2-5-2021

Differential Privacy for Industrial Internet of Things: Opportunities, Applications and Challenges

Bin Jiang
Shenzhen University

Houbing Song
Embry-Riddle Aeronautical University, SONG4@erau.edu

Jianqiang Li
Shenzhen University

Guanghui Yue
Shenzhen University

To be appear at: IEEE Internet of Things Journal, Vol.XX, No.XX, 2021

Differential Privacy for Industrial Internet of Things: Opportunities, Applications and Challenges

Bin Jiang, *Member, IEEE*, Jianqiang Li, Guanghui Yue, and Houbing Song, *Senior Member, IEEE*

***Abstract*—The development of Internet of Things (IoT) brings new changes to various fields. Particularly, industrial Internet of Things (IIoT) is promoting a new round of industrial revolution. With more applications of IIoT, privacy protection issues are emerging. Specially, some common algorithms in IIoT technology such as deep models strongly rely on data collection, which leads to the risk of privacy disclosure. Recently, differential privacy has been used to protect user-terminal privacy in IIoT, so it is necessary to make in-depth research on this topic. In this paper, we conduct a comprehensive survey on the opportunities, applications and challenges of differential privacy in IIoT. We firstly review related papers on IIoT and privacy protection, respectively. Then we focus on the metrics of industrial data privacy, and analyze the contradiction between data utilization for deep models and individual privacy protection. Several valuable problems are summarized and new research ideas are put forward. In conclusion, this survey is dedicated to complete comprehensive summary and lay foundation for the follow-up researches on industrial differential privacy.**

***Index Terms*—Differential privacy, industrial Internet of things, privacy disclosure, privacy metrics, deep models**

I. Introduction

THE rapid rise of Internet of Things (IoT) brings new demands and scenarios for humans daily life. For example, development of applications such as wearable devices [1], smart appliances [2], autonomous driving [3], intelligent robots [4], have prompted billions of new devices to connect by each other, which is accelerating interconnection in IoT system [5], [6]. For industry, wireless communication and artificial intelligence (AI) jointly promote the development of industrial Internet of Things (IIoT) [7]. Specially, IIoT continuously integrates various kinds of sensors and controllers with sensing network [8], monitoring capabilities [9], mobile communication [10], intelligent analysis [11] and other technologies, so as to greatly improve manufacturing efficiency and product quality, reduce product cost and resource consumption, and finally achieve the upgrading of traditional industry [12], [13]. In addition, large number of industrial data are analyzed by cloud computing mode, so IIoT is essentially machine to machine (M2M) support that extends to the cloud and edge [14].

Rapid development brings unexpected problems. Under the background of increasing application types, how to protect industrial individual privacy has become an important topic in IIoT [15]–[17]. In current research, various privacy protection methods have been applied to IIoT technologies, and it has witnessed some effective algorithms [18]–[20]. Among existing technologies, differential privacy has been identified as the most attractive, especially in the process of individual data publishing for the group network. For IIoT, the application of differential privacy is still in its infancy and trial stage, but this topic is very valuable and there are also preliminary research results to be summarized and compared [21].

A. Motivations

Many cases of privacy leakage in IIoT have been reported. For example, in industrial power consumption, an adversary can infer production efficiency and production type from different types of electricity consumption and peak power consumption period. In this context, the leakage of power consumption information will lead to more dangerous privacy issues. In this way, differential privacy in IIoT is very promising, and it is generally necessary to conduct further research in this direction. The motivations of this paper can be summarized in following three aspects.

Differential privacy in IIoT is not same as commonly used as in traditional IoT systems. Specially, the privacy protection of IIoT is an integrated problem. In order to design novel algorithms, it not only considers the inherent characteristics of IIoT, but also fully exploits the advanced combination of differential privacy with industry demand. So it is the primary motivation of this paper, in order to present the state of the art of differential privacy in IIoT.

Big data and intelligent decision gradually play a dynamic role in the field of modern IIoT [28], and the privacy protection issues in this process are gradually highlighted. We hope that this survey can help researchers to promote the power of differential privacy in IIoT, and it can also attract more researchers to pay attention to this topic. Specially, data distribution has become an inevitable choice for the development of IIoT.

While differential privacy in IIoT has been recognized, many open issues need to be identified to provide guidance for the follow-up research, which is also an important motivation in this paper. In second half of this survey, it will summarize some valuable research hotspots for reference. In this way,

This work was partially supported by China Postdoctoral Science Foundation (No. 2020M680125), National Natural Science Foundation of China (No. U1713212) and the National Science Foundation under Grant No. 1956193. *(Corresponding author: Jianqiang Li.)*

B. Jiang and J. Li are with College of Computer Science and Software Engineering, Shenzhen University, Shenzhen, 518000, China (email: jiangbin@ieee.org; lijq@szu.edu.cn).

G. Yue is with School of Biomedical Engineering, Health Science Center, Shenzhen University, Shenzhen, 518000, China (email: yueguanghui@szu.edu.cn).

H. Song is with the Security and Optimization for Networked Globe Laboratory (SONG Lab), Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University, Daytona Beach, FL, 32114, USA. (email: h.song@ieee.org).

TABLE I: Related survey papers

Ref	Year	Survey Description	Main Contributions	DP Related	IIoT Related	Distinction with This Survey
[22]	2017	Differentially private data publishing and analysis	Focus on practical aspects for differential privacy Present the concepts and practical aspects of DP	☆☆☆☆☆	☆	It restricted observations to data publishing and analysis scenarios
[23]	2017	Improving data utility in differentially private sequential data publishing	Classifications for existing DP-based methods Utility comparison in different categories Application scenario analysis	☆☆☆☆☆	☆	It mainly considered differential privacy in sequential data publishing
[24]	2018	Challenges, opportunities, and directions in IIoT	Clarify the concepts of IoT, IIoT and Industry 4.0 Highlight the opportunities brought in by IIoT Systematic overview of the state-of-the-art research	☆	☆☆☆☆☆	It focused on the Internet of things as a whole, less content for privacy
[25]	2019	Privacy preservation in big data from the communication perspective	Review privacy-preserving framework in big data Especially differential privacy for big data Consider it from communication perspective	☆☆☆	☆☆	There is obvious distinction between big data and Industrial IoT
[26]	2020	Differential privacy in cyber physical systems	Firstly highlight some DP in CPSs domains Outline certain open issues and challenges	☆☆☆☆☆	☆☆	IIoT and CPS have obvious differences in application scenarios
[27]	2020	Challenges and opportunities in securing the industrial Internet of things	Identify differences regarding security from IoT to IIoT Derive distinct security goals and challenges in IIoT Survey current best practices for IIoT security	☆	☆☆☆☆☆	It considered most of the security issues for IIoT

it can indirectly promote the development of IIoT privacy protection, in order to solve the existing important problems.

B. Related Survey Papers

It is very important to collect and compare the survey papers in this topic or the papers which are related to privacy in IIoT. There are several survey papers as listed in Table I.

Zhu *et al.* provided a structured survey on differentially private data publishing and analysis [22]. Specially, authors discussed this issue along two directions: data publishing and data analysis on differential privacy. The typical algorithms are analyzed and compared for diverse mechanisms of differential privacy.

Yang *et al.* investigated the existing schemes on differentially private sequential data publishing, from the perspective of proving data utility [23]. Specially, authors summarized this topic from five aspects: distribution optimization, correlations exploitation, sensitivity calibration, transformation and decomposition.

Sisinni *et al.* conducted a comprehensive survey on IIoT, and authors clarified the concepts of IoT, IIoT, and Industry 4.0 [24]. In this paper, authors made an in-depth analysis on IIoT, and focused on the development of intelligent manufacturing.

Wang *et al.* systematically summarized the privacy preservation with the advancement in big data, and particularly from the communication perspective [25]. In this survey, authors discussed the related issues on sensitive information about individuals and covered the fundamental privacy-preserving framework, especially on differential privacy.

Hassan *et al.* presented a comprehensive survey on differential privacy in cyber-physical systems (CPS) [26]. Specially, authors summarized the application and implementation based on energy systems, transportation systems, healthcare and medical systems, and IIoT, which can be classified as four major applications.

Serror *et al.* conducted a survey of security issues in IIoT with challenges and opportunities for future reeaserch [27]. In many scenarios, information security and data privacy can work together. Therefore, the summary work done by the authors also provides some important references for this field.

TABLE II: Abbreviations in this paper

Abbreviation	Referred
DP	Differential privacy
IoT	Internet of things
IIoT	Industrial Internet of things
M2M	Machine to machine
IM	Intelligent manufacturing
LBS	Location based services
AMR	Autonomous mobile robot
CPS	Cyber physical systems
GAN	Generative adversarial networks
RNN	Recurrent neural network
PSPU	Pseudonym swap with provable unlinkability
UAV	Unmanned aerial vehicle
PLO	Power line obfuscation
LDP	Local differential privacy
SSA	Singular spectrum analysis
CDP	Cost-friendly differential privacy-preserving
OPF	Optimal power flow
PPDP	Privacy-preserving data publishing
DPLP	Differential privacy-based location protection
RA-SP	Risk-averse two-stage stochastic problem
DRW	Directed random walk
STBD	Spatial temporal budget distribution
DAOs	Decentralized autonomous organizations
VANETs	Wireless communication, vehicle ad hoc networks
i2b2	Informatics for integrating biology and the bedside
AGV	Automated guided vehicle
QRC	Quick response code
RFID	Radio frequency identification
ERP	Enterprise resource planning

Compared with the above related reviews, this survey mainly focuses on differential privacy on IIoT, which is the obvious distinction with existing survey papers. The special comparisons can be referred in Table I.

C. Contributions and Organization

As a survey paper, it aims to investigate the application value and potential of differential privacy in the field of IIoT. In this paper, it focuses on the following issues: privacy measure-

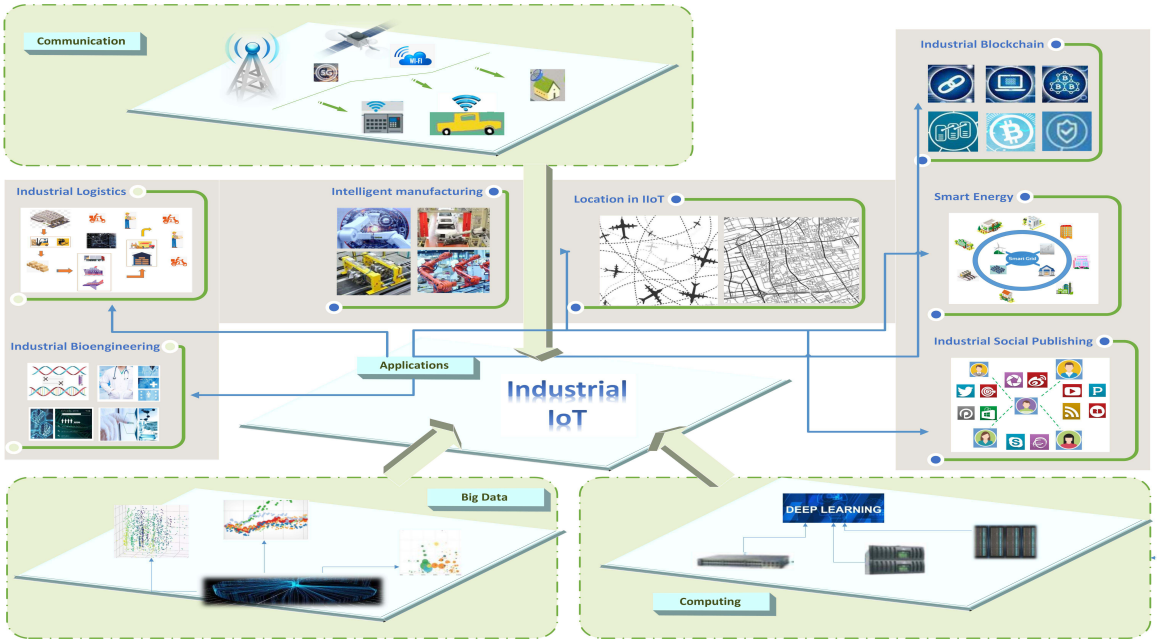

Fig. 1: The architecture of IIoT

ment in IIoT system, data contradiction between deep network and differential privacy, analysis on industrial applications of differential privacy, existing problems and solutions in this field. On the whole, the main contributions of this paper can be summarized as follows:

1) As far as we know, there is no direct review article to summarize the application of differential privacy in IIoT. As a new research direction, this paper summarizes the related privacy issues in the IIoT, and compares the existing methods.

2) This paper discusses the privacy measurement and the balance of privacy data in deep models. These two subtopics are very popular in the field of privacy protection. This paper summarizes its application migration in the field of IIoT.

3) In this paper, the application cases, existing problems and solutions of differential privacy in IIoT are analyzed in detail. For future researchers, it can lay the foundation and provide more valuable new ideas.

The abbreviations used in this paper are presented in Table II and readers can refer to the abbreviations used in this paper. The remainder of this survey is organized as follows. In Sections II and III, we conduct brief surveys on IIoT and differential privacy, respectively. In Sections IV and V, we discuss the two hot issues in this topic: privacy metrics and the conflicts between differential privacy and deep learning. In Section VI, we will present and compare some typical applications based on privacy in IIoT. More importantly, this paper will conclude the current problems and valuable issues in this topic and present future research directions, which will be included in Sections VII and VIII, respectively. At last, the final conclusions are given in Section IX.

II. Privacy Protection in Industrial IoT

A. From IoT to IIoT

The concept and development of IoT has been widely known [29], while the definition of IIoT is often confused. In fact, the generalized IIoT contains not only the common electronic equipment used in traditional IoT, but also achieves the connection of intelligent industrial production equipment [24]. In short, the concept of IIoT simply points to the industrial production process based on IoT. Generally, the architecture of IIoT can be shown in Fig. 1.

In IIoT, operators can connect devices, assets and sensors to collect undeveloped data. It also enables users to deliver scalable, reliable applications faster to meet the changing needs of industrial customers [30]. For example, in connected factory, sensor-enabled device can provide data information which can be analyzed to predict when and where the equipment will fail, thus helping the factory to prevent shutdown. If fault occurs, factory can analyze the data to identify the problem and take corrective actions to prevent it from occurring in advance [31].

Liang *et al.* summarized the edge computing and deep learning technology in IIoT [32]. In addition, authors leveraged the edge computing paradigm and proposed an edge computing-based deep learning model, which can migrate deep learning between cloud servers and edge nodes.

In order to achieve defined constrained optimization, Dai *et al.* proposed a nature-inspired genetic algorithm to keep connected confident information coverage, which is very important for IIoT [33]. However, this issue is very specific, and it is not a general summary and analysis of IIoT.

