An Overview of Privacy Preserving Schemes for Industrial Internet of Things

Yan Huo[1,*], Chun Meng[1], Ruinian Li[2], Tao Jing[1]

[1] School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China
[2] The Department of Computer Science, Bowling Green State University, Bowling Green, Ohio, 43403, USA
* The corresponding author, email: yhuo@bjtu.edu.cn

Abstract: The concept of Internet of Everything is like a revolutionary storm, bringing the whole society closer together. Internet of Things (IoT) has played a vital role in the process. With the rise of the concept of Industry 4.0, intelligent transformation is taking place in the industrial field. As a new concept, an industrial IoT system has also attracted the attention of industry and academia. In an actual industrial scenario, a large number of devices will generate numerous industrial datasets. The computing efficiency of an industrial IoT system is greatly improved with the help of using either cloud computing or edge computing. However, privacy issues may seriously harmed interests of users. In this article, we summarize privacy issues in a cloud- or an edge-based industrial IoT system. The privacy analysis includes data privacy, location privacy, query and identity privacy. In addition, we also review privacy solutions when applying software defined network and blockchain under the above two systems. Next, we analyze the computational complexity and privacy protection performance of these solutions. Finally, we discuss open issues to facilitate further studies.

Keywords: privacy preserving; cloud computing; edge computing; industrial Internet of Things

I. INTRODUCTION

Industry 4.0 is the final goal to achieve deep integration of traditional industrial platforms with the latest intelligent technology, e.g., big data and artificial intelligence. Due to the digitization of manufacturing, the way of production is in the midst of a significant transformation [1, 2]. Global industries are constantly exploring new ways to break through bottlenecks of intelligent manufacturing. It mainly focuses on large-scale deployments and feasible utilization for machine-to-machine systems to provide increased automation, including adaptive monitoring, data analysis and mining, fault diagnosis, and emergency treatment [3].

Although intelligent manufacturing can free up employees and provide a smoother production process, data security during production is one of the key issues for reliable manufacturing [4]. For example, a company can gather raw data from its devices, sensors, and even assets. The raw data enable the company to supply scalable and reliable applications faster to meet changeable demands of a customer. Yet, there may exist private information in the raw data [5], such as customer behavior characteristics [6], production detail scheduling, and device running status [7]. The private information may be illegally mined from raw

Received: Apr. 15, 2020
Revised: May 17, 2020
Editor: Fuhong Lin

In this paper, we make a comprehensive overview of privacy issues and the related solutions for either the cloud- and edge-based industrial IoT architecture.

data, used for undisclosed commercial purposes, or even sold publicly online. Thus, who can access, securely use, and legally publish raw data is an obstacle to the development of industrial IoT [8, 9]. Appropriate data privacy protection not only enables a company to effectively use data while ensuring data security, but also has significance for the sustainable and healthy ecosystem of industrial IoT.

Technically, privacy preserving studies include three categories [10]: data perturbation, data encryption, and publishing restriction. For the first category, data perturbation can distort dataset values while keeping its basic statistical distribution properties [11, 12]. In particular, it can utilize probability distribution technique to convert original data or introduce additive or multiplicative noise directly into original raw data.

Second, the cryptography-based privacy preserving method can hide sensitive data [13, 14]. Take secure multiparty computation as an example. This method aims to solve the problem of cooperative computing with privacy protection between a group of distrusting parties. In this way, each party in the cooperative multiparty system only knows its own data and the final result of all data computing.

The third category can selectively publish original data, such as not publishing or publishing data with low accuracy, to achieve privacy protection [15, 16]. A typical method is to anonymize sensitive data, e.g., K-anonymity, L-diversity, T-closeness, and artificial intelligence methods [17, 18]. Using this method, disclosure risk of sensitive data can be within a certain tolerance range. Although it enables secure data release without revealing sensitive information by converting an original data into an anonymous dataset, it may be an NP-hard problem when finding the optimal partition into anonymous groups.

The above works mainly focus on the design of privacy preserving schemes for a general scenario rather than a typical industrial IoT application. In this article, we investigate the industrial IoT from the perspective of application scenarios and present the corresponding general architectures. After discussing privacy issues hidden in these architectures, we analyze mainstream solutions in detail, provide issues they can solve, and compare these solutions using complexity analysis methods. In summary, our contributions are threefold in this paper.

- We summarize existing architectures of industrial IoT, including the cloud paradigm, the edge paradigm. Then we present privacy challenges for the paradigms.
- We review effective solutions to cope with privacy challenges of industrial IoT applications from three different technical perspective.
- We analyze and evaluate the privacy performance of existing solutions and discuss computational complexity.

The remaining of this paper is organized as follows. Industrial IoT systems with different paradigms as well as privacy challenges are introduced in Section II. Next, we summarize a series of privacy challenges solutions based on location, data, identity and query in Section III. For these solutions, we evaluate and discuss their performance from the privacy performance and computational complexity in Section IV. Finally, we present open issues and conclude the paper in Section V and Section VI, respectively.

II. Industrial IoT Systems

An industrial IoT system refers to use communication and computer technologies and intelligent analysis to connect devices, gather data, and mine information to increase manufacturing efficiency, improve products quality, lower costs and resource consumption, and finally realize the upgrade of traditional industries to intelligent.

Although a general IoT system and an industrial IoT system have many common technologies, such as cloud platforms, network connections, and machine-to-machine communication, they still have different characteristics. In summary, the differences can be concluded in following four aspects. The first

one is different types of services. The general IoT is a human-centric system with the capability of increasing perception and response to surroundings. An industrial IoT system mainly focuses on monitoring and controlling equipment, environment, and materials in manufacturing, and then realize the goal of intelligent manufacturing in factories. The second one is different connected devices. The general IoT focuses on designing new standards, connecting new devices to the Internet ecosystem in a flexible and friendly manner, but the industrial IoT uses to integrate and connect factories and machines to provide more efficient production service. Third, the network requirements are different. The former supports mobile network structures which have low timing and reliability requirements. The latter is to achieve a machine-to-machine communication, which usually uses a fixed network structure and must satisfy the strict real-time and reliable demand. Finally, the scale of data volume of these two scenarios is different. The data generated by a general IoT system comes from typical applications. Its data volume is determined by different application scenarios. Yet, an industrial IoT system usually has a huge amount of data transmitted or stored in networks due to the rapid growth of connected terminal devices.

According to the characteristics of an industrial IoT system, we first abstract typical architectures and then analyze privacy issues in these architectures.

2.1 Industrial IoT with cloud computing

As a typical centralized computing method, cloud computing can access a resource center anytime and anywhere through the Internet [19]. Based on powerful computing and storage functions of central servers, it can satisfy processing and analysis requirements for a large number of heterogeneous data generated by the industrial IoT. Similar to the traditional architecture of cloud computing, cloud based industrial IoT can be divided into three layers as shown in Figure 1, including an infrastructure layer, a platform layer, and a software service layer for different applications.

