IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 12, 2021, accepted October 14, 2021, date of publication October 29, 2021,
date of current version November 22, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3124309

Differential Privacy for IoT-Enabled Critical Infrastructure: A Comprehensive Survey

MUHAMMAD AKBAR HUSNOO[1], ADNAN ANWAR[1], (Member, IEEE), RIPON K. CHAKRABORTTY[2], (Member, IEEE), ROBIN DOSS[1], (Senior Member, IEEE), AND MIKE J. RYAN[3], (Senior Member, IEEE)

[1]Centre for Cyber Security Research and Innovation (CSRI), School of Information Technology, Deakin University, Geelong, VIC 3216, Australia
[2]School of Engineering and IT, University of New South Wales (UNSW), Canberra, ACT 2610, Australia
[3]Capability Associates, Canberra, ACT 2610, Australia

Corresponding author: Adnan Anwar (adnan.anwar@deakin.edu.au)

This work was supported in part by the Centre of Cyber Security Research and Innovation (CSRI) funded by Deakin University through the CSRI 2020 Summer Scholarship.

ABSTRACT The rapid evolution of the Internet of Things (IoT) paradigm during the last decade has lead to its adoption in critical infrastructure. However, the multitude of benefits that are derived from the IoT paradigm are short-lived due to the exponential rise in the associated security and privacy threats. Adversaries carry out privacy-oriented attacks to gain access to the sensitive and confidential data of critical infrastructure for various self-centered, political and commercial gains. In the past, researchers have employed several privacy preservation approaches including cryptographic encryption and k-anonymity to secure IoT-enabled critical infrastructure. However, for various reasons, those proposed solutions are not well suited for modern IoT-enabled critical infrastructure. Therefore, Dwork's differential privacy has emerged as the most viable privacy preservation strategy for IoT-enabled critical infrastructure. This paper provides a comprehensive and extensive survey of the application and implementation of differential privacy in four major application domains of IoT-enabled critical infrastructure: Smart Grids (SGs), Intelligent Transport Systems (ITSs), healthcare and medical systems, and Industrial Internet of Things (IIoT). Finally, we discuss some promising future research directions in differential privacy for IoT-enabled critical infrastructure.

INDEX TERMS Differential privacy, healthcare systems, the Internet of Things (IoT), intelligent transport system (ITS), industrial Internet of Things (IIoT), privacy preservation, smart grid (SG).

I. INTRODUCTION

The rapid evolution of ubiquitous computing has led to the advent of a novel communication paradigm known as the Internet of Things (IoT). The IoT envisions an intelligent inter-connected network of everything to allow interaction and exchange of information based on agreed protocols without requiring human intervention. Throughout the last decade, several economic giants including USA and China have prioritized the developments and advancements of IoT-enabled systems and there have been remarkable advancements in this interesting field ever since. By the end of 2020, the global number of IoT-enabled systems is predicted to surpass 50 billion with China alone accounting for 24 billion IoT-enabled systems [1], [2]. Some years ago, independent embedded systems and sensors were utilized for conducting and monitoring a variety of processes and tasks in a range of sectors. The exponential growth of their applications precipitated the inter-connection of everything under a common infrastructure to provide information and control of state of objects [3] which ultimately led to the birth of IoT-enabled systems.

In addition to the ability of IoT-enabled systems to inter-connect several 'things' for efficient communication and data sharing across a single network, its vast array of benefits derived has grasped the attention of several technologists [4], [5]. Surprisingly, in a short span of time, IoT-enabled systems have become an integral part of several sectors, such as manufacturing, healthcare, transport and logistics, giving rise to IoT-enabled critical infrastructure (CI) [6]. Due to its increased architectural complexity and the use of several heterogeneous devices, privacy threats are strenuous to identify,

The associate editor coordinating the review of this manuscript and approving it for publication was Nadeem Iqbal.

assess and mitigate. Furthermore, those complex large-scale IoT-enabled systems create a data deluge. Since sensitive and confidential data are constantly being shared across the networks, security and privacy are the major prevailing concerns in the IoT-enabled CI [7]. Any cyber attack on those vulnerable systems can compromise the privacy and integrity of massive amounts of sensitive data.

There are several types of attacks performed on IoT-enabled CI including Sybil attacks, Denial of Service attacks and so on [8], [9]. Cyber attacks based on the access level of IoT-enabled critical networks can be categorized into active and passive attacks [10]. Active attacks, also known as security-oriented attacks, disrupt the network communication by evading the available security protection. On the other hand, passive attacks, also called privacy-oriented attacks, include eavesdropping the network, without causing any disruption, to gain illicit access to sensitive confidential information [10], [11]. The rapidly evolving IoT-enabled CIs are now becoming susceptible to several attacks launched by hackers and organized criminal syndicates [12]. Motivated by the rise in the number of privacy threats targeted for IoT-enabled CIs, several solutions are being developed. However, most of those proposed security approaches lack in applicability which may be due to computational complexity, costs as well as other related factors [11].

A. MOTIVATION: DIFFERENTIAL PRIVACY FOR IoT-ENABLED CRITICAL SYSTEMS

Over the last decade, a wide range of *cryptographic approaches* have been proposed by researchers in the view of tackling privacy concerns in IoT-enabled CIs [13]. Cryptographic techniques are the traditional data privacy mechanisms that encrypt the data using public or private keys prior to transmission at the sending end/node and decrypt data using those keys at the receiving end/node [14]. While several of those developed techniques can efficiently safeguard data privacy in IoT-enabled CIs, the usage of cryptographic encryption and decryption techniques with public and private keys present several drawbacks:

- The implementation of cryptographic measures for IoT-enabled CIs is rather challenging due to the increased computational complexities involved [14];
- A node failure within the whole IoT-enabled critical network prevents the decryption and collection of data from the other network nodes due to missing network keys [14], [15];
- Asymmetric key cryptography techniques require the generation and distribution of the public and/or private keys. The processes involved are quite time-consuming, hence diminishing the whole CI speed [14], [15]; &
- Computational resources and costs associated with cryptography techniques on huge public datasets are relatively high [14].

Furthermore, several researchers have also proposed *data anonymization techniques* for data privacy preservation in IoT-enabled CIs [16]. During data anonymization techniques, unique personal identifiers such as name, ID number, etc. are discarded prior to query evaluation [17]. Sweeney [18] first proposed a practical application of k-anonymity for privacy preservation on static datasets. Its application has, since then, been extended to privacy preservation in dynamic high dimensional datasets whereby new data are continuously updated, anonymized and shared [19]. However, data anonymization techniques present certain drawbacks when applied for IoT-enabled CI:

- The data anonymization trade-off between data quality and utility results in the loss of original data during sharing and publishing [18]. For instance, the faster the anonymization, the greater the loss of original data [17];
- In IoT-based critical networks, data streams may also consist of missing data values. However, most of the conventional data anonymization techniques fail to handle missing values in data streams [17];
- Adversaries with background knowledge of the data may compromise data privacy through several privacy breach attacks such as unsorted matching attacks, temporal attacks and complementary release attacks [20];
- In large datasets, the risks of data re-identification from the already anonymized data still prevail [21].

The aforementioned existing data privacy preservation techniques failed to tackle the security issues faced by IoT CI. In response, several research efforts were geared towards the development of a more effective practical solution to overcome those rising threats. Dwork [22], [23] first developed a novel scheme entitled ***differential privacy*** (DP). In brief, DP, a statistical anonymity model, safeguards privacy of data by adding a desired amount of randomised noises using various mathematical algorithms [22]. An in-depth explanation of DP is given in the later section. Following Dwork's proposed privacy preservation schemes, DP gained industry-wide acclaims for its low complexity and resilience against privacy breaches.

As opposed to the other previously mentioned data privacy preservation methods, the DP approach further guarantees the definition of a formal level of privacy [23]. Furthermore, DP assumes that an adversary has the maximum background knowledge of a database. Therefore, DP approaches ignore an enemy's background knowledge of the dataset whilst still protecting privacy of records [24]. In 2010, Rastogi and Nath [25] first proposed the application of DP for distributed time-series data within a network. The researchers implemented a two-staged distributed protocol, PASTE, making usage of Distributive Fourier Transform, homomorphic encryption and threshold encryption. The proposed solution was evaluated using three real datasets: GPS trace from Microsoft's Multiperson Local Survey, Body weight trace from a weight-monitoring website and Traffic trace from the Department of Transportation of San Antonio, Texas. This research, showing an improved accuracy, managed to solve the issues that hindered participatory data mining by ensuring data privacy through the adoption of DP and the provision of a formal privacy guarantee during data publishing.

Rastogi and Nath's [25] innovative approach for privacy preservation in distributed data sources illustrated the accuracy of DP and its extensions for IoT networks. Within the last five years, major companies have initiated the utilization of DP in several IoT-enabled systems [26]. Similarly, DP approaches have found their way into IoT-enabled CI. For instance, Bohli *et al.* [27] first introduced the application of DP in modern energy systems (smart-grids) to provide the 'perfect privacy' under certain conditions. Similarly, Shi *et al.* [28] put forward the application of differential privacy for railway freights systems. Lin *et al.* [29] proposed a light-weight DP-based privacy preservation scheme for sensitive big data in WBANs. Additionally, several other researchers have introduced the notion of differential privacy for privacy preservation in IoT-enabled CIs.

B. SCOPE: OUR SURVEY

Only a handful of previous survey articles have focused on DP techniques either in general IoT-enabled domains or are limited to certain IoT-enabled critical domains. However, to the best of our knowledge, there is very little or no other previous surveys that have addressed DP approaches in the critical IoT-enabled infrastructure domains. Therefore, this survey is the first to comprehensively include the practical aspects and application of current state-of-the-art DP schemes for the critical IoT-enabled critical energy, medical, transport and industrial infrastructure. To this regard, Table 1 provides a chronological format such that previous related survey articles in these research domains can be compared and contrasted with this study. This enables the reader to have a clearer overview of the scope of this survey.

C. CONTRIBUTIONS: OUR SURVEY

As far as it can be recalled, there is a lack of comprehensive survey on the adoption and utilization of DP approaches in critical IoT-enabled infrastructures which gave rise to unresolved future directives in this field. Therefore, in this paper, we present a thorough survey on the current state-of-the-art literature on DP approaches applied to each of the critical IoT-enabled infrastructure domains. The contributions of the review are as follows:

- We review existing survey articles on DP to highlight their major contributions.
- We provide an extensive and comprehensive survey of the implementation of DP in IoT-Enabled Critical Infrastructure.
- We emphasize the focus of this manuscript to review the practical implementation of DP on the four main application domains namely Energy, Transport, Healthcare and Industrial IoT-enabled CIs.
- Lastly, we summarize some open challenges and possible future research directions to help advance research in the implementation of DP in IoT-enabled CIs.

In our work, we address the lack of surveys as highlighted in Table 1 below. We divide and survey the papers related to the application of DP in four major critical areas namely Energy, Transport, Healthcare and Industrial IoT-enabled Systems. For each related aforementioned area, we first give a brief overview of the application domains and then survey the existing literature through into sub-fields of each domain. Lastly, we also provide some future research directions to help the readers and researchers advance the several aspects of DP applications and implementation in the related CIs.

D. ARTICLE ORGANISATION: OUR SURVEY

This survey paper has been structurally organized to ease reader's understanding. This section gives an brief introduction to the topic in question with Table 2 presenting the list of abbreviations used throughout the survey. The remaining sections of this paper are organised as follows: Sections II and III provide an overview of IoT-enabled CIs and security aspects, and, DP and its relation to IoT-enabled CIs respectively. Sections V, IV, VI, VII surveys in details the application of DP for privacy preservation of IoT-enabled infrastructures in each scoped critical sector namely Energy, Healthcare, Transportation and Industry respectively. Section VIII gives an outline of prevailing open issues, challenges and future vital research areas to focus on. Lastly, Section X concludes this survey manuscript.

II. IoT-ENABLED CIs AND SECURITY ASPECTS

The advent of computers followed by the birth of the internet motivated the concept of 'connected things'. While smart devices are now a common buzzword in the 21st century, interest in the development and deployment of connected electrical and electronics equipment began in the early 1980's. The famous Coca Cola vending machine at Carnegie Mellon University was the first IoT-type equipment to be connected to the internet. In the start of the following decade, major advancements in the connected equipment concept included the Trojan Room Coffee Pot at the University of Cambridge which had a camera connected to the internet and John Romkey's toaster which could be operated wirelessly through the internet [53], [54].

In 1999, Kevin Ashton coined the term ***IoT*** as the title of a presentation made at Procter & Gamble [55]. Since then, IoT industry experienced a major leap with electronics giant, LG, initiating IoT commercialisation by developing a smart refrigerator that intelligently realise any food stock replenishment and alert its user [53]. The following decades witnessed a remarkable progress towards IoT, which became the preferred solution to countless challenges affecting every aspect of life ranging from homes to manufacturing plants and beyond [41].

Whilst research in IoT has seen remarkable growth, no exact universal formal definition has yet been adopted for the term. Table 3 provides a list of definitions adopted by some organisations. In an IoT perspective, 'Things' can be regarded as any internet-connected physical or virtual objects (including people) which have the ability to communicate and interact among each other or with human users [56]. IoT in 2021 has come down the road burgeoning and

TABLE 1. Chronological comparison of prior survey articles based on the adoption and implementation of DP in several domains.

Survey	Year	Contributions	Application Domain
[30]	2011	Extensive survey on privacy schemes in social media.	Social Media
[31]	2012	Historical survey of two separate applications of DP:location pattern mining and health data.	Statistical Databases
[32]	2012	Overview of DP and its use in privacy-preservation sampling.	Statistical Databases
[33]	2012	Short review of the literature on DP implementations on Health datasets.	Statistical Databases
[34]	2012	Survey of the implementation of DP for non-interactive publication of anonymized real-life datasets.	Statistical Databases
[35]	2012	Survey of the existing standards for adapting DP to network data and analyse the feasibility of several common social-network analysis techniques under these standards.	Social Networks Analysis
[36]	2013	Review of the progress made on differentially private machine learning and signal processing.	Sensitive Data Mining and Signal Processing
[37]	2013	Comparative study of the existing protocols, security schemes and DP mechanisms in terms of their complexity and security characteristics.	Participatory sensing and statistical databases
[38]	2013	Survey of the DP, its interactive versus non-interactive settings, perturbation mechanisms, and typical applications found in recent research.	Statistical Databases
[39]	2014	Exploration of the interplay between machine learning and DP, namely privacy-preserving machine learning algorithms and learning-based data release mechanisms.	Mining Sensitive Data
[40]	2014	Survey of the implementation of DP in various data mining algorithms with interface-based/fully access-based modes and the evaluation of the performance of the algorithms.	Statistical Data mining
[41]	2015	Review of of basic concepts and implementation mechanisms related to DP.	Statistical Databases and Pattern Mining
[42]	2016	Overview of privacy preservation schemes for collecting and storing data in mobile recommender systems.	Mobile Recommender Systems
[43]	2016	Study of the methods for quantification of privacy where the semantics are bounded by finite precision.	Semantics
[44]	2016	Overview of DP and its technical aspects in huge structured and unstructured datasets.	Big Data
[45]	2017	Comprehensive Survey on query processing and data publishing though DP.	N/A
[46]	2018	Comparative study of DP as compared to other privacy approaches.	Big Data
[47]	2019	Survey of how DP interacts with each of the components that constitute decision tree algorithms.	Statistical Data mining
[48]	2019	Extensive Survey of the application of LDP in securing IoV.	IoV
[49]	2020	Comprehensive survey on LDP towards data statistics and analysis in crowdsensing.	Crowdsensing
[50]	2020	Detailed analysis over integration of differential privacy in blockchain scenarios.	Blockchain
[51]	2021	A review on differentially private machine learning.	Machine Learning
[52]	2021	A comprehensive review on privacy attacks on social networks, types of differential privacy in social network analysis, a degree distribution analysis, subgraph counting and edge weights.	Social Network Analysis
[Our survey]	2021	Comprehensive in-depth survey covering the adoption and implementation of DP in four critical areas:energy, transportation, healthcare and Industrial.	IoT-enabled CIs

continuously evolving where opportunities and imaginations have been rendered boundless. As we enter the start of the third IoT decade, the number of IoT devices is expected to double to 31 billion by the end of 2025 [1].

TABLE 2. Common abbreviations in our survey with corresponding definitions.

Abbreviations	Definitions
ARP	Address Resolution Protocol
CI	Critical Infrastructure
CIDS	Collaborative Intrusion Detection Systems
CSP	Constraints Satisfacion Problem
DCS	Distributed Control Systems
DoS	Denial of Service
DP	Differential Privacy
DR	Demand Response
DSM	Demand Side Management
EHR	Electronic Health Records
EV	Electric Vehicle
HIoT	Healthcare - Internet of Things
IIoT	Industrial Internet of Things
ITS	Intelligent Transport Systems
IoT	Internet of Things
IoV	Internet of Vehicles/Internet of connected Vehicles
IT	Information Technology
LDP	Local Differential Privacy
MITM	Man In The Middle
NILM	Non-Intrusive Load Monitoring
NP-hard	Non-deterministic Polynomial-time Hardness
PII	Personal Identifiable Information
SG	Smart Grid
T&D	Transmission and Distribution
VANET	Vehicle Ad-hoc Networks
WBAN	Wireless Body Area Network

A. IoT-ENABLED CRITICAL INFRASTRUCTURE

The real IoT-enabled CI era initiated around 10 years ago when Wen Jiabao, former Chinese Premier, identified IoT to revamp and foster China's economy and strength [2]. Since then, China has invested huge sums on IoT-enabled CIs [60]. Other major economic powers also followed in the same footsteps. With everything going smart, there is a strong tendency to closely link 'smart cities' to IoT-enabled CIs. While a smart city is heavily dependent on the deployment of IoT technology to collect data for insights [61], IoT-enabled CIs only form part of the 'smart city' technological framework.

According to the United Nation's Department of Economic and Social Affairs, it is estimated that 68% of the global population is expected to live in urban cities by 2050 [62]. With the influx of people rushing to mega cities, the issue remains whether basic resources are optimally and efficiently distributed to citizens. To tackle this complex issue, governments are making significant efforts to develop effective solutions by leveraging Information Technology in view of balancing overpopulation and resources crisis. CIs are vital to an economy's cohesiveness and performance. Being regarded as the basis of digital data-driven economies, IoT is the key to enable the design of smart CIs, also known as ***IoT-enabled Critical Infrastructure*** for optimum distribution of resources, production of goods and services as well as usage of infrastructures [55]. IoT-enabled CIs are intelligent inter-related internet-connected networks of systems that work collaboratively and synergistically to manufacture and distribute an uninterrupted flow of essential goods or services [63].

With smart cities as the top agenda of several countries for the next decade, new devices are constantly being added to the network. Hence, the increases in heterogeneous network nodes lead to over complexity of the architecture of IoT-enabled CIs [64].