In summary, the IIoT has three main characteristics. Firstly, IIoT mainly emphasizes the application of reproduction and service, usually involving higher value equipment and assets, such as energy, transportation and industrial control. At the same time, it also has higher requirements for data operation

security [34]. On the contrary, the traditional IoT pays more attention to the field of consumption, such as home application. Secondly, IIoT is built on the industrial infrastructure and is used to upgrade rather than replace the original industrial production equipment. Thirdly, IIoT can be considered as a subset of the IoT, which focuses on productivity improvement.

B. IIoT Characteristics with Main Technologies

Before the emergence of the IIoT, many industrial scenarios still did not have networking capacity, or only provided one-way communication. With IIoT, two-way communication can be achieved: data is provided to the controller and cloud, and feedback is provided to the terminal. For example, a production run can be supported by changing the parameters on the sensor. IIoT provides the opportunity to collect and utilize previously unused information from the warehouse to the plant floor, and correlate existing and new different data sets, ultimately driving improvement and forming new solutions. In this survey, we summarize the main characteristics of IIoT in five aspects: intelligent self-decision, real-time monitoring, smart operation, logistics optimization and energy control.

1) Intelligent Self-decision: For industrial production, the improvement of equipment self decision-making ability means the basic realization of IIoT. In this mode, industrial equipment can make self decision and adjust the production process under certain authority [43]. For example, it is very difficult for any equipment to produce products or provide services with full rate. Through the intelligent self-decision, it can automatically detect the unqualified products, so as to eliminate the low-quality products.

2) Real-time Monitoring: After the realization of IIoT, the supervision of industrial production will become easier. Real-time monitoring and error correction has become an important guarantee for industrial products and services [9]. For normal industrial operation process, it is lack of response to emergency. Through real-time monitoring in IIoT, it can predict and evaluate the possible risks in advance and effectively eliminate.

3) Smart Operation: For industrial products and services, the operation efficiency is very important. Through smart operation based on IIoT, it can improve productivity and achieve valid operation [44]. At the same time, smart operation in IIoT can be competent for more complex and dangerous production activities, which can be in low-risk.

4) Logistics Optimization: In the context of IIoT, intelligent logistics is very important. IIoT can also make it more intelligent, automated warehouse management, including warehousing, inventory, outbound, picking, replenishment, delivery and so on, which can ensure timely and accurately grasping real inventory data [45]. Intelligent logistics is the use of integrated intelligent technology, so that the logistics system can imitate human intelligence, with the ability of thinking, perception, learning, reasoning and judgment and solving some problems in logistics by itself.

5) Smart Energy: IIoT provides better energy management solutions for production, which can not only effectively help improve production efficiency, but also maximize energy utilization, so as to reduce unnecessary waste and environmental pollution, and help save energy and increase production [46].

C. Industrial Privacy

In the promotion process of IIoT, it is also constantly putting forward new requirements and application scenarios, especially on privacy. From the application perspective, there are many aspects on privacy issue in IIoT. In this paper, we summarized it into three main categories: network security, data value and interconnection protocol.

1) Network security: IIoT is a complex infrastructure involving Internet and data transmission. Therefore, it has unprecedented network attack potential. The ownership and security of data are the main challenges of IIoT applications [47]. In addition, the bad performance of network security brings more privacy disclosing.

2) Data value: In general, IIoT data consider how to collect more data and how to process data, but how to find the value of data is more important. Data is an important part of IIoT system, and user privacy data is usually the most critical factor. Therefore, how to mine the potential value of user information is related to effectiveness and efficiency of IIoT [48].

3) Interconnection protocol: IoT is the foundation of the IIoT, but it is not enough to connect the sensor with the equipment, but also need to connect with the Internet. However, for the wireless device network with relatively short distance, there are several protocols competing locally, such as Bluetooth, ZigBee and thread, which must face the interoperability problem [49]. Privacy risk will be brought by the complex interconnection protocol.

For the IIoT, the protection of user privacy has been paid more and more attentions. Therefore, the privacy issues in the IIoT can be classified and summarized in Table III.

Mouratidis *et al.* conducted an analysis on security requirements and identification of attack paths for mitigation of potential vulnerabilities [35]. Mcginthy *et al.* put forward the critical infrastructure node design for IIoT [36]. Mouratidis *et al.* analyzed the cyber threat called as targeted ransomware for fog-computing IIoT [37]. Urbina *et al.* designed the SoC architecture defined as smart sensor for IIoT [38].

Zolanvari *et al.* made a network vulnerability analysis based on deep models for IIoT [39]. Wang *et al.* proposed an intelligent trust evaluation method for IIoT considering sensor-cloud-enabled condition [40]. Boudagdigue *et al.* discussed the trust management issues in IIoT [41]. Zheng *et al.* designed a privacy-preserved data sharing method which can be used for multiple parties in IIoT [42].

All the above researches have investigated the privacy security of IIoT from different perspectives. However, the use of differential privacy technology is still in its infancy, and it is only a preliminary attempt. Therefore, it is necessary to explore the relationship between differential privacy and IoT.

III. Development and Opportunities of Differential Privacy for Industrial IoT

Differential privacy is widely accepted as a strict privacy protection model. Before the advent of differential privacy, the existing privacy preserving algorithms are still problematic, such as k-anonymity [50]. And differential privacy uses more stringent constraints and definitions. It protects the potential

TABLE III: Typical papers on security and privacy in IIoT

Authors	Ref	Description	Year	Focused Subfield in IIoT	On Privacy
Mouratidis *et al.*	[35]	Security analysis method for industrial Internet of things	2018	Security analysis	✓
Dai *et al.*	[33]	Nature-inspired node deployment strategy for connected confident IIoT	2019	Connected confidence	×
Mcginthy *et al.*	[36]	Critical infrastructure node design for secure industrial Internet of things	2019	Infrastructure node design	×
Mouratidis *et al.*	[37]	Targeted ransomware in edge system of brownfield industrial Internet of things	2019	Edge system	×
Urbina *et al.*	[38]	SoC architecture that satisfies IIoT operational requirements	2019	Smart sensor	×
Zolanvari *et al.*	[39]	Deep learning driven network vulnerability analysis for IIoT	2019	Network vulnerability	✓
Wang *et al.*	[40]	Trust evaluation scheme in sensor-cloud-enabled industrial Internet of things	2020	Trust evaluation scheme	✓
Boudagdigue *et al.*	[41]	Dynamic trust management model suitable for industrial environments	2020	Trust management	✓
Zheng *et al.*	[42]	Privacy-preserved data sharing towards multiple parties in Industrial IoTs	2020	Multiple privacy	✓

user privacy information in the published data by adding interference noise. Even if the attacker has mastered certain information, it still can't infer the information. Therefore, this is a method to completely eliminate the possibility of privacy information disclosure from the data source and the detailed technology flow is shown in Fig. 2.

The design goal of differential privacy is to complete the analysis of the whole data set without disclosing the information of a single sample. On the one hand, differential privacy can resist the attacker's possible background knowledge. On the other hand, differential privacy is based on a solid mathematical foundation and can quantitatively evaluate the memory of privacy protection.

It is well known that Dwork *et al.* proposed differential privacy and authors explained the related algorithmic foundations of differential privacy [51]. In [52], Li *et al.* analyzed differential privacy from theory to practice and relevant contents are summarized in depth.

A. Definitions

It is necessary to give the most basic definition of travel privacy here. For a random algorithm M, P_m is the set of all the values that algorithm M can output. If for any pair of adjacent data sets D and $D^{'}$, any subset S_m of P_m, algorithm M satisfies the

$$Pr[M(D) \in S_m] \leqslant e^{\varepsilon} Pr[M(D^{'}) \in S_m] \tag{1}$$

Then the algorithm M satisfies differential privacy, where ε is the privacy protection budget.

For the definition of differential privacy, researchers are also fully mining, exploring and expanding. In [53], Pathak *et al.* proposed the large margin gaussian mixture models based on differential privacy. In their work, the greatest contribution is the large marginal loss function with perturbed regularities. In [54], Geng *et al.* discussed the optimal multidimensional setting mechanism in differential privacy, which improved the optimal mechanism while protecting privacy. In [55], Wang *et al.* analyzed the relationship between identifiability, mutual-information privacy and differential privacy. Inan *et al.* discussed the sensitivity analysis for non-interactive differential privacy. In [56], authors studied how to answer statistical range queries with batch mode accurately in privacy condition. For caching problem in IoT, Zhang *et al.* proposed a data-driven caching method for information-centric networks based on local differential privacy in [57]. In order to solve the multi-party data publishing, Cheng *et al.* proposed the multi-party publishing method for high-dimensional data in differential privacy [58]. In [59], Oneto *et al.* addressed randomized learning and generalization for private classifiers. Specially, authors considered the problem from PAC-Bayes to stability and imported the definition of differential privacy.

B. Progress and Development

At the same time, many methods extended by differential privacy are proposed. Of course, these developments are usually produced in the context of changes in information technology. For example, the popularity of the IoT puts forward new requirements for the privacy protection of sensor data, and the emerging research is constantly approaching this direction. In this survey, we summarize the relevant information and preliminary work, and summarize the development of differential privacy.

In [60], Xiao *et al.* tried differential privacy based on wavelet transforms and achieved better results. In [61], Fouad *et al.* proposed the supermodularity-based differential privacy method, which is valid on data anonymization. For individualdifferential privacy, Soria *et al.* proposed the utility-preserving formulation for differential privacy guarantees in [62].

In [63], Wang *et al.* developed the CTS-DP, which can be used for correlated time-series data publishing based on differential privacy. In [64], Goryczka *et al.* made comprehensive comparison on multiparty secure additions while implementing differential privacy. At the same time, Zhu *et al.* [65] solved the ADMM-based distributed classification learning based on dynamic differential privacy. In addition,

Cao *et al.* quantified the differential privacy for continuous data release with temporal correlations in [66].

In [67], Kalantari *et al.* achieved the robust privacy-utility tradeoffs with the combination of hamming distortion and differential privacy. In [68], Du *et al.* designed the training model for differential privacy under the condition of wireless big data and fog computing. In addition, Lu *et al.* proposed the releasing correlated trajectories in [69], which can be used with high utility and optimal differential privacy.

In [70], Zhang *et al.* proposed the correlated differential privacy and it is helpful for feature selection in machine learning. In [71], Brinkrolf *et al.* put forward the differential privacy method for learning vector quantization. In addition, Gong *et al.* made use of differential privacy for regression analysis based on relevance in [72], and Ke *et al.* proposed the AQ-DP in [73], which can be used as new differential privacy scheme designed for big data quasi-identifier classifying. Huang *et al.* put forward a method for logistic classification mechanism based on differential privacy [74].

In [75], Li *et al.* designed the secure metric learning method based on differential pairwise privacy. In [76], Katewa *et al.* conducted a survey on differential privacy in network identification.

C. Implementation Mechanisms

Implementing differential privacy is very important, and adding noise is the main technology to achieve differential privacy protection. As two common addition mechanisms, Laplace mechanism is suitable for numerical results, while exponential mechanism is suitable for non numerical results [77]. Some typical studies have also discussed the mechanism of noise addition.

In [78], Soria *et al.* proposed the optimal data-independent noise method for differential privacy implementation. For approximate differential privacy, Geng *et al.* discussed the related optimal noise adding method in [79]. In addition, Wang *et al.* analyzed the principal component for local differential privacy in [80]. From the perspective of engineering technology, the mainstream implementation schemes of differential privacy are generally classified into two types: laplace mechanism and index mechanism.

1) Laplace Mechanism: Given the data set D, the sensitivity of function $f : D \to R^d$ is defined as Δf, then the random algorithm $M(D) = f(D) + Y$ provides differential privacy protection. And $Y \to Lap(\Delta f/\varepsilon)$ is the random noise, which obeys the Laplace distribution with the scale parameter $\Delta f/\varepsilon$.

$$M(D) = f(D) + (Lap_1(\frac{\Delta f}{\varepsilon}), Lap_2(\frac{\Delta f}{\varepsilon}), ..., Lap_d(\frac{\Delta f}{\varepsilon}))^T \quad (2)$$

In [81], Li *et al.* discussed the optimal upper bound of the number of queries for Laplace mechanism under differential privacy.

2) Index Mechanism: The input of algorithm M is data set D, and the output is an entity object $r \in Range$, $q(D, r)$ is an availability function, Δq is the sensitivity of function $q(D, r)$. If the algorithm M is proportional to the probability of $exp(\frac{\varepsilon q(D,r)}{2\Delta q})$, all possible values can be normalized to get the corresponding probability value, then it can provide differential privacy protection.

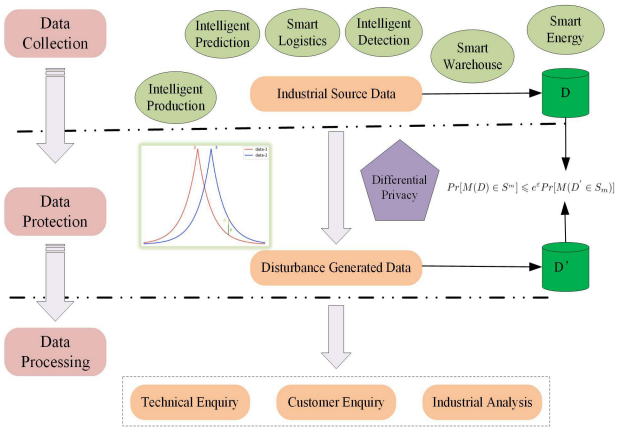

Fig. 2: Differential privacy in IIoT

D. Basic Properties

As far as differential privacy is concerned, it has many inherent properties, which can be used directly by algorithm designers.

For inherent properties, Geng *et al.* discussed in depth and improves the differential privacy mechanism by using the related properties. In [82] and [83], they achieved the optimal mechanism in differential privacy with help of multidimensional setting. In [84], authors also proposed the staircase mechanism for differential privacy.

After literature review, we summarize four properties of differential privacy as follows: sequential synthesis, parallel synthesis, transformation invariance, and convexity.

1) Sequential Synthesis: If a differential privacy algorithm is composed of several algorithms, the level of privacy protection of the composite algorithm is the total budget of all algorithms. And this property is conditionally for the same dataset.

2) Parallel Synthesis: Suppose there are algorithms $M_1, M_2, ..., M_n$, and the budget for privacy protection is $\varepsilon_1, \varepsilon_2, ..., \varepsilon_n$. Then, for disjoint dataset $D_1, D_2, ..., D_n$, the combination algorithm $M(M_1(D), M_2(D), ..., M_n(D))$ composed of these algorithms provides differential privacy protection.