In Figure 1, massive industrial IoT devices with sensors in an infrastructure layer locate at the bottom of the system. It may gather raw data from industrial devices. These raw data then are transmitted to cloud servers through a platform layer. The platform layer is the backbone of the entire cloud based industrial IoT. With the powerful data computation and analysis capabilities, a central cloud server can process, analyze, and store these raw data conveniently. Next, data processing results are finally fed back to the service layer. This layer corresponds to various application scenarios. By extracting these results from cloud computing, we can easily achieve production scheduling and management, equipment monitoring and control, resource allocation and optimization in industrial scenarios [20]. In this case, it can realize an intelligent industry with deep knowledge learning. Based on the general model in Figure 1, some works further introduce new technologies into industrial IoT with cloud computing, e.g. software defined networking (SDN) and blockchain.

2.1.1 SDN based cloud-industrial IoT

The number of devices connected to the Internet will increase dramatically in the future. Then, challenges of heterogeneous data and different interfaces will inevitably arise. The architecture of a traditional network is not designed for a cloud computing scenario, and

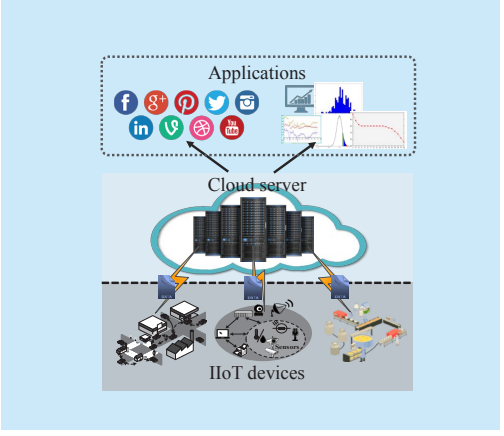


Fig. 1. *Architecture of Industrial IoT with cloud computing.*

therefore, it cannot handle numerous new demands such as virtual local area networks, end-to-end quality-of-service (QoS), and load balancing [21]. As a result, it undoubtedly increases difficulties of network management for cloud computing.

As an emerging open network architecture, an SDN is different from a traditional architecture. It separates the control plane from the data plane and uses a centralized control mode. At the network layer of an SDN based cloud-industrial IoT system, sensors, terminals, communication modules, and gateways in industrial production are centrally managed through a southbound interface of an SDN controller. The network layer can exploit the plug-and-play technology to implement automatic deployment of devices. It can also support device security certification and operation functions such as condition monitoring and remote upgrade, so as to cope with management issues of numerous terminals in industrial applications. A user can also customize data transmission rules on a controller, which makes more flexible and intelligent industrial data transmission. Using SDN, network administrators can introduce new functions by simple software programs to achieve dynamic requirements of the industrial IoT.

An SDN based cloud-industrial IoT integrates a data plane and a control plane of SDN into the platform layer. In particular, a data plane is in charge of transmitting data packets from network facilities according to forwarding rules. A logically centralized and programmable controller in the control plane can obtain global network information so as to manage and configure networks and deploy new protocols. A controller in the control plane can use the southbound interface to make various forwarding rules for forwarding devices. The forwarding devices conduct forwarding or discarding of new coming data packets. A data link is established between applications and the control plane through a northbound interface. A typical SDN based cloud-industrial IoT is as shown in Figure 2.

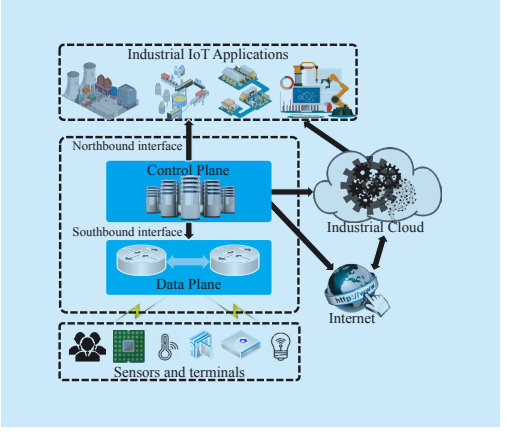


Fig. 2. *Architecture of SDN based cloud-industrial IoT.*

2.1.2 Blockchain-based cloud-industrial IoT

In an industrial IoT system, enterprises inevitably use cloud services provided by a third party to realize highly integrated industrial production. In the system, we can achieve a security certification between devices by using the blockchain technology and exploit the InterPlanetary file system (IPFS) as data encryption and distributed storage. In this case, although a cloud service provider obtains a data block, it cannot decrypt this block. And enterprises can continue to use third-party cloud services without worrying about data leakage. In addition, an enterprise can establish its private chain and only allow certified equipment to participate in the industrial production process to ensure production security.

In Figure 3, we provide an architecture of blockchain based cloud-industrial IoT. The cloud-based industrial IoT may bring risks of vulnerabilities and incompatibilities. Since cloud services use centralized authorization [22], it is a key issue to ensure data security and privacy. Using the blockchain technology, all data operations are transparent and permanently recorded. As a result, it is easy to establish trust between nodes and cloud service providers.

Compared with the centralized control mode of an SDN enabled cloud computing, blockchain has a typical distributed structure. In this case, it can effectively avoid the risk

of a single point failure. Using a public ledger in blockchain-based cloud- industrial IoT, all nodes on a chain can verify and store data, exploit a distributed node consensus algorithm to generate and update data, and use encryption to ensure security of data transmission and access. The application of blockchain technology in an industrial IoT system can guarantee the reliability of data sharing.

Due to utilizing powerful capabilities of computing and storage, either SDN-based or blockchain-based cloud-industrial IoT system can easily cope with massive data processing. Yet, cloud computing has to face constraints such as transmission bandwidth, latency, and limited terminal device energy. These constraints make it difficult to process data in real time in typical application scenarios, e.g. an automated guided vehicle in a smart factory. Thus, some works, introduced in the next subsection, investigate an industrial IoT system with edge computing.

2.2 Industrial IoT with edge computing

Although a cloud server with powerful computing and storage capabilities can perform highly complex calculations, it requires high bandwidth requirements and exists a significant amount of time delay. It is serious in an industrial IoT system with a large number of smart devices accessing [23]. Massive data generated by these smart devices occupy extremely high bandwidth to be transmitted to cloud servers. Also, the queuing of tasks not only causes delayed quality of service, but also increases burden of central servers. Accordingly, extensive researches integrate edge computing into industrial IoT.

Different from cloud computing, an industrial IoT system with edge computing decentralizes cloud functions to the edge of a network, i.e., data sources and terminals. It is a distributed system to integrate various functions of networking, computing, storage, and applications. It can satisfy key requirements of digitalization for an industrial IoT system in agile connection, real-time services, data optimization, and smart application. A typical industrial IoT model with edge computing is as shown in Figure 4.

