the Ph.D. degree with the Swinburne University of Technology, Hawthorn, VIC, Australia. His research interests include privacy preservation, blockchain, game theory, and smart grid. He was a recipient of the Gold Medal in bachelor's degree for being topper of Electrical Engineering Department. He served in the TPC for the IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2019). He is a Reviewer of various journals, such as the IEEE COMMUNICATIONS SURVEYS & TUTORIALS, the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, *Future Generation Computing Systems* (Elsevier), the *Journal of Network and Computer Applications*, *Computers & Electrical Engineering*, IEEE ACCESS, the *Transactions on Emerging Telecommunications Technologies* (Wiley), the IEEE JOURNAL OF COMMUNICATIONS AND NETWORKS, *Wireless Networks* (Springer), *Human-Centric Computing and Information Sciences*, and the *KSII Transactions on Internet and Information Systems*. He also has been a Reviewer for various conferences, such as IEEE Vehicular Technology Conference (VTC)-Spring in 2019, Vehicular Technology Conference (VTC)-Fall in 2018, IEEE International Conference on Communications (ICC) in 2019, International Workshop on e-Health Pervasive Wireless Applications and Services e-HPWAS'18, IEEE Globecom 2018 Workshop: Security in Health Informatics (SHInfo2018), Frontiers of Information Technology in 2019, Frontiers of Information Technology in 2018.

Mubashir Husain Rehmani (M'14–SM'15) received the B.Eng. degree in computer systems engineering from the Mehran University of Engineering and Technology, Jamshoro, Pakistan, in 2004, the M.S. degree from the University of Paris XI, Paris, France, in 2008, and the Ph.D. degree from University Pierre and Marie Curie, Paris, in 2011. He is currently an Assistant Lecturer with the Cork Institute of Technology, Ireland. From September 2017 to October 2018, he was a Post-Doctoral Researcher with the Telecommunications Software and Systems Group, Waterford Institute of Technology, Waterford, Ireland. He was an Assistant Professor with the COMSATS Institute of Information Technology, Wah Cantt., Pakistan, for five years. He has authored/edited two books published by IGI Global, USA, one book published by CRC Press, USA, and one book with Wiley, U.K. He was a recipient of the "Best Researcher of the Year 2015 of COMSATS Wah" Award in 2015, Certificate of Appreciation, "Exemplary Editor of the IEEE COMMUNICATIONS SURVEYS & TUTORIALS for the year 2015" from the IEEE Communications Society, the Best Paper Award from IEEE ComSoc Technical Committee on Communications Systems Integration and Modeling in IEEE ICC 2017, and the Best Paper Award in 2017 from Higher Education Commission, Government of Pakistan. He consecutively received Research Productivity Award in 2016–17 and also ranked #1 in all Engineering disciplines from Pakistan Council for Science and Technology, Government of Pakistan. He is currently an Area Editor of the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS. He served as an Associate Editor for the IEEE COMMUNICATIONS SURVEYS & TUTORIALS from 2015 to 2017. He currently serves as an Associate Editor for the *IEEE Communications Magazine*, the *Journal of Network and Computer Applications* (Elsevier), and the *Journal of Communications and Networks*, a Guest Editor for *Ad Hoc Networks* (Elsevier), *Future Generation Computer Systems* (Elsevier), the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and *Pervasive and Mobile Computing* (Elsevier).

Jinjun Chen received the Ph.D. degree in information technology from the Swinburne University of Technology, Australia, where he is a Professor and the Deputy Director with Swinburne Data Science Research Institute. His research results have been published in over 160 papers in international journals and conferences, including various IEEE/ACM TRANSACTIONS. His research interests include scalability, big data, data science, data systems, cloud computing, data privacy and security, health data analytics, and related various research topics.