3) Transformation Invariance: Given that any algorithm A_1 satisfies differential privacy, $A(\cdot) = A_2(A_1(\cdot))$ satisfies differential privacy for any algorithm A_2, where A_2 does not necessarily satisfy differential privacy.

4) Convexity: Given two algorithms A_1 and A_2, both of them satisfy differential privacy. For any probability $p \in [0, 1]$, the symbol A_p is used as a mechanism, which uses the probability of p to use algorithm A_1 and the probability of $1-p$ to use algorithm A_2, then mechanism A_p satisfies differential privacy.

Based on the above properties and definitions, differential privacy algorithm is constantly improved to meet the needs of IIoT environment. The demand of differential privacy of IIoT

is gradually rising, which has experienced the transformation from traditional IoT to IIoT [85].

IV. Metrics for Differential Privacy in IIoT

Differential privacy is an important tool for privacy protection in the field of data publishing, but its advantages and disadvantages can only be evaluated posteriorly, and it is highly dependent on the privacy budget of empirical choice.

Some previous researches have been done for privacy metrics. Chen *et al.* proposed an evaluation method on the risk of data disclosure under differential privacy and it is based on noise estimation [86]. Zhao *et al.* discussed the privacy metrics on vehicular communication technologies and authors compared 41 privacy metrics in terms of four novel criteria [87].

Traditional privacy algorithm evaluation relies on the quantization of probability. Specifically, subjective probability judgment is widely used. However, the IIoT under the background of big data puts forward dynamic requirements for privacy risk assessment [88]. In this survey, we summarize the current state of the art in privacy metrics for IIoT, especially differential privacy.

For privacy measurement, it mainly considers the choice of privacy protection technology and the professional background of attackers. In this way, privacy measurement originated from privacy anonymity technology [89]. When the risk of privacy disclosure in data is zero, the data achieves perfect privacy protection, which can achieve the maximum protection of privacy information. The data without any protection measures is regarded with the greatest risk of privacy information disclosure. Previous researches have proposed privacy measurement methods based on information entropy, set pair theory and differential privacy. The traditional privacy measurement methods mainly aim at small-scale and structured data stored in traditional relational databases [90].

In addition, there are also some methods for privacy measurement on cloud data. While cloud data are usually in industrial level, large-scale, multi-source, with multi-dimensional and unstructured mode. Therefore, compared with the traditional privacy protection measurement technology, the privacy measurement of cloud data should consider not only the privacy leakage measurement of small-scale and structured data, but also the privacy leakage measurement of large-scale and unstructured data.

This survey will focus on privacy protection principle, measurement effect and main advantages and disadvantages. Generally, we summarize the existing privacy measurement for differential privacy in IIoT.

A. Graph Theory and Mutual Information

Differential privacy quantification model based on graph theory and mutual information can be used for privacy leakage calculation method. Based on the distance regularization and point transfer of graph, the privacy disclosure mutual information quantification method can be used, and the information upper bound of differential privacy disclosure has been proved and calculated [26].

The analysis and comparisons have shown that the privacy disclosure upper bound has a good functional relationship with the number of attributes, attribute values and privacy budget parameters of the original data set. Graph theory and mutual information can provide theoretical support for the design and evaluation of differential privacy algorithms.

B. Information Entropy Measurement

Aiming at the problem of composite data set with non interactive multi-attribute based on differential privacy, the information entropy measurement can be used to build assessment method for privacy degree, data utility and privacy leakage risk.

In principle, mutual information is used to analyze the attribute correlation, and the relational dependency graph model is used to express the attribute [91]. Based on the key privacy leakage paths in the graph, Markov privacy disclosure chain is constructed, and an associated attribute privacy measurement model and method can be proposed based on information entropy, which can effectively measure the amount of privacy leakage caused by associated attributes [92].

C. Utility Optimization with Rate Distortion

The solution of the contradiction between privacy protection and data utility is a research hotspot in the field of privacy protection, which will be discussed in Section V. Aiming at the problem of privacy and utility balance in the off-line data publishing scenario of differential privacy, the optimal differential privacy mechanism to balance privacy and data utility is studied by using rate distortion theory [26]. Based on the communication theory, such method abstracts the noise channel model of differential privacy, measures the privacy and utility of data publishing by mutual information and distortion function, and constructs the optimization model based on rate distortion theory [86].

V. Conflicts: Differential Privacy and Deep Models

In the application of IIoT, AI methods driven by deep learning are playing an important role. The performance of deep models strongly depends on the data size and data quality. Meanwhile, the widespread use of data brings the risk of privacy disclosure. Therefore, the contradiction between the two is often concerned by researchers. In order to establish a more stable and secure IIoT, it is necessary to consider how to improve data availability and fully protect privacy. Ha *et al.* conducted a survey paper on differential privacy in deep learning, which discussed the conflicts between privacy protection and deep models [93].

A. Relationship between Differential Privacy and Deep Learning

The primary task of deep learning is data training and test. However, in the process of data collection, privacy disclosure will occur, which is not conducive to the development of AI.

It is well known that three changes have driven the great success of deep learning in various fields: (1) Exponential increase of data volume: in the implementation of IIoT, it will be more convenient to collect data and establish certain scale of dataset for deep learning algorithm. (2) Breakthrough in computing power: The increasing computing hardware such as GPU clusters makes it available for deep learning in IIoT. (3) Algorithm breakthrough: algorithm breakthrough for IIoT promotes AI technology maturity and practicality in industry.

Although deep learning brings great benefits, there is a need to collect a large number of data, which involves the industrial privacy information. The leakage of these privacy data will lead to unpredictable problems for industrial operators. In view of this problem, many scholars have carried on thorough research.

Xu *et al.* proposed the GANobfuscator, which can deal with the mitigating information leakage while using generative adversarial networks (GAN) based on Differential Privacy [94] . In addition, Zhu *et al.* made a discussion on differential privacy in AI, especially on multi-agent systems, reinforcement learning, and knowledge transfer [92].

B. Attack Types in Industrial Deep Learning Model

In [95], Chen *et al.* proposed the RNN-DP, which can be used as a differential privacy scheme base on recurrent neural network (RNN). Based on this scheme, we can achieve dynamic trajectory privacy protection.

In [96], Gong *et al.* put forward the differential privacy based on adaptive noise imposition, which can be used for general deep neural networks.

It is necessary to summarize current attach types in deep learning, especially in IIoT. Generally, we can classify it into adversarial attacks and cooperative attacks.

1) Adversarial Attacks: In the field of machine learning, the deep model used for classification is usually easily affected by the adverse examples. At the same time, the learning model components have linear characteristics. In this context, attackers can construct adverse examples to achieve the purpose of attack.

2) Cooperative Attacks: In deep learning, the training set with large amount of data can get more accurate prediction model. However, data sets are usually unbalanced. In order to solve this problem, cooperation and complementarity is a common method. Different data providers expand the training set by sharing data. In this context, individual data providers will shield their private data, which will bring the disadvantage of data closeness.

C. Federated Learning

Federated learning is a popular privacy protection model in deep learning, and its performance is also worthy of attention. It is quite different from the privacy protection theories commonly used in big data and data mining, such as K anonymity and L diversity. Federated learning protects user data privacy through parameter exchange under special mechanism with homomorphic encryption. In this way, the data and model in federated learning will not be transmitted, so there is no possibility of leakage at the data level, and it does not violate more stringent data protection laws.

Wei *et al.* proposed the NbAFL, which can be regarded as a framework on federated learning with differential privacy [97]. Authors added artificial noises to the parameters at the clients side before aggregating. In [98], Nuria *et al.* discussed the federated learning in differential privacy in view of software tools analysis. In addition, Hu *et al.* also put forward a method on personalized federated learning with differential privacy [99].

The methods based on differential privacy commonly add noise to the data, or use generalization method to blur some sensitive attributes until the third party can not distinguish individuals, so that the data can not be restored with high probability, so as to protect privacy. However, in essence, these methods still carry out the transmission of original data, and there is a potential possibility of being attacked, and under the more stringent data protection schemes. Correspondingly, federated learning is a more powerful solution.

In addition, Lu *et al.* put forward the differentially private asynchronous federated learning towards mobile edge computing in urban environment [100], and Hao *et al.* proposed the efficient and privacy-enhanced federated learning for IIoT based on AI [101].

D. Final Balance

The balance between differential privacy and deep learning model is very important. It mainly protects privacy in training and testing stages. In general, the defender can introduce noise for differential privacy, but it will reduce the accuracy of the model. How to balance the two has become a hot topic in academia.

Sarwate *et al.* conducted a review paper on machine learning and differential privacy in the view of signal processing, especially for continuous data [102]. Authors discussed the topic on algorithms design and current challenges. Wang *et al.* proposed the DNN-DP which can be used for sensitive crowdsourcing data, considering the balance between differential privacy and deep neural network [103]. Zheng *et al.* discussed the balance problem between local differential privacy and federated machine learning [104].

VI. Applications of Differential Privacy in IIoT

Traditional industrial network modes are unable to meet the requirements of modern industry in terms of computing power, interaction speed, data analysis and so on. After years of development, the concept of new IIoT has been widely understood and accepted by industry. It is worth discussing what improvements differential privacy have been made to industrial scenarios.

Generally, the core elements of IIoT contain intelligent machine, advanced analytic and human-machine interaction. In this survey, we summarize the application scenarios in following aspects: industrial logistics system, smart grid, industrial bioengineering, industrial unmanned aerial vehicle, intelligent manufacturing, intelligent manufacturing, industrial blockchain and industrial social network. And the whole review flow can be found in Fig. 3.

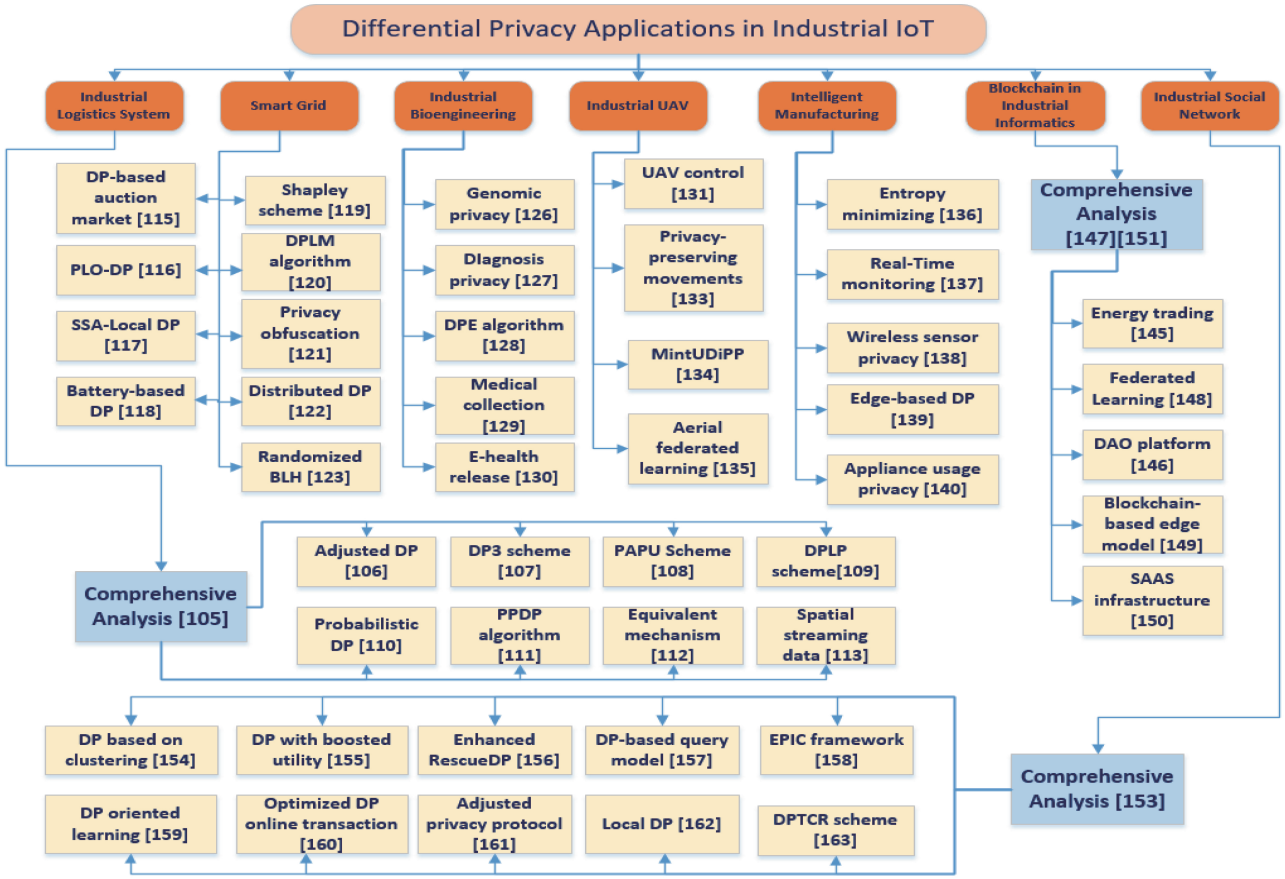

Fig. 3: Industrial application scenarios based on differential privacy

TABLE IV: Differential privacy for industrial logistics system

Ref	Year	Privacy Technology	Problem Solved	Criterion	Contributions
[105]	2019	Comprehensive survey	Location privacy	Diversification	Provide an up-to-date vision on location privacy Organise LPPMs into three use cases
[106]	2018	Adjusted differential privacy	Location privacy	ε-differential privacy	LPT for representing location data DP-k model Extensive experiments on real-world datasets
[107]	2018	DP3 scheme	Privacy-preserving indoor localization	ε-differential privacy	Balance the trade-off between data privacy and data utility Online real-time operating phase
[108]	2020	PAPU for differential privacy	Protecting vehicles¡¯ trajectory privacy	ε-differential privacy	Pseudonym swap process based on differential privacy New pseudonym swap mechanism Guarantee the unlinkability
[109]	2019	DPLP scheme	Location protection in spatial crowdsourcing	ε-differential privacy	Novel DP-based location protection ε_1-ATGD and ε_2-DPACPG
[110]	2018	Probabilistic differential privacy	Location recommendations	(ε, σ)-differential privacy	Investigate fine-grained location recommendations Lower bound of the variety of aggregate statistics Extensive experiments on accuracy, privacy and efficiency
[111]	2020	PPDP algorithm	Transit card data privacy	ε-differential privacy	New prefix tree structure Incremental privacy allocation mechanism Spatial-temporal domain reduction model
[112]	2019	Equivalent mechanism	Releasing location data	(ε, σ)-differential privacy	Determine location errors on indistinguishability Equivalent mechanism to enforce differential privacy
[113]	2018	Spatial streaming data with differential privacy	Trajectory privacy protection	(ω, n)-differential privacy	Flexible trajectory privacy model of w-event n2-block Spatial temporal budget distribution (STBD) algorithm

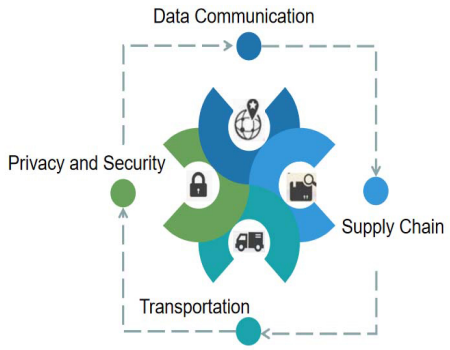

Fig. 4: Industrial logistics

A. Industrial Logistics System

Industrial logistics is the guarantee of timely and effective transportation system, which can help improve the efficiency of industrial production. Generally, industrial logistics system has four pillars: IT security and privacy, communication system, supply chain monitoring and transportation tracking, as shown in Fig. 4. It is difficult to migrate between customers with different industry attributes, so industrial logistics focuses on matching autonomous mobile robot (AMR) technology with user value, and realizes intelligent enabling in complex environment.