In this architecture, industrial IoT devices exploit sensors to gather production information, devices states, and material data, and then upload these data to local servers rather than cloud servers. The local servers will filter and analyze data, split tasks, and schedule resources to feedback industrial control and increase productivity and save production costs. In essential, these local servers at an edge computing layer is an effective solution to enhance capabilities of cloud computing. For a simple task, we can directly compute on an independent node and return the corresponding result. For a complex task, using edge computing is to emphasize distributed cooperative computing, i.e., using multiple nodes to achieve crowdsourcing services. Using edge

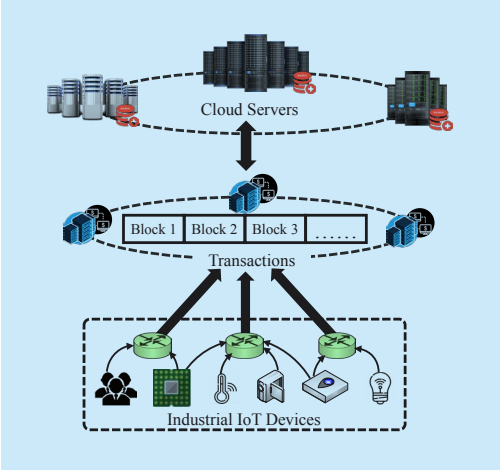


Fig. 3. *Architecture of blockchain based cloud-industrial IoT.*

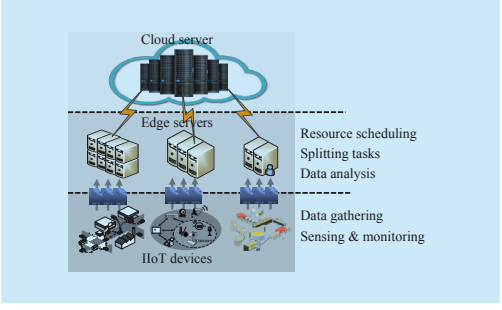


Fig. 4. *Architecture of Industrial IoT with edge computing.*

computing in an industrial IoT, massive raw data can be analyzed and processed at local servers without having to upload to the cloud. This can protect user sensitive data and reduce the risk of disclosing raw data of terminal devices.

Based on the distributed architecture, an edge-based industrial IoT has following advantages. First, in an industrial manufacturing scenario, we need to monitor and control devices in real-time. If we continue to upload gathered data to cloud servers, the time cost is relatively long and even causes major accidents. Thus, tasks should be done at the local of an industrial system to achieve real-time response. Second, it is difficult for network bandwidth to satisfy cloud-based transmission rates due to the exponential growth of data volume. Edge computing can process data at the edge of the industrial IoT, greatly saving transmission bandwidth, reducing network costs, and improving production efficiency. Third, it is more effective for an industrial IoT scenario with energy-constrained terminals by offloading computing tasks to an edge server rather than uploading to a cloud server [24]. Finally, data analysis and processing at an edge server can protect raw data from being intercepted or mined by competitors. In addition, we can use general interfaces on edge computing to deal with coexistence issues of devices and achieve security enhancement for different types of devices without managing complex large-scale cloud servers.

2.2.1 SDN based edge-industrial IoT

Although applications of edge computing further satisfy requirements of terminals and

Table I. *Privacy issues in a cloud-based industrial IoT architecture.*

Architecture	References	Privacy issues	Solutions	Essence of solutions
Only cloud-based industrial IoT	[28]	Privacy leakage when data classification	A multi-class support vector machine client-server protocol	Symmetric cryptosystem
	[29]	Privacy leakage during data search	A keyword search scheme using pairing-free multi-recipient certificateless encryption	Public key cryptosystem
	[30]	Privacy leakage of data stored in a cloud server	A certificateless searchable public key encryption scheme	Public key cryptosystem
	[31]	Privacy leakage during data outsourcing to a cloud server	Lightweight searchable public-key encryption with forward privacy	Public key cryptosystem
	[32]	Privacy leakage of image data on a cloud server	A secure local binary pattern descriptor extraction scheme	Order-preserving encryption local binary pattern
	[8][33]	Privacy leakage during data clustering	A tensor-based multiple clustering privacy protection algorithm or the SHOCFS algorithm	Symmetric cryptosystem
	[45]	Location leakage of location-based service	The EPQ scheme using encrypted location perturbation and homomorphic encryption	Symmetric cryptosystem
	[49]	Privacy leakage when smart devices share information	A biometrics-based authentication privacy protection scheme	Public key cryptosystem
SDN based cloud industrial IoT	[34]	Privacy leakage during cross-domain routing optimization	Cross-domain routing optimization protocol	Symmetric cryptosystem
	[35]	Privacy leakage for end-to-end QoS implementation	The PRIME-Q scheme	Adaptive learning
Blockchain based cloud industrial IoT	[36]	Data leakage of transaction verification	A decentralized attribute-based encryption scheme	Public key cryptosystem
	[37]	Privacy leakage when using keywords search over encrypted data	A bloom filter-enabled multi-keyword search protocol	Symmetric cryptosystem
	[38]	Privacy leakage during data outsourcing to a cloud server	A privacy preserving tucker train decomposition based on gradient descent	Symmetric cryptosystem Tensor train theory

improve QoS of cloud computing, it still faces challenges in practical applications, e.g., limited edge resources and energy, network scalability, and privacy protection. The introduction of edge computing also complicates the management of an industrial IoT system and puts forward new demands for a management system.

Using inherent features of SDN, edge computing can maximize its potential in applications of an industrial IoT system. An SDN controller can achieve data flow management and service orchestration. This process is transparent to all terminals [25]. In addition, using SDN in an edge-industrial IoT system can simplify network management, improve network capabilities and promote network virtualization. An SDN enabled edge-industrial IoT utilize available resources efficiently based on control mechanisms to reduce the complexity of edge computing implementation. Because a network control capability is on an SDN controller, it can perform complex network operations, such as the formulation of packet forwarding rules. As a result, an SDN for edge-industrial IoT system can reduce the load of edge servers and improve QoS of industrial systems.

2.2.2 Blockchain based edge-industrial IoT

In a distributed industrial IoT system with scattered devices and complex environments, edge devices with weak computing abilities are prone to data leakage and difficult to achieve self-security protection. Similar to the blockchain-based cloud-industrial IoT system, we can exploit characteristics of blockchain, such as distributed data storage, point-to-point transmission, consensus mechanism, and encryption, to solve security and privacy issues of edge computing enabled industrial IoT. By integrating blockchain into an edge-industrial IoT system, we can provide reliable access and control for networking, storage and computation of massive distributed edge nodes [26].

The combination of edge computing and blockchain technology can achieve complementary advantages. Decentralized storage and management mode of blockchain make up for shortcomings of edge computing in storage and device management capabilities, while edge computing provides real-time computation. The joint of both provides the ability to solve heterogeneity of industrial IoT systems. This will promote the development of industrial production towards intelligent manufacturing.

2.3 Privacy issues in an industrial IoT system

Although a general IoT system and an industrial IoT system have many common technologies, they are used for different purposes. Admittedly, both general IoT and industrial IoT have privacy leakage issues. In a general IoT system, it may cause a trouble for human's lives rather than occurring an emergency situation if there is a privacy leakage problem [27]. However, for an industrial IoT scenario, it emphasizes integration and interconnection of factories and machines so as to provide more efficient production. Due to the heterogeneity of communication protocols and data generated by devices, data processing becomes extremely complicated. Also, privacy leakage is easy to occur during this process. Thus, it is particularly important to protect privacy in an industrial IoT application.