B. ARCHITECTURE PARADIGMS: IoT-ENABLED CI

The unprecedented growth of IoT, complemented mainly due to its inter-connectivity and real-time data sharing abilities, is set to continue in the next decade. As the application domains of IoT expand, it is now the right time to take a look at the several issues faced by IoT networks related to their architectural designs. One of the prevailing issues is the number of languages, protocols, standards and heterogeneous connected nodes that make up the IoT stack [63]. Until now, there is not a single unified IoT/IoT-enabled CI architectural model that has been agreed upon. Discussions regarding proposing a universally accepted architecture for IoT-enabled infrastructures started as early as 2013 although experts suggest even then, it may have already been well behind as IoT evolution has been dramatic [65].

Numerous initiatives, such as the IoT-A, IoT-I, EU FP7 Internet of Things Architecture project and so on, have been funded by reputed institutions to design new architectures [66]. This section prescribes some of the most common and widely adopted ones across several domains in the view of giving the reader a better comprehension of the core functional layers of an end-to-end IoT-enabled CI.

1) THREE TIER IoT ARCHITECTURE

The *three tier architecture*, as shown in Figure 1, is the most fundamental architecture blueprint introduced [65]. As its name suggests, this architectural model comprises of three layers [67] namely:

1) *Perception Layer*: Consists of physical devices, sensors and actuators chosen according to the application domain needs, that interact with the environment and continuously gather vast amounts of data which is then transferred to the network layer [65].
2) *Network Layer*: Consists of wireless and wired mediums of transmission responsible for transmitting information and translating devices in accordance with the application layer [65].
3) *Application Layer*: Responsible for delivering the specific services to users based on application type. It defines all the various instances of IoT-enabled

TABLE 3. Definitions of IoT adopted by some organisations.

Definition	Organisation
A network, which can collect information from the physical world or control the physical world objects through various deployed devices with the capability of perception, computation, execution and communication, and support communications between human and things or between things by transmitting, classifying and processing information [2].	CCSA
A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies [2].	ITU-T
A global network infrastructure, linking physical and virtual objects through the exploitation of data capture and communication capabilities [2].	EU FP7 CASAGRAS
A world-wide network of interconnected objects uniquely addressable based on standard communication protocols [2].	IETF
A network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment [57].	Gartner
A network of uniquely identifiable end points (or things) that communicate bi-directionally without human interaction using IP connectivity [58].	IDC
The connection of devices — any devices — to the internet using embedded software and sensors to communicate, collect and exchange data with one another [59].	EY

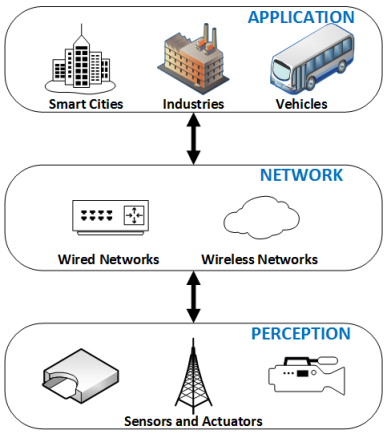

FIGURE 1. Three tier IoT architecture layers.

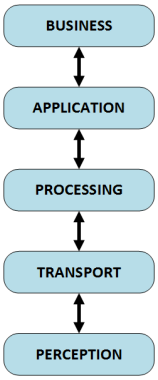

FIGURE 2. Five tier IoT architecture layers.

infrastructure deployments such as in smart grids, industries, smart cities, etc [65].

However, this three tier architecture is very basic and is unable to sustain the growing needs of a more robust IoT architecture [68]. Therefore, a five tier IoT architecture was proposed.

2) FIVE TIER IoT ARCHITECTURE

The *five tier architecture* model, as illustrated in Figure 2 comprises of the perception layer and application layer with similar responsibilities as in the three tier architecture. It additionally consists of three layers [65] namely:

1) *Transport Layer*: Comprises of wired and wireless networks such as 5G, LoRaWAN, LAN, etc. and is responsible for converting and transmitting data to and through the perception layer and the processing layer [68].
2) *Processing Layer*: Accountable for pre-processing, analysing and storing the huge chunks of data collected from the transport layer [65]. It also plays a vital role in processing and filtering the data to increase the efficiency of limited resources [68].
3) *Business Layer*: Oversees the whole infrastructure, its applications, functionalities, business and profit models while still safeguarding data and user privacy [68].

3) DISTRIBUTED IoT NETWORK ARCHITECTURES

Recent works [69] to integrate high performance distributed computing paradigms has brought about innovations in IoT Network architectures. Some of the latest ones are briefly discussed below:

1) *Cloud Based IoT Architecture*: Enables centralized deployment of huge IoT-enabled CIs. The cloud layer is responsible for everything related to data processing and storage [68]. This architecture, as depicted in Figure 4 offers flexibility and scalability of various

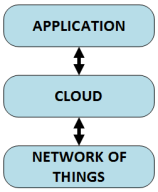

FIGURE 3. Cloud IoT architecture layers.

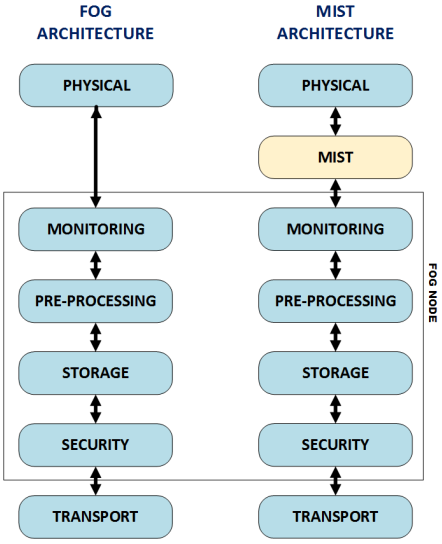

FIGURE 4. Differences between Fog and Mist IoT architecture layers.

resources such as data storage, robust infrastructure for development, analytical software and tools, etc [70].

2) *Fog Based IoT Architecture*: Moves certain processes such as monitoring and data pre-processing closer to the edge (physical layer) to enable faster automation [70]. Within Fog-based IoT architectures, the Fog Node consists of:
   a) Monitoring layer: Controls and manages power, resources, responses and services [70].
   b) Pre-processing Layer: Filters, tidies, processes and analyses data and commands [71].
   c) Storage Layer: Stores cleansed data after pre-processing [68].
   d) Security Layer: Encrypts and decrypts data for privacy preservation and cyber threats mitigation [70].

   By moving data processing closer to the edge, transmission bandwidth and cloud consumption is reduced, hence real-time performance increases. Moreover, it also solves the issue of security in IoT networks through the addition of the security layer [68], [70], [71].
3) *Mist Based IoT Architecture*: An additional mist layer is included between the physical layer and the fog node to allow real-time information across the several nodes of the network through mesh connectivity [72].

III. OVERVIEW OF DIFFERENTIAL PRIVACY

Broadly speaking, privacy is the right to freedom from interference or intrusion. However, to a more technical audience, information privacy, also known as data privacy, can be defined as the protection of sensitive and personal information relating to individuals and/or organizations. The major threat faced by IoT-enabled CIs is privacy preservation. Sensitive and personal information is being collected by those IoT infrastructure, curated and shared to both public and private organizations for various reasons including for research and statistical purposes and improvement of services. As mentioned earlier, the public sharing and dissemination of personal sensitive data can put the privacy of individuals at high risk. Privacy preservation has now become an urgent priority four IoT-enabled critical infrastructures and therefore, is an emerging field of research both in academia and in industry.

Privacy preservation, also known as statistical disclosure control, is the method of safeguarding personal and sensitive information of individuals [22]. Effective privacy preservation is a far more complex issue such that one can think of privacy as a multi-faceted concept involving several forms, for instance, only sensitive information must be safeguarded, identity of the users must be preserved, etc [73]. Furthermore, the analysis, correlation and linkage of different information sources can as well lead to unintended re-identification and disclosure of personal information [74].

A. PRIVACY ATTACKS IN IoT-ENABLED CIs

In recent years, the number of privacy attacks on IoT-enabled CIs have grown exponentially. Table 4 provides a brief overview of some of the privacy attacks in conjunction with DP and IoT-enabled CIs.

B. DIFFERENTIAL PRIVACY

Most of the state-of-the-art developments in statistical disclosure control have been completed in respect to databases. Those works can be further classified into two main groups: the first group being preservation of the entire dataset and the second one being the implementation of a theoretical framework on the basis of privacy requirement [80]. K-anonymity, L diversity and T-closeness are viable anonymization techniques related to the preservation of entire dataset [81]. The prevalent concerns of other privacy preservation techniques include lack of data usefulness after anonymization, risk of re-identification after anonymization, unprotected queries, unsafe query auditing, etc [22].

Motivated by those concerns regarding statistical databases, Dwork proposed the quantification of privacy through a concept known as DP [22], [23]. It is critical to note that DP is not an algorithm but a concept. Since its proposal, DP has born fruit and is being thoroughly applied to IoT-enabled CIs. With the assumption that the curator is trustworthy, DP is totally independent of the prior knowledge of the adversary. The major goal of DP is make sure that every record in the dataset is given the same amount of privacy regardless of whether

TABLE 4. Privacy attacks in conjunction with DP and IoT-enabled CIs.

Privacy Attacks	Description
Correlation	During this attack, the intruder aims at finding the correlations that may exist from different de-identified datasets based on some previous knowledge of the data [75]. From the correlations, the intruder is able to re-identify the sensitive data of an individual and this leads to privacy breaches. Therefore, an effective privacy preservation mechanism is required to reduce the risk of breaches during data sharing.
Differencing	During this attack, the adversary sends multiple indirect queries from background knowledge of the dataset and the individual in the view of gaining sensitive information [76]. If a direct query about any individual record is made, the query is automatically blocked. Differencing attacks are one of the simplest and most common forms of attacks. Therefore it is necessary to have a privacy preserving mechanism that safeguards the data from adversaries.
Disclosure	During this traffic pattern analysis attack, the attacker aims to identify mutually disjoint sets of receivers on the basis of observed traffic and aims to compromise the communication [77]. However, it is worth noting that the two main issues with disclosure attacks are time taken for the operation to complete which is exponential to the number of traffic data analysed and the tedious implementation which is equivalent to solving the Constraints Satisfaction Problem (CSP) which is NP-hard [78]. Nonetheless, the data being communicated from one node to another of an IoT-enabled CI must be protected such that even if an attacker is able to compromise the communication, privacy is still preserved.
Linking	During this attack the adversary aims to link and combine an external data source together with a de-identified dataset with the aim of re-identifying the records and inferring the sensitive information of individuals [79]. With huge amount of data available, linking attacks are becoming more and more popular. Thus, it is essential to have an effective privacy preservation approach for databases.

the observation is included in the dataset [82]. From a more technical perspective, DP is a formal framework to quantify to what extent individual privacy in a statistical database is preserved while releasing useful aggregate information about the database [83].

1) MATHEMATICAL DEFINITIONS

Let R be the randomized algorithmic function applied by a curator while releasing information. The randomized function guarantees that the output of a query is indistinguishable whether or not a specific observation is present in a dataset. Considering datasets to be made up of rows, it is implicit that two neighbouring datasets,B_1 and B_2 are different by at least one additional row [82].

1) *Definition 1 (Adjacent Datasets):* A randomized algorithmic function, R, gives ϵ-DP if any two neighbouring datasets, B_1 and B_2, differ by at most one element for any possible outcome, S, $S \subseteq Range(R)$ where $Range(R)$ is the range of resultant output function R [80], [82]. The mathematical definition is as follows:

$$P[R(B_1) \in S] \leq exp(\epsilon) \times P[R(B_2 \in S)] \qquad (1)$$

where ϵ is the privacy parameter which sets the desired level of privacy.

2) *Definition 2 (Sensitivity):* Consider a query is a function f and a database is X, the global sensitivity is the value of $f(X)$. The sensitivity value sets the desired amount of perturbation in the differentially private mechanism [82], [84]. The mathematical definition is as follows:

For $f: B \rightarrow R^k$, the sensitivity Δf is:

$$\Delta f = \max_{B_1,B_2} \|f(B_1 - f(B_2)\|_1 \qquad (2)$$

where for $k = 1$, the sensitivity of f is the maximum possible difference between query outputs from two adjacent datasets that differ by at most one element.

2) EXISTING METHODS

Existing approaches for DP can be further classified into two groups [80]:

1) *Methods that do not take into consideration the datasets*: DP Optimization protocols [80] do not take into consideration the database while performing noise addition via Laplacian or Exponential mechanism [85], [85]–[89]. On the other hand, DP Sensitivity Calibration protocols [80] involve the smoothing and balancing of the sensitivity value, Δf, to a healthy trade-off to maintain data utility [90]–[95].
To preserve the data privacy in relation to a probability distribution, it is desired to use DP optimization protocols. On the other hand, to preserve the data privacy in relation to a sensitivity value, it is desired to use DP Sensitivity Calibration protocols. However, it must be noted that both the protocols can be used together to adjust both the probability density and the sensitivity value to achieve the desired amount of privacy.
2) *Methods that take into consideration the datasets*: The correlation among the different records and attributes [80] of a dataset is exploited to maintain a healthy trade-off between data utility and data privacy [96]–[98]. Furthermore, DP Database Synopsis [80]

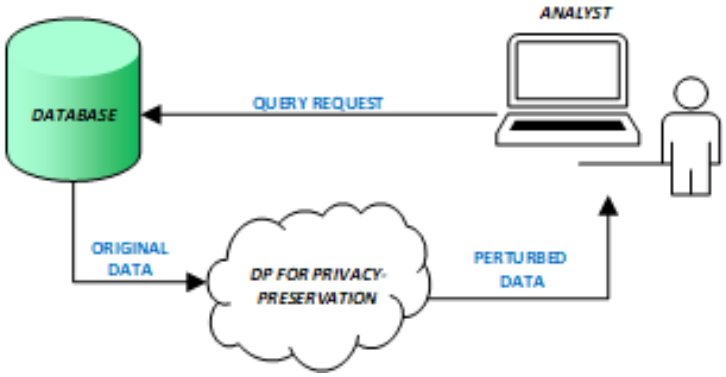

FIGURE 5. Basic block diagram of data perturbation using DP.

enables the creation of a database synopsis through several techniques such as decomposition, transformation and/or compression. The main aim of this method is to optimize the error rate and data utility while satisfying ϵ-DP during noise addition [25], [99]–[101].

3) NOISE ADDITION MECHANISMS

Noise Addition Mechanisms, also referred to as data perturbation mechanisms [85], are methods through which noise can be added to the data in the view of preserving data privacy. The amount of noise to be incorporated in the dataset is directly proportional to the sensitivity value, Δf and the privacy loss, ϵ [102]. The three noise addition mechanisms for DP are:

1) *Laplace Mechanism*: Laplace Mechanism is one of the most utilized methods for adding Laplace distributed artificial noise to sensitive data [103]. The magnitude of the noise added will be calibrated by $Lap(\Delta f/\epsilon)$ [82]. Low sensitivity queries require very little noise. Considering the database, B, the Randomized Function, R and the sensitivity value, Δf, the randomized Laplace Algorithm, L can be denoted as:

$$L = R(B) + Lap(\frac{\Delta f}{\epsilon}) \tag{3}$$

2) *Exponential Mechanism*: Exponential Mechanism is another commonly used methods for DP whenever the outputs are not numerical. The exponential mechanism was developed for instances whereby the best response must be picked, for example, adding noise directly to an optimal value will highly impact data utility [82]. Considering the database, B, l can be considered a potential element of the answer set L, $l \in L$ for the scoring function, $s : B \times L \rightarrow L$. The randomized Exponential Algorithm, E, can be denoted as:

$$E(B, s) = l : \|P[l \in L] \propto exp(\epsilon s(B, s)/2\Delta s)\| \tag{4}$$

3) *Gaussian Mechanism*: Gaussian Mechanism is another well-known method used for implementation of DP. The use of Gaussian noise makes it easier to comprehend and enhance the effect mechanism on the statistical analysis of a database as the sum of two Gaussians is a Gaussian. Unlike the Laplace mechanism, the magnitude of the noise added through Gaussian Mechanism can be calibrated by $\Delta fln(1/\delta)/\epsilon$ [82]. Considering a query function f and the privacy loss, ϵ be in the range of 0 to 1, the Gaussian Mechanism with parameter, σ can be denoted as:

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

4) TECHNICAL ISSUES ENCOUNTERED DURING DIFFERENTIAL PRIVACY IMPLEMENTATION

Whilst the basic logic behind DP is fairly simple, there are some few technical difficulties that are usually faced by researchers during the implementation of DP both in academia and in industry. This section briefly introduces the various issues faced and can be potentially faced during the application of DP to IoT-enabled CIs.

1) *Decision of ϵ-value*: The lack of sound guidelines and methods for choosing the ϵ-value makes it difficult to choose the optimal value to have a healthy trade-off between utility and privacy [104]. Choosing a small ϵ-value inputs a large amount of noise and guarantees higher privacy preservation but results in lower data utility and query accuracy. On the other hand, choosing a large ϵ-value inputs a small amount of noise and guarantees data utility and query accuracy while compromising on privacy. Indeed, to overcome this issue, researchers have employed a number of approaches [104]–[108]. However, these proposed methods only work for certain circumstances and a sound approach is still missing.
2) *Decision of sensitivity value*: Similarly, a lack of effective frameworks and guidelines makes it difficult to choose the optimal value of sensitivity in the view of balancing a healthy trade-off between sensitivity and data utility [104]. In general, researchers tend to use a low sensitivity value on statistical databases [87] since

it works well with global sensitivity. While using a low sensitivity value guarantees data utility, it is important to note that privacy is greatly compromised. On the other hand, a high sensitivity value tends to negatively impact data utility but guarantees better privacy. Several methods [109]–[111] have been proposed to tackle the decision of the sensitivity value. Proposed methods have been able to find near optimal values for a particular dataset but a certain amount of privacy is still allowed to be compromised [112]. However, an efficient method for choosing the optimal sensitivity value for a healthy privacy-utility trade-off is still lacking.

3) *Overcoming data coupling*: Overcoming data correlation is one of the biggest challenges faced during the implementation of DP [80], [104]. In real-world scenarios, datasets often include correlation amongst the several attributes present which can indefinitely help the attacker to perform inferences in the view of obtaining personal information relating to the individual [113]. Some few transformation based methods have been proposed but those methods [25], [90], [114]–[118] work in specific circumstances only and may even compromise data utility in other circumstances [112]. Therefore, effective methods of transforming the data and decreasing the correlation are still lacking.
4) *Dealing with Structural and Sampling Zeros*: In 2017, the US Census Bureau announced the usage of DP as the privacy preservation mechanism for the US 2020 Population of Housing Census [119]. In statistics, there are two types of zeros, namely, structural zeros and sampling zeros. Since this discussion is out of the scope of this survey, an example of sampling zero can be 'No Man over 75 years was living in this house.' while an example of structural zero can be 'It is impossible to have a 15 year old mother with a 30 year old son.' During the implementation of DP, it was found that noise added through the different data perturbation mechanisms may make sampling zeros and structural zeros positive in some cases [104].