In terms of longer development cycle, industrial logistics has changed from automation to intelligence, and the protection of logistics privacy data is highlighted [114]. Specially, differential privacy is worthy of attention. We summarized the important existing papers in Table IV.

In the beginning, some research results focus on the privacy protection of logistics or location, instead of particular differential privacy. Primault *et al.* proposed a survey on computational location privacy, and authors focused on privacy threats in common IoT scenarios [105]. It can be concluded that many essential contents of IIoT scenarios are the same as traditional ones. Yin *et al.* studied this problem in the context of big data of IIoT, especially in low density of location data with high value. Authors built the multilevel location information tree model [106].

Some research results focus on the direct use of differential privacy. Wang *et al.* proposed the DP3 for privacy-preserving indoor localization mechanism based on differential privacy [107]. Li *et al.* built the PAPU (Pseudonym Swap with Provable Unlinkability) for VANETs (Wireless communication technology, vehicle ad hoc networks) based on differential privacy [108]. Wei *et al.* focused the location protection in spatial crowdsourcing under the help of differential privacy [109]. Zhang *et al.* proposed a method for location recommendations protection based on enabling probabilistic differential privacy [110]. Li *et al.* solved the smart card data transiting with privacy-preserving data publishing algorithm based on differential privacy [111]. Wang *et al.* proposed the equivalent mechanism, which can be used for releasing location data based on differential privacy [112]. Liu *et al.* achieved trajectory privacy protection designed for spatial streaming data under the help of differential privacy [113].

In addition to cloud and analysis, the IIoT is the driving force connecting the logistics field, and freight monitoring is one of the leading application scenarios. In industrial transportation system, logistics planning and location information involve data privacy.

B. Smart Grid

In order to achieve smart city [124], smart grid is the most important foundation. With the wide application of smart devices in smart grid, the relationship between power users and providers has become more and more close. This two-way interaction ensures the real-time transmission of power consumption data. At the same time, the privacy problems of users are increasingly obvious, the privacy information leakage of power users is closely related to everyone, especially the performance, which is the limiting factor for the further development of smart grid. Therefore, it is of great significance to carry out the research on the privacy protection of power users in smart grid.

For the privacy issues of smart grid under the help of differential privacy, we summarized the important existing papers in Table V.

Li *et al.* proposed the online double auction method for smart grid based on differential privacy [115]. Fioretto *et al.* discussed the application of differential privacy in power grid obfuscation and proposed the Power Line Obfuscation(PLO) [116]. Ou *et al.* made a detailed singular spectrum analysis on smart grid classifications based on local differential privacy [117] . Zhang *et al.* exploited the dual roles of noise and made use of cost-friendly differential privacy on smart meters [118]. Lou *et al.* discussed the cost and pricing of differential privacy under demand reporting for smart grids [119]. Hassan *et al.* proposed the renewable energy resources based smart metering based on differential privacy [120]. Mak *et al.* put forward the distributed power systems based on privacy-preserving obfuscation [121]. Wang *et al.* designed a method to achieve data-driven optimization for utility providers based on differential privacy [122]. Zhao *et al.* achieved data disclosure in smart grid based on differential privacy [123].

C. Industrial Bioengineering

In recent years, the industrial development of bioengineering has also attracted much attention, and the protection of personal sensitive data such as biometrics is extremely important, as shown in Fig. 5. Therefore, many researchers have begun to focus on the privacy protection of bio sensitive data, so as to lay the foundation for the further development of bio industry.

With the development of computer, optics, acoustics, biosensor and biostatistics, it is more and more common to use the inherent physiological characteristics of human body, such as fingerprint, face, iris, and behavioral characteristics, such as handwriting, voice, gait, etc. Fingerprint recognition and face recognition are the most widely used. And privacy

TABLE V: Differential privacy for power and energy: smart grid

Ref	Year	Privacy Technology	Problem Solved	Criterion	Contributions
[115]	2019	DP-based auction market	Island MicroGrids	(ε, σ)-differential privacy	Novel online double auction scheme Two-phase differential privacy Extensive performance evaluation
[116]	2020	PLO-differential privacy	Power grid obfuscation	ε-differential privacy	Power Line Obfuscation (PLO) mechanism Strong theoretical properties Handle time-series network data
[117]	2020	SSA-Local differential privacy	Prevent inferring household appliance classification	ε-differential privacy	Singular spectrum analysis Fourier spectral noise Detailed theoretical analysis
[118]	2017	Battery-based differential privacy	Achieve DP and cost saving simultaneously	(ε, σ)-differential privacy	Battery-based DP-preserving Cost-friendly DP-preserving schemes Detailed theoretical analysis
[119]	2020	Shapley cost sharing scheme	Demand reporting for smart grids	ε-differential privacy	Apply the principle of Shapley value Analytic expression for the total privacy cost Demand reporting scheme
[120]	2019	DPLM algorithm	Renewable energy resources	ε-differential privacy	Preserve privacy of RERs integrated smart meter users Preserve information about intermittent availability Develop an algorithm for monthly accumulation
[121]	2020	Privacy-preserving obfuscation	Distributed power systems	ε-differential privacy	Novel and distributed PD-OPF mechanism Experiments on large collection of OPF benchmarks
[122]	2018	Distributed differential privacy	Achieve DP and cost saving simultaneously	(ε, σ)-differential privacy	Datadriven differential privacy Formulate the cost minimization problem into a RASP
[123]	2014	Randomized BLH and Multitasking-BLH-Exp3	Prevent inferring household appliance information	(ε, σ)-differential privacy	Investigate the privacy issues of the smart meters Utilize Exp3 algorithm for MAB

protection in this process is also very important [125]. We summarized the important existing papers in Table VI.

Raisaro *et al.* discussed the protecting privacy for genomic data in i2b2 (Informatics for Integrating Biology and the Bedside) under help of homomorphic encryption and differential privacy [126]. Liu *et al.* proposed a method for coronary heart disease diagnosis in mobile edge computing based on blockchain-enabled contextual online learning [127]. Wei *et al.* made use of differential privacy to achieve genetic matching for personalized medicine [128]. Wang *et al.* put forward a method for secure medical data collection based on local differential privacy [129]. Li *et al.* explored the efficient e-health data release based on differential privacy with consistency guarantee [130].

D. Industrial Unmanned Aerial Vehicle

UAV control technology also occupies an important position in IIoT [131], [132]. In some industrial scenarios, UAV data acquisition and user privacy are difficult to separate. Therefore, it is necessary to focus on how to protect UAV data protection methods in the IIoT, and differential privacy also contributes to this direction. We summarized the important existing papers in Table VII.

Kim *et al.* explored the differential privacy-preserving movements issues for UAV [133]. And they also proposed the UDiPP as a whole framework for DP-privacy preserving movements of UAV in the background of smart cities [134]. In addition, Wang *et al.* put forward a method for aerial secure federated learning, which can be used for UAV-assisted crowdsensing [135].

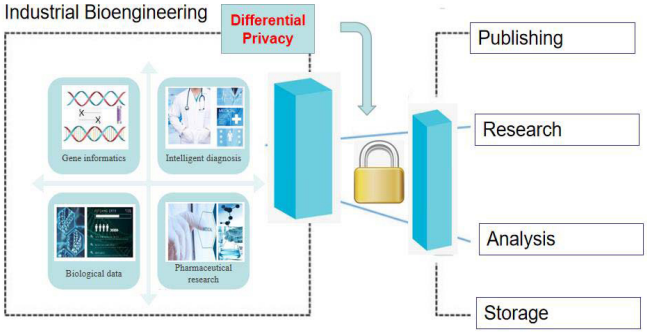

Fig. 5: Differential privacy for bioengineering

E. Industry 4.0: Intelligent Manufacturing

Intelligent manufacturing (IM) is a man-machine integrated intelligent system composed of intelligent machines and human experts. It can carry out intelligent activities in the manufacturing process, such as analysis, reasoning, judgment, conception and decision-making, as shown in Fig. 6. Through the cooperation of human and intelligent machines, we can expand, extend and partially replace the mental work of human experts in the manufacturing process. It updates the concept of manufacturing automation and extends it to flexible, intelligent and highly integrated.

In fact, the privacy protection of industrial data is also very important. For example, the AGV (Automated Guided Vehicle) used in factory warehouse automation usually uses industrial WiFi for communication, and data leaks in this process are very common. Therefore, more and more researchers begin to discuss how to use differential privacy in intelligent manufac-

TABLE VI: Differential privacy for bioengineering

Ref	Year	Privacy Technology	Problem Solved	Criterion	Contributions
[126]	2018	Combine DP and homomorphic encryption	Genomic data privacy	ε-differential privacy	Advanced privacy-enhancing technologies Build system by most widespread framework
[127]	2020	Local differential privacy	Coronary heart disease diagnosis	ε-differential privacy	Novel context-aware online learning algorithm Adaptively expanding tree structure Adopt the local DP method
[128]	2020	DPE algorithm with DPNM	Genetic matching in personalized medicine	ε-differential privacy	DP-based genetic matching (DPGM) DP-based EIGENSTRAT (DPE) algorithm DP-based Norder Markov (DPNM) algorithm
[129]	2018	Local differential privacy	Secure medical data collection	ε-differential privacy	Secure medical data collection framework Apply framework on synthetic data
[130]	2015	Consistency guarantee under DP	E-health data release	$\varepsilon_1/\varepsilon_2$-differential privacy	Design a new private partition algorithm Apply constrained inference in post-processing stage

TABLE VII: Differential privacy for industrial UAV

Ref	Year	Privacy Technology	Problem Solved	Criterion	Contributions
[133]	2017	Privacy-preserving UAV framework	Minimizing movements of UAVs	-	Provide privacy-preserving movements of UAVs New UDiPP graph model
[134]	2019	UDiPP	privacy for UAV in Smart Cities	ε-differential privacy	Support privacy preserving UAV movement strategies Define a MintUDiPP problem Creation of UDiPP graph
[135]	2020	Aerial secure federated learning	UAV-assisted crowdsensing	ε-differential privacy	Proposed SFAC as federated learning Investigate a consortium blockchain network Evaluated via extensive simulations

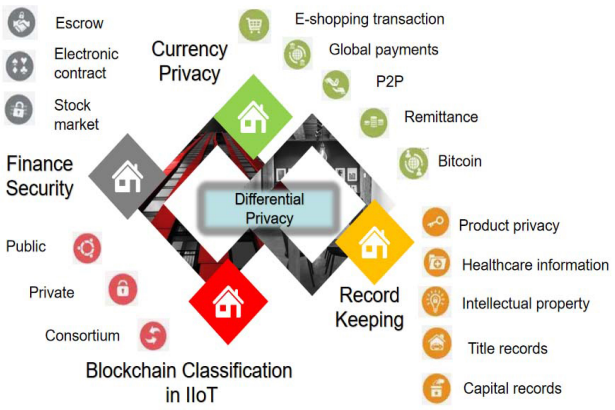

Fig. 6: Differential privacy for IIoT blockchain

turing. We summarized the important existing papers in Table VIII.

Zhu *et al.* discussed the differential privacy for linear distributed control systems, which can be used for entropy minimizing mechanisms with performance tradeoffs [136]. Fan *et al.* proposed an adaptive approach to realize the real-time aggregate monitoring based on adjusted differential privacy [137]. For sensor system, Chakraborty *et al.* explored the temporal differential privacy for industrial wireless sensor networks [138]. And Tian *et al.* put forward edge-based differential privacy computing method for industrial sensor-cloud systems [139]. In addition, Barbosa *et al.* proposed the technique to provide differential privacy for appliance usage in smart metering, which can be used for industrial intelligent privacy [140].

F. Blockchain in Industrial Informatics

IIoT has profoundly changed the mode of production, organization and business model of traditional industries. Traditional technology has been unable to meet the needs of the future IIoT, but the blockchain technology provides trust, transparency and security communication guarantee for the IIoT with the characteristics of decentralization, openness, transparency and unforgeability [141]. For more basic content, Dai *et al.* made a comprehensive survey on blockchain for IoT [142].

Blockchain technology can provide point-to-point direct interconnection for the IIoT to transmit data, rather than through the CPU, so that distributed computing can handle hundreds of millions of transactions. At the same time, it can also make full use of the computing power, storage capacity and bandwidth of hundreds of millions of idle equipment distributed in different locations for transaction processing and greatly reduce the cost of calculation and storage [143]. The security of blockchain in IIOT is more critical, and it puts forward new requirements for privacy protection technology. Blockchain technology superimposed with smart contract can turn each intelligent device into an independent network node that can maintain and adjust itself [144]. These nodes can exchange information with other nodes or verify their identity on the basis of pre-defined or embedded rules. We summarized the important existing papers in Table IX.

Gai *et al.* designed a framework for privacy-preserving consortium blockchain for energy trading , and it can help keep privacy in industrial smart grid [145]. In addition, Yao *et al.* proposed the method for resource trading in blockchain which can be used for IIoT [146]. The above papers focused on blockchain in IoT or IIoT, and there are also some researches focusing on differential privacy in blockchain directly.