In this section, we propose privacy leakage issues under different industrial IoT architectures, especially in applying SDN and blockchain technologies in either the cloud-based industrial IoT architecture or the edge-based industrial IoT architecture. These privacy issues involve data privacy, location privacy, query method privacy, and identity privacy of network entities.

- **Data privacy**: Data is an important resource in the IoT era. For an industrial IoT system, one can obtain much valuable information through data mining, such as device operating states, rates of return, and manufacturing status [12, 28-44]. Therefore, all kinds of data generated in an industrial IoT system are vulnerable to hackers' attack. The leakage of data privacy will

cause severe economic losses to all walks of life.

- **Location privacy**: This refers to the leakage of nodes' location when using network services. Private location information of an entity in either cloud systems or edge systems is not willing to be accessed to other nodes, including a server or even the entity's friends. When the location information is disclosure, others can track the entity without authorization [13, 45-47].
- **Query methods and identity privacy**: The data integrity verification process and the query process may involve privacy leakage of query methods and ranges. In addition, a node may also suffer malicious privacy interception or eavesdropping when participating in network activities, and resulting in the disclosure of identity information [49-52].

In general, there exist a series of privacy issues for the cloud-based industrial IoT architecture. For example, private information may be disclosed when clustering and searching nodes raw data; location privacy may be leaked when a cloud server provides location-based services; and node's identity privacy is also leaked when sharing data with other nodes. Table I lists privacy issues that exist in the cloud based industrial IoT architecture, including an SDN enabled cloud system and blockchain based cloud Industrial IoT. According to Table I, we divide privacy issues existing in the cloud-based industrial

Table II. *Privacy issues in an edge-based industrial IoT architecture.*

Architecture	References	Privacy issues	Solutions	Essence of solutions
Only edge-based industrial IoT	[39]	Privacy leakage during data aggregation in edge computing	A lightweight privacy protection data aggregation scheme based on signature technology, Paillier homomorphic encryption, and double trapdoor chameleon hash function	Symmetric cryptosystem Hash function
	[40]	Privacy leakage during resource allocation at edge nodes	A privacy protection resource allocation scheme using contributory public key searchable encryption	Public key cryptosystem
	[51]	Privacy of data and query methods when verifying integrity of edge data	ICE protocol	Public key cryptosystem
	[52]	Privacy of data and query range when performing data query	A privacy protection range query scheme based on range query expression, decomposition, composition, and BGN homomorphic encryption	Symmetric cryptosystem
	[42]	Location data leakage in an edge server	The privacy-preserving scheme against poisoning attacks	Feature learning model
	[48]	Data privacy leakage during transmission	A lightweight privacy-preserving communication protocol	Symmetric cryptosystem
	[46][47]	Privacy for location-based services	An irreversible elliptic random obfuscation function scheme Paillier encryption and Diffie-Hellman key agreement	Public key cryptosystem
SDN based edge industrial IoT	[41]	Privacy leakage in cross-domain attack detection in SDN	A perturbed encryption and K-nearest neighbor algorithm	Public key cryptosystem KNN algorithm
	[43]	Content and filtering rules leakage in deep packet filtering	A privacy protection DPF protocol	One-way hash function
Blockchain based edge industrial IoT	[44]	Privacy leakage in reputation management scheme in mobile crowdsensing	A two-phase reputation update scheme based on additive secret sharing	Additive blinding secret sharing Public blockchain
	[50]	Identity and location privacy in blockchain-edge computing	A privacy enhancement scheme based on an elliptic curve encryption system	Public key cryptosystem

IoT architecture into three situations: 1) Privacy issues for cloud-based Industrial IoT (not involving SDN and blockchain technologies); 2) Cloud-based industrial IoT involving SDN; and 3) Cloud-based industrial IoT involving blockchain. We point out the privacy issues in these three cases, respectively.

Similarly, privacy issues existing in the edge-based industrial IoT architecture are also divided into three scenarios, including a typical edge-based industrial IoT system, an SDN enabled edge Industrial IoT system and an edge Industrial IoT system with blockchain. We also indicate privacy issues in these three scenarios in Table II. In the first scenario, private information may be leakage when data aggregation and query of edge servers as well as resource allocation of edge nodes. In the second one, privacy leakage may be occurred when cross-domain collaboration in an SDN environment. Third, when blockchain is applied to an edge-based industrial IoT architecture, there are also leakage issues of data privacy, node's identity privacy, and location privacy.

Privacy leakage in an industrial IoT system is a major challenge for the security of intelligent manufacturing processes in factories. From terminal equipment, transmission links to cloud platforms where data is stored and processed, malicious competitors may use private data to infer factory production information, or even steal factory secret files to carry out targeted advanced persistent threat attacks. Thus, privacy leakage should weaken the security of the entire manufacturing process and make an enterprise suffer severe economic losses.

III. Privacy Preserving in Industrial IoT

In this section, we provide existing privacy preserving solutions in both cloud- and edge-based industrial IoT architectures, which are summarized in Table I and Table II. It can be seen that no matter what kind of architectures, these solutions can be analyzed from the aspects of data privacy preserving, location privacy preserving, and query and identity privacy preserving. We will elaborate on these in the following subsections.

3.1 Data protection strategies

In this subsection, we review solutions of data privacy protection in an industrial IoT system, and introduce key technologies involved in the implementation of each solution in detail.

In [28], the authors aim to prevent leakage of data samples uploaded by clients and that of training datasets at a classification server. Combining with Paillier homomorphic encryption technology, they proposed a privacy protection multi-class support vector machine data classification method to protect privacy of cloud outsourced data classification. To cope with a privacy issue in the cloud storage data search process, the authors presented a keyword search scheme using pairing-free multi-recipient certificate-less encryption in [29]. This scheme can protect data from leaking during the cloud retrieval process and effectively defend against keyword guessing attacks. In [30], the authors proposed a certificateless searchable public key encryption scheme to solve the privacy leakage of data stored in a cloud server. To cope with a privacy issue during data outsourcing to a cloud server, the authors presented a lightweight searchable public-key encryption with a forward privacy method in [31]. In [32], the authors proposed a secure local binary pattern descriptor extraction scheme to protect the privacy of image data stored in cloud servers. This scheme can ensure the image data confidentiality. For privacy issues of clustering data in a typical cloud industrial IoT, [12] and [33] proposed different solutions. In [12], the authors designed a tensor-based multiple clustering privacy protection algorithm. This algorithm can ensure a public cloud only knows encrypted data and encrypted clustering results, while a private cloud can only obtain a perturbed cipher text instead of an original text after decryption. In this case, this method can protect privacy of source data. The work of [33]

proposed a secure high-order clustering algorithm. This algorithm can fast search density peaks on a hybrid cloud industrial IoT system. Using the proposed algorithm, it can encrypt data before it is outsourced to a cloud and not expose private information when performing big data clustering in a cloud system. In an SDN enabled cloud industrial IoT system, the work of [34] designed a cryptography- based privacy preserving scheme for cross-domain routing optimization. The authors of [35] provided a PRIME-Q scheme for a multi-domain SDN industrial IoT. The scheme distributively processes data and then makes a binary decision. In addition, [36] exploited blockchain to design a decentralized attribute-based encryption scheme. It can prevent data leakage when verifying transactions. The authors in [37] proposed a bloom filter-enabled multi-keyword search protocol over encrypted data to solve privacy leakage. In [38], the authors proposed a privacy preserving tucker train decomposition method based on gradient descent. It can protect privacy during data outsourcing to the cloud.