5) DIFFERENTIAL PRIVACY STRENGTHS

The preservation of privacy in databases whilst safeguarding data utility is indeed a tedious task. Although Dwork's proposed DP has some drawbacks, it is a promising and powerful privacy preservation technique that is trending in major technology companies such as Apple, Microsoft, etc. This section briefly lists the strengths of DP that sustains its applications for several uses.

1) *Protection against Linkage attacks*: As previously mentioned, linkage attacks are some of the easiest attacks that is performed by attackers to gain illicit access to private sensitive information of individuals. In most of the cases, DP ensures the neutralization of linkage attacks and indefinitely solves the risks of re-identification [82], [84].
2) *Measurement of Privacy Loss*: The measurement of privacy loss enables the control on the amount of information leakage allowed whilst preserving data utility and comparison of the different techniques of privacy preservation [22], [23], [82]. Furthermore, from the quantification of privacy loss, the cumulative privacy loss over several iterations can be analysed through composition in the view of implementing much more complex DP algorithms [84].

6) DIFFERENTIAL PRIVACY LIMITATIONS

Apart from the previously mentioned technical difficulties encountered by researchers during the implementation of DP both in academia and in industry, it very significant that DP does not promise a complete privacy preservation. In instances whereby a dataset consists of very strongly correlated data with specific sensitive attributes, DP may fail to provide its promises [82]. Haeberlen *et al.* [120] reported that major well-known implementations of DP such as PINQ, Airavat, Fuzz, etc. consisted of vulnerabilities that can be further exploited by attackers to leak private sensitive attacks through covert channel attacks. It is critical to ensure that a channel is unable to learn anything about the data as a single bit of information learnt by a channel destroys all of DP's promises [120].

Furthermore, DP suffers from three major limitations [46], [121], [122] as in the following:

1) *Large Query Sensitivity*: Achieving DP during large query sensitivity is challenging while still maintaining the desired statistical properties needed for precise inference.
2) *Privacy Budget*: Maintaining an inferentially useful data which allows multiple queries in theory is already a daunting challenge faced by researchers. However, in practice, such challenges are amplified which hinders its application in scenarios where multiple queries are required.
3) *Uncertainty of outcome*: Differentially private mechanisms tend to produce results that differ enormously which decreases the reliability. For instance, Laplacian mechanism leads to significant differences in answers [123].

C. DIFFERENTIAL PRIVACY THREAT MODELS

Despite the various core strengths of DP as an outright paradigm for solving the global privacy problem, there are only specialized implementations by some few industries and academic. DP is still not used at a larger enterprise implementation scale as it is not an algorithm or technique but is merely a mathematical definition of privacy [124]. It is of no doubt that the deployment of practical systems that satisfy DP is very complex as in that case, it would be necessary to store all the data on one server which runs the system. Still, DP does not protect against any hacking of the server but rather only protects the output. Therefore, the design and deployment of differentially private systems requires the consideration

of threat models [125]. This section briefly discusses the three main threat models to be considered while deploying differentially private large scale enterprise IoT-enabled CIs.

1) CENTRAL MODEL OF DIFFERENTIAL PRIVACY

The most popular threat model used in DP research over the past 15 years is the Central Model of DP, as depicted in Figure 6, whereby it is assumed that all the sensitive data is stored in a single centralized server which is 'impregnable' and the data curator is assumed to be a trusted one (meaning that the data curator will neither peek at the sensitive data not dishonestly share it with an adversary). In the central DP threat model, the analyst is untrusted and data perturbation typically happens for the query results. This model enables the addition of a minimal amount of perturbation which generally increases data utility. However, as earlier mentioned, the data curator must be trustworthy and must not 'sell the secrets'.

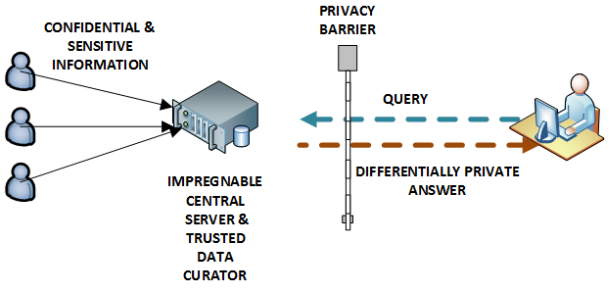

FIGURE 6. Central differential privacy threat model.

2) LOCAL MODEL OF DIFFERENTIAL PRIVACY

As previously highlighted, central DP threat model requires a trustworthy data curator. The Local Model of DP, as presented in Figure 7, addresses this concern through the elimination of a trustworthy data curator. Instead, data perturbation occurs prior to sending the data to the central server and the data curator, which implies that the data curator sees the noisy data. Furthermore, if in case, the central server is compromised, the adversaries only get access to perturbed data. However, the cumulative noise amount added by each data owner becomes pretty large and hence affects data utility.

3) HYBRID MODEL OF DP

Since both traditional central and local models of DP have their individual strengths and weaknesses, achieving the best of both threat models is being actively researched. The shuffle model [126]–[128], a recently proposed alternative, bridges the gap between central DP and local DP models. In addition to addressing the issue of the untrusted data curator, a partially trusted shuffler middleware, whose role is to randomly permute the data, is incorporated. Each individual data owner adds a smaller amount of noise to the data and sends it to the shuffler which randomly shuffles the data and may or may not add some additional noise before further sending the data batches to the central server whereby the data curator has access. Since the shuffler operates on batched inputs, it enables a smaller utility loss as compared to local DP model and guarantees privacy preservation. However, the amount of noise added is more than central DP.

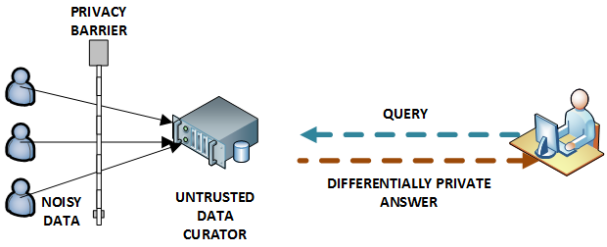

FIGURE 7. Local differential privacy threat model.

IV. APPLICATION OF DIFFERENTIAL PRIVACY IN IoT-ENABLED CRITICAL INFRASTRUCTURE FOR THE ENERGY SECTOR

Modern-day energy systems, commonly referred to as Smart Grids (SGs), are holistic approaches to the traditional power grids of the 21st Century [129]. As opposed to traditional power grids, the integration of IoT within SG technologies enables intelligent, multi-directional communication and automated capabilities to facilitate real-time pricing, energy loss detection, early power cut warnings, etc [130], [131]. However, the benefits of SGs were short-lived as SGs have now become a luring playground for adversaries [132]. The disclosure of sensitive energy usage information of a particular building or house can pose a serious threat towards an organization or the individual in question.

Non-Intrusive Load Monitoring (NILM) technique is an approach utilized by modern energy systems to analyse in detail the consumption of electricity in a particular house or building. This technique enables up to the fine-grained analysis of how much electricity is being consumed by a particular electric appliance in a particular time frame of an individual's house [133]–[135]. The amount of details and data generated by the NILM technique can easily fall in the wrong hands and the privacy, security and safety of an individual or an organization is at risk. For example, the data can be analysed by thieves to plan robberies or for targeted advertisements [80]. In this view, researchers have proposed several techniques to tackle the privacy and security related issues in SGs. However, DP has proven to be the most successful as per the aforementioned reasons. This section contains a detailed review and survey of the works carried out over the past few years.

A. DEMAND RESPONSE

Demand Side Management involves all the related procedures and steps required for the effective management of demand response with the goal of reducing operational expenses, blackout and emission of greenhouse gasses [136], [137]. To effectively and efficiently analyse, calculate, manage and predict demand response, smart meters collect data about

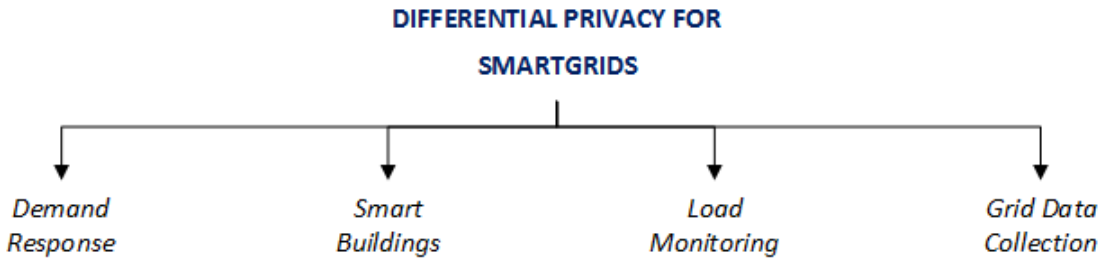

FIGURE 8. Taxonomy of surveyed differential privacy techniques as applied in perspective of SGs.

clients' energy consumption. Due to the high dimension and resolution of the point-wise and specific data collection, intruders tend to illegitimately profit on such data for unethical purposes [138]. Therefore, data protection and privacy preservation is a highly regarded aspect of demand response [139].

Though the real-time data collected can be protected through the implementation of DP, demand response analytics becomes a major challenge through data perturbation. This has been resolved through the Barbosa *et al.*'s [15] DP Laplacian Noise perturbation and demand response analytics through individual appliances. This resulted in an improved real-time data privacy and utility. Furthermore, the work in [140] introduced a novel cost-effective differential privacy scheme which preserves data privacy through alternating the state of charge of rechargeable batteries to generate Laplace distributed random noise. Theoretical analysis and simulations revealed the cascading of renewable energy sources and rechargeable batteries enhances the performance of their proposed scheme in terms of privacy preservation and practicability. Gough *et al.* [141] proposed an cost-effective innovative Differential Privacy (DP) compliant algorithm based on cooperative game theory which resulted in a scalable computer efficient mechanism and performs effectively with a large number of smart meter devices.

B. SMART BUILDINGS

According to the United Nation's Department of Economic and Social Affairs, it is estimated that 68% of the global population is expected to live in urban cities by 2050, with Delhi set to become the world's most populated city on earth by 2030 [62]. With the influx of people rushing to mega cities due to increased job prospects and higher living standards, the issue remains whether basic resources such as food, water, transport, healthcare, etc. are being optimally and efficiently distributed to the citizens. To tackle this complex issue, several governments, including the US and China [1], [2], are making significant efforts to design effective solutions by leveraging IoT) in the view of balancing the overpopulation and dearth of resources crisis for optimum and efficient distribution of resources, production of goods and services as well as usage of infrastructures [55].

Smart buildings are one such solution to tackle the aforementioned issue. Smart buildings, also referred to as intelligent buildings, include the residential homes and commercial buildings that are able to self-use resources and technologies in a coordinated and intelligent way to enhance sustainability and habitability [142]. IoT technologies play a major role in home/building automation and will be currently one of the hottest markets of the next decade. A large number of sensors, actuators and controllers are installed in those buildings which indeed generate enormous amounts of data. These data are then processed and used for regulation of processes, internal monitoring of structural health, analytics and prediction [143]. However, it is without mention that, wherever sensitive data is being generated, the number of data integrity attacks are more likely to spike. Adversaries can unethically use the available data for other unintended usage which can even go to the extent of risking one's life. Indeed, privacy preservation through DP is one method to overcome this issue.

As earlier highlighted, the different sensors installed in smart buildings produce heaps of real-time data that can be used to analytics purposes. Therefore, it is of high priority to prevent any data leakage and breaches in order to safeguard the privacy and confidentiality of the building and its inhabitants [144]. To tackle this issue, Chen *et al.* proposed PeGaSus [145] as a viable solution to integrate DP with real-time sensors' data before transmission. The proposed solution made use of perturbation techniques (Pe), grouping (Ga) and smoothing (Sus) of data for protecting data privacy as well as query evaluation for hierarchical streams. The researchers then tested and evaluated the performance of their proposed mechanism on real-world data from 4000 access points gathered over a period covering 6 months. Even through PeGaSus was very effective as a data preservation technique for sensor data streaming, it was not yet tested on smart buildings and cities. Therefore, a couple of years later, Ghayyur *et al.* further evaluated PeGaSus solution on real-world IoT-generated data from smart buildings [146]. After conducting their experiments, they concluded that DP-based PeGaSus is indeed a solution for smart building sensors' streaming privacy as well as offer lower numerical error (data utility enhancement) as compared to competing methods.

Moreover, in smart buildings, the majority of sensor-based devices are connected to the internet for monitoring, controlling and optimizing the resources available. This inter-woven connectivity of different devices form the basis of Smart Community [144]. After collection of data from various sensors, the data is transmitted over the internet in real-time to enable timely decisions and automation. Unfortunately, Liu *et al.* highlighted that in internet traffic can be exploited by attackers to cause data integrity attacks in perspective of smart homes [147]. Their paper showed the sensitive data can be easily leaked through analysis of internet traffic as well as the failure of privacy preservation even through cyrptographic techniques because of the novel advanced machine learning algorithms being used by adversaries during attacks. Therefore, the researchers proposed an utility-aware and exponential DP mechanism for obfuscating internet traffic and selecting gateway. After extensive testing of their proposed solution, the authors finally concluded that their technique enhanced data privacy preservation while simultaneously decreasing the latency in IoT-CI networks for smart houses.

Furthermore, Alisic *et al.* [148] found that sensors in smart buildings are susceptible to privacy leakage in terms of occupancy change. Therefore, they proposed a simple differential privacy method to mitigate such leaks using Gaussian noises in order to hide when the occupancy changes in an apartment. Simulation results on a KTH Live-In Lab testbed simulator revealed that a slow eigenvalue is not enough to draw a conclusion about the privacy leakage and that their scheme successfully preserved the privacy of the occupants without compromising data quality.

C. LOAD MONITORING

Without a doubt, one of, if not the, main issues of successful implementation and application of SGs is the preservation of customer privacy. Smart meters are responsible for the collection of energy usage data. Those smart meters are inter-linked to each other and are as well connected to a main SG utility through a strong and highly complex network known as Advanced Metering Infrastructure (AMI) [149]. Smart meters are designed to send their updated readings at each specific time interval to the main electricity grid utility. This transfer of sensitive information is at very high risk of breaches and leakages. Adversaries can illegitimately make use of those data which can then have serious implications. Therefore, the development and implementation of a secure privacy preservation strategy is definitely required to ensure secure real-time monitoring of SG data while still maintaining a healthy trade-off for data utility.

Previous literature of load monitoring privacy preservation include the use of several cryptographic encryption techniques to preserve data privacy such that only SG utilities are able to decipher the exact consumption of energy of SG users [146], [150]–[152]. However, it is worth noting that the use of encryption techniques on real-time load monitoring is an exhaustive and complex computational procedure, hence requiring expensive computational resources [153]. Furthermore, in case of failure of one smart meter, the whole network will be down due to lack of fault distribution and divergence [15]. Similarly, anonymization techniques [154] and the transmission of data using low-frequency and high-frequency ID [155] has been proposed but the risk of re-identification is still a considerable threat.

Therefore, the focus of researchers shifted to the implementation of DP as a viable alternative to preserve data privacy without much compromising on system performance, latency and data utility [156]. In perspective of DP privacy approaches to energy systems, the number of literature suggest that most work has been done in the field of load monitoring. Therefore, the works carried out can be grouped into two categories, namely, Battery Load Hiding (BLH) and direct noise addition through DP [80]. BLH is a customer-oriented approach that enables the preservation of data privacy of smart meters through the balancing of a load by making use of an external battery [157]. However, BLH techniques lack the theoretical proofs for privacy protection since relative entries, regressions, and clustering classifications are some of the only methods to measure their protection and privacy generation accuracy [158]. Therefore, in the view of being able to exactly quantify the privacy and accuracy, Zhang *et al.* proposed the perturbation of smart metering data using DP and multi-armed bandit (MAB) algorithm in respect to the battery constraints to decrease battery operational costs [159]. In addition, the researchers in [160] proposed stateless and stateful differential privacy BLH mechanisms in the view of optimizing mutual information sharing for different battery capacities. Zhang *et al.* further proposed an enhancement to the privacy loss of a battery using DP and the reduction of costs for both static and dynamic pricing environments through the development of two approaches [161]. Moreover, Zhao *et al.* proposed a multi-tasking BLH technique to further improve the shortcomings of traditional DP-based BLH techniques through the optimization of event detection accuracy [158].

On the other hand, many researchers have adopted another technique to preserve data privacy through direct perturbation of real-time smart-metering data. During data perturbation, the choice of the correct ϵ-value and the injection of the optimal amount of noise, also known as noise dimensioning, are some of the important factors for effective quantification of the level of privacy. Several papers concentrate on the different approaches to choose the optimum ϵ-value [162]. Furthermore, sensitivity must be taken into consideration while implementing DP for smart metering data. Whenever DP is applied on counting time-series data [25], the value of $f(X)$ is usually considered to be 1. However, in the case of smart metering data, the value of $f(X)$ is unknown [163]. Ács and Castelluccia proposed the perturbation of real-time smart-metering data through Γ-distribution and encrypted aggregation strategy for making the aggregation secure [164].

The proposed solution was found to decrease error rate due to clustering as well as safeguard appliance multiple slot privacy. Barbosa *et al.* proposed a less complex DP strategy that depends on an empirical model and error rate for generating a random masking value [165]. The solution was applied to both residential and industrial SG scenarios and an analysis was carried out. Savi *et al.* calculated the ϵ-value for quantifying the level of privacy through a priori information and perturbed the data (from various smart meters) through Gaussian white and coloured noise and concluded that the coloured Gaussian noise is an optimal solution for privacy [166].

Baloglu and Demir put forward a DP-based cryptosystem for smart metering using Gaussian noise perturbation, task assigning algorithm and encryption [167]. The researchers also claimed that their DP-based cryptosystem can also protect smart meters from filtering and time value attacks. After analysis of the privacy-utility trade-off in smart metering, Eibl and Engel introduced a point-wise privacy strategy based on DP and claimed that the requirements for the implementation of DP for real-time data vs. statistical data differ [163]. Liao *et al.* suggested Di-PriDA, a 3ϵ-DP strategy using Arduino micro-controller [168]. Their simulation results highlighted the fact that their approach optimized the efficiency value and reported fine-grained accuracy and results while eliminating the need of a trusted third party. Pal *et al.* proposed HIDE, a computationally efficient, and rigorous information-theoretic privacy engineering framework to tackle the privacy-utility trade-off of DP approaches in perspective of SGs through the use of queries, greedy algorithm, Markov assumption model and Laplace noise for differential privacy [169]. On the other hand, Xiong *et al.* introduced PADC, a light weight, secure and private data clustering technique for SGs based on DP and k -means algorithm [170]. They then evaluated it on different ϵ-values and found that the proposed solution outperforms other existing DP-based k-means algorithms for SGs.