TABLE VIII: Differential privacy for intelligent manufacturing

Ref	Year	Privacy Technology	Problem Solved	Criterion	Contributions
[136]	2017	Entropy minimizing mechanisms for DP	Linear distributed control systems	ε-differential privacy	Differential privacy of agents' preference vectors Achieve DP by adding noise to shared information
[137]	2014	Adaptive approach based on DP	Real-time aggregate monitoring	ε-differential privacy	Establish the state-space model for the time series Sample the time series data as needed Formal analysis on filtering with fixed-rate sampling
[138]	2020	Temporal differential privacy	Wireless sensor networks	ε-differential privacy	Temporal DP preserving mechanism Time of occurrence is made indistinguishable
[139]	2020	Edge-based differential privacy computing	Sensor-cloud systems	ε-differential privacy	Three-layer storage architecture Research on the characteristics of raw data
[140]	2016	Lightweight approach based on DP	Appliance usage in smart metering	ε-differential privacy	Measure privacy achieved by appliances Evaluate attack to eliminate noise

Hassan *et al.* made a detailed survey for differential privacy in blockchain technology, and it conducted the review with a futuristic perspective [147]. For subtopics, Lu *et al.* put forward a method based on blockchain with federated learning, which can be used for privacy-preserved data sharing in IIoT [148]. Gai *et al.* discussed the differential privacy-based blockchain technology for IIoT [149]. Roy *et al.* proposed the blockchain-enabled safety-as-a-service for industrial IoT applications [150].

G. Industrial Social Network

The social network model is also applicable in industrial IOT. In industrial IOT sensing, the information collected by each sensor can be regarded as personal information release of social network terminal. Privacy data is related to the quality of a production system.

In fact, social networks in industrial environments involve more production information and commercial information, and their privacy protection needs are more prominent than those of traditional social networks [152].

The original intention of differential privacy is to protect the sensitive information of data release, which can be directly applied to the information collection of industrial IoT sensor, and help the industrial system to control the macro data such as production quality and product stability. We summarized the important existing papers in Table X.

Abawajy *et al.* conducted the survey on data publication method for privacy preserving social network [153]. And Huang *et al.* put forward the privacy-preserving approach PBCN for social network based on differential privacy [154]. In [155], Hong *et al.* designed the collaborative search log sanitization under help of differential privacy and boosted utility. Wang *et al.* proposed method for protection crowd-sourced social network data by enhanced RescueDP, especially for the real-time and spatio-temporal data [156]. Du *et al.* put forward the query model designed for sustainable fog data under the help of differential privacy [157]. Liu *et al.* defined the EPIC as a Framework to weaken the Internet traffic analysis, which is also under help of differential privacy [158]. And Wei *et al.* focused on mobile social video prefetching based on DP-oriented distributed online learning [159]. In addition, Lin *et al.* tried to protect user's shopping preference based on differential privacy and it can help protect the social trading privacy [160]. Chamikara *et al.* explored the related methods for privacy preserving face recognition by differential privacy [161]. Liu *et al.* discussed the social network publishing based on local differential privacy [162] and Wei *et al.* focused the differential privacy application in social network on trajectory community recommendation [163].

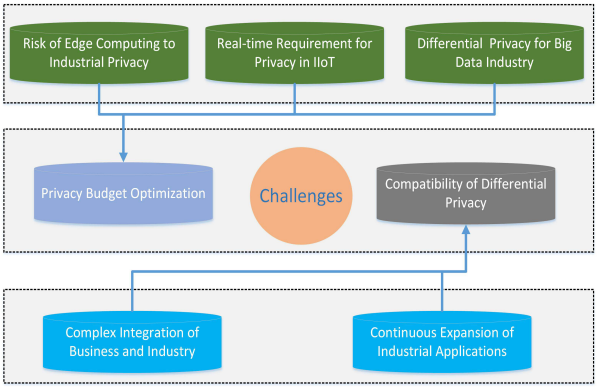

Fig. 7: Current challenges for DP in IIoT

VII. Challenges of Differential Privacy in IIoT

At present, the development of differential privacy is still in a dynamic process, especially in the field of IIoT. In this survey, we summarize seven different problems in Fig. 7, which are urgent and meaningful. Specially, it contains the compatibility of differential privacy for industry, complex integration of business and industry, differential privacy for big data industry, risk of edge computing to industrial privacy, real-time requirement for privacy in IIoT, privacy budget optimization for privacy in IIoT and continuous expansion of industrial applications.

A. Compatibility of Differential Privacy for Industry

In initial stage, differential privacy algorithm is designed for data publishing. Therefore, it has ushered an explosive development in the field of social and personal privacy information. However, the types of industrial data and social information vary greatly, and the implementation means are different [19], [164].

In this background, direct migration of differential privacy algorithm to industrial data will encounter a variety of complex contradictions [24]. In the past, researchers usually directly

TABLE IX: Differential privacy for industrial blockchain

Ref	Year	Privacy Technology	Problem Solved	Criterion	Contributions
[151]	2019	Comprehensive survey	Blockchain privacy for IoT	Diversification	Brief introduction on IoT and blockchain Convergence of blockchain and IoT Blockchain for 5G-beyond networks in IoT
[145]	2019	Privacy-preserving consortium blockchain	Energy trading	ε-differential privacy	Hide the trading distribution trends Design mechanism to introduce dummy accounts
[148]	2020	Blockchain and federated learning	Data sharing in Industrial IoT	ε-differential privacy	Transform data sharing into machine learning problem New blockchain empowered collaborative architecture Integrate differential privacy into federated learning
[146]	2019	IIoT DAO platform	Resource trading in blockchain for IIoT	-	Use blockchain to construct decentralized trading platform Model interaction between cloud provider and miners
[149]	2020	Blockchain-based Internet of edge model	Scalable and controllable IoT system	ε-differential privacy	Integrates IoT with edge computing and blockchain Prevent data mining-based attacks
[147]	2020	From futuristic perspective	DP in blockchain technology	Diversification	Provide importance of DP in blockchain Presented future research directions
[150]	2020	Safety-as-a-service infrastructure	Prior intimation for safety-related information	-	Blockchain integration into the Safe-aaS Overall throughput follows an increasing trend

migrate the differential privacy algorithm, which led to poor results. Therefore, how to properly migrate and use differential privacy algorithm in industrial IoT is always one of the most important challenges.

B. Complex Integration of Business and Industry

The combination of business and industry brings more sensitive privacy data to industrial field. And IIoT systems are also built based on integration of information technology and business process. For example, Mottola *et al.* conducted research on simplifying the integration of wireless sensor networks into business processes [165]. And Culot *et al.* [166] explored the the integration and scale in the context of industry 4.0.

In addition, how to manage the balance between production and orders is an important problem for operators. In order to solve it, more user data should be collected and used, which leads to more privacy threats. Therefore, how to solve the privacy problem of IIoT under the commercial background has become a new problem.

C. Differential Privacy for Big Data Industry

Industrial big data is a series of technologies and methods to excavate and display the value of data planning, collection, preprocessing, storage, analysis, mining, visualization and intelligent control [167]. The essential goal of the research and breakthrough of industrial big data technology is to discover new patterns and knowledge from complex data sets, and to obtain valuable new information, so as to promote product innovation of manufacturing [168]. Big data means big risk. In industrial environment, the use of big data is diverse, and the data sources are complex. So leakage risk of private data may be enhanced. Therefore, the application difficulty of differential privacy in this field is also obvious.

In this field, Zhou *et al.* discussed the multimedia big data retrieval based on edge computing under the differentially-private and trustworthy framework [169] . However, the challenge of increasing the amount of data is very obvious. In addition, D'Alconzo *et al.* [170] conducted a survey on big data for network traffic monitoring and analysis, which also mentioned the privacy challenges brought by big data.

D. Risk of Edge Computing to Industrial Privacy

Industrial applications require more and more timely model updating. Due to the protection of sensitive data, some industrial operators such as factories are not willing to share data to the cloud. As a solution, edge training plays a important role. In this way, what challenges need to be solved in order to achieve edge training and how can cloud edge work together better has been the focus of the industrial IoT.

For edge training in IIoT, some nodes provide data, and others are server nodes for training. So how to take differential privacy in this processing and how to divide the roles between nodes with suitable communication protocol are all the discussions under way. In order to solve this problem, Feng *et al.* proposed the privacy preserving high-order Bilanczos in fog computing, which is particularly designed for industrial applications [171]. In addition, Usman *et al.* defined the RaSEC, which is an intelligent framework for reliable multi-level edge computing in industrial environments [172].

E. Real-time Requirement for Privacy in IIoT

The industrial field has high requirements for real-time and cooperative work with almost zero tolerance for delay. Langrica *et al.* explored the real-time fault diagnosis in industrial motors, which require fast computing IIoT [173]. Real time not only requires real-time computing, but also real-time data transmission. Parizad *et al.* discussed the power system real-time emulation, and proposed a practical virtual instrumentation [174].

In addition, industry is often a system rather than a single node running, requires the cooperation between the nodes. It is inevitable to transmit and share data. Within a certain delay range, data can be guaranteed to arrive from one node to another, which is also the embodiment of real-time. In this way, differential privacy algorithm design under real-time transmission is also big problem for IIoT.

TABLE X: Differential privacy for industrial social network

Ref	Year	Privacy Technology	Problem Solved	Criterion	Contributions
[153]	2016	Comprehensive survey	Social network data publication	Diversification	High level social network threat analysis Categorize a spectrum of adversarial knowledge Graph structural-based privacy attack models
[154]	2020	DP based on clustering and noise	Social network privacy	ε-differential privacy	PBCN framework Privacy measure by adjacency degree Data sets with different sizes
[155]	2015	Differential privacy with boosted utility	Collaborative search log sanitization	(ε, σ)-differential privacy	Address deficiency by presenting sanitization Prove differential privacy and protocol security for CELS
[156]	2018	Enhanced RescueDP	Crowd-sourced social network data	ε-differential privacy with w-event	Proposed RescueDP Enhanced RescueDP scheme Evaluate method with real-world and synthetic datasets
[157]	2019	Differential privacy-based query model	Sustainable fog data centers	(ε, σ)-differential privacy	Differential privacy-based query model New query model for fog computing QMA based on differential privacy
[158]	2018	EPIC: A Differential Privacy Framework	Preventing Internet traffic analysis	εd_x-differential privacy	DP mechanism for the selection of proxy gateways DRW scheme for data transmissions Simulations based on the real community topology
[159]	2019	DP oriented distributed online learning	Mobile social video prefetching	ε-differential privacy	Investigate relationship of user playback and demand Provide the privacy attacking model Conduct a series simulation tests
[160]	2020	Optimized differential private online transaction	Protecting shopping preference	(ε, σ)-differential privacy	Protect consumption privacy in online banks The RO-DIOR scheme The privacy loss is less than 0.5
[161]	2020	Adjusted privacy-preserving protocol	Privacy preserving face recognition	ε-differential privacy	Privacy using eigenface perturbation Towards controlled information release
[162]	2020	Local differential privacy	Social network publishing	ε-differential privacy	DP-LUSN Implementation method for DP-LUSN Evaluate on three real-life social network datasets
[163]	2019	DPTCR scheme	Trajectory community recommendation in social network	ε-differential privacy	Novel DP-based trajectory community recommendation Semantic expectation-based location transition algorithm

F. Privacy Budget Optimization for Privacy in IIoT

For IIoT, differential privacy aims to strike a balance between data and privacy, but it is not the end of the privacy puzzle. Differential privacy relies privacy budget to adjust the privacy degree in system, which plays a decisive role in the effectiveness of privacy protection. In [175], Zhao *et al.* designed a budget-feasible incentive mechanisms for crowdsourcing tasks. And Han *et al.* proposed another differentially private mechanisms, which is also for budget limited mobile crowdsourcing [176].

In this field, how to define the rationality of privacy budget and how to control such privacy budget are still at the stage of research and exploration. At the same time, many differential privacy algorithms used to generate noisy data depend on the industrial data to reach a certain size and meet a certain distribution, which may be difficult to meet in some specific IIoT scenarios. Especially when the added noise is too large, many application scenarios that provide personalized services based on personal information will encounter great challenges.

G. Continuous Expansion of Industrial Applications

At present, the achieved applications of IIoT mainly focus on intelligent industrial manufacturing, electric energy, automobile transportation, smart city and smart logistics. With the continuous enrichment of industrial types, ways for realizing of IIoT are expanding. So the requirements for privacy protection are also rising. In [27], authors emphasized this problem.

In addition, the rapid development of AI has brought many new challenges to differential privacy, and the intelligent attack and defense technology in this area is becoming one of the most urgent research hotspots. Moren *et al.* discussed the new type of IIoT, which can be defined as growth through franchises in kowledge-intensive industries [177]. These emerging IIoT Applications are bringing new challenges to differential privacy.

VIII. Future Open Issues

One of the main objectives in this survey is to propose more open ideas for research about differential privacy in IIoT. Based on the analysis of the Section VII, several challenging problems have been summarized, and the hot directions are clear. Here we put forward seven valuable subtopics in this field and discuss the feasibility of the related research one by one, as summarized in Fig. 8.

A. Big Data IIoT System with Robust Differential Privacy

Industrial big data refers to the data generated in the application of informatization. With the deep integration of informatization and industrialization, information technology has penetrated into all aspects of the industrial chain of industry, such as QRC (Quick Response Code), RFID (Radio Frequency Identification), ERP (Enterprise Resource Planning) and so on. The expansion of data also provides a sufficient

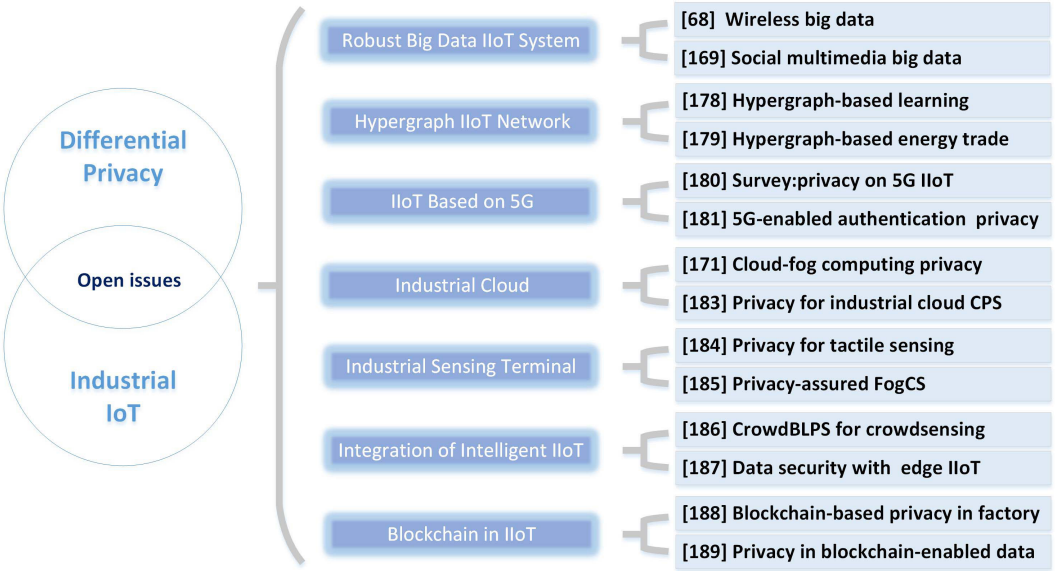

Fig. 8: Future open issues for DP in IIoT

basis for AI algorithm, so as to launch more intelligent IIoT products. In this way, it will be very valuable to study the differential privacy of industrial big data, especially based on differential privacy.