In an edge-based industrial IoT scenario, there also exist many works to deal with privacy issues. In [39], the authors used the signature technology, Paillier homomorphic encryption, and the double trapdoor chameleon hash function to design a lightweight protection scheme. This scheme can prevent an edge server from obtaining node's private data during data aggregation. Using contributory public key searchable encryption, the work of [40] proposed a resource allocation scheme with privacy protection. It can protect terminal data when allocating resource to edge

Table III. *Comparison of privacy performance and complexity in cloud-based industrial IoT.*

References	Solutions	Privacy performance	Complexity
[12]	A tensor-based multiple clustering privacy protection algorithm	Achieve source data confidentiality Achieve data clustering results confidentiality	$O(n^2)$
[28]	A multi-class support vector machine client-server protocol	Achieve data confidentiality during classification process Achieve confidentiality of classification training dataset and classification parameters	$O(n)$
[29]	A keyword search scheme using pairing-free multi-recipient certificateless encryption	Achieve data information confidentiality Respond to keyword guessing attacks	$O(n)$
[30]	Certificateless searchable public key encryption scheme	Achieve data confidentiality Defend against chosen keyword attack	$O(n)$
[31]	Lightweight searchable public-key encryption with forward privacy	Achieve forward privacy and chosen-keyword attack resilient	$O(n)$
[32]	A secure local binary pattern descriptor extraction scheme	Achieve image data confidentiality and eliminate the possible collusion threat	$O(n^2)$
[33]	The SHOCFS algorithm	Achieve data confidentiality Achieve data clustering results confidentiality	$O(n^2)$
[34]	Cross-domain routing optimization protocol	Achieve forwarding rules confidentiality among domains	$O(n)$
[35]	The PRIME-Q scheme	Achieve sharing data confidentiality and security among domains	$O(n)$
[36]	A decentralized attribute-based encryption scheme	Achieve transaction data confidentiality	$O(n)$
[37]	A bloom filter-enabled multi-keyword search protocol	Achieve encrypted data security	$O(n)$
[38]	A privacy preserving tucker train decomposition based on gradient descent	Achieve data confidentiality Achieve data integrity	$O(n)$
[45]	The EPQ scheme using encrypted location perturbation and homomorphic encryption	Achieve user's query location confidentiality	$O(n^2)$
[49]	A biometrics-based authentication privacy protection scheme	Achieve user's anonymity and untraceability	$O(n)$

nodes. Facing increased privacy issues in SDN enabled edge industrial IoT, the work in [41] proposed a privacy protection detection method to protect data privacy during cross-domain attack detection. This method is designed based on perturbed encryption and the K-nearest neighbor algorithm. In [42], the authors presented a privacy-preserving scheme against poisoning attacks. This scheme designed a feature learning model to protect location privacy in an edge server. Then, the authors of [43] presented a deep packet filtering protocol with privacy protection. The protocol can effectively prevent privacy leakage because of using an oblivious transfer protocol and an encrypted one-way hash chain. In addition, the work of [44] used the two-phase reputation update scheme based on additive secret sharing. It effectively solves the problem of privacy leakage in the data sensing process caused by the blockchain application for the edge-based industrial IoT architecture.

3.2 Location protection strategies

In general, two main methods are used to protect location information, i.e., obfuscation and encryption. Here, we summary protection solutions for location privacy issues in the cloud- and edge-based industrial IoT architecture, respectively.

For the cloud-based industrial IoT architecture, the authors in [45] proposed an EPQ scheme using encrypted location perturbation and homomorphic encryption to ensure privacy of users' query locations. For the edge-based industrial IoT architecture, the authors used an irreversible elliptic random obfuscation function algorithm in [46] to ensure that a node can enjoy location-based services without leaking the original location to an Internet service provider. In [47], the authors exploited Paillier encryption and the Diffie-Hellman key agreement to protect location. This work can hide the real location and also effectively resist location privacy attacks inside and outside of a network. The authors in [48] presented a lightweight communication protocol based on symmetric cryptosystem to protect location privacy during transmission process.

3.3 Query and identity protection strategies

For a cloud-based industrial IoT architecture, the authors in [49] proposed a biometrics-based authentication privacy protection scheme. The scheme supports user's biometric information update and is anonymous and untraceable. For an edge-based industrial IoT architecture, the authors proposed a privacy enhancement scheme based on an elliptic curve encryption system in [50]. It can ensure the integrity of blockchain transactions and the anonymity and untraceability of users. In [51], the authors proposed an integrity check protocol. The protocol can allow the third party to check data integrity while ensuring that the privacy of user query methods is not leaked to the third party. In addition, the authors in [52] proposed a privacy protection range query scheme based on range query expression, decomposition, composition, and BGN homomorphic encryption. It can protect privacy of a user's query range when performing data query.

IV. Evaluation and Discussion

In this section, we compare the privacy performance and the computational complexity of existing privacy solutions in detail.

4.1 Analysis of privacy protection performance

We first analyze privacy performance of the existing privacy preserving solutions in either a cloud- or an edge-based industrial IoT architecture.

In Table III and Table IV, we provide performance comparison of privacy protection algorithms for the above system architectures, respectively. It can be seen that privacy issues in a cloud- or an edge-based industrial IoT architecture can be effectively solved by conducting various privacy protection measures. In particular, the use of the above methods is different for various application scenarios. We

will elaborate on the privacy protection methods in different application scenarios.

For the cloud-based industrial IoT architecture, the multi-class SVM client-server protocol applied in the data classification process has two advantages. It can achieve data confidentiality uploaded by a client during classification process and implement confidentiality of classification training dataset and parameters. For data retrieval process, the keyword search scheme can prevent keyword guessing attacks. During data clustering, the tensor-based multiple clustering scheme and the SHOCFS algorithm can achieve confidentiality of both source raw data and data clustering results. For data stored in a cloud server, the certificateless searchable public key encryption scheme can achieve data confidentiality and defend against the chosen keyword attack. During the process of data outsourcing to the cloud, the lightweight searchable public-key encryption with a forward privacy method and the secure local binary pattern descriptor extraction scheme can achieve data confidentiality, but the latter focuses on the privacy of image data. In an SDN cloud-industrial IoT scenario, the cross-domain routing optimization protocol in the network layer can achieve rules confidentiality among domains and the PRIME-Q scheme applied in end-to-end QoS implementation can achieve sharing data confidentiality and security. For a blockchain system, the decentralized attribute-based encryption scheme used in transaction verification can achieve transaction confidentiality. The bloom filter-enabled multi-keyword search protocol applied for encrypted data search can implement encrypted data security. The privacy preserving tucker train decomposition based on gradient descent can achieve data confidentiality and integrity. In addition, the EPQ scheme can achieve query location confidentiality. The biometrics-based authentication privacy protection scheme can provide

Table IV. *Comparison privacy performance and complexity in edge-based industrial IoT.*