Gai *et al.* [171] proposed lightweight local differentially private data aggregation scheme in which smart meters can perturb their generated data by randomized response locally without a trusted third party. Performance analysis of their approach revealed that their scheme is highly efficient in minimizing computation and communication overhead while still maintaining the data utility within acceptable error brackets. Similarly, Ou *et al.* [172] additionally applied singular spectrum analysis optimization to LDP with the addition of Fourier spectrum noise via geometric sum and resulted in increased data utility for any specified ϵ-value. The work in [173] developed the maximization of data utility in aggregated load monitoring and fair billing while preserving users privacy by using differential privacy with noise cancellation technique. Experimental validations of several periodic noise cancellation schemes on privacy and utility revealed that their proposed mechanism outperforms the existing scheme in terms of preserving the privacy while accurately calculating the bill.

D. GRID DATA COLLECTION

In modern SGs, fog computing has been thriving as a viable alternative to traditional cloud computing technologies for data aggregation and storage for its advantages of low latency and geographical distribution [80]. On the flip side of the coin, those advantages are short-lived due to recent literature [174] suggesting their vulnerability to privacy and security attacks. Fog nodes are highly susceptible to adversarial threats [175]. Indeed, data privacy preservation at fog nodes is a pressing issue. Therefore, in order to tackle this issue, Cao *et al.* put forward a DP-based Factorial Hidden Markov Model (FHMM) for privacy preservation at the nodes level in perspective of SGs [176]. The electricity usage for each appliance is directly perturbed using FHMM and then transferred to the fog layer for data storage. Their research improved the F1-score and Kullback Leibler divergence and proved to be an optimal solution as opposed to other existing methods. Moreover, Fan *et al.* [177] proposed a local differential privacy-based classification algorithm for data centers by adding Laplace noise to the data during pattern mining to ensure that data centres do not leak any sort of confidential information. Experimental validations revealed their proposed strategy has excellent reliability, efficiency and accuracy.

V. APPLICATION OF DIFFERENTIAL PRIVACY IN IoT-ENABLED CRITICAL INFRASTRUCTURE FOR THE TRANSPORT SECTOR

The transportation sector is one of the most thriving industries of the 21st century. Through integration with the state-of-the-art technologies, the transportation industry aims at seamlessly enhancing both drivers and passengers experience [178]–[180]. Modern day Intelligent Transport Systems (ITS) have been constantly evolving from the early 1970s [181] and are now a fusion of novel technological paradigms including wireless data transmission, automated sensing, intelligent control, to name a few [182]. The array of wireless devices in ITS enable two types of communications: Vehicle-to-Device (V2D) and Vehicle-to-Vehicle (V2V) communications [183]. Vehicular and other external information are constantly shared in real-time amongst ITSs through several technologies such as Mobile Ad-Hoc Network (MANET), Dedicated Short-Range Communication (DSRC), cognitive radio and/or Heterogeneous Vehicular Networks (HetVNET) [80]. Indeed, due to the enormous amounts of sensitive information being constantly shared, participating nodes of V2V and V2D communication schemes need a robust privacy preservation strategy to ensure no data leakage or breaches [184].

One of the major issues faced by ITSs are the rising number of adversarial privacy attacks being revealed through latest literature [185]. The severity and impact of those threats in perspective of ITSs can prove fatal which therefore hinders the expansion of the ITSs market to the daily life. In view of tackling this pressing issue, researchers have come up with

several privacy preservation solutions for different scenarios in ITSs. However, this section provides a detailed review and survey of the works carried out in respect to DP for ITSs over the past few years.

A. SMART FREIGHTS

Regarded as one of the most critical modes of freight transportation, modern railway infrastructure has been combined with several technologies including Big Data for achieving efficacy and efficiency in the transportation industry [80]. However, it has been highlighted that the advantages achieved through the fusion of traditional railway infrastructure with advanced technologies is short lived due to the exponential rise in adversarial privacy and confidentiality breaches during information sharing within an ITS network [186], [187]. Huawei and Yusong proposed a non-cooperative game theory model obtained its pure strategic Nash Equilibrium solution and hybrid strategic Nash Equilibrium solution to protect rail freight data but however did not include any implementation of the strategy [188]. However, in relation of DP, at the time of writing, there has been only one proposed solution by Shi *et al.* [28]. The authors put forward a first of its kind DP-based correlation approach for railway freight systems. Since railway datasets are mostly of statistical type [80], the original data was first sliced to an optimal length before injecting Laplace noise in the datasets through DP [28]. The results of the experimentation highlighted successful privacy preservation and a viable light-weight alternative for bar illicit access even with background knowledge of the data.

Similarly, out of other modes of transportation in the logistics industry, maritime modes, also known as ships, account for over 90% of the world's trade economy [189]. Maritime logistic operations are preferred due to their massive capacity and reduced operational costs as opposed to air shipping. With the latest IoT technologies being incorporated for the enhanced safety of large carriers and real-time information being transferred to and from different nodes in those critical ITS infrastructure, any adversary can easily get access to the data and it can be used to track the movement and location trajectory of ships. This can indeed have unintended consequences especially from a criminal perspective. To tackle this issue, Jiang et al came up with a DP-based Sampling Distance and Direction (SDD) technique to publish ship trajectories [190]. The researchers concluded that their proposed mechanism achieved a healthy privacy-utility trade-off while delivering ship trajectories as compared to other traditional noise perturbation techniques which would result in zigzag shapes and with many crossings, thus rendering the data useless.

B. ELECTRIC VEHICLES

As opposed to traditional vehicles, new technologies have enabled the drivers and vehicles to communicate internally and externally to provide a smooth driving experience and ensure road traffic safety through intelligent decisions [191], [192]. Connected smart and sustainable mobility is a futuristic concept that signifies a global connectivity of every vehicle to the internet and the real-time sharing of information to introduce a decongested and safe transportation system [193]. Although advanced technologies have brought about several advantages in latest vehicular infrastructure, the sharing of real-time information lures several adversarial attacks on the privacy of individuals through unethical vehicle location tracking [194], passive eavesdropping of V2V and V2D communication [183], etc. The breaches and leakage of vehicle trajectory information can have adverse unintended consequences on the life of an individual [195]–[197]. Moreover, corporation and companies that may exploit the sensitive location trajectory information for selfish business purposes [198]. To tackle this issue, Zhou *et al.* proposed an exponential DP-based vehicular trajectory partitioning and clustering technique for VANETs [199]. The researchers found that their proposed technique enhanced both efficiency and data utility. Ma *et al.* also proposed a dynamic sampling technique for processing real-time location data, Kalman filter for ensuring data availability and DP through Laplace noise addition for privacy preservation [200]. The authors concluded that data privacy, utility and availability increased as compared to other existing techniques.

Furthermore, Electric Vehicles (EVs) are now equipped with flexible energy storage and bi-directional Inductive Power Transfer technology meaning that they can be charged with a low energy source and can even sell their energy to other EVs [201]. The sale and purchase of energy to other EVs or IoT-enabled CIs are done at swap stations [202] through a game-theoretic Normalized Nash Equilibrium auction process [80], [203]. Undeniably, the eavesdropping and leakage of discharge/charge cycle data and energy auction data at swap stations can compromise one's privacy and have unintended adverse consequences [204]. Prior works to overcome this issue included the use of cryptographic encryption techniques [205] for preserving auction data privacy which however was found to be computationally exhaustive. Therefore, Zhai *et al.* proposed ExPO, an exponential DP-based privacy preserving online auction scheme, to enable cyber-secure energy trading at swap stations [206]. Through the use of auctioneers, their proposed strategy improves social welfare performance and load peak without compromising on privacy. Moreover, Han *et al.* put forward a joint DP strategy to restrict the users from influencing the scheduling process for energy auctions [207]. Through this proposed scheme, the authors were able to ensure data privacy even in cases where data is misreported to mediator. Indeed, DP serves as an excellent privacy strategy for auction energy swapping and outputting only the minimal required information [80].

Moreover, due to the abrupt increase in cyber-attacks, EVs are now equipped with intrusion detection systems to curb threats through adversarial detection using signature and/or anomaly based techniques [208]. In particular, EVs consists of Collaborative Intrusion Detection Systems (CIDS) that enable them to inter-share information about previous

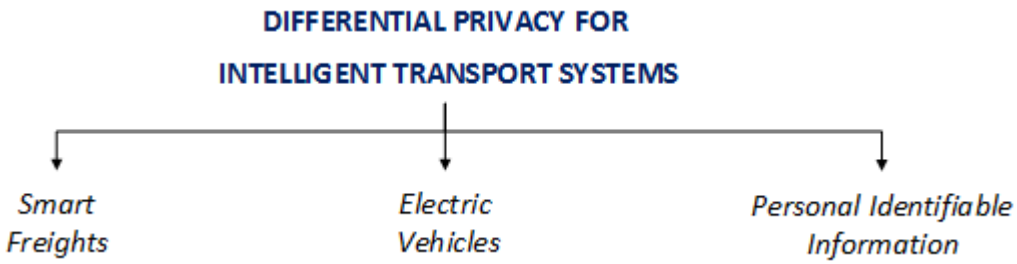

FIGURE 9. Taxonomy of surveyed DP techniques as applied in perspective of ITSs.

attacks that decreases training time and improves detection accuracy [209], [210]. However, the sharing of information among EVs in CIDS is not fully protected. The leakage or breach of data can enable an attacker to illegitimately manipulate the training process of CIDS for other illicit purposes with unintended adverse consequences on the life of an individual [80]. To mitigate this issue, Zhang and Zhu came up with a DP-based machine learning CIDS for VANETs [211]. Through the use of alternate-directional multipliers, the authors enhanced the empirical risk in VANETs using dual variable perturbation for data privacy preservation. Furthermore, the authors analyzed the performance their proposed scheme and the trade-off between security and privacy to conclude the effectiveness of their method as opposed to other existing ones. Therefore, we can derive the importance of DP for securing the data communication amongst modern EVs.

An *et al.* [212] proposed a differentially private strategy to preserve the location information along with the charging times of electric vehicles by leveraging Laplace noise addition mechanism. Experimental validations highlight that their work achieves the properties of incentive compatibility, individual rationality and better performance with respect to EV utility, buyer satisfaction ratio, electricity allocation efficiency and EV State-of-Charge (SoC), in comparison with existing schemes. Furthermore, their research is able to successfully protect EV location information with low chances of leakage with minimized computational overhead. The work in [213] put forward a differentially private dynamic data stream publishing mechanism to protect the release of sensitive EV information in V2G networks by leveraging the use of sampling intervals and variable sliding windows. Through experimental analysis on real data sets, and comparison with two representative w event privacy protection methods, the authors proved that their method exceeds in performance against the existing schemes and improves the utility of the data.

C. PERSONAL IDENTIFIABLE INFORMATION

ITSs tend to communicate data through a connected network. In so doing, they sometimes pass over sensitive Personal Identifiable Information (PII) in the form of names, tracking IDs etc [80]. Therefore, it is important to preserve the privacy of the PII. In this view, Kargl *et al.* brought forward a DP-based policy enforcement framework such as PRECIOSA PeRA in the view of preserving the privacy of floating car data storage in traffic data centres [214]. Furthermore, they proved that DP is a much better strategy for addition of noise in PIIs and for preserving information privacy during ITS data communication according to their different requirements.

VI. APPLICATION OF DIFFERENTIAL PRIVACY IN IoT-ENABLED CRITICAL INFRASTRUCTURE FOR THE HEALTHCARE SECTOR

One of the most important sectors of an economy is the healthcare sector. It is certainly undeniable that much of the recent healthcare research and progress is mainly due to the integration of advanced technological paradigms in medicine [215]. Among the various benefits of this healthcare sector revolution phenomenon include improved quality of life followed by an increase in life expectancy, reduction of operational costs, etc. Early patient health monitoring was limited to physical visits, calls and texts. However, through the deployment of IoT technologies in healthcare, a world of benefits with the inclusion of real-time health monitoring, fitness programs, remote health monitoring, remote diagnosis and so on have been unleashed to patients, doctors, insurance companies, clinics, etc [216].

One of most critical benefits of IoT technologies in the healthcare industry is the transfer, report and communication of sensitive confidential healthcare data to different nodes of an IoT-enabled CI [217]. HIoTs most commonly use wireless technologies including 4G long-term evolution (LTE), ultra-narrow band (UNB), ingenu, and low power wide area (LPWA) technologies for data communication [218]. These technologies enable the smooth transmission and communication process with minimum latency. However, since medical records are extremely sensitive, it is of highest priority to preserve the privacy of the individuals as even the slightest data tampering can cause the loss of lives [217]. Therefore, to overcome one of the biggest hurdles of the IoT employment in such critical infrastructure settings, researchers have come up with several privacy preservation mechanisms such as cryptographic encryption methods, anonymization techniques, public and private keys, etc [80]. Similarly, those

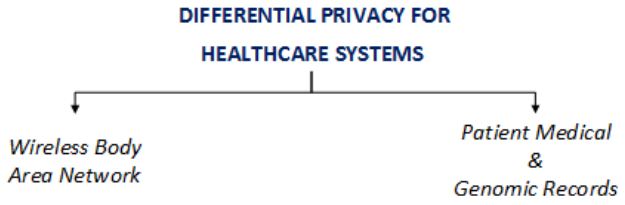

FIGURE 10. Taxonomy of surveyed DP techniques as adopted in IoT-enabled Healthcare systems.

previously devised techniques were found to be computationally exhaustive [205]. Therefore, the most viable privacy preservation strategy was found to be DP. In this view, this section deals with a survey of the state-of-the-art work.

A. WIRELESS BODY AREA NETWORK

As highlighted earlier, health data e.g. heart rate, sleep conditions, blood pressure, walk steps of patients are periodically transmitted to centres to track users health, for insurance premium purposes, etc [219]. WBAN, through the form of wearable sensors, contribute towards non-invasive monitoring and transmission of health data of individuals [220]. Due to the life and critical health patterns present in the data being transferred, experts fear that the personal data of any individual can fall in the wrong hands which may have following adverse consequences. Therefore, a strong privacy preservation scheme is important to tackle this issue. However, it is important to also note that privacy preservation is health records must also take into account the utility of the data. In this view, DP emerged as the most viable solution for safeguarding the privacy of WBANs data transfer. Lin *et al.* proposed a light-weight DP-based privacy preservation scheme for sensitive big data in WBANs [29]. The authors firstly constructed a tree structure to improve the error rates and provide long range queries followed by Haar Wavelet transformation method for converting the histogram into a complete binary tree. After simulation, the authors concluded that their proposed tree structure decreases the associated computational complexity for privacy preservation while maintaining a healthy trade-off with data utility. Zhang *et al.* put forward Re-DPoctor, a DP-based mechanism, for budget allocation and adaptive sampling [219]. Through the use of a Proportional Integral Plus (PIP) and simulation on real-time health data, the researchers were able to conclude that their proposed scheme also reduces mean relative error and mean absolute error of the transmitted data.

Moreover, Sun *et al.* proposed a DP-based classification algorithm based on ensemble decision tree for WBANs [221]. The authors also used a bagging framework of ensemble learning in their proposed method to improve the stability and accuracy of the classification. The results of the different decision trees (trained on the bootstrap samples) were aggregated using weight-based voting. After simulation, the authors concluded that their novel algorithm resulted in better accuracy and stability on small datasets since the larger tree nodes depth mitigates the issue of excessive noise and finds the most optimal ϵ-value as opposed to other existing approaches. Chakraborty *et al.* brought forward a temporal DP technique by selectively delaying traffic traces at the nodes of Wireless Sensor Networks (WSNs) which are present in the routing paths of the messages to the sink while preventing the adversary any access to data from the start to the end of the communication [222]. After simulation, the jitter was estimated to be roughly between 436.15ms and 503.42ms. In relation to their work, the authors also highlighted that their proposed solution can be used to conceal temporal information about the traffic corresponding to any node even in WBANs. Moreover, Tang *et al.* proposed a DP-based signature technique for collecting health data from various nodes and guaranteeing fair incentives for contributing patients [223]. The authors also combined Boneh-Goh-Nissim crypto system, and Shamir's secret sharing for improving the data privacy and fault tolerance of the system. After the evaluation, the authors revealed that their proposed method reduced the computational, communication and storage overhead. Kang *et al.* proposed a two-tier data inference framework with the first layer involving a data inference algorithm to reduce redundancy so as for decreased energy usage and the second layer involving encryption and differential privacy techniques to protect sensitive health records [224]. The results after evaluation proved enhanced privacy preservation, improved data utility, significant data savings and lastly energy efficiency. Furthermore, Guo *et al.* [225] proposed the application of temporal differential privacy on physiological signals collected health IoT wearables within WBANs which effectively protects the privacy of IoT-based users.

B. PATIENT MEDICAL AND GENOMIC RECORDS

Throughout this decade, the traditional hospitals are revolutionizing their daily procedures through the use of novel technological paradigms such as cloud computing, etc. Leaving the manual traditional tedious tasks of storing and organizing patients' records, hospitals are now starting to adopt a digital approach for patient health records [226]. Those digitized patient-centered records are also known as Electronic Health Records (EHR) [227]. EHR consists of highly confidential and sensitive data such as medical conditions, names, date of birth, allergies, etc. Therefore, it is of extremely high priority to safeguard the data and only share them with authorized personnel. Several previous methods have been proposed such as obscuring and cryptographic encryption techniques [228], [229]. However, obscuring carries the risks of re-identification [230] and data encryption fails to preserve privacy during querying [231]. Therefore, DP emerged as the most viable alternative for storing and publicizing e-health data for query execution without compromising privacy and utility [232].

Li *et al.* took the first step towards developing an efficient e-health data release and heuristic hierarchical query scheme with consistency guarantee under a private partition

algorithm for differential privacy [233]. They concluded that their proposed method was able to increase the accuracy of data release through consistency as well as enhancing time, computational overhead and query error. Beaulieu-Jones *et al.* proposed an end-to-end DP stochastic gradient descent based deep learning approach to enhance training accuracy and efficiency while preserving sensitive data privacy [234]. To further secure their proposed strategy, the researchers included the use of encryption. After testing the solution on eICU collaborative Research Database and The Cancer Genome Atlas, the researchers concluded that their strategy efficiently protects privacy and security along with decreasing computational overhead. Guan *et al.* proposed EDPDCS, an efficient DP-based data clustering technique, to optimize the privacy budget allocation and the improved selection of initial centroids for enhancing the accuracy of K-means clustering algorithm. [235]. After comparing the Normalized Intra-Cluster Variance on Blood and Adult from the UCI Knowledge Discovery Archive database, the authors then concluded that the proposed MapReduce based framework can improve the accuracy of the DP k-means algorithm. Alnemari *et al.* proposed DP-based improvements partitioning mechanisms through a greedy algorithms for partitioning counts' vectors and an adaptive mechanism that considers he sensitivity of the given queries before providing results [236]. The authors preserved privacy using Laplacian noise and worked over data partitioning and work load for optimization of error rate of queries. Similarly Mohammed *et al.* proposed a light-weight DP-based Laplacian noise for preserving data privacy on cancer patient's data [231]. After simulation and evaluation, the researchers concluded that their proposed strategy decreased the computational overhead and supported complex data mining tasks and a variety of SQL queries.