In this direction, some preliminary research results have been reported. Du *et al.* explored the differential privacy preserving of training model under the background of wireless big data [68]. And Zhou *et al.* focused on online social multimedia big data for privacy-preserving method [169].

B. Differential Privacy for Hypergraph IIoT Network

At present, the existing IIoT information interaction technology has shortcomings in solving the problem of intelligent interaction, which is mainly manifested in failing to reflect the multidimensional, dynamic and complex network interaction relationship between IIoT entities, which can not meet the requirements of intelligent interaction. According to the data characteristics of multidimensional dynamic mesh between entities, hypergraph theory can construct an entity relationship network model of IIoT.

In this context, it is necessary to propose more differential privacy algorithms for hypergraph IIoT network and achieve more valid protection for complex IIoT network. Although the problem has not been solved completely, some preliminary studies have been developed. Wang *et al.* proposed a directed hypergraph-based learning scheme based on security enhanced content sharing in social IoT [178]. In addition, Karumba *et al.* defined the HARB, which can be regarded as hypergraph-based adaptive consortium blockchain for decentralised energy trading [179].

C. Differential Privacy of IIoT Based on 5G Communication

In traditional communication technology, the main body of communication services is humans. For 5G Communication, situation will change. It has been demonstrated that main users of communication services will gradually migrate from human to things, and the proportion will be higher and higher. For IIoT, more industrial equipments can independently use communication tools to exchange information.

Because of this fundamental change, 5G will give birth to countless new fields, trigger a new round of industrial transformation, and become a new driver to promote IIoT development. In this background, the role of differential privacy is more important. It will provide a solid guarantee for the protection of equipment data privacy and keep maintain the safe operation of industrial systems. The combination of differential privacy and new wireless communication technology will become a new research hotspot. For example, Khan *et al.* conducted a comprehensive survey on security and privacy of 5G [180]. And Zhang *et al.* proposed the edge computing-based authentication framework considering privacy-preserving 5G-enabled vehicular networks [181].

D. New Differential Privacy for Industrial Cloud Data

How to keep cloud data privacy without leaking has become the main problem faced by the development of cloud computing, especially for IIoT. It is particularly important to establish a set of security mode based on heterogeneous data, which can ensure data privacy in the system and application at the same time.

Edge computing and fog computing are often used interchangeably because they both involve pushing intelligence and processing power [182]. While there are clear differences between how and why to deploy which type of infrastructure, both are critical to a successful IIoT strategy. In order to enable the future of IIoT, it is necessary to adopt the next generation solution including edge computing and fog computing in privacy, so as to expand the devices, networks and applications. In [171], Feng *et al.* discussed the privacy preserving problem in cloud-fog computing for industrial applications. And Xu

et al. put forward the privacy-aware deployment of machine learning for industrial cyber-physical could system [183].

E. Differential Privacy for Industrial Sensing Terminal

As an important means to realize the comprehensive perception of IIoT, industry takes terminal sensors with various communication methods as the basic perception unit, in order to realize the distribution of perception tasks and the collection of sensing data. In this way, it can finally complete large-scale and complex perception tasks for IIoT.

Swarm intelligence sensing applications need a large number of sensors to participate, and these data can carry sensitive information, making it face the risk of privacy disclosure. In this way, how to make use of differential privacy in IIoT sensing terminals is a hot topic for future research. In this filed, Daniele *et al.* discussed the integration of robotic vision and tactile sensing for wire-terminal insertion tasks [184]. In [185], Zhang *et al.* defined the privacy-assured FogCS, which can be used as chaotic compressive sensing for secure industrial big image data processing.

F. Differential Privacy for Integration of Intelligent IIoT

One of the ultimate goals of IIoT is to realize the intelligent industrial production, so intelligence is also an important development trend for IIoT. With the introduction of AI platform, intelligent innovation in the field of IIoT will continue to emerge.

It has been demonstrated in Section VII-B that the integration poses more challenges for privacy protection in IIoT. As a main solution, the potential role of differential privacy is highlighted and has important research value. For example, Yu *et al.* integrated the data security with edge intelligent IIoT [186]. And Zou *et al.* proposed the CrowdBLPS, which integrated the blockchain with location-privacy-preserving for mobile crowdsensing system [187]. On the whole, more integrations are needed to promote the further development of privacy technology.

G. Differential Privacy for Blockchain in IIoT

Most of the existing IIoT application systems take data transmission architecture in centralized and all terminals uniformly upload data to the cloud server. Under this architecture, the security and stability of cloud server is the key to the normal operation of the whole IIoT system. The application of blockchain in the industrial field can solve this problem.

Generally, the overall research of blockchain technology is still in hot spot, and its application in IIoT is more unique and has research value. How to directly or indirectly use differential privacy technology to protect the privacy information of blockchain will become the next research focus. Wan *et al.* proposed the blockchain-based solution designed for enhancing security and privacy in smart factory [188]. And Liu *et al.* also discussed the privacy in blockchain-enabled data collection and sharing for IIoT with the help of reinforcement learning [189].

IX. Conclusions

In this survey, we comprehensively reviewed the related researches on differential privacy in IIoT. In order to provide more research ideas in the field of IIoT privacy protection, this survey presents an in-depth analysis of relevant topics. Specially, we reviewed related literature on IIoT and privacy protection, respectively. Then we focused on the metrics of industrial data privacy, and analyzed contradiction between deep model data utilization and individual privacy protection. In current background, this survey also conducted detailed analysis of the opportunities, applications and challenges of differential privacy in IIoT. Several valuable problems were identified and new research ideas were proposed in this survey. It is hoped that this study can provide valuable references for researchers and promote the development of privacy protection of industrial IoT.

References

[1] S. Seneviratne, Y. Hu, T. Nguyen, G. Lan, S. Khalifa, K. Thilakarathna, M. Hassan, and A. Seneviratne, "A survey of wearable devices and challenges," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 4, pp. 2573–2620, 2017.

[2] M. Ma, W. Lin, J. Zhang, P. Wang, Y. Zhou, and X. Liang, "Toward energy-awareness smart building: Discover the fingerprint of your electrical appliances," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1458–1468, 2018.

[3] J. Wang, J. Liu, and N. Kato, "Networking and communications in autonomous driving: A survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 2, pp. 1243–1274, 2019.

[4] K. Morioka, J. H. Lee, and H. Hashimoto, "Human-following mobile robot in a distributed intelligent sensor network," *IEEE Transactions on Industrial Electronics*, vol. 51, no. 1, pp. 229–237, 2004.

[5] H. Tran-Dang, N. Krommenacker, P. Charpentier, and D. S. Kim, "Towards the internet of things for physical internet: Perspectives and challenges," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4711–4736, 2020.

[6] H. Song, D. B. Rawat, S. Jeschke, and C. Brecher, *Cyber-physical systems: foundations, principles and applications*. Morgan Kaufmann, 2016.

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

[8] C. W. Chen, "Internet of video things: Next-generation iot with visual sensors," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6676–6685, 2020.

[9] L. Zhao, I. B. M. Matsuo, Y. Zhou, and W. J. Lee, "Design of an industrial iot-based monitoring system for power substations," *IEEE Transactions on Industry Applications*, vol. 55, no. 6, pp. 5666–5674, 2019.

[10] C. Pereira, A. Pinto, D. Ferreira, and A. Aguiar, "Experimental characterization of mobile iot application latency," *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 1082–1094, 2017.

[11] M. Shen, B. Ma, L. Zhu, X. Du, and K. Xu, "Secure phrase search for intelligent processing of encrypted data in cloud-based iot," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1998–2008, 2019.

[12] Z. Cai and X. Zheng, "A private and efficient mechanism for data uploading in smart cyber-physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 2, pp. 766–775, 2020.

[13] D. Chong, Z. Bo, L. Qilian, L. Shenghong, and G. Ying, "Learning automata-based access class barring scheme for massive random access in machine-to-machine communications," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6007–6017, 2019.

[14] W. Shi, C. Jie, Z. Quan, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637–646, 2016.

[15] M. Siddula, Z. Cai, and D. Miao, "Privacy preserving online social networks using enhanced equicardinal clustering," in *IEEE 37th International Performance Computing and Communications Conference (IPCCC)*, 2018.

[16] S. R. Pokhrel, Y. Qu, and L. Gao, "Qos-aware personalized privacy with multipath tcp for industrial iot: Analysis and design," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4849–4861, 2020.

[17] H. Song, G. Fink, and S. Jeschke, *Security and Privacy in Cyber-Physical Systems*. Wiley Online Library, 2017.

[18] X. Zheng, Z. Cai, and Y. Li, "Data linkage in smart internet of things systems: a consideration from a privacy perspective," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 55–61, 2018.

[19] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[20] G. Drosatos, K. Rantos, D. Karampatzakis, T. Lagkas, and P. Sarigiannidis, "Privacy-preserving solutions in the industrial internet of things," in *16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2020.

[21] 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 Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6092–6102, 2020.

[22] T. Zhu, G. Li, W. Zhou, and P. S. Yu, "Differentially private data publishing and analysis: A survey," *IEEE Transactions on Knowledge and Data Engineering*, vol. 29, no. 8, pp. 1619–1638, 2017.

[23] X. Yang, T. Wang, X. Ren, and W. Yu, "Survey on improving data utility in differentially private sequential data publishing," *IEEE Transactions on Big Data*, vol. PP, no. 99, pp. 1–1, 2017.

[24] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial internet of things: Challenges, opportunities, and directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, 2018.

[25] T. Wang, Z. Zheng, M. H. Rehmani, S. Yao, and Z. Huo, "Privacy preservation in big data from the communication perspective - a survey," *IEEE Communications Surveys and Tutorials*, vol. 21, no. 1, pp. 753–778, 2019.

[26] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy techniques for cyber physical systems: A survey," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 746–789, 2020.

[27] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, pp. 1–1, 2020.

[28] Z. Cai and Z. He, "Trading private range counting over big iot data," in *IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 2019.

[29] L. Xu, W. He, and S. Li, "Internet of things in industries: A survey," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[30] S. Jeschke, C. Brecher, H. Song, and D. Rawat, *Industrial Internet of Things: Cybermanufacturing Systems*. Cham, Switzerland: Springer, 2017.

[31] Q. Zhang, C. Zhu, L. T. Yang, Z. Chen, L. Zhao, and P. Li, "An incremental cfs algorithm for clustering large data in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 3, pp. 1193–1201, 2017.

[32] F. Liang, W. Yu, X. Liu, D. Griffith, and N. Golmie, "Toward edge-based deep learning in industrial internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4329–4341, 2020.

[33] L. Dai, B. Wang, L. T. Yang, X. Deng, and L. Yi, "A nature-inspired node deployment strategy for connected confident information coverage in industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9217–9225, 2019.

[34] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2019.

[35] H. Mouratidis and V. Diamantopoulou, "A security analysis method for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4093–4100, 2018.

[36] J. M. Mcginthy and A. J. Michaels, "Secure industrial internet of things critical infrastructure node design," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8021–8037, 2019.

[37] M. Al-Hawawreh, F. D. Hartog, and E. Sitnikova, "Targeted ransomware: A new cyber threat to edge system of brownfield industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 7137–7151, 2019.

[38] M. Urbina, T. Acosta, J. Lazaro, A. Astarloa, and U. Bidarte, "Smart sensor: Soc architecture for the industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6567–6577, 2019.

[39] M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine learning based network vulnerability analysis of industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6822–6834, 2019.

[40] T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie, "Mtes: An intelligent trust evaluation scheme in sensor-cloud-enabled industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2054–2062, 2020.

[41] C. Boudagdigue, A. Benslimane, A. Kobbane, and J. Liu, "Trust management in industrial internet of things," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3667–3682, 2020.

[42] X. Zheng and Z. Cai, "Privacy-preserved data sharing towards multiple parties in industrial iots," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.

[43] H. Tang, D. Li, J. Wan, M. Imran, and M. Shoaib, "A reconfigurable method for intelligent manufacturing based on industrial cloud and edge intelligence," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4248–4259, 2020.

[44] G. Fortino, F. Messina, D. Rosaci, G. M. L. SarnÃ©, and C. Savaglio, "A trust-based team formation framework for mobile intelligence in smart factories," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6133–6142, 2020.

[45] Z. Guo, Y. Zhang, X. Zhao, and X. Song, "Cps-based self-adaptive collaborative control for smart production-logistics systems," *IEEE Transactions on Cybernetics*, vol. 52, no. 2, pp. 188–198, 2021.

[46] Q. Sun, H. Li, Z. Ma, C. Wang, J. Campillo, Q. Zhang, F. Wallin, and J. Guo, "A comprehensive review of smart energy meters in intelligent energy networks," *IEEE Internet of Things Journal*, vol. 3, no. 4, pp. 464–479, 2016.

[47] D. Ma and Y. Shi, "A lightweight encryption algorithm for edge networks in software-defined industrial internet of things," in *IEEE International Conference on Computer and Communications (ICCC)*, 2019.

[48] G. Luo and L. J. Frey, "Efficient execution methods of pivoting for bulk extraction of entity-attribute-value-modeled data," *IEEE Journal of Biomedical and Health Informatics*, vol. 20, no. 2, pp. 644–654, 2015.

[49] M. Hassan, S. Huda, S. Sharmeen, J. Abawajy, and G. Fortino, "An adaptive trust boundary protection for iiot networks using deep-learning feature extraction based semi-supervised model," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2860–2870, 2021.

[50] J. Wang, Z. Cai, and J. Yu, "Achieving personalized k-anonymity-based content privacy for autonomous vehicles in cps," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4242–4251, 2019.

[51] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211–407, 2013.

[52] L. Ninghui, M. Lyu, D. Su, and Y. Weining, *Differential Privacy: From Theory to Practice*, 2016.

[53] M. A. Pathak and B. Raj, "Large margin gaussian mixture models with differential privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 4, pp. 463–469, 2012.

[54] P. Kairouz, S. Oh, and P. Viswanath, "The composition theorem for differential privacy," *IEEE Transactions on Information Theory*, vol. 63, no. 6, pp. 4037–4049, 2015.

[55] W. Wang, Y. Lei, and J. Zhang, "On the relation between identifiability, differential privacy and mutual-information privacy," *IEEE Transactions on Information Theory*, vol. 62, no. 9, pp. 5018–5029, 2016.