References	Solutions	Privacy performance	Complexity
[39]	A lightweight privacy protection data aggregation scheme	Achieve nodes' private information confidentiality	$O(n)$
[40]	A privacy protection resource allocation scheme using contributory public key searchable encryption	Achieve mete-data privacy security Achieve attacks resistance even if the private key of the edge node is destroyed	$O(n)$
[41]	A perturbed encryption and K-nearest neighbor algorithm	Prevent privacy leakage of each network domain when performing cross-domain attack detection	$O(n)$
[42]	The privacy-preserving scheme against poisoning attacks	Achieve location information confidentiality Prevent poisoning attacks	$O(n)$
[43]	A privacy protection DPF protocol	Achieve data and filtering rules security	$O(n)$
[44]	A two-phase reputation update scheme based on additive secret sharing	Achieve perceived aggregation results confidentiality Prevent users from injecting malicious information into the system	$O(n)$
[46]	An irreversible elliptic random obfuscation function scheme	Achieve original location information confidentiality when providing location-based services	$O(n^{1/2})$
[47]	Paillier encryption and Diffie-Hellman key agreement	Achieve location data confidentiality Achieve location privacy attacks resistance inside and outside the network	$O(n)$
[48]	A lightweight privacy-preserving communication protocol	Achieve location confidentiality	$O(n)$
[50]	A privacy enhancement scheme based on an elliptic curve encryption system	Achieve transactions integrity and user's anonymity and untraceability	$O(n)$
[51]	ICE protocol	Achieve query methods confidentiality	$O(n^{5/3})$
[52]	A privacy protection range query scheme	Achieve query range confidentiality Achieve terminal devices' data confidentiality	$O(n^2)$

anonymity and untraceability of nodes in cloud-industrial IoT.

In the edge-based IoT architecture, the lightweight privacy protection data aggregation scheme can achieve nodes' private information confidentiality. The privacy protection resource allocation scheme can achieve mete-data privacy security and attacks resistance even if the private key of an edge node is destroyed. The lightweight privacy-preserving communication protocol can achieve data confidentiality during transmission process. In SDN enabled edge-based IoT, the DPF protocol can achieve data and filtering rules security. The scheme based on perturbed encryption and K-nearest neighbor algorithm in cross-domain attack detection has the advantage of preventing privacy leakage of each network domain. For blockchain enabled edge computing, the privacy enhancement scheme can implement transactions integrity and user's anonymity and untraceability. The two-phase reputation update scheme in mobile crowdsensing can achieve perceived data and aggregation results confidentiality. It also can prevent users from injecting malicious information into the system. During data query process, using the ICE protocol can achieve a secure query method. And the privacy protection range query scheme can be used to protect the query range and achieve terminal devices' data confidentiality. In addition, for location privacy, the obfuscation function algorithm can implement original location information confidentiality when providing location-based services. And the Paillier encryption solution can not only protect private location information but also achieve location privacy attacks resistance inside and outside the network. The privacy-preserving scheme against poisoning attacks can achieve location information confidentiality and prevent poisoning attacks.

4.2 Computational complexity comparison

Computational complexity refers to the amount of resources required for a task, including time resources and memory resources. It is an important criterion to analyze and assess the kinds of resources that are needed for the task. In this subsection, we compare the computational complexity of the typical privacy protection algorithms summarized above, as shown in Table III for a cloud industrial IoT system and Table IV for an edge industrial IoT system, respectively.

It can be seen from Table III that the complexity of the tensor-based multiple clustering privacy protection algorithm and the SHOCFS algorithm for the data clustering process have reached $O(n^2)$. These two methods protect privacy by encrypting data before it is outsourced to a cloud. And the complexity of the secure local binary pattern descriptor extraction scheme for image data privacy has also reached $O(n^2)$. Similarly, the complexity of the EPQ scheme for location privacy is also $O(n^2)$, while that of other privacy protection algorithms is $O(n)$. Yet, these methods focus on different scenarios, including classification, retrieval, cross-domain collaboration in an SDN environment, the process of data outsourcing to the cloud, transaction verification and encrypted data search on the blockchain, and the identity authentication process.

In Table IV, similarly, computational complexity of the ICE protocol is $O(n^{5/3})$ to protect privacy during data query. The privacy protection range query scheme based on range query expression, decomposition, composition, and BGN homomorphic encryption has reached $O(n^2)$. It is slightly higher than the ICE protocol. For location privacy preserving, the computational complexity of the irreversible elliptic random obfuscation function algorithm is $O(n^{1/2})$, and that of the protection algorithm based on Paillier encryption and Diffie-Hellman key agreement and the lightweight communication protocol based on symmetric cryptosystem have reached $O(n)$. In addition, the complexity of other privacy protection methods is $O(n)$. Similarly, their application scenarios are also different, including data aggregation, data transmission, resource allocation, deep packet filtering and cross-domain attack detection in an SDN environment,

and user authentication and reputation management scheme in mobile crowdsensing on blockchain.

V. Open Issues

As discussed in Section III, we have reviewed a series of solutions for different privacy issues. However, we noted that there are several limitations in a cloud- or an edge-based industrial IoT system, including integration with SDN and blockchain. In this section, we discuss open research issues for an industrial IoT system from different aspects.

5.1 Low complexity outsourcing privacy

In the application of industrial IoT, it is necessary to outsource data generated by industrial devices to the cloud through a network. Using the capabilities of powerful data calculation and storage of a loud computing platform, we can conveniently analyze data and finally achieve high-quality services. However, it is vulnerable to illegal hijacking by malicious nodes for valuable industrial data during the process of outsourcing data to a public cloud system. This may result in serious privacy leakage. Therefore, outsourced data privacy preservation remains a challenge for both cloud- and edge-based industrial IoT. In addition, the workload of a cloud system may be substantial growth because the volume of data that needs to be processed is increasing in the future. This also reduces the quality of service of cloud-based applications. In order to efficiently process outsourced data in a cloud system, we need to design a feasible algorithm to reduce the complexity of data secure computing, so as to reduce computing time and cloud workload.

5.2 Privacy preserving with energy constraints

Energy constraints of an IoT device have always been an important factor affecting service quality. It is especially important for an edge-based industrial IoT system. Although an application of edge-industrial IoT can effectively solves a series of issues such as cloud computing delay and transmission bandwidth, edge nodes with low energy require a lightweight privacy preserving scheme when performing data aggregation on edge nodes. Its purpose is to extend the working life cycle of an edge device by reducing computation energy consumption. As a result, it is an important open issue to study how to design an excellent privacy protection algorithm for an edge node subjected to energy constraints.

5.3 Nodes mobility in an industrial IoT system

In an industrial IoT system, the mobility of a device node is a bottleneck to be solved [53]. Although using a mobile device can effectively address shortcomings of terminal location restrictions in an actual industrial production activity, it may seriously threaten user privacy. For example, engineers can access an industrial network through a mobile terminal and gather real-time production data. Using these gathered data, engineers can monitor and control the operation of a processing line through an edge computing or cloud computing platform. However, due to the openness nature of a wireless network and the freedom of a mobile terminal when accessing the industrial network, it is vulnerable to attacks by malicious nodes during the data transmission process. An eavesdropper can infer and then reveal users' location information based on the location of a requested service. Furthermore, it can illegally obtain and mine factory production and management information based on the wiretapped data. This seriously damages interests of an enterprise. Therefore, while enjoying the increased production efficiency of using mobile devices, we still need to solve data and location privacy leakage issues caused by mobile devices access to an industrial IoT system.