Genomics is also another research field that has been burgeoning since the early 2000s [237]. Genomics is the field of research that deals with whole genomes of organisms, and incorporates elements from genetics. Genomics uses a combination of recombinant DNA, DNA sequencing methods, and bioinformatics to sequence, assemble, and analyse the structure and function of genomes [238]. With the help of genomic data, biologists are able to understand, analyse, sequence and even edit genomes for an array of benefits. In smart hospitals, clinical genomic data are recorded, stored and distributed for respective purposes. However, it is as well vital to preserve the privacy of genomic data to mitigate the unwanted threats involved. Therefore, Raisaro *et al.* proposed the privacy preservation of genomic and distributed clinical data through cryptographic encryption measures followed by data perturbation using DP [239]. The authors also worked over Informatics for Integrating Biology and Bedside (i2b2) framework, and improved privacy preservation while decreasing the network overhead. Similarly, the authors in [240] took a further step by preserving genomic data privacy by using traditional differential privacy approach followed by a two way decryption method. They concluded that they were able to enhance both the privacy and execution time of i2b2 framework for electronic genomic data records. He *et al.* proposed a DP-based genomic data releasing method [241]. Firstly, the authors executed belief propagation on factor graph to factorize the distribution of sensitive genomic data into a set of local distributions followed by the injection of DP-based noise to these local distributions. The synthetic sensitive data created and factor graph are then used to construct approximate distribution of non-sensitive data which is then sampled to construct a synthetic genomic dataset. Almadhoun *et al.* put forward a DP-based privacy preservation mechanism for genomic datasets while taking into consideration the dependence between tuples [242]. After simulation of different genomic datasets, the authors empirically claimed that their proposed technique achieved up to 50% better privacy than traditional DP-based solutions.

VII. APPLICATION OF DIFFERENTIAL PRIVACY IN IoT-ENABLED CRITICAL INFRASTRUCTURE FOR THE INDUSTRIAL SECTOR

With the fast pace advancement of IoT technologies in several aspects of the world [55], the integration of IoT with industrial procedures has grown exponentially due to the various benefits [243], [244] which include scalability, analytics, standardization, interoperability, communication, etc [245]. Industrial IoT (IIoT) is the term used to refer to the use of certain IoT technologies and various smart objects in an industrial setting for the promotion of goals distinctive to the industry [246]. IIoT systems are capable of intelligently self-monitoring and operating without the need of any human intervention. However, modern IIoTs require hostile environment operations, predictable throughput, maintenance by some other than communication specialists, and extremely low down time [80]. To do so, IIoT components require efficient data communication through Fieldbus and Supervisory Control and Data Acquisition (SCADA) [247] between the different network nodes and components.

With the growing associated commercial and political interests [248] and the extreme vulnerability to cyberattacks [245], competitors and adversaries tend to illicitly obtain confidential and sensitive data for selfish gains. Therefore, privacy preservation in modern IIoT systems has gained momentum in the recent years as a hot area of research. Similar to the other previously discussed application areas, a number of techniques [249]–[252] including limit release [253], data distortion [254] and encryption [255], [256] have been proposed to tackle privacy preservation. However, most of them result in extreme computational overhead, energy inefficiency, time delays or are very specific to only one IIoT scenario. Therefore, DP emerged as the most viable solution for privacy preservation in IIoT systems. In this section, we survey the state-of-the-art literature of DP application in perspective of IIoT.

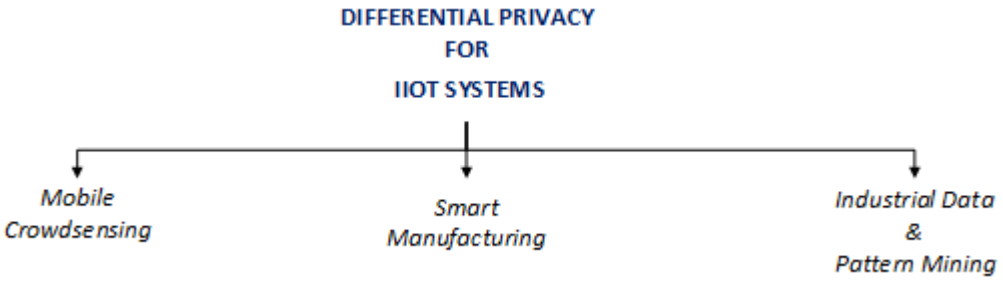

FIGURE 11. Taxonomy of surveyed DP techniques as adopted in IIoT systems.

A. MOBILE CROWDSENSING

With the widespread and rapid digitization of industries, mobile crowdsensing has emerged as a novel intelligent data collection and processing paradigm in IIoT that leverages pervasive mobile devices to efficiently collect the big sensory data, enabling various large-scale applications [257], [258]. Mobile crowdsensing is capable of providing a large amount of data via pervasive mobile terminals for IIoTs. However, the generated data often contains users' sensitive information such as PIIs, etc., which reveals the urgent need for effective privacy-preservation strategies in data aggregation and analysis for IIoT [259]. To tackle the privacy preservation issues in mobile crowdsensing, a number of approaches [260]–[263] have been proposed. However, it was found that those previously devised techniques were found to be computationally exhaustive [205] and increased latency of data communication. Therefore, DP was found to be one of the most effective solutions to tackle data privacy preservation for mobile crowdsensing.

DP-based solutions for mobile crowdsensing have attracted the attention of researchers for the past couple of years. In this view, a number of research and literature mostly in relation to crowdsensing location privacy protection [264]–[275] and bid privacy preservation [276], [277] have been produced for several application areas. At the time of writing, not much work been done in perspective of DP-based solutions for mobile crowdsensing for IIoTs. Yin *et al.* proposed a DP-based location privacy preservation mechanism without compromising on data utility for IIoT via building a multilevel location information tree model and select data according to the tree node accessing frequency followed by Laplacian data perturbation of the accessing frequency [278]. The authors concluded that their proposed method enhanced security, privacy, and applicability.

B. SMART MANUFACTURING

Large-scale process control in industries has been constantly evolving from the late 1950s. With the introduction of electronic processors and graphic displays, the need for automated process control systems gave birth to the first Distributed Control System (DCS) [279]. During the past two decades, the industrial sector has been reformed and revolutionized with the exponential increase of intelligent DCSs. Through the utilization of those inter-connected and intelligent DCSs, industries are now taking a leap forward to automated production approaches, also known as smart manufacturing [280]. Smart manufacturing heavily benefits the industries through cost-efficient production lines, automated diagnostics and control, etc. This is usually achieved through real-time sensing and sharing of information using a multitude of sensors and actuators [281]. However, the growing complexity of modern DCSs make them extremely vulnerable and the rate of attacks leading to data breaches and leakages have grown exponentially over the last decade [282]. Therefore, the preservation crucial data privacy in modern DCSs has become a very crucial step for enabling safer industrial operations in the upcoming Industry 5.0 plan. So far, researchers have proposed several techniques including encryption [283]–[286] and k-anonymity [287]. Due to their respective drawbacks, DP emerged as the most promising privacy preservation approach for enhanced data utility, computational overhead and time delay.

Recent research in perspective of linear DCSs with quadratic cost functions [288] found that DP is the optimal privacy preservation strategy for safeguarding real-time continuously varying data. In this view, Wang *et al.* proposed a metric-based DP solution through the perturbation of data using Laplacian noise to the shared information in a way that depends on the sensitivity of the control system to the private data [289]. The researchers claimed that their proposed strategy achieved minimal system entropy and enhanced data privacy. Furthermore, Giraldo *et al.* proposed a DP-based methodology define the inherent DP of feedback-control systems without the addition of an external DP noise [290]. After perturbation of the data using the minimal required amount of Gaussian noise using bi-level optimization, the authors concluded that their novel solution enhanced performance, privacy and data utility of DCSs. Hu *et al.* proposed a DP-based solution and optimization of privacy parameters to achieve a healthier privacy-utility trade-off [291]. After evaluation on the modeling of cutting power consumption in computer numerical control turning processes, the authors claimed that their proposed strategy enhanced data utility by 9.4% and privacy by 13.1% for smart manufacturing processes.

C. INDUSTRIAL DATA AND PATTERN MINING

As highlighted earlier, modern industrial devices are equipped with a multitude of sensors and actuators that constantly collect environmental and behavioral data that are transmitted and stored in real-time. With an influx of industrial data available, pattern recognition tools and techniques are being applied to convert the raw data into information. However, during query evaluation, there are possible threats of data leakages as machine learning algorithms are easy to fool [292]. Ni *et al.* proposed MCDBScan, a DP-based data mining technique through the prior perturbation of data using Laplacian noise [293]. After simulation, the authors claimed that their proposed schema enhanced efficiency, accuracy and privacy as compared to other existing techniques. Taking a leap further, Zhu *et al.* initiated the implementation of machine learning along with differential privacy for efficient query evaluation [294]. The researchers concluded that their proposed transfer of data publishing problem to a machine learning problem achieved a lower mean absolute error and enhanced the privacy guarantee. Similarly, Arachchige *et al.* introduced PriModChain an amalgamation of DP, federated ML, Ethereum blockchain and smart contracts for trustworthy machine learning in IIoTs [295]. Moreover, Hou *et al.* put forward a low-cohesion DP-based algorithm for frequent pattern mining for application-level privacy protection in IIoTs [296].The authors utilized Top-k frequent mode to combine the factors of index mechanism and low cohesive weight of each mode followed by Laplacian perturbation for each mode. The researchers then concluded that the proposed mechanism achieves an optimal privacy-utility trade-off for IIoT scenarios.

VIII. FUTURE RESEARCH DIRECTIONS

For the last few years, DP has starting caught the research momentum as the most viable and promising privacy preservation technique in several application domains. Currently, however, DP faces certain challenges while being implemented on dynamic IoT-enabled CIs [297]. While some of the issues of DP have already been successfully addressed by researchers, there is exists other pressing issues that require urgent attention. Therefore, in this section, we briefly discuss some few open challenges and future directions in hope of advancing research in the implementation of DP for IoT-enabled CIs.

A. BLOCKCHAIN TECHNOLOGY

More than a decade ago, S. Nakamoto introduced blockchain as a novel technological paradigm that enables the decentralization of data storage from the traditional centralized approach where one data author controls everything [298]. For the past few years, blockchain has successfully evolved, from being tightly associated with Bitcoin, into the talk of the down with several applications into different scenarios including the energy sector [299]–[301], financial sector [302], [303], healthcare sector [304], [305], etc. The application of blockchain in IoT-enabled CIs is proliferating at enormous pace due to its distributed ledger and the elimination of a central data owner [306].

Blockchain is well-known for its secure transaction mechanisms through the use of authentication and encryption [50]. However, the dearth of established blockchain protocols [307] has opened issues related to transaction and data privacy. In order to tackle this critical issue, researchers are currently proposing several privacy preservation strategies such as anonymity, and identity [308]–[311]. From the different drawbacks of the existing implementations of several privacy preservation strategies, we indeed that the advances in DP and its noise perturbation algorithms can be incorporated with blockchain-based IoT-enabled CI solutions in the aim of mitigating privacy issues during both private and public query evaluation. The non-complex underlying mathematical concept combined with its light-weight privacy approach will indeed be the major advantages of DP application in blockchain-based IoT-enabled CI solution. Therefore, it is necessary to encourage advanced research to integrate blockchain and DP to successfully eradicate privacy loss issues in IoT-enabled CIs.

B. LIGHTWEIGHT DIFFERENTIAL PRIVACY

For the past few years, DP popularity, research, adoption and implementation has grown exponentially both in academic and industry. This has brought forward several increasingly complex and sophisticated algorithms that enables the public publishing and sharing of information without compromising privacy. Furthermore, coupled with the increase in the complexity of modern DP algorithms, the number of wrong DP mechanisms and techniques, with several bugs that violate their claimed privacy, are also being developed [312]. It becomes necessary to have verification methods to filter sophisticated DP algorithms being proposed. However, using customised logical verification techniques to prove the claims of those algorithms requires high computational overheads [313].

Furthermore, the considerable rise in the adoption of fog and edge computing paradigms in IoT-enabled CIs has enabled low latency, location awareness, real-time data sharing and communication as well as quality of services [314], [315]. However, edge-deployed fog devices in IoT-enabled CIs are susceptible to privacy attacks [316]. In this view, several privacy preservation techniques, including modern sophisticated and traditional DP algorithms [317] have been proposed. Similarly, the implementation of those existing DP methods in edge/fog-based IoT-enabled CI solutions require expensive computational overhead. Therefore, we believe that researchers should shift focus to produce reliable works on DP techniques for IoT-enabled CIs that require minimal computational overhead.

C. BIG DATA ANALYTICS

Big Data, another buzzword of this decade, has been associated with several scenarios and are particularly the key advantages of IoT-enabled CIs. In perspective of DP applications

for big data of IoT-enabled CIs, privacy level quantification and optimization are still two unsolved key areas Even after a decade of guaranteeing stronger privacy preservation as compared to other techniques and the several soundproof mathematical backgrounds of DP, it is still a challenge to derive the exact privacy level while handling loads of real-time data for IoT-enabled CIs [318]. Furthermore, the optimal calculation of composition of DP in big data analytics is still an unsolved issue [80], [319]. Moreover, one characteristic of big data for IoT-enabled CIs is its dimensionality [320]. DP preservation for high dimensional data is a big challenge for researchers [321]. Therefore, we believe that the design and derivation of optimal privacy level along with the preservation of high dimensional data must be the next focus of interested researchers.

D. DYNAMIC DATASETS

Most of the differentially private algorithms proposed to-date has been mostly focused on static unchanging datasets where queries are performed [322]. However, with the growing amount of data sensed by edge devices, datasets tend to evolve and change over time. Within situations where data keeps on updating, it is important to note that not all the data is available at the time of primary curation. The usage of current DP approaches on dynamic datasets poses three main issues [323], namely:

1) The adversary continuously observes the output of the sanitizer.
2) The adversary examines the internal state of the sanitizer.
3) Entries during updates may be mutually inclusive or singletons.

Very few works [96], [324] have been carried out within this area. In this view, we recommend that future works in this focus area should be targeted on:

1) The conversion of static algorithms to dynamic ones by using parallel accumulators with counters and finally aggregating the number of accumulators utilized.
2) Pan-Private algorithms which enables an untrusted curator to accumulate statistical information but never stores sensitive data about individuals. In other words, the internal state completely hides the appearance pattern of any individual: presence, absence, frequency, etc.

Therefore, we believe that designing effective and efficient differential privacy mechanisms is highly crucial for practicability of using DP within an industrial setting.

IX. LIMITATIONS OF OUR SURVEY

Within our survey, we have considered the four main IoT-enabled critical infrastructure namely power systems, transport systems, healthcare systems and lastly industrial systems. We have focused our work to comprehensively survey the applications of differential privacy within those four aforementioned critical infrastructure. However, we acknowledge that there are other critical fields such as military and defence sector, supply chain sector, etc. where differential privacy approaches are constantly being applied by researchers to protect the privacy of confidential data. Furthermore, within our paper, we do not specifically target our survey to cover either local DP or global DP, but we rather cover both applications within the four critical domains.

X. CONCLUSION

With fast paced developments in novel technological paradigms, IoT-enabled CIs have undeniably become the core of several economic sectors as well as our lives. On the flip side of the coin, the number of associated cyber threats are also on the rise. Adversaries tend to attack IoT-enabled CIs to gain illicit access to sensitive information which can then be used for selfish commercial and political gains. While several privacy preservation techniques have been proposed and tried, DP has evolved as the most viable solution to mitigate privacy threats through the noisy perturbation of data. Throughout this paper, we have covered an in-depth state-of-the-art survey of DP approaches for IoT-enabled CIs particularly in four application domains, namely energy, healthcare, transportation and industrial sectors. Within the energy sector, we covered privacy preservation for demand response, smart buildings and load monitoring. Moreover, within the transport sector, we surveyed the different DP applications in perspective of smart freights, electric vehicles and personal identifiable information. Similarly, in the healthcare sector, we presented the adoption of DP techniques for wireless body area networks as well as patient medical & genomic records. Lastly, we surveyed the application of DP mechanisms within the industrial sector though mobile crowdsensing, smart manufacturing and, industrial data and pattern mining. The paper then ends with a brief highlight of some challenges and future research directions for DP in IoT-enabled CIs. We believe that our survey can serve as the basis for further research and development of novel DP mechanisms to tackle several existing data privacy issues in IoT-enabled CIs.

REFERENCES

[1] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.
[2] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of IoT: Applications, challenges, and opportunities with China perspective," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 349–359, Aug. 2014.
[3] H.-D. Ma, "Internet of Things: Objectives and scientific challenges," *J. Comput. Sci. Technol.*, vol. 26, no. 6, pp. 919–924, Nov. 2011.
[4] C. Formisano, D. Pavia, L. Gurgen, T. Yonezawa, J. A. Galache, K. Doguchi, and I. Matranga, "The advantages of IoT and cloud applied to smart cities," in *Proc. 3rd Int. Conf. Future Internet Things Cloud*, Aug. 2015, pp. 325–332.
[5] E. Adi, A. Anwar, Z. Baig, and S. Zeadally, "Machine learning and data analytics for the IoT," *Neural Comput. Appl.*, vol. 32, no. 20, pp. 16205–16233, 2020.
[6] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Bus. Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[7] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1606–1616, Apr. 2019.

[8] L. Briesemeister, S. Cheung, U. Lindqvist, and A. Valdes, "Detection, correlation, and visualization of attacks against critical infrastructure systems," in *Proc. 8th Int. Conf. Privacy, Secur. Trust*, Aug. 2010, pp. 15–22.

[9] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and A. Anwar, "TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," *IEEE Access*, vol. 8, pp. 165130–165150, 2020.

[10] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," in *Proc. 3rd Int. Conf. Electron. Design (ICED)*, Aug. 2016, pp. 321–326.

[11] 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.

[12] A. Wilner, "Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation," *Comparative Strategy*, vol. 36, no. 4, pp. 309–318, Aug. 2017.

[13] N. Sklavos and I. D. Zaharakis, "Cryptography and security in Internet of Things (IoTs): Models, schemes, and implementations," in *Proc. 8th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Nov. 2016, pp. 1–2.