[56] A. Inan, M. E. Gursoy, and Y. Saygin, "Sensitivity analysis for non-interactive differential privacy: Bounds and efficient algorithms," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 1, pp. 194–207, 2020.

[57] X. Zhang, J. Wang, H. Li, Y. Guo, and M. Pan, "Data-driven caching with users' local differential privacy in information-centric networks," in *IEEE Global Communications Conference*, 2018.

[58] X. Cheng, P. Tang, S. Su, R. Chen, Z. Wu, and B. Zhu, "Multi-party high-dimensional data publishing under differential privacy," *IEEE Transactions on Knowledge and Data Engineering*, vol. 32, no. 8, pp. 1557–1571, 2020.

[59] L. Oneto, M. Donini, M. Pontil, and J. Shawe-Taylor, "Randomized learning and generalization of fair and private classifiers: from pac-bayes to stability and differential privacy," *Neurocomputing*, vol. 416, pp. 231–243, 2020.

[60] X. Xiao, G. Wang, and J. Gehrke, "Differential privacy via wavelet transforms," *IEEE Transactions on Knowledge and Data Engineering*, vol. 23, no. 8, pp. 1200–1214, 2011.

[61] R. Fouad, Mohamed, K. Elbassioni, and E. Bertino, "A supermodularity-based differential privacy preserving algorithm for data anonymization," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 7, pp. 1–1, 2014.

[62] J. Soria-Comas, J. Domingo-Ferrer, D. SÃ¡nchez, and D. MegÃas, "Individual differential privacy: A utility-preserving formulation of differential privacy guarantees," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1418–1429, 2017.

[63] H. Wang and Z. Xu, "Cts-dp: Publishing correlated time-series data via differential privacy," *Knowledge Based Systems*, vol. 122, pp. 167–179, 2017.

[64] S. Goryczka and L. Xiong, "A comprehensive comparison of multiparty secure additions with differential privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 5, pp. 463–477, 2017.

[65] Q. Zhu and T. Zhang, "Dynamic differential privacy for admm-based distributed classification learning," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp. 172–187, 2017.

[66] Y. Cao, M. Yoshikawa, Y. Xiao, and L. Xiong, "Quantifying differential privacy in continuous data release under temporal correlations," *IEEE Transactions on Knowledge and Data Engineering*, vol. 31, no. 7, pp. 1281–1295, 2019.

[67] K. Kalantari, L. Sankar, and A. D. Sarwate, "Robust privacy-utility tradeoffs under differential privacy and hamming distortion," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2816–2830, 2018.

[68] M. Du, K. Wang, Z. Xia, and Y. Zhang, "Differential privacy preserving of training model in wireless big data with edge computing," *IEEE Transactions on Big Data*, vol. 6, no. 2, pp. 283–295, 2020.

[69] O. Lu, Q. Zheng, L. Shaolin, H. Yuan, and J. Xiaohua, "Releasing correlated trajectories: Towards high utility and optimal differential privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 1109–1123, 2020.

[70] T. Zhang, T. Zhu, P. Xiong, H. Huo, and W. Zhou, "Correlated differential privacy: Feature selection in machine learning," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2115–2124, 2020.

[71] J. Brinkrolf, C. Goepfert, and B. Hammer, "Differential privacy for learning vector quantization," *Neurocomputing*, vol. 342, pp. 125–136, 2019.

[72] M. Gong, K. Pan, and Y. Xie, "Differential privacy preservation in regression analysis based on relevance," *Knowledge-Based Systems*, vol. 173, pp. 140–149, 2019.

[73] H. Ke, A. Fu, S. Yu, and S. Chen, "Aq-dp: A new differential privacy scheme based on quasi-identifier classifying in big data," in *IEEE Global Communications Conference (GLOBECOM)*, 2019.

[74] W. Huang, S. Zhou, Y. Liao, and H. Chen, "An efficient differential privacy logistic classification mechanism," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10 620–10 626, 2019.

[75] J. Li, Y. Pan, Y. Sui, and I. W. Tsang, "Secure metric learning via differential pairwise privacy," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3640–3652, 2020.

[76] V. Katewa, A. Chakrabortty, and V. Gupta, "Differential privacy for network identification," *IEEE Transactions on Control of Network Systems*, vol. 7, no. 1, pp. 266–277, 2020.

[77] Q. Geng and P. Viswanath, "The optimal noise-adding mechanism in differential privacy," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 925–951, 2016.

[78] J. Soria-Comas and J. Domingo-Ferrer, "Optimal data-independent noise for differential privacy," *Information Sciences*, vol. 250, pp. 200–214, 2013.

[79] Q. Geng and P. Viswanath, "Optimal noise adding mechanisms for approximate differential privacy," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 952–969, 2016.

[80] D. Wang and J. Xu, "Principal component analysis in the local differential privacy model," in *International Joint Conference on Artificial Intelligence*, 2019.

[81] X. Li, H. Li, H. Zhu, and M. Huang, "The optimal upper bound of the number of queries for laplace mechanism under differential privacy," *Information Sciences*, vol. 503, pp. 219–237, 2019.

[82] Q. Geng and P. Viswanath, "The optimal mechanism in differential privacy," in *IEEE international symposium on information theory*, 2014, pp. 2371–2375.

[83] Q. Geng, P. Kairouz, S. Oh, and P. Viswanath, "The optimal mechanism in differential privacy: Multidimensional setting," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1176–1184, 2015.

[84] B. Niu, Y. Chen, B. Wang, J. Cao, and F. Li, "Utility-aware exponential mechanism for personalized differential privacy," in *IEEE Wireless Communications and Networking Conference*, 2020.

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

[86] H. L. Chen, J. Y. Chen, Y. T. Tsou, C. M. Yu, B. C. Tai, S. C. Li, Y. Huang, and C. M. Lin, "Evaluating the risk of data disclosure using noise estimation for differential privacy," in *IEEE Pacific Rim International Symposium on Dependable Computing*, 2017.

[87] Y. Zhao and I. Wagner, "On the strength of privacy metrics for vehicular communication," *IEEE Transactions on Mobile Computing*, vol. 18, no. 2, pp. 390–403, 2019.

[88] 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 of Things Journal*, vol. 6, no. 2, pp. 1530–1540, 2019.

[89] B. Rassouli and D. GÃ¼ndÃ¼z, "Optimal utility-privacy trade-off with total variation distance as a privacy measure," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 594–603, 2019.

[90] O. Gunlu and G. Kramer, "Privacy, secrecy, and storage with multiple noisy measurements of identifiers," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2872–2883, 2018.

[91] T. Naghibi, S. Hoffmann, and B. Pfister, "A semidefinite programming based search strategy for feature selection with mutual information measure," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 37, no. 8, pp. 1529–1541, 2014.

[92] T. Zhu, D. Ye, W. Wang, W. Zhou, and P. Yu, "More than privacy: Applying differential privacy in key areas of artificial intelligence," *IEEE Transactions on Knowledge and Data Engineering*, vol. PP, no. 99, pp. 1–1, 2020.

[93] T. Ha, T. K. Dang, T. T. Dang, T. A. Truong, and M. T. Nguyen, "Differential privacy in deep learning: An overview," in *International Conference on Advanced Computing and Applications (ACOMP)*, 2020.

[94] C. Xu, J. Ren, D. Zhang, Y. Zhang, Z. Qin, and K. Ren, "Ganobfuscator: Mitigating information leakage under gan via differential privacy," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 9, pp. 2358–2371, 2019.

[95] S. Chen, A. Fu, J. Shen, S. Yu, H. wang, and H. Sun, "Rnn-dp: A new differential privacy scheme base on recurrent neural network for dynamic trajectory privacy protection," *Journal of Network and Computer Applications*, vol. 168, p. 102736, 2020.

[96] M. Gong, K. Pan, Y. Xie, A. K. Qin, and Z. Tang, "Preserving differential privacy in deep neural networks with relevance-based adaptive noise imposition," *Neural Networks*, vol. 125, pp. 131–141, 2020.

[97] K. Wei, J. Li, M. Ding, C. Ma, H. H. Yang, F. Farhad, S. Jin, T. Q. S. Quek, and H. V. Poor, "Federated learning with differential privacy: Algorithms and performance analysis," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3454–3469, 2020.

[98] N. Rodriguez-Barroso, G. Stipcich, D. Jimenez-Lopez, J. A. Ruiz-Millan, and F. Herrera, "Federated learning and differential privacy: Software tools analysis, the sherpa.ai fl framework and methodological guidelines for preserving data privacy," *Information Fusion*, vol. 64, pp. 270–292, 2020.

[99] R. Hu, Y. Guo, H. Li, Q. Pei, and Y. Gong, "Personalized federated learning with differential privacy," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9530–9539, 2020.

[100] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Differentially private asynchronous federated learning for mobile edge computing in urban informatics," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2134–2143, 2020.

[101] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6532–6542, 2020.

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

[103] Y. Wang, M. Gu, J. Ma, and Q. Jin, "Dnn-dp: Differential privacy enabled deep neural network learning framework for sensitive crowdsourcing data," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 1, pp. 215–224, 2020.

[104] H. Zheng, H. Hu, and Z. Han, "Preserving user privacy for machine learning: Local differential privacy or federated machine learning," *IEEE Intelligent Systems*, vol. 35, no. 4, pp. 5–14, 2020.

[105] V. Primault, A. Boutet, S. B. Mokhtar, and L. Brunie, "The long road to computational location privacy: A survey," *Communications surveys and tutorials*, vol. 21, no. 3, pp. 2772–2793, 2019.

[106] 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 Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3628–3636, 2018.

[107] Y. Wang, M. Huang, Q. Jin, and J. Ma, "Dp3: A differential privacy-based privacy-preserving indoor localization mechanism," *IEEE Communications Letters*, vol. 22, no. 12, pp. 2547–2550, 2018.

[108] X. Li, H. Zhang, Y. Ren, S. Ma, and X. Huang, "Papu: Pseudonym swap with provable unlinkability based on differential privacy in vanets," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11 789–11 802, 2020.

[109] J. Wei, Y. Lin, X. Yao, and J. Zhang, "Differential privacy-based location protection in spatial crowdsourcing," *IEEE Transactions on Services Computing*, vol. PP, no. 99, pp. 1–1, 2019.

[110] J. D. Zhang and C. Y. Chow, "Enabling probabilistic differential privacy protection for location recommendations," *IEEE Transactions on Services Computing*, vol. PP, no. 99, pp. 1–1, 2018.

[111] Y. Li, D. Yang, and X. Hu, "A differential privacy-based privacy-preserving data publishing algorithm for transit smart card data," *Transportation Research Part C: Emerging Technologies*, vol. 115, p. 102634, 2020.

[112] T. Wang, Z. Zheng, and M. Elhoseny, "Equivalent mechanism: Releasing location data with errors through differential privacy," *Future Generation Computer Systems*, vol. 98, pp. 600–608, 2019.

[113] X. Liu, Y. Guo, Y. Chen, and X. Tan, "Trajectory privacy protection on spatial streaming data with differential privacy," in *IEEE Global Communications Conference*, 2018.

[114] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6492–6499, 2019.

[115] D. Li, Q. Yang, W. Yu, D. An, and W. Zhao, "Towards differential privacy-based online double auction for smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 971–986, 2019.

[116] F. Fioretto, T. W. K. Mak, and P. Van Hentenryck, "Differential privacy for power grid obfuscation," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 1356–1366, 2020.

[117] 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 of Things Journal*, vol. 7, no. 6, pp. 5246–5255, 2020.

[118] Z. Zhang, Z. Qin, L. Zhu, J. Weng, and K. Ren, "Cost-friendly differential privacy for smart meters: Exploiting the dual roles of the noise," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 619–626, 2017.

[119] X. Lou, D. Yau K. Y., R. Tan, and P. Cheng, "Cost and pricing of differential privacy in demand reporting for smart grids," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 3, pp. 2037–2051, 2020.

[120] M. U. Hassan, M. H. Rehmani, R. Kotagiri, J. Zhang, and J. Chen, "Differential privacy for renewable energy resources based smart metering," *Journal of Parallel and Distributed Computing*, vol. 131, pp. 69–80, 2019.

[121] T. W. K. Mak, F. Fioretto, and P. V. Hentenryck, "Privacy-preserving obfuscation for distributed power systems," *Electric Power Systems Research*, vol. 189, p. 106718, 2020.

[122] J. Wang, X. Zhang, H. Zhang, H. Lin, and Z. Han, "Data-driven optimization for utility providers with differential privacy of users' energy profile," in *IEEE Global Communications Conference*, 2018.

[123] J. Zhao, T. Jung, Y. Wang, and X. Li, "Achieving differential privacy of data disclosure in the smart grid," in *IEEE Global Communications Conference*, 2014.

[124] H. Song, R. Srinivasan, T. Sookoor, and S. Jeschke, *Smart cities: foundations, principles, and applications*. NJ: Wiley, 2017.

[125] C. Lin, Z. Song, H. Song, Y. Zhou, Y. Wang, and G. Wu, "Differential privacy preserving in big data analytics for connected health," *Journal of medical systems*, vol. 40, no. 4, p. 97, 2016.

[126] 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 Transactions on Computational Biology and Bioinformatics*, vol. 15, no. 5, pp. 1413–1426, 2018.

[127] X. Liu, P. Zhou, T. Qiu, and D. O. Wu, "Blockchain-enabled contextual online learning under local differential privacy for coronary heart disease diagnosis in mobile edge computing," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 8, pp. 2177–2188, 2020.

[128] J. Wei, Y. Lin, X. Yao, J. Zhang, and X. Liu, "Differential privacy-based genetic matching in personalized medicine," *IEEE Transactions on Emerging Topics in Computing*, vol. PP, no. 99, pp. 1–1, 2020.

[129] Z. Wang, P. Ma, R. Wang, J. Zhang, and T. Yang, "Secure medical data collection via local differential privacy," in *IEEE International Conference on Computer and Communications (ICCC)*, 2018.

[130] H. Li, Y. Dai, and X. Lin, "Efficient e-health data release with consistency guarantee under differential privacy," in *International Conference on E-health Networking, Application and Services (HealthCom)*, 2015.

[131] M. Zhang and X. Li, "Drone-enabled internet-of-things relay for environmental monitoring in remote areas without public networks," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7648–7662, 2020.

[132] B. Jiang, J. Yang, H. Xu, H. Song, and G. Zheng, "Multimedia data throughput maximization in internet-of-things system based on optimization of cache-enabled uav," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3525–3532, 2019.