5.4 Privacy in 5G-enabled industrial IoT

The 3GPP has defined three major scenarios

for 5G applications, i.e., enhanced mobile broadband (eMBB), massive machine type of communications (mMTC), and ultra-reliable and low latency communications (URLLC). These the technical standards may well satisfy related requirements of a communication system in an industrial field [54]. In 5G-enabled industrial IoT, the widely existing sensors are gathering data of production or manufacturing execution at all times. These data are stored, transmitted, and processed in a complicated and heterogeneous network interacted by multiple access technologies, multiple terminals, and multiple participants. It may cause private data to be scattered in all corners of a network and finally make privacy leakage. In addition, although the virtualization technology used in 5G can achieve flexible and controllable wireless network, it may also blur boundaries of network security. When multiple users share cloud computing resources, users' private data is more vulnerable to attacks and leaks. Therefore, we still need to solve the privacy and security issues when exploiting 5G technologies in an Industrial IoT system, so as to reduce the risk of privacy leakage.

VI. Conclusion

In this paper, we make a comprehensive overview of privacy issues and the related solutions for either the cloud- and edge-based industrial IoT architecture. According to the different types of privacy issues, we investigate the privacy issues from the aspects of data, location, identity and query. In addition, we compared the computational complexity and the privacy protection performance of various privacy solutions under these two architectures. As a result, we can understand clearly the advantages and disadvantages of each method. At the end of our work, we provide open issues that remain in current studies. We want this survey can serve as useful references and valuable guidelines for further privacy investigation on an industrial IoT system.

Acknowledgement

We are very grateful to all reviewers who have helped improve the quality of this paper. This work was partially supported by the National Natural Science Foundation of China (Grant No. 61871023 and 61931001) and Beijing Natural Science Foundation (Grant No. 4202054).

References

[1] D. Wang, "An enterprise data pathway to industry 4.0," *IEEE Engineering Management Review*, vol. 46, no. 3, 2018, pp. 46-48.

[2] 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, 2020, pp. 766-775.

[3] W. Yu, T. Dillon, F. Mostafa, W. Rahayu, and Y. Liu, "A global manufacturing big data ecosystem for fault detection in predictive maintenance," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, 2020, pp. 183-192.

[4] 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, 2020, pp. 968-979.

[5] X. Zheng, Z. Cai, J. Yu, C. Wang, and Y. Li. "Follow but no track: Privacy preserved profile publishing in cyber-physical social systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, 2017, pp. 1868-1878.

[6] Z. Cai and Z. He, "Trading private range counting over big IoT data," *Proc. IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 2019, pp. 144-153.

[7] Y. Liang, Z. Cai, J. Yu, Q. Han, and Y. Li, "Deep learning based inference of private information using embedded sensors in smart devices," *IEEE Network*, vol. 32, no. 4, 2018, pp. 8-14.

[8] H. Hui, C. Zhou, S. Xu, and F. Lin, "A novel secure data transmission scheme in industrial internet of things," *China Communications*, vol. 17, no. 1, 2020, pp. 73-88.

[9] 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, 2018, pp. 55-61.

[10] F. Lin, Y. Zhou, X. An, I. You, and K. Choo, "Fair resource allocation in an intrusion-detection system for edge computing: ensuring the security of internet of things devices," *IEEE Consumer Electronics Magazine*, vol. 7, no. 6, 2018, pp. 45-50.

[11] Y. Huo, C. Yong, and Y. Lu, "Re-ADP: Real-time data aggregation with adaptive ω-event dif-

ferential privacy for fog computing," *Wireless Communications and Mobile Computing*, vol. 2018, 2018, pp.1-13.
[12] Y. Zhao, L. T. Yang, and J. Sun, "Privacy-preserving tensor-based multiple clusterings on cloud for industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 4, 2019, pp. 2372-2381.
[13] Y. Huo, C. Hu, X. Qi, and T. Jing, "LoDPD: A location difference-based proximity detection protocol for fog computing," *IEEE Internet of Things Journal*, vol. 4, no. 5, 2017, pp. 1117-1124.
[14] 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, 2019, pp. 6492-6499.
[15] J. Mao, W. Tian, J. Jiang, Z. He, Z. Zhou, and J. Liu, "Understanding structure-based social network de-anonymization techniques via empirical analysis," *EURASIP Journal Wireless Communications and Networking*, vol. 2018, 2018, pp. 279.
[16] 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, 2020, pp. 4242-4251.
[17] Z. Xiong, W. Li, Q. Han, and Z. Cai, "Privacy-preserving auto-driving: A GAN-based approach to protect vehicular camera data," *Proc. IEEE International Conference on Data Mining (ICDM)*, 2019, pp. 668-677.
[18] L. Zhang, Z. Cai, and X. Wang, "FakeMask: A novel privacy preserving approach for smartphones," *IEEE Transactions on Network and Service Management*, vol. 13, no. 2, 2016, pp. 335-348.
[19] L. Yu, H. Shen, K. Sapra, L. Ye, and Z. Cai, "CoRE: cooperative end-to-end traffic redundancy elimination for reducing cloud bandwidth cost," *IEEE Transactions on Parallel and Distributed Systems*, vol. 28, no. 2, 2017, pp. 446-461.
[20] J. Mao, Y. Zhang, P. Li, T. Li, Q. Wu, and J. Liu, "A position-aware Merkle tree for dynamic cloud data integrity verification," *Soft Computing*, vol.21, no.8, 2017, pp.2151-2164.
[21] M. Wang, J. Liu, J. Mao, H. Cheng, J. Chen, and C. Qi, "RouteGuardian: Constructing secure routing paths in software-defined networking," *Tsinghua Science and Technology*, vol. 22, no. 4, 2017, pp. 400-412.
[22] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," *Proc. The 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, 2017, pp. 468-477.
[23] C. Gong, F. Lin, X. Gong, and Y. Lu, "Intelligent cooperative edge computing in the internet of things," *IEEE Internet of Things Journal*, 2020, pp.1-1.
[24] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, 2016, pp. 637-646.
[25] A. C. Baktir, A. Ozgovde, and C. Ersoy, "How can edge computing benefit from software-defined networking: A survey, use cases, and future directions," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, 2017, pp. 2359-2391.
[26] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, 2019, pp. 1508-1532.
[27] 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, 2018, pp. 577-590.
[28] Y. Rahulamathavan, R. C. Phan, S. Veluru, K. Cumanan, and M. Rajarajan, "Privacy-preserving multi-class support vector machine for outsourcing the data classification in cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 5, 2014, pp. 467-479.
[29] Y. Lu, J. Li, and Y. Zhang, "Privacy-preserving and pairing-free multirecipient certificateless encryption with keyword search for cloud-assisted IIoT," *IEEE Internet of Things Journal*, vol. 7, no. 4, 2020, pp. 2553-2562.
[30] M. Ma, D. He, N. Kumar, K. R. Choo, and J. Chen, "Certificateless searchable public key encryption scheme for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, 2018, pp. 759-767.
[31] B. Chen, L. Wu, N. Kumar, K. R. Choo, and D. He, "Lightweight searchable public-key encryption with forward privacy over IIoT outsourced data," *IEEE Transactions on Emerging Topics in Computing*, 2019, pp. 1-13.
[32] Z. Xia, L. Jiang, X. Ma, W. Yang, P. Ji, and N. N. Xiong, "A privacy-preserving outsourcing scheme for image local binary pattern in secure industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 1, 2020, pp. 629-638
[33] Y. Zhao, L. T. Yang, and J. Sun, "A secure high-order cfs algorithm on clouds for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, 2018, pp. 3766-3774.
[34] Q. Chen, S. Shi, X. Li, C. Qian, and S. Zhong, "SDN-based privacy preserving cross domain routing," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 6, 2019, pp. 930-943.
[35] K. D. Joshi and K. Kataoka, "PRIME-Q: Privacy aware end-to-end QoS framework in multi-domain SDN," *Proc. 2019 IEEE Conference on Net-*