[14] V. K. Mithali and A. Sharma, "A survey on various cryptography techniques," *Int. J. Emerg. Trends Technol. Comput. Sci.*, vol. 3, no. 4, pp. 307–312, 2014.

[15] 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.

[16] S. Wachter, "Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR," *Comput. Law Secur. Rev.*, vol. 34, no. 3, pp. 436–449, Jun. 2018.

[17] A. Otgonbayar, Z. Pervez, and K. Dahal, "Toward anonymizing IoT data streams via partitioning," in *Proc. IEEE 13rd Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Oct. 2016, pp. 331–336.

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

[19] K. Guo and Q. Zhang, "Fast clustering-based anonymization approaches with time constraints for data streams," *Knowl.-Based Syst.*, vol. 46, pp. 95–108, Jul. 2013.

[20] J. Domingo-Ferrer and V. Torra, "Ordinal, continuous and heterogeneous *k*-anonymity through microaggregation," *Data Mining Knowl. Discovery*, vol. 11, no. 2, pp. 195–212, Sep. 2005.

[21] 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.

[22] C. Dwork, "Differential privacy," in *Proc. 33rd Int. Colloq. Automata, Lang., Program. (ICALP)*. Berlin, Germany: Springer-Verlag, 2006, pp. 1–12.

[23] C. Dwork, "Differential privacy: A survey of results," in *Proc. 5th Int. Conf. Theory Appl. Models Comput. (TAMC)*. Berlin, Germany: Springer-Verlag, 2008, pp. 1–19.

[24] Z. Li, H. Lv, and Z. Liu, "Noise-added selection method for location-based service using differential privacy in Internet of Things," *Adv. Mech. Eng.*, vol. 11, no. 1, Jan. 2019, Art. no. 168781401882239.

[25] V. Rastogi and S. Nath, "Differentially private aggregation of distributed time-series with transformation and encryption," in *Proc. ACM SIGMOD Int. Conf. Manage. Data*. New York, NY, USA: Association for Computing Machinery, Jun. 2010, pp. 735–746.

[26] A. Greenberg. (Jul. 2017). *Uber's New Tool Lets its Staff Know Less About You*. [Online]. Available: https://www.wired.com/story/uber-privacy-elastic-sensitivity/

[27] J.-M. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in *Proc. IEEE Int. Conf. Commun. Workshops*, May 2010, pp. 1–5.

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

[29] C. Lin, P. Wang, H. Song, Y. Zhou, Q. Liu, and G. Wu, "A differential privacy protection scheme for sensitive big data in body sensor networks," *Ann. Telecommun.*, vol. 71, nos. 9–10, pp. 465–475, Oct. 2016.

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

[31] M. Hilton, "Differential privacy: A historical survey," California Polytech. State Univ., San Luis Obispo, CA, USA, Tech. Rep., 2012.

[32] N. Li, W. Qardaji, and D. Su, "On sampling, anonymization, and differential privacy or, *k*-anonymization meets differential privacy," in *Proc. 7th ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS)*. New York, NY, USA: Association for Computing Machinery, 2012, pp. 32–33.

[33] F. K. Dankar and K. El Emam, "The application of differential privacy to health data," in *Proc. Joint EDBT/ICDT Workshops (EDBT-ICDT)*. New York, NY, USA: Association for Computing Machinery, 2012, pp. 158–166.

[34] D. Leoni, "Non-interactive differential privacy: A survey," in *Proc. 1st Int. Workshop Open Data (WOD)*. New York, NY, USA: Association for Computing Machinery 2012, pp. 40–52.

[35] C. Task and C. Clifton, "A guide to differential privacy theory in social network analysis," in *Proc. IEEE/ACM Int. Conf. Adv. Social Netw. Anal. Mining (ASONAM)*. Washington, DC, USA: IEEE Computer Society, Aug. 2012, pp. 411–417.

[36] A. D. Sarwate and K. Chaudhuri, "Signal processing and machine learning with differential privacy: Algorithms and challenges for continuous data," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 86–94, Sep. 2013.

[37] S. Goryczka, L. Xiong, and V. Sunderam, "Secure multiparty aggregation with differential privacy: A comparative study," in *Proc. Joint EDBT/ICDT Workshops (EDBT)*. New York, NY, USA: Association for Computing Machinery, 2013, pp. 155–163.

[38] H. H. Nguyen, J. Kim, and Y. Kim, "Differential privacy in practice," *J. Comput. Sci. Eng.*, vol. 7, no. 3, pp. 177–186, 2013.

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

[40] P. Xiong, T.-Q. Zhu, and X.-F. Wang, "A survey on differential privacy and applications," *Chin. J. Comput.*, vol. 37, no. 1, pp. 101–122, 2014.

[41] J. Wang, S. Liu, and Y. Li, "A review of differential privacy in individual data release," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 10, pp. 1–18, 2015.

[42] K. Xu and Z. Yan, "Privacy protection in mobile recommender systems: A survey," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage* (Lecture Notes in Computer Science). Cham, Switzerland: Springer, 2016, pp. 305–318.

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

[44] X. Yao, X. Zhou, and J. Ma, "Differential privacy of big data: An overview," in *Proc. IEEE IEEE 2nd Int. Conf. Big Data Secur. Cloud (BigDataSecurity), Int. Conf. High Perform. Smart Comput. (HPSC), IEEE Int. Conf. Intell. Data Secur. (IDS)*, Apr. 2016, pp. 7–12.

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

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

[47] S. Fletcher and M. Z. Islam, "Decision tree classification with differential privacy: A survey," *ACM Comput. Surv.*, vol. 52, no. 4, pp. 1–33, Sep. 2019.

[48] P. Zhao, G. Zhang, S. Wan, G. Liu, and T. Umer, "A survey of local differential privacy for securing internet of vehicles," *J. Supercomput.*, vol. 76, no. 11, pp. 8391–8412, Nov. 2020.

[49] T. Wang, X. Zhang, J. Feng, and X. Yang, "A comprehensive survey on local differential privacy toward data statistics and analysis," *Sensors*, vol. 20, no. 24, p. 7030, Dec. 2020, doi: 10.3390/s20247030.

[50] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy in blockchain technology: A futuristic approach," *J. Parallel Distrib. Comput.*, vol. 145, pp. 50–74, Nov. 2020.

[51] M. Gong, Y. Xie, K. Pan, K. Feng, and A. K. Qin, "A survey on differentially private machine learning [review article]," *IEEE Comput. Intell. Mag.*, vol. 15, no. 2, pp. 49–64, May 2020.

[52] H. Jiang, J. Pei, D. Yu, J. Yu, B. Gong, and X. Cheng, "Applications of differential privacy in social network analysis: A survey," *IEEE Trans. Knowl. Data Eng.*, early access, Apr. 13, 2021, doi: 10.1109/TKDE.2021.3073062.

[53] T. Liu and D. Lu, "The application and development of IoT," in *Proc. Int. Symp. Inf. Technol. Med. Educ.*, vol. 2, 2012, pp. 991–994.

[54] P. Suresh, J. V. Daniel, V. Parthasarathy, and R. H. Aswathy, "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," in *Proc. Int. Conf. Sci. Eng. Manage. Res. (ICSEMR)*, Nov. 2014, pp. 1–8.

[55] M. A. Ezechina, K. K. Okwara, and C. A. U. Ugboaja, "The Internet of Things (IoT): A scalable approach to connecting everything," *Int. J. Eng. Sci.*, vol. 4, no. 1, pp. 9–12, 2015.
[56] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT security: Ongoing challenges and research opportunities," in *Proc. IEEE 7th Int. Conf. Service-Oriented Comput. Appl.*, Nov. 2014, pp. 230–234.
[57] Gartner. *Definition of Internet of Things (IoT)—Gartner Information Technology Glossary*. Accessed: Mar. 30, 2021. [Online]. Available: https://www.gartner.com/en/information-technology/glossary/internet-of-things
[58] *Internet of Things and Data Placement: Edge to Core and the Internet of Things*. Accessed: Mar. 30, 2021. [Online]. Available: https://infohub.delltechnologies.com/l/edge-to-core-and-the-internet-of-things-2/internet-of-things-and-data-placement
[59] *Internet of Things (IoT)*. Accessed: Mar. 30, 2021. [Online]. Available: https://www.ey.com/en_au/internet-of-things-iot
[60] China Daily. *Experts Say China has the Edge in Internet of Things*. Accessed: Mar. 30, 2021. [Online]. Available: https://www.chinadaily.com.cn/a/201909/09/WS5d754649a310cf3e3556a5b9.html
[61] E. Ismagilova, L. Hughes, Y. K. Dwivedi, and K. R. Raman, "Smart cities: Advances in research—An information systems perspective," *Int. J. Inf. Manage.*, vol. 47, pp. 88–100, Aug. 2019.
[62] United Nations Department of Economic and Social Affairs. *68% of the World Population Projected to Live in Urban Areas by 2050, Says UN*. Accessed: Mar. 30, 2021. [Online]. Available: https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html
[63] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A literature review," *J. Comput. Commun.*, vol. 3, no. 5, pp. 164–173, 2015.
[64] D. Li, Z. Cai, L. Deng, and X. Yao, "IoT complex communication architecture for smart cities based on soft computing models," *Soft Comput.*, vol. 23, no. 8, pp. 2799–2812, 2019.
[65] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, "IoT architecture challenges and issues: Lack of standardization," in *Proc. Future Technol. Conf. (FTC)*, Dec. 2016, pp. 731–738.
[66] S. Krco, B. Pokric, and F. Carrez, "Designing IoT architecture(s): A European perspective," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 79–84.
[67] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: A survey," *J. Cloud Comput.*, vol. 7, no. 1, pp. 1–20, Dec. 2018.
[68] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, protocols, and applications," *J. Electr. Comput. Eng.*, vol. 2017, pp. 9324035:1–9324035:25, Jan. 2017.
[69] M. Weyrich and C. Ebert, "Reference architectures for the Internet of Things," *IEEE Softw.*, vol. 33, no. 1, pp. 112–116, Jan. 2016.
[70] N. M. Kumar and P. K. Mallick, "The Internet of Things: Insights into the building blocks, component interactions, and architecture layers," *Proc. Comput. Sci.*, vol. 132, pp. 109–117, Jan. 2018.
[71] A. Calihman. (Jan. 2019). *IoT Architectures—Common Approaches and Ways to Design IoT at Scale*. [Online]. Available: https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization/
[72] H. R. Arkian, A. Diyanat, and A. Pourkhalili, "MIST: Fog-based data analytics scheme with cost-efficient resource provisioning for IoT crowdsensing applications," *J. Netw. Comput. Appl.*, vol. 82, pp. 152–165, Mar. 2017.
[73] S. de Capitani di Vimercati, S. Foresti, G. Livraga, and P. Samarati, "Data privacy: Definitions and techniques," *Int. J. Uncertainty, Fuzziness Knowl.-Based Syst.*, vol. 20, no. 6, pp. 793–817, 2012.
[74] C. A. Cassa, S. C. Wieland, and K. D. Mandl, "Re-identification of home addresses from spatial locations anonymized by Gaussian skew," *Int. J. Health Geograph.*, vol. 7, no. 1, p. 45, 2008.
[75] X. Zhou, S. D. Wolthusen, C. Busch, and A. Kuijper, "Feature correlation attack on biometric privacy protection schemes," in *Proc. 5th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Sep. 2009, pp. 1061–1065.
[76] *Statistical Language—Correlation and Causation*. Accessed: Dec. 16, 2020. [Online]. Available: https://www.abs.gov.au/
[77] D. Agrawal and D. Kesdogan, "Measuring anonymity: The disclosure attack," *IEEE Secur. Privacy*, vol. 1, no. 6, pp. 27–34, Nov./Dec. 2003.
[78] S. Gambs, M.-O. Killijian, and M. N. D. P. Cortez, "De-anonymization attack on geolocated data," *J. Comput. Syst. Sci.*, vol. 80, no. 8, pp. 1597–1614, Dec. 2014.
[79] A. Harmanci and M. Gerstein, "Quantification of private information leakage from phenotype-genotype data: Linking attacks," *Nature Methods*, vol. 13, no. 3, pp. 251–256, Mar. 2016.
[80] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 746–789, 1st Quart., 2020.
[81] P. R. M. Rao, S. M. Krishna, and A. P. S. Kumar, "Privacy preservation techniques in big data analytics: A survey," *J. Big Data*, vol. 5, no. 1, p. 33, Dec. 2018.
[82] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, nos. 3–4, pp. 211–407, Aug. 2014.
[83] P. Kairouz, S. Oh, and P. Viswanath, "The composition theorem for differential privacy," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 4037–4049, Jun. 2017.
[84] T. Zhu, G. Li, W. Zhou, and P. S. Yu, "Preliminary of differential privacy," in *Differential Privacy and Applications*, vol. 69. Cham, Switzerland: Springer, 2017, pp. 7–16. [Online]. Available: http://link.springer.com/10.1007/978-3-319-62004-6_2
[85] 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.
[86] F. Eigner, A. Kate, M. Maffei, F. Pampaloni, and I. Pryvalov, "Differentially private data aggregation with optimal utility," in *Proc. 30th Annu. Comput. Secur. Appl. Conf. (ACSAC)*. New York, NY, USA: Association for Computing Machinery, Dec. 2014, pp. 316–325.
[87] J. Soria-Comas and J. Domingo-Ferrer, "Optimal data-independent noise for differential privacy," *Inf. Sci.*, vol. 250, pp. 200–214, Nov. 2013.
[88] A. Ghosh, T. Roughgarden, and M. Sundararajan, "Universally utility-maximizing privacy mechanisms," in *Proc. 41st Annu. ACM Symp. Symp. Theory Comput. (STOC)*. New York, NY, USA: Association for Computing Machinery, 2009, pp. 351–360.
[89] M. Gupte and M. Sundararajan, "Universally optimal privacy mechanisms for minimax agents," in *Proc. 29th ACM SIGMOD-SIGACT-SIGART Symp. Princ. Database Syst. Data (PODS)*. New York, NY, USA: Association for Computing Machinery, 2010, pp. 135–146.
[90] 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.
[91] Y. Xiao and L. Xiong, "Protecting locations with differential privacy under temporal correlations," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*. New York, NY, USA: Association for Computing Machinery, Oct. 2015, pp. 1298–1309.
[92] G. Kellaris and S. Papadopoulos, "Practical differential privacy via grouping and smoothing," *Proc. VLDB Endowment*, vol. 6, no. 5, pp. 301–312, Mar. 2013.
[93] X. Xiao, G. Bender, M. Hay, and J. Gehrke, "IReduct: Differential privacy with reduced relative errors," in *Proc. Int. Conf. Manage. Data (SIGMOD)*. New York, NY, USA: Association for Computing Machinery, 2011, pp. 229–240.
[94] K. Nissim, S. Raskhodnikova, and A. Smith, "Smooth sensitivity and sampling in private data analysis," in *Proc. 39th Annu. ACM Symp. Theory Comput. (STOC)*. New York, NY, USA: Association for Computing Machinery, 2007, pp. 75–84.
[95] A. Inan, M. E. Gursoy, and Y. Saygin, "Sensitivity analysis for non-interactive differential privacy: Bounds and efficient algorithms," *IEEE Trans. Depend. Sec. Comput.*, vol. 17, no. 1, pp. 194–207, Jan. 2020.
[96] 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. Manage. (CIKM)*. New York, NY, USA: Association for Computing Machinery, Oct. 2015, pp. 1001–1010, doi: 10.1145/2806416.2806441.
[97] 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.
[98] L. Fan, L. Bonomi, L. Xiong, and V. Sunderam, "Monitoring web browsing behavior with differential privacy," in *Proc. 23rd Int. Conf. World Wide Web (WWW)*. New York, NY, USA: Association for Computing Machinery, 2014, pp. 177–188.
[99] G. Cormode, C. Procopiuc, D. Srivastava, E. Shen, and T. Yu, "Differentially private spatial decompositions," in *Proc. IEEE 28th Int. Conf. Data Eng.*, Apr. 2012, pp. 20–31.
[100] G. Acs, C. Castelluccia, and R. Chen, "Differentially private histogram publishing through lossy compression," in *Proc. IEEE 12th Int. Conf. Data Mining*, Dec. 2012, pp. 1–10.

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

[102] A. Machanavajjhala, X. He, and M. Hay, "Differential privacy in the wild: A tutorial on current practices & open challenges," in *Proc. ACM Int. Conf. Manage. Data (SIGMOD)*. New York, NY, USA: Association for Computing Machinery, May 2017, pp. 1727–1730.

[103] F. Koufogiannis, S. Han, and G. J. Pappas, "Optimality of the Laplace mechanism in differential privacy," 2015, *arXiv:1504.00065*.

[104] S. L. Garfinkel, J. M. Abowd, and S. Powazek, "Issues encountered deploying differential privacy," in *Proc. Workshop Privacy Electron. Soc. (WPES)*, New York, NY, USA: Association for Computing Machinery, Jan. 2018, pp. 133–137.

[105] J. Hsu, M. Gaboardi, A. Haeberlen, S. Khanna, A. Narayan, B. C. Pierce, and A. Roth, "Differential privacy: An economic method for choosing epsilon," in *Proc. IEEE 27th Comput. Secur. Found. Symp.*, Jul. 2014, pp. 398–410.

[106] J. Lee and C. Clifton, "How much is enough? Choosing ε for differential privacy," in *Information Security*, vol. 7001. Berlin, Germany: Springer, 2011, pp. 325–340.

[107] P. Dandekar, N. Fawaz, and S. Ioannidis, "Privacy auctions for recommender systems," *ACM Trans. Econ. Comput.*, vol. 2, no. 3, pp. 1–22, Jul. 2014.

[108] C. Li, D. Y. Li, G. Miklau, and D. Suciu, "A theory of pricing private data," *Commun. ACM*, vol. 60, no. 12, pp. 79–86, Nov. 2017.

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

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

[111] Q. Xiao, R. Chen, and K.-L. Tan, "Differentially private network data release via structural inference," in *Proc. 20th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*. New York, NY, USA: Association for Computing Machinery, Aug. 2014, pp. 911–920.

[112] 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.

[113] C. Han and K. Wang, "Sensitive disclosures under differential privacy guarantees," in *Proc. IEEE Int. Congr. Big Data*, Jun. 2015, pp. 110–117.

[114] E. Shen and T. Yu, "Mining frequent graph patterns with differential privacy," in *Proc. 19th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*. New York, NY, USA: Association for Computing Machinery, Aug. 2013, pp. 545–553.

[115] B. Yang, I. Sato, and H. Nakagawa, "Bayesian differential privacy on correlated data," in *Proc. ACM SIGMOD Int. Conf. Manage. Data (SIGMOD)*. New York, NY, USA: Association for Computing Machinery, May 2015, pp. 747–762.