[133] H. Kim, J. Benothman, and L. Mokdad, "On differential privacy-preserving movements of unmanned aerial vehicles," in *IEEE International Conference on Communications*, 2017.

[134] H. Kim, J. Ben-Othman, and L. Mokdad, "Udipp: A framework for differential privacy preserving movements of unmanned aerial vehicles in smart cities," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3933–3943, 2019.

[135] Y. Wang, Z. Su, N. Zhang, and A. Benslimane, "Learning in the air: Secure federated learning for uav-assisted crowdsensing," *IEEE Transactions on Network Science and Engineering*, vol. PP, no. 99, pp. 1–1, 2020.

[136] Y. Wang, Z. Huang, S. Mitra, and G. E. Dullerud, "Differential privacy in linear distributed control systems: Entropy minimizing mechanisms and performance tradeoffs," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 118–130, 2017.

[137] L. Fan and L. Xiong, "An adaptive approach to real-time aggregate monitoring with differential privacy," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 9, pp. 2094–2106, 2014.

[138] B. Chakraborty, S. Verma, and K. P. Singh, "Temporal differential privacy in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 155, p. 102548, 2020.

[139] T. Wang, Y. Mei, W. Jia, X. Zheng, G. Wang, and M. Xie, "Edge-based differential privacy computing for sensor - cloud systems," *Journal of Parallel and Distributed Computing*, vol. 136, pp. 75–85, 2020.

[140] P. Barbosa, A. Brito, and H. Almeida, "A technique to provide differential privacy for appliance usage in smart metering," *Information Sciences*, vol. 370-371, pp. 355–367, 2016.

[141] M. Abdallah, O. A. Dobre, P. H. Ho, S. Jabbar, and J. J. P. C. Rodrigues, "Blockchain-enabled industrial internet of things: Advances, applications, and challenges," *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 16–18, 2020.

[142] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[143] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3690–3700, 2018.

[144] M. Liu, R. Yu, Y. Teng, V. Leung, and M. Song, "Performance optimization for blockchain-enabled industrial internet of things (iiot) systems: A deep reinforcement learning approach," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3559–3570, 2019.

[145] K. Gai, Y. Wu, L. Zhu, M. Qiu, and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3548–3558, 2019.

[146] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, "Resource trading in blockchain-based industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3602–3609, 2019.

[147] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differential privacy in blockchain technology: A futuristic approach," *Journal of Parallel and Distributed Computing*, vol. 145, pp. 50–74, 2020.

[148] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial iot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2020.

[149] K. Gai, Y. Wu, L. Zhu, Z. Zhang, and M. Qiu, "Differential privacy-based blockchain for industrial internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4156 – 4165, 2020.

[150] C. Roy, S. Misra, and S. Pal, "Blockchain-enabled safety-as-a-service for industrial iot applications," *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 19–23, 2020.

[151] H. N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," *Internet of Things Journal, IEEE*, vol. 6, no. 5, pp. 8076–8094, 2019.

[152] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2016.

[153] J. Abawajy, M. I. Ninggal, and T. Herawan, "Privacy preserving social network data publication," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3, pp. 1974–1997, 2016.

[154] H. Huang, D. J. Zhang, F. Xiao, K. Wang, and R. Wang, "Privacy-preserving approach pbcn in social network with differential privacy," *IEEE Transactions on Network and Service Management*, vol. PP, no. 99, pp. 1–1, 2020.

[155] Y. Hong, J. Vaidya, H. Lu, P. Karras, and S. Goel, "Collaborative search log sanitization: Toward differential privacy and boosted utility," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 5, pp. 504–518, 2015.

[156] Q. Wang, Y. Zhang, X. Lu, Z. Wang, Z. Qin, and K. Ren, "Real-time and spatio-temporal crowd-sourced social network data publishing with differential privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 591–606, 2018.

[157] M. Du, K. Wang, X. Liu, S. Guo, and Y. Zhang, "A differential privacy-based query model for sustainable fog data centers," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 2, pp. 145–155, 2019.

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

[159] M. Wang, C. Xu, X. Chen, H. Hao, L. Zhong, and S. Yu, "Differential privacy oriented distributed online learning for mobile social video prefetching," *IEEE Transactions on Multimedia*, vol. 21, no. 3, pp. 636–651, 2019.

[160] J. Lin, J. Niu, X. Liu, and M. Guizani, "Protecting your shopping preference with differential privacy," *IEEE Transactions on Mobile Computing*, vol. PP, no. 99, pp. 1–1, 2020.

[161] M. A. P. Chamikara, P. Bertok, I. Khalil, D. Liu, and S. Camtepe, "Privacy preserving face recognition utilizing differential privacy," *Computers and Security*, vol. 97, p. 101951, 2020.

[162] P. Liu, Y. X. Xu, Q. Jiang, Y. Tang, Y. Guo, L. E. Wang, and X. Li, "Local differential privacy for social network publishing," *Neurocomputing*, vol. 391, pp. 273–279, 2020.

[163] J. Wei, Y. Lin, X. Yao, and V. K. Arthursandora, "Differential privacy-based trajectory community recommendation in social network," *Journal of Parallel and Distributed Computing*, vol. 133, pp. 136–148, 2019.

[164] B. Jiang, J. Yang, G. Ding, and H. Wang, "Cyber-physical security design in multimedia data cache resource allocation for industrial networks," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6472–6480, 2019.

[165] L. Mottola, G. P. Picco, F. J. Opperman, J. Eriksson, and T. Voigt, "Makesense: Simplifying the integration of wireless sensor networks into business processes," *IEEE Transactions on Software Engineering*, vol. 45, no. 6, pp. 576–596, 2019.

[166] G. Culot, G. Orzes, and M. Sartor, "Integration and scale in the context of industry 4.0: The evolving shapes of manufacturing value chains," *IEEE Engineering Management Review*, vol. 47, no. 1, pp. 45–51, 2019.

[167] Y. Sun, H. Song, A. Jara, and R. Bie, "Internet of things and big data analytics for smart and connected communities," *IEEE Access*, vol. 4, pp. 766–773, 2016.

[168] 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," *Annals of Telecommunications*, vol. 71, pp. 465–475, 2016.

[169] P. Zhou, K. Wang, J. Xu, and D. Wu, "Differentially-private and trustworthy online social multimedia big data retrieval in edge computing," *IEEE Transactions on Multimedia*, vol. 32, no. 3, pp. 539–554, 2019.

[170] A. D'Alconzo, I. Drago, A. Morichetta, M. Mellia, and P. Casas, "A survey on big data for network traffic monitoring and analysis," *IEEE Transactions on Network and Service Management*, vol. 16, no. 3, pp. 800–813, 2019.

[171] J. Feng, L. T. Yang, R. Zhang, W. Qiang, and J. Chen, "Privacy preserving high-order bi-lanczos in cloud-fog computing for industrial applications," *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, pp. 1–1, 2020.

[172] M. Usman, A. Jolfaei, and M. A. Jan, "Rasec: An intelligent framework for reliable and secure multi-level edge computing in industrial environments," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4543–4551, 2020.

[173] S. Langarica, C. RÃ¼ffelmacher, and F. NÃºnez, "An industrial internet application for real-time fault diagnosis in industrial motors," *IEEE Transactions on Automation Science and Engineering*, vol. 17, no. 1, pp. 284–295, 2020.

[174] A. Parizad, S. Mohamadian, M. E. Iranian, and J. M. Guerrero, "Power system real-time emulation: A practical virtual instrumentation to complete electric power system modeling," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 2, pp. 889–900, 2019.

[175] D. Zhao, X. Li, and H. Ma, "Budget-feasible online incentive mechanisms for crowdsourcing tasks truthfully," *IEEE/ACM Transactions on Networking*, vol. 24, no. 2, pp. 647–661, 2016.

[176] K. Han, H. Liu, S. Tang, M. Xiao, and J. Luo, "Differentially private mechanisms for budget limited mobile crowdsourcing," *IEEE Transactions on Mobile Computing*, vol. 18, no. 4, pp. 934–946, 2019.

[177] L. Moren, C. Y. Rok, and H. Juliana, "Growth through franchises in knowledge-intensive industries: Interplay of routine program and expansion mode," *IEEE Transactions on Engineering Management*, vol. 66, no. 4, pp. 496–513, 2019.

[178] B. Wang, Y. Sun, T. Q. Duong, L. D. Nguyen, and N. Zhao, "Security enhanced content sharing in social iot: A directed hypergraph-based learning scheme," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4412–4425, 2020.

[179] S. Karumba, S. K. Salil, R. Jurdak, and S. Sethuvenkatraman, "Harb: A hypergraph-based adaptive consortium blockchain for decentralised energy trading," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–1, 2020.

[180] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements and future directions," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 196–248, 2020.

[181] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu, and L. Liu, "Edge computing-based privacy-preserving authentication framework and protocol for 5g-enabled vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7940–7954, 2020.

[182] P. Hu, H. Ning, T. Qiu, H. Song, Y. Wang, and X. Yao, "Security and privacy preservation scheme of face identification and resolution framework using fog computing in internet of things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1143–1155, 2017.

[183] X. Xu, R. Mo, X. Yin, M. R. Khosravi, F. Aghaei, V. Chang, and G. Li, "Pdm: Privacy-aware deployment of machine-learning applications for industrial cyber-physical cloud systems," *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, pp. 1–1, 2020.

[184] D. G. Daniele, Z. Riccardo, P. Gianluca, P. Salvatore, and M. Claudio, "Integration of robotic vision and tactile sensing for wire-terminal insertion tasks," *IEEE Transactions on Automation Science and Engineering*, vol. 16, no. 2, pp. 585–598, 2019.

[185] Y. Zhang, P. Wang, H. huang, Y. Zhu, D. Xiao, and Y. Xiang, "Privacy-assured fogcs: Chaotic compressive sensing for secure industrial big image data processing in fog computing," *IEEE Transactions on Industrial Informatics*, vol. PP, no. 99, pp. 1–1, 2020.

[186] Y. Yu, R. Chen, H. Li, Y. Li, and A. Tian, "Toward data security in edge intelligent iiot," *IEEE Network*, vol. 33, no. 5, pp. 20–26, 2019.

[187] S. Zou, J. Xi, H. Wang, and G. Xu, "Crowdblps: A blockchain-based location-privacy-preserving mobile crowdsensing system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4206–4218, 2020.

[188] J. Wan, J. Li, M. Imran, D. Li, and F. E-Amin, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3652–3660, 2019.

[189] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learning," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3516–3526, 2019.

Bin Jiang (M'20) received the B.S., M.S. and Ph.D. degrees in communication and information engineering from Tianjin University, China, in 2013, 2016, and 2020, respectively. He was a visiting scholar in the Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University, Daytona Beach, FL, USA, from Nov.2017 to Feb.2019 and from Oct. 2018 to Oct. 2019.

Dr.Jiang is currently a Postdoctoral Research Fellow in the College of Computer and Software Engineering, Shenzhen University, Shenzhen, China, and he is also the member of the Security and Optimization for Networked Globe Laboratory, FL, USA. He is the Editor for Frontiers in Communications and Networks, Guest Editor for Sensors, TCP Member for IEEE International Conference on Innovations in Information Technology and Program Committee Member for International Conference on Computer Engineering and Artificial Intelligence. His research interests lie in cybersecurity and privacy protection, industrial Internet of things and multimedia quality control.

Jianqiang Li received the B.S. and Ph.D. degrees from the South China University of Technology, Guangzhou, China, in 2003 and 2008, respectively. He is a Professor with the College of Computer and Software Engineering, Shenzhen University, Shenzhen, China. He led three projects of the National Natural Science Foundation and three projects of the Natural Science Foundation of Guangdong, China. His major research interests include robotic, hybrid systems, Internet of Things, and embedded systems.

Guanghui Yue received the B.S. and the Ph.D. degree in information and communication engineering from Tianjin University, Tianjin, China, in 2014 and 2019, respectively. He was a joint Ph.D. student with the School of Computer Science and Engineering, Nanyang Technological University, Singapore, from 2017 to 2019. He is currently an Assistant Professor with the School of Biomedical Engineering, Health Science Center, Shenzhen University, Shenzhen, China. His research interests include bioelectrical signal processing and medical image analysis.

Houbing Song (M'12-SM'14) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, in August 2012, and the M.S. degree in civil engineering from the University of Texas, El Paso, TX, in December 2006.

In August 2017, he joined the Department of Electrical Engineering and Computer Science, Embry-Riddle Aeronautical University, Daytona Beach, FL, where he is currently an Assistant Professor and the Director of the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us). He served on the faculty of West Virginia University from August 2012 to August 2017. In 2007 he was an Engineering Research Associate with the Texas AM Transportation Institute. He has served as an Associate Technical Editor for IEEE Communications Magazine (2017-present), an Associate Editor for IEEE Internet of Things Journal (2020-present) and a Guest Editor for IEEE Journal on Selected Areas in Communications (J-SAC), IEEE Internet of Things Journal, IEEE Transactions on Industrial Informatics, IEEE Sensors Journal, IEEE Transactions on Intelligent Transportation Systems, and IEEE Network. He is the editor of six books, including Big Data Analytics for Cyber-Physical Systems: Machine Learning for the Internet of Things, Elsevier, 2019, Smart Cities: Foundations, Principles and Applications, Hoboken, NJ: Wiley, 2017, Security and Privacy in Cyber-Physical Systems: Foundations, Principles and Applications, Chichester, UK: Wiley-IEEE Press, 2017, Cyber-Physical Systems: Foundations, Principles and Applications, Boston, MA: Academic Press, 2016, and Industrial Internet of Things: Cybermanufacturing Systems, Cham, Switzerland: Springer, 2016. He is the author of more than 100 articles. His research interests include cyber-physical systems, cybersecurity and privacy, internet of things, edge computing, AI/machine learning, big data analytics, unmanned aircraft systems, connected vehicle, smart and connected health, and wireless communications and networking. His research has been featured by popular news media outlets, including IEEE GlobalSpec's Engineering360, USA Today, U.S. News and World Report, Fox News, Association for Unmanned Vehicle Systems International (AUVSI), Forbes, WFTV, and New Atlas.

Dr. Song is a senior member of ACM and an ACM Distinguished Speaker. Dr. Song was a recipient of the Best Paper Award from the 12th IEEE International Conference on Cyber, Physical and Social Computing (CPSCom-2019), the Best Paper Award from the 2nd IEEE International Conference on Industrial Internet (ICII 2019), the Best Paper Award from the 19th Integrated Communication, Navigation and Surveillance technologies (ICNS 2019) Conference, the Best Paper Award from the 6th IEEE International Conference on Cloud and Big Data Computing (CBDCom 2020), and the Best Paper Award from the 15th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2020).