work Softwarization (NetSoft), 2019, pp. 169-177.

[36] Y. Rahulamathavan, R. C. Phan, M. Rajarajan, S. Misra and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," *Proc. IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2017, pp. 1-6.

[37] S. Jiang, J. Cao, J. A. McCann, Y. Yang, Y. Liu, X. Wang, and Y. Deng, "Privacy-preserving and efficient multi-keyword search over encrypted data on blockchain," *Proc. IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 405-410.

[38] J. Feng, L. T. Yang, R. Zhang, and B. S. Gavuna, "Privacy preserving tucker train decomposition over blockchain-based encrypted industrial iot data," *IEEE Transactions on Industrial Informatics*, 2020, pp. 1-10.

[39] J. Zhang, Y. Zhao, J. Wu, and B. Chen, "LPDA-EC: A lightweight privacy-preserving data aggregation scheme for edge computing," *Proc. IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2018, pp. 98-106.

[40] L. Zhang and J. Li, "Enabling robust and privacy-preserving resource allocation in fog computing," *IEEE Access*, vol. 6, 2018, pp. 50384-50393.

[41] L. Zhu, X. Tang, M. Shen, X. Du, and M. Guizani, "Privacy-preserving DDoS attack detection using cross-domain traffic in software defined networks," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, 2018, pp. 628-643.

[42] P. Zhao, H. Huang, X. Zhao, and D. Huang, "P^3: Privacy-preserving scheme against poisoning attacks in mobile-edge computing," *IEEE Transactions on Computational Social Systems*, vol. 7, no. 3, 2020, pp. 818-826.

[43] Y. Lin, S. Shen, M. Yang, D. Yang, and W. Chen, "Privacy-preserving deep packet filtering over encrypted traffic in software-defined networks," *Proc. IEEE International Conference on Communications (ICC)*, 2016, pp. 1-7.

[44] K. Zhao, S. Tang, B. Zhao, and Y. Wu, "Dynamic and privacy-preserving reputation management for blockchain- based mobile crowdsensing," *IEEE Access*, vol. 7, 2019, pp. 74694-74710.

[45] H. Zhu, R. Lu, C. Huang, L. Chen, and H. Li, "An efficient privacy-preserving location-based services query scheme in outsourced cloud," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 9, 2016, pp. 7729-7739.

[46] C. Naik, M Siddhartha, J. P. Martin, and K. Chandrasekaran, "Location privacy using data obfuscation in fog computing," *Proc. IEEE Region 10 Conference (TENCON)*, 2019, pp. 1286-1291.

[47] X. Zhu, Y. Lu, X. Zhu, and S. Qiu, "A location privacy-preserving protocol based on homomorphic encryption and key agreement," *Proc. International Conference on Information Science and Cloud Computing Companion*, 2013, pp. 54-59.

[48] X. Luo, L. Yin, C. Li, C. Wang, F. Fang, C. Zhu, and Z. Tian, "A lightweight privacy-preserving communication protocol for heterogeneous IoT environment," *IEEE Access*, vol. 8, 2020, pp. 67192-67204.

[49] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues, "Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment," *IEEE Internet of Things Journal*, vol. 5, no. 6, 2018, pp. 4900-4913.

[50] B. Ernest, J. Shiguang, "Privacy enhancement scheme (PES) in a blockchain-edge computing environment," *IEEE Access*, vol. 8, 2020, pp. 25863-25876.

[51] W. Tong, B. Jiang, F. Xu, Q. Li, and S. Zhong, "Privacy-preserving data integrity verification in mobile edge computing," *Proc. IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, 2019, pp. 1007-1018.

[52] R. Lu, "A new communication-efficient privacy- preserving range query scheme in fog-enhanced IoT," *IEEE Internet of Things Journal*, vol. 6, no. 2, 2019, pp. 2497-2505.

[53] S. Wang, A. Zhou, M. M. Komarov, and S. S. Yau, "Services and communications in fog computing," *China Communications*, vol. 14, no. 11, 2017, pp. iii-iv.

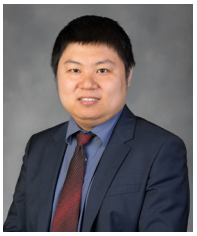
[54] J. Zhang, W. Xie, F. Yang, and Q. Bi, "Mobile edge computing and field trial results for 5G low latency scenario," *China Communications*, vol. 13, no. 2, 2016, pp. 174-182.

Biographies

Yan Huo, received the B.E. and Ph.D. degrees in Communication and Information System from Beijing Jiaotong University, Beijing, China, in 2004 and 2009 respectively. He has been a faculty member of School of Electronics and Information Engineering at Beijing Jiaotong University since 2011, where he is currently a professor. His major research interests include wireless communication theory, physical layer security, security and privacy, and signal processing. He is a senior member of IEEE. Email: yhuo@bjtu.edu.cn

Chun Meng, received the B.E. degree in School of Computer and Information Engineering from Henan Normal University, Xinxiang, China, in 2019. He is a master student at Shu Hua Wireless Network and Informa-

tion Perception Center in Beijing Jiaotong University. His research interests are industrial IoT security and privacy, edge computing.



Ruinian Li, is currently an assistant professor in the department of computer science at BGSU (Bowling Green State University). Before joining BGSU, Dr. Li earned his Ph.D degree of computer science from the George Washington University in 2018. His research interests include security and privacy-preserving computations, applied cryptography and Blockchain technology. He has been working in a wide area of social networks, auction systems and Internet of Things, and his work has been published at top-tier journals such as IoT journal, IEEE Transactions on Services Computing, and IEEE Transactions on Network Science and Engineering.

Tao Jing, received his M.S. and Ph.D. degree in Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, in 1994 and 1999, respectively. He is a professor in the School of Electronic and Information Engineering, Beijing Jiaotong University, China. His research interests include capacity analysis, spectrum prediction and resource management in cognitive radio networks, RFID in intelligent transporting system, smart phone application.