[116] W. Jiang, C. Xie, and Z. Zhang, "Wishart mechanism for differentially private principal components analysis," in *Proc. 13th AAAI Conf. Artif. Intell. (AAAI)*. Palo Alto, CA, USA: AAAI Press, 2016, pp. 1730–1736.

[117] 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. (SIGMOD)*. New York, NY, USA: Association for Computing Machinery, May 2014, pp. 11–20.

[118] 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.

[119] U.S. Census Bureau. *Census Scientific Advisory Committee: September 14–15, 2017*. Accessed: Apr. 3, 2021. [Online]. Available: https://www.census.gov/about/cac/sac/meetings/2017-09-meeting.html

[120] A. Haeberlen, B. C. Pierce, and A. Narayan, "Differential privacy under fire," in *Proc. 20th USENIX Conf. Secur. (SEC)*. Berkeley, CA, USA: USENIX Association, 2011, p. 33.

[121] J. Domingo-Ferrer, D. Sánchez, and A. Blanco-Justicia, "The limits of differential privacy (and its misuse in data release and machine learning)," *Commun. ACM*, vol. 64, no. 7, pp. 33–35, Jul. 2021.

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

[123] R. Sarathy and K. Muralidhar, "Evaluating Laplace noise addition to satisfy differential privacy for numeric data," *Trans. Data Privacy*, vol. 4, no. 1, pp. 1–17, 2011.

[124] (Feb. 2020). *Differential Privacy From Theory to Practice*. [Online]. Available: https://leapyear.io/resources/blog-posts/differential-privacy-from-theory-to-practice/

[125] (Sep. 2020). *Threat Models for Differential Privacy*. [Online]. Available: https://www.nist.gov/blogs/cybersecurity-insights/threat-models-differential-privacy

[126] A. Bittau, Ú. Erlingsson, P. Maniatis, I. Mironov, A. Raghunathan, D. Lie, M. Rudominer, U. Kode, J. Tinnes, and B. Seefeld, "Prochlo: Strong privacy for analytics in the crowd," in *Proc. 26th Symp. Oper. Syst. Princ. (SOSP)*. New York, NY, USA: Association for Computing Machinery, Oct. 2017, pp. 441–459.

[127] B. Balle, J. Bell, A. Gascón, and K. Nissim, "The privacy blanket of the shuffle model," in *Proc. Annu. Int. Cryptol. Conf.*, vol. 11693. Cham, Switzerland: Springer, 2019, pp. 638–667. [Online]. Available: http://link.springer.com/10.1007/978-3-030-26951-7_22

[128] A. Cheu, A. Smith, J. Ullman, D. Zeber, and M. Zhilyaev, "Distributed differential privacy via shuffling," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, vol. 11476. Cham, Switzerland: Springer, 2019, pp. 375–403. [Online]. Available: http://link.springer.com/10.1007/978-3-030-17653-2_13

[129] 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.

[130] W.-L. Chin, W. Li, and H.-H. Chen, "Energy big data security threats in IoT-based smart grid communications," *IEEE Commun. Mag.*, vol. 55, no. 10, pp. 70–75, Oct. 2017.

[131] 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.

[132] 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.

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

[134] 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.

[135] 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.

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

[137] 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.

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

[139] 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.

[140] M. B. Hossain, I. Natgunanathan, Y. Xiang, and Y. Zhang, "Cost-friendly differential privacy of smart meters using energy storage and harvesting devices," *IEEE Trans. Services Comput.*, early access, May 18, 2021, doi: 10.1109/TSC.2021.3081170.

[141] M. B. Gough, S. F. Santos, T. AlSkaif, M. S. Javadi, R. Castro, and J. P. S. Catalao, "Preserving privacy of smart meter data in a smart grid environment," *IEEE Trans. Ind. Informat.*, vol. 18, no. 1, pp. 707–718, Jan. 2022.

[142] D. Snoonian, "Smart buildings," *IEEE Spectr.*, vol. 40, no. 8, pp. 18–23, Aug. 2003.

[143] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, "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.

[144] 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.

[145] Y. Chen, A. Machanavajjhala, M. Hay, and G. Miklau, "PeGaSus: Data-adaptive differentially private stream processing," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*. New York, NY, USA: Association for Computing Machinery, Oct. 2017, pp. 1375–1388.

[146] S. Ghayyur, Y. Chen, R. Yus, A. Machanavajjhala, M. Hay, G. Miklau, and S. Mehrotra, "IoT-detective: Analyzing IoT data under differential privacy," in *Proc. Int. Conf. Manage. Data (SIGMOD)*. New York, NY, USA: Association for Computing Machinery, May 2018, pp. 1725–1728.
[147] 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.
[148] R. Alisic, M. Molinari, P. E. Paré, and H. Sandberg, "Bounding privacy leakage in smart buildings," 2020, *arXiv:2003.13187*.
[149] J. Zhou, R. Q. Hu, and Y. Qian, "Scalable distributed communication architectures to support advanced metering infrastructure in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1632–1642, Sep. 2012.
[150] M. Jawurek, F. Kerschbaum, and G. Danezis, "Privacy technologies for smart grids—A survey of options," Microsoft Res., Cambridge, U.K., Tech. Rep. MSR-TR-2012-119, 2012.
[151] Z. Erkin, J. R. Troncoso-Pastoriza, R. L. Lagendijk, and F. Perez-Gonzalez, "Privacy-preserving data aggregation in smart metering systems: An overview," *IEEE Signal Process. Mag.*, vol. 30, no. 2, pp. 75–86, Mar. 2013.
[152] C. Rottondi, G. Verticale, and C. Krauss, "Privacy-preserving smart metering with multiple data consumers," *Comput. Netw.*, vol. 57, no. 7, pp. 1699–1713, May 2013.
[153] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in *Proc. 3rd ACM Workshop Cloud Comput. Secur. Workshop (CCSW)*, New York, NY, USA: Association for Computing Machinery, 2011, pp. 113–124.
[154] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 238–243.
[155] C. A. Zukowski, "High-speed data transmission using low-frequency clocks," *IEEE Trans. Circuits Syst.*, vol. 38, no. 3, pp. 273–280, Mar. 1991.
[156] L. Fan and L. Xiong, "Real-time aggregate monitoring with differential privacy," in *Proc. 21st ACM Int. Conf. Inf. Knowl. Manage. (CIKM)*. New York, NY, USA: Association for Computing Machinery, 2012, pp. 2169–2173.
[157] Y. Sun, L. Lampe, and V. W. S. Wong, "EV-assisted battery load hiding: A Markov decision process approach," in *Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Nov. 2016, pp. 160–166.
[158] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, Apr. 2014, pp. 504–512.
[159] 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/ACM 25th Int. Symp. Quality Service (IWQoS)*, Jun. 2017, pp. 1–9.
[160] 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," 2015, *arXiv:1507.03000*.
[161] 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.
[162] C. Clifton and T. Tassa, "On syntactic anonymity and differential privacy," in *Proc. IEEE 29th Int. Conf. Data Eng. Workshops (ICDEW)*, Apr. 2013, pp. 88–93.
[163] G. Eibl and D. Engel, "Differential privacy for real smart metering data," *Comput. Sci.*, vol. 32, nos. 1–2, pp. 173–182, Mar. 2017.
[164] G. Ács and C. Castelluccia, "I have a DREAM! (Differentially private smart metering)," in *Proc. 13th Int. Conf. Inf. Hiding (IH)*. Berlin, Germany: Springer-Verlag, 2011, pp. 118–132.
[165] 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. (SAC)*. New York, NY, USA: Association for Computing Machinery, Mar. 2014, pp. 531–538.
[166] 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.
[167] U. B. Baloglu and Y. Demir, "Lightweight privacy-preserving data aggregation scheme for smart grid metering infrastructure protection," *Int. J. Crit. Infrastruct. Protection*, vol. 22, pp. 16–24, Sep. 2018.
[168] X. Liao, P. Srinivasan, D. Formby, and R. A. Beyah, "Di-PriDA: Differentially private distributed load balancing control for the smart grid," *IEEE Trans. Depend. Sec. Comput.*, vol. 16, no. 6, pp. 1026–1039, Nov. 2019.
[169] R. Pal, P. Hui, and V. Prasanna, "Privacy engineering for the smart micro-grid," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 5, pp. 965–980, May 2019.
[170] J. Xiong, J. Ren, L. Chen, Z. Yao, M. Lin, D. Wu, and B. Niu, "Enhancing privacy and availability for data clustering in intelligent electrical service of IoT," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1530–1540, Apr. 2019.
[171] N. Gai, K. Xue, P. He, B. Zhu, J. Liu, and D. He, "An efficient data aggregation scheme with local differential privacy in smart grid," in *Proc. 16th Int. Conf. Mobility, Sens. Netw. (MSN)*, Dec. 2020, pp. 73–80.
[172] L. Ou, Z. Qin, S. Liao, T. Li, and D. Zhang, "Singular spectrum analysis for local differential privacy of classifications in the smart grid," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5246–5255, Jun. 2020.
[173] K. Hafeez, M. H. Rehmani, and D. OShea, "DPNCT: A differential private noise cancellation scheme for load monitoring and billing for smart meters," 2021, *arXiv:2102.09458*.
[174] S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in *Proc. WASA*, 2015, pp. 685–695.
[175] 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.
[176] H. Cao, S. Liu, L. Wu, Z. Guan, and X. Du, "Achieving differential privacy against non-intrusive load monitoring in smart grid: A fog computing approach," *Concurrency Comput., Pract. Exp.*, vol. 31, no. 22, Nov. 2019, Art. no. e4528.
[177] W. Fan, J. He, M. Guo, P. Li, Z. Han, and R. Wang, "Privacy preserving classification on local differential privacy in data centers," *J. Parallel Distrib. Comput.*, vol. 135, pp. 70–82, Jan. 2020.
[178] S. An, B. Lee, and D. Shin, "A survey of intelligent transportation systems," in *Proc. 3rd Int. Conf. Comput. Intell., Commun. Syst. Netw.*, 2011, pp. 332–337.
[179] N.-E.-E. 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, Jan. 2011.
[180] 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.
[181] 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.
[182] L. Qi, "Research on intelligent transportation system technologies and applications," in *Proc. Workshop Power Electron. Intell. Transp. Syst.*, Aug. 2008, pp. 529–531.
[183] 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.
[184] C. Gosman, C. Dobre, and F. Pop, "Privacy-preserving data aggregation in intelligent transportation systems," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manage. (IM)*, May 2017, pp. 1059–1064.
[185] A.-S. K. Pathan, *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*. Boca Raton, FL, USA: CRC Press, 2019.
[186] A. Thaduri, D. Galar, and U. Kumar, "Railway assets: A potential domain for big data analytics," *Proc. Comput. Sci.*, vol. 53, pp. 457–467, Jan. 2015.
[187] 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.
[188] H. Duan and Y. Yan, "Study on game between high-speed railway and traditional express delivery businesses based on non-cooperative game," *Logistics Technol.*, vol. 7, pp. 101–105, Jul. 2015.
[189] (Apr. 2020). *Types of Transportation in Logistics*. [Online]. Available: https://www.purolatorinternational.com/types-of-transportation-in-logistics/
[190] K. Jiang, D. Shao, S. Bressan, T. Kister, and K.-L. Tan, "Publishing trajectories with differential privacy guarantees," in *Proc. 25th Int. Conf. Sci. Stat. Database Manage. (SSDBM)*. New York, NY, USA: Association for Computing Machinery, 2013, pp. 1–12.
[191] 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.
[192] 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.

[193] S. Paiva, M. A. Ahad, S. Zafar, G. Tripathi, A. Khalique, and I. Hussain, "Privacy and security challenges in smart and sustainable mobility," *Social Netw. Appl. Sci.*, vol. 2, no. 7, p. 1175, Jul. 2020.

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

[195] 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.

[196] 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, May 2018.

[197] 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.*, vol. 14, no. 4, pp. 1068–1083, Jul. 2021.

[198] 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. [Online]. Available: http://link.springer.com/10.1007/978-3-319-98161-1_5

[199] 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, p. e9, May 2018.

[200] 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. 68, no. 8, pp. 8091–8102, Aug. 2019.

[201] 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.

[202] 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.

[203] 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.

[204] M. Naor, B. Pinkas, and R. Sumner, "Privacy preserving auctions and mechanism design," in *Proc. 1st ACM Conf. Electron. Commerce (EC)*. New York, NY, USA: Association for Computing Machinery, 1999, pp. 129–139.

[205] 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.

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

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

[208] W. Zhang, R. Rao, G. Cao, and G. Kesidis, "Secure routing in ad hoc networks and a related intrusion detection problem," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, vol. 2, Oct. 2003, pp. 735–740.

[209] Q. M. Alriyami, E. Asimakopoulou, and N. Bessis, "A survey of intrusion detection systems for mobile ad hoc networks," in *Proc. Int. Conf. Intell. Netw. Collaborative Syst.*, Sep. 2014, pp. 427–432.

[210] T. Anantvalee and J. Wu, "A survey on intrusion detection in mobile ad hoc networks," in *Wireless Network Security*. New York, NY, USA: Springer, 2007, pp. 159–180. [Online]. Available: http://link.springer.com/10.1007/978-0-387-33112-6_7

[211] 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.

[212] D. An, Q. Yang, W. Yu, D. Li, and W. Zhao, "LoPrO: Location privacy-preserving online auction scheme for electric vehicles joint bidding and charging," *Future Gener. Comput. Syst.*, vol. 107, pp. 394–407, Jun. 2020.

[213] R. Qiu, X. Liu, R. Huang, F. Zheng, L. Liang, and Y. Li, "Differential privacy EV charging data release based on variable window," *PeerJ Comput. Sci.*, vol. 7, p. e481, Apr. 2021.

[214] F. Kargl, A. Friedman, and R. Boreli, "Differential privacy in intelligent transportation systems," in *Proc. 6th ACM Conf. Secur. Privacy Wireless Mobile Netw. (WiSec)*. New York, NY, USA: Association for Computing Machinery, 2013, pp. 107–112.

[215] J. Ovretveit, T. Scott, T. G. Rundall, S. M. Shortell, and M. Brommels, "Improving quality through effective implementation of information technology in healthcare," *Int. J. Quality Health Care*, vol. 19, no. 5, pp. 259–266, Aug. 2007.

[216] 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.

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

[218] 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.

[219] J. Zhang, X. Liang, Z. Zhang, S. He, and Z. Shi, "Re-DPoctor: Real-time health data releasing with W-day differential privacy," in *Proc. GLOBECOM*, Dec. 2017, pp. 1–6.

[220] H. Habibzadeh, K. Dinesh, O. R. Shishvan, A. Boggio-Dandry, G. Sharma, and T. Soyata, "A survey of healthcare Internet of Things (HIoT): A clinical perspective," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 53–71, Jan. 2020.

[221] X. Sun, L. Shi, L. Wu, Z. Guan, X. Du, and M. Guizani, "A differentially private classification algorithm with high utility for wireless body area networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, May 2020, pp. 1–6.

[222] B. Chakraborty, S. Verma, and K. P. Singh, "Temporal differential privacy in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 155, Apr. 2020, Art. no. 102548.

[223] 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.*, vol. 6, no. 5, pp. 8714–8726, Oct. 2019.

[224] J. J. Kang, M. Dibaei, G. Luo, W. Yang, and X. Zheng, "A privacy-preserving data inference framework for Internet of Health Things networks," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 1209–1214.

[225] J. Guo, M. Yang, and B. Wan, "A practical privacy-preserving publishing mechanism based on personalized k-anonymity and temporal differential privacy for wearable IoT applications," *Symmetry*, vol. 13, no. 6, p. 1043, Jun. 2021.

[226] B. Shickel, P. J. Tighe, A. Bihorac, and P. Rashidi, "Deep EHR: A survey of recent advances in deep learning techniques for electronic health record (EHR) analysis," *IEEE J. Biomed. Health Inform.*, vol. 22, no. 5, pp. 1589–1604, Sep. 2018.

[227] 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)*, Oct. 2013, pp. 249–253.

[228] R. Agrawal and R. Srikant, "Privacy-preserving data mining," in *Proc. ACM SIGMOD Int. Conf. Manage. Data (SIGMOD)*. New York, NY, USA: Association for Computing Machinery, 2000, pp. 439–450.

[229] X. Jiang, S. Cheng, and L. Ohno-Machado, "Quantifying fine-grained privacy risk and representativeness in medical data," in *Proc. Workshop Data Mining Med. Healthcare (DMMH)*. New York, NY, USA: Association for Computing Machinery, 2011, pp. 64–67.

[230] P. Shi, L. Xiong, and B. C. M. Fung, "Anonymizing data with quasi-sensitive attribute values," in *Proc. 19th ACM Int. Conf. Inf. Knowl. Manage. (CIKM)*. New York, NY, USA: Association for Computing Machinery, 2010, pp. 1389–1392.

[231] 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.*, Jun. 2015, pp. 191–196.

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

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

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

[235] 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.
[236] 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)*, Aug. 2017, pp. 397–402.
[237] D. Lockhart and E. Winzeler, "Genomics, gene expression and dna arrays," *Nature*, vol. 405, pp. 827–836, Jun. 2000.
[238] C. D. Bustamante, F. M. D. L. Vega, and E. G. Burchard, "Genomics for the world," *Nature*, vol. 475, no. 7355, pp. 163–165, 2011.
[239] J. L. Raisaro, J. R. Troncoso-Pastoriza, M. Misbach, J. S. Sousa, S. Pradervand, E. Missiaglia, O. Michielin, B. Ford, and J.-P. Hubaux, "MedCo: Enabling secure and privacy-preserving exploration of distributed clinical and genomic data," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, vol. 16, no. 4, pp. 1328–1341, Jul. 2019.
[240] J. L. Raisaro, G. Choi, S. Pradervand, R. Colsenet, N. Jacquemont, N. Rosat, V. Mooser, and J.-P. Hubaux, "Protecting privacy and security of genomic data in i2b2 with homomorphic encryption and differential privacy," *IEEE/ACM Trans. Comput. Biol. Bioinf.*, vol. 15, no. 5, pp. 1413–1426, Sep./Oct. 2018.
[241] Z. He, Y. Li, J. Li, K. Li, Q. Cai, and Y. Liang, "Achieving differential privacy of genomic data releasing via belief propagation," *Tsinghua Sci. Technol.*, vol. 23, no. 4, pp. 389–395, Aug. 2018.
[242] N. Almadhoun, E. Ayday, and Ö. Ulusoy, "Differential privacy under dependent tuples—The case of genomic privacy," *Bioinformatics*, vol. 36, 2020, Art. no. btz837.
[243] 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. Manage.*, vol. 13, no. 4, pp. 205–216, Dec. 2012.
[244] K. R. Sollins, "IoT big data security and privacy versus innovation," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1628–1635, Apr. 2019.
[245] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102481.
[246] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The industrial Internet of Things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, Oct. 2018.
[247] H. Li, A. 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.
[248] X. Lu, Z. Qu, Q. Li, and P. Hui, "Privacy information security classification for Internet of Things based on internet data," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 8, Aug. 2015, Art. no. 932941.
[249] D. V. Jose and A. Vijyalakshmi, "An overview of security in Internet of Things," *Proc. Comput. Sci.*, vol. 143, pp. 744–748, Jan. 2018.
[250] 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*, Jun. 2009, pp. 47–52.
[251] B. Shen and Y. Liu, "Privacy and security in the exploitation of Internet of Things," *J. Dialectics Nature*, vol. 33, no. 6, pp. 77–83, 2011.
[252] 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.
[253] L. Sweeney, "Achieving K-anonymity privacy protection using generalization and suppression," *Fuzziness Knowl.-Based Syst.*, vol. 10, no. 5, pp. 571–588, Oct. 2002.
[254] Y. Saygin, V. S. Verykios, and A. K. Elmagarmid, "Privacy preserving association rule mining," in *Proc. 12th Int. Workshop Res. Issues Data Eng., Eng. E-Commerce/E-Bus. Syst. (RIDE-2EC)*, 2002, pp. 151–158.
[255] A. C.-C. Yao, "How to generate and exchange secrets," in *Proc. 27th Annu. Symp. Found. Comput. Sci. (SFCS)*, Oct. 1986, pp. 162–167.
[256] 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, Dec. 2002.
[257] E. Wang, M. Zhang, X. Cheng, Y. Yang, W. Liu, H. Yu, L. Wang, and J. Zhang, "Deep learning-enabled sparse industrial crowdsensing and prediction," *IEEE Trans. Ind. Informat.*, vol. 17, no. 9, pp. 6170–6181, Sep. 2021.
[258] C. R. G. Rodríguez and S. E. G. Barrantes, "Using differential privacy for the Internet of Things," *Privacy and Identity Management. Facing Up to Next Steps* (IFIP Advances in Information and Communication Technology). Cham, Switzerland: Springer, 2016, pp. 201–211.
[259] X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu, and M. S. Hossain, "PPCS: An intelligent privacy-preserving mobile-edge crowdsensing strategy for industrial IoT," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10288–10298, Jul. 2021.
[260] Y. Zheng, H. Duan, and C. Wang, "Learning the truth privately and confidently: Encrypted confidence-aware truth discovery in mobile crowdsensing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 10, pp. 2475–2489, Oct. 2018.
[261] J. Ni, K. Zhang, Q. Xia, X. Lin, and X. Shen, "Enabling strong privacy preservation and accurate task allocation for mobile crowdsensing," *IEEE Trans. Mobile Comput.*, vol. 19, no. 6, pp. 1317–1331, Jun. 2020.
[262] L. Ma, X. Liu, Q. Pei, and Y. Xiang, "Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing," *IEEE Trans. Services Comput.*, vol. 12, no. 5, pp. 786–799, Sep./Oct. 2019.
[263] C. Zhang, L. Zhu, C. Xu, X. Liu, and K. Sharif, "Reliable and privacy-preserving truth discovery for mobile crowdsensing systems," *IEEE Trans. Depend. Sec. Comput.*, vol. 18, no. 3, pp. 1245–1260, May/Jun. 2019.
[264] L. Wang, D. Zhang, D. Yang, B. Y. Lim, and X. Ma, "Differential location privacy for sparse mobile crowdsensing," in *Proc. IEEE 16th Int. Conf. Data Mining (ICDM)*, Dec. 2016, pp. 1257–1262.
[265] J. Chen, H. Ma, D. Zhao, and L. Liu, "Correlated differential privacy protection for mobile crowdsensing," *IEEE Trans. Big Data*, vol. 7, no. 4, pp. 784–795, Oct. 2017.
[266] M. Yang, T. Zhu, Y. Xiang, and W. Zhou, "Density-based location preservation for mobile crowdsensing with differential privacy," *IEEE Access*, vol. 6, pp. 14779–14789, 2018.
[267] L. Wang, D. Yang, X. Han, T. Wang, D. Zhang, and X. Ma, "Location privacy-preserving task allocation for mobile crowdsensing with differential geo-obfuscation," in *Proc. 26th Int. Conf. World Wide Web (WWW)*. Geneva, Switzerland: International World Wide Web Conferences Steering Committee, Apr. 2017, pp. 627–636.
[268] J. Wang, Y. Wang, G. Zhao, and Z. Zhao, "Location protection method for mobile crowd sensing based on local differential privacy preference," *Peer-to-Peer Netw. Appl.*, vol. 12, no. 5, pp. 1097–1109, Sep. 2019.
[269] F. Peng, S. Tang, B. Zhao, and Y. Liu, "A privacy-preserving data aggregation of mobile crowdsensing based on local differential privacy," in *Proc. ACM Turing Celebration Conf. (China)*. New York, NY, USA: Association for Computing Machinery, May 2019, pp. 1–5.
[270] L. Wang, D. Zhang, D. Yang, B. Y. Lim, X. Han, and X. Ma, "Sparse mobile crowdsensing with differential and distortion location privacy," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2735–2749, 2020.
[271] L. Li, X. Zhang, R. Hou, H. Yue, H. Li, and M. Pan, "Participant recruitment for coverage-aware mobile crowdsensing with location differential privacy," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2019, pp. 1–6.
[272] Z. Li, Z. Song, and X. Chen, "Privacy-preserving cost minimization in mobile crowd sensing supported by edge computing," *IEEE Access*, vol. 8, pp. 121920–121928, 2020.
[273] X. Chen, X. Wu, X. Wang, W. Zhao, and W. Xue, "Real-location reporting based differential privacy trajectory protection for mobile crowdsensing," in *Proc. 5th Int. Conf. Big Data Comput. Commun. (BIGCOM)*, Aug. 2019, pp. 142–150.
[274] Z. Wang, J. Hu, R. Lv, J. Wei, Q. Wang, D. Yang, and H. Qi, "Personalized privacy-preserving task allocation for mobile crowdsensing," *IEEE Trans. Mobile Comput.*, vol. 18, no. 6, pp. 1330–1341, Jun. 2019.
[275] J. Xiong, R. Ma, L. Chen, Y. Tian, Q. Li, X. Liu, and Z. Yao, "A personalized privacy protection framework for mobile crowdsensing in IIoT," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4231–4241, Jun. 2020.
[276] Z. Wang, J. Li, J. Hu, J. Ren, Z. Li, and Y. Li, "Towards privacy-preserving incentive for mobile crowdsensing under an untrusted platform," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, Apr. 2019, pp. 2053–2061.
[277] C. Ying, H. Jin, X. Wang, and Y. Luo, "Double insurance: Incentivized federated learning with differential privacy in mobile crowdsensing," in *Proc. Int. Symp. Reliable Distrib. Syst. (SRDS)*, Sep. 2020, pp. 81–90.

[278] 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. 2018.

[279] M. Khalgui and O. Mosbahi, "Intelligent distributed control systems," *Inf. Softw. Technol.*, vol. 52, no. 12, pp. 1259–1271, Dec. 2010.

[280] A. Kusiak, "Smart manufacturing," *Int. J. Prod. Res.*, vol. 56, nos. 1–2, pp. 508–517, 2017.

[281] J. Wan, B. Chen, M. Imran, F. Tao, D. Li, C. Liu, and S. Ahmad, "Toward dynamic resources management for IoT-based manufacturing," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 52–59, Feb. 2018.

[282] M. B. Line, A. Zand, G. Stringhini, and R. Kemmerer, "Targeted attacks against industrial control systems: Is the power industry prepared?" in *Proc. 2nd Workshop Smart Energy Grid Secur. (SEGS)*. New York, NY, USA: Association for Computing Machinery, Nov. 2014, pp. 13–22.

[283] A. Shahzad, S. Musa, A. Aborujilah, and M. Irfan, "Industrial control systems (ICSs) vulnerabilities analysis and SCADA security enhancement using testbed encryption," in *Proc. 8th Int. Conf. Ubiquitous Inf. Manage. Commun. (ICUIMC)*. New York, NY, USA: Association for Computing Machinery, 2014, pp. 1–6.

[284] A. Perez-Resa, M. Garcia-Bosque, C. Sánchez-Azqueta, and S. Celma, "Chaotic encryption applied to optical Ethernet in industrial control systems," *IEEE Trans. Instrum. Meas.*, vol. 68, no. 12, pp. 4876–4886, Dec. 2019.

[285] S. Zhou, Z. Yu, E. S. A. Nasr, H. A. Mahmoud, E. M. Awwad, and N. Wu, "Homomorphic encryption of supervisory control systems using automata," *IEEE Access*, vol. 8, pp. 147185–147198, 2020.

[286] M. Schulze Darup, A. Redder, and D. E. Quevedo, "Encrypted cooperative control based on structured feedback," *IEEE Control Syst. Lett.*, vol. 3, no. 1, pp. 37–42, Jan. 2019.

[287] W. Jiang and C. Clifton, "Privacy-preserving distributed k-anonymity," in *Data and Applications Security XIX* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2005, pp. 166–177.

[288] Z. Huang, Y. Wang, S. Mitra, and G. E. Dullerud, "On the cost of differential privacy in distributed control systems," in *Proc. 3rd Int. Conf. High Confidence Netw. Syst. (HiCoNS)*. New York, NY, USA: Association for Computing Machinery, Apr. 2014, pp. 105–114.

[289] 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.

[290] 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)*, Aug. 2017, pp. 1313–1318.

[291] Q. Hu, R. Chen, H. Yang, and S. Kumara, "Privacy-preserving data mining for smart manufacturing," *Smart Sustain. Manuf. Syst.*, vol. 4, no. 2, Jul. 2020, Art. no. 20190043.

[292] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," *Pattern Recognit.*, vol. 84, pp. 317–331, Dec. 2018.

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

[294] T. Zhu, P. Xiong, G. Li, W. Zhou, and P. S. Yu, "Differentially private model publishing in cyber physical systems," *Future Gener. Comput. Syst.*, vol. 108, pp. 1297–1306, Jul. 2020.

[295] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "A trustworthy privacy preserving framework for machine learning in industrial IoT systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6092–6102, Sep. 2020.

[296] J. Hou, Q. Li, S. Cui, S. Meng, S. Zhang, Z. Ni, and Y. Tian, "Low-cohesion differential privacy protection for industrial internet," *J. Supercomput.*, vol. 76, no. 11, pp. 8450–8472, Nov. 2020.

[297] C. Clifton and B. Anandan, "Challenges and opportunities for security with differential privacy," in *Information Systems Security* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2013, pp. 1–13.

[298] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Bus. Inf. Syst. Eng.*, vol. 59, no. 3, pp. 183–187, 2017.

[299] V. Brilliantova and T. W. Thurner, "Blockchain and the future of energy," *Technol. Soc.*, vol. 57, pp. 38–45, May 2019.

[300] M. Andoni, V. Robu, D. Flynn, S. Abram, D. Geach, D. Jenkins, P. Mccallum, and A. Peacock, "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renew. Sustain Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019.

[301] J. Wu and N. Tran, "Application of blockchain technology in sustainable energy systems: An overview," *Sustainability*, vol. 10, no. 9, p. 3067, Aug. 2018.

[302] P. Treleaven, R. G. Brown, and D. Yang, "Blockchain technology in finance," *Computer*, vol. 50, no. 9, pp. 14–17, 2017.

[303] L. Carlozo, "What is blockchain?" *J. Accountancy*, vol. 224, no. 1, p. 29, 07 2017.

[304] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Sep. 2016, pp. 1–3.

[305] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, Jun. 2019.

[306] A. Rahman, M. J. Islam, Z. Rahman, M. M. Reza, A. Anwar, M. A. P. Mahmud, M. K. Nasir, and R. M. Noor, "DistB-condo: Distributed blockchain-based IoT-SDN model for smart condominium," *IEEE Access*, vol. 8, pp. 209594–209609, 2020.

[307] 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.

[308] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 180–184.

[309] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.

[310] 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.

[311] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the Internet of Things," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 12–18, Dec. 2018.

[312] Z. Ding, Y. Wang, G. Wang, D. Zhang, and D. Kifer, "Detecting violations of differential privacy," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*. New York, NY, USA: Association for Computing Machinery, Oct. 2018, pp. 475–489.

[313] D. Zhang and D. Kifer, "LightDP: Towards automating differential privacy proofs," *ACM SIGPLAN Notices*, vol. 52, no. 1, pp. 888–901, May 2017.

[314] A. V. Dastjerdi and R. Buyya, "Fog computing: Helping the Internet of Things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, 2016.

[315] R. Deng, R. Lu, C. Lai, and T. H. Luan, "Towards power consumption-delay tradeoff by workload allocation in cloud-fog computing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 3909–3914.

[316] M. Mukherjee, R. Matam, L. Shu, L. Maglaras, M. A. Ferrag, N. Choudhury, and V. Kumar, "Security and privacy in fog computing: Challenges," *IEEE Access*, vol. 5, pp. 19293–19304, 2017.

[317] 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.

[318] X. Yang, T. Wang, X. Ren, and W. Yu, "Survey on improving data utility in differentially private sequential data publishing," *IEEE Trans. Big Data*, vol. 7, no. 4, pp. 729–749, Oct. 2021.

[319] J. Murtagh and S. Vadhan, "The complexity of computing the optimal composition of differential privacy," *Theory of Cryptography* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2015.

[320] Y. Zhai, Y.-S. Ong, and I. W. Tsang, "The emerging 'big dimensionality,'" *IEEE Comput. Intell. Mag.*, vol. 9, no. 3, pp. 14–26, Aug. 2014.

[321] 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.

[322] J. Leny, *Differential Privacy for Dynamic Data*. Cham, Switzerland: Springer, 2020.

[323] C. Dwork, M. Naor, T. Pitassi, and G. N. Rothblum, "Differential privacy under continual observation," in *Proc. 42nd ACM Symp. Theory Comput. (STOC)*. New York, NY, USA: Association for Computing Machinery, 2010, pp. 715–724, doi: 10.1145/1806689.1806787.

[324] T. Zhang and Q. Zhu, "Dynamic differential privacy for ADMM-based distributed classification learning," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 172–187, Jan. 2017.

MUHAMMAD AKBAR HUSNOO received the dual B.Sc. degree (Hons.) in software engineering from Staffordshire University, U.K., and the Asia Pacific University of Technology & Innovation, Malaysia, in 2019, and the Master of Data Science degree from Deakin University, Burwood, VIC, Australia, in 2021, where he is currently pursuing the Ph.D. degree. He has participated in several hackathons and is the ''Champion Winner'' of the SAS Malaysia FinTech Competition 2017–2018. His research interests include privacy preservation, adversarial learning, deep learning, machine learning, and other related topics. Furthermore, he has been awarded ''The University Prize for Best Project of the B.Sc. (Hons.) in Software Engineering Award 2018/2019'' for his honors thesis. Moreover, he was awarded the Deakin International Meritorious Scholarship for his master's degree, a recipient of the CSRI 2020 Summer Scholarship, and a full Deakin University Postgraduate Research Scholarship to pursue his doctorate.

ADNAN ANWAR (Member, IEEE) received the master's (by Research) and Ph.D. degrees from UNSW. He is currently a Lecturer and the Deputy Director of postgraduate cybersecurity studies at the School of Information Technology, Deakin University. Previously, he has worked as a Data Scientist at Flow Power. He has over eight years of research and teaching experience in universities and research labs, including NICTA, La Trobe University, and the University of New South Wales. He is broadly interested in the security research for critical infrastructures, including smart energy grid, SCADA system, and application of machine learning and optimization techniques to solve cyber security issues for industrial systems. He has authored over 40 articles, including high-impact journals (mostly in Q1), conference articles, and book chapters in prestigious venues. He has been a recipient of several awards, including UPA Scholarship, UNSW TFR Scholarship, Best Paper Award, and several travel grants, including ACM and Postgraduate Research Student Support (PRSS) travel grants. He is an Active Member of IEEE for over nine years and serving different committees.

RIPON K. CHAKRABORTTY (Member, IEEE) received the B.Sc. and M.Sc. degrees in industrial and production engineering from the Bangladesh University of Engineering and Technology, in 2009 and 2013, respectively, and the Ph.D. degree from the University of New South Wales (UNSW Australia), in 2017. He is currently a Lecturer on system engineering and project management and also the Program Coordinator for Master of Decision Analytics and Master of Engineering Science at the School of Engineering and Information Technology, UNSW Australia, Canberra. He is currently the Group Leader of Cross-Disciplinary Optimization Under Capability Context Research Team. He has written two book chapters and over 80 technical journal and conference papers. His research interests include a wide range of topics in operations research, project management, supply chain management, artificial intelligence, cyber-physical systems, and information systems management. His research program has been funded by many organizations, such as the Department of Defence-Commonwealth Government, Australia.

ROBIN DOSS (Senior Member, IEEE) is currently a Professor and the Research Director of the Strategic Centre for Cyber Security Research & Innovation (CSRI), Deakin University. In this role, he provides scientific leadership for this multidisciplinary research center focused on the technical, business, human, policy and legal aspects of cybersecurity. In addition, he also leads the Next Generation Authentication Technologies theme for the Critical Infrastructure Security research program of the national Cyber Security Cooperative Research Centre (CSCRC). Prior to this role, he was the Deputy Head of School for the School of Information Technology, Deakin University. He has an extensive research publication portfolio and, in 2019, he was a recipient of the ''Cyber Security Researcher of the Year Award'' from the Australian Information Security Association (AISA). His research interests include the broad areas of system security, protocol design and security analysis with a focus on smart, cyber-physical, and critical infrastructures. His research program has been funded by the Australian Research Council (ARC), government agencies, such as the Defence Signals Directorate (DSD) and the Department of Industry, Innovation and Science (DIIS), and industry partners. He has contributed to large multi-year projects under the European Union's Framework Program (FP6) and been funded by the Indian Government under the Scheme for Promotion of Academic and Research Collaboration (SPARC). He is a member of the executive council of the IoT Alliance Australia (IoTAA). He is the Founding Chair of the Future Network Systems and Security (FNSS) conference series and is an Associate Editor of the *International Journal of Cyber Physical Systems*.

MIKE J. RYAN (Senior Member, IEEE) received the bachelor's, master's, and D.Phil. degrees in engineering. In addition, he has completed two years formal engineering management training in the U.K. He is currently the Director of Capability Associates at Canberra. He has over 35 years of experience in communications engineering, systems engineering, project management, and management. Since joining UNSW, he has lectured in a range of subjects, including communications and information systems, systems engineering, requirements engineering, and project management, and he regularly consults in those fields. He is the author/coauthor of 12 books, three book chapters, and over a 250 refereed journal and conference papers. He is a fellow of Engineers Australia (FIEAust), the International Council on Systems Engineering (INCOSE), and the Institute of Managers and Leaders (FIML), and a Chartered Professional Engineer (CPEng) in electrical and ITEE colleges.