Hindawi
Security and Communication Networks
Volume 2020, Article ID 8872586, 13 pages
https://doi.org/10.1155/2020/8872586

Review Article

Artificial Intelligence for Securing IoT Services in Edge Computing: A Survey

Zhanyang Xu, Wentao Liu, Jingwang Huang, Chenyi Yang, Jiawei Lu, and Haozhe Tan

School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China

Correspondence should be addressed to Wentao Liu; liuwentao@nuist.edu.cn

Received 30 July 2020; Revised 17 August 2020; Accepted 29 August 2020; Published 14 September 2020

Academic Editor: Dou Wanchun

With the explosive growth of data generated by the Internet of Things (IoT) devices, the traditional cloud computing model by transferring all data to the cloud for processing has gradually failed to meet the real-time requirement of IoT services due to high network latency. Edge computing (EC) as a new computing paradigm shifts the data processing from the cloud to the edge nodes (ENs), greatly improving the Quality of Service (QoS) for those IoT applications with low-latency requirements. However, compared to other endpoint devices such as smartphones or computers, distributed ENs are more vulnerable to attacks for restricted computing resources and storage. In the context that security and privacy preservation have become urgent issues for EC, great progress in artificial intelligence (AI) opens many possible windows to address the security challenges. The powerful learning ability of AI enables the system to identify malicious attacks more accurately and efficiently. Meanwhile, to a certain extent, transferring model parameters instead of raw data avoids privacy leakage. In this paper, a comprehensive survey of the contribution of AI to the IoT security in EC is presented. First, the research status and some basic definitions are introduced. Next, the IoT service framework with EC is discussed. The survey of privacy preservation and blockchain for edge-enabled IoT services with AI is then presented. In the end, the open issues and challenges on the application of AI in IoT services based on EC are discussed.

1. Introduction

With the widespread deployment of sensors in the real world, increasing physical entities are connected to the Internet of Things (IoT) through sensors to achieve information sharing. Currently, IoT technology has been widely applied in various fields such as smart city, smart home, wearable medical, and environmental perception, [1–3]. In conventional IoT services, those sensors and devices interconnected with IoT need to upload the data to the cloud servers to handle computing tasks. After the tasks are completed, the processed data will be returned to the IoT devices. Although the cloud reduces the computing burden of sensors and devices, huge transmission overhead of the data cannot be ignored. In 2018, the total amount of devices connected to IoT around the world reached 11.2 billion, and it is predicted to grow to 20 billion in 2020 [4], which brings rapid data growth. However, the current growth of network bandwidth is far behind the speed of data growth, and the complex network environment greatly hinders the reduction of latency. Network bandwidth has become the major bottleneck that should be solved for the traditional IoT services.

To solve the abovementioned bottleneck, a new computing paradigm called edge computing (EC) has been proposed recently and gets widespread attention. EC refers to the technology that deploys computing tasks to the edge of the network [5, 6]. Compared with cloud computing, EC has many advantages, including protecting end-users' privacy, reducing the latency while data transmission, decreasing the burden of network bandwidth, and lessening the energy consumption of data center. Under EC, the raw data generated by IoT devices are no longer required to be uploaded to the centralized cloud platform but can be computing, stored, and transmitted at edge nodes (ENs), reducing the latency time owing to voiding redundant data transmission. Those IoT applications and mobile

computing that have strict requirements on response time will be better supported by EC.

However, EC is not a panacea. On the one hand, the potential of IoT devices under the EC has been greatly expanded in many fields (computation offloading, precise positioning, real-time processing, etc.), giving the credit for low-latency data processing near end-users. On the other hand, EC introduces more security issues and widens the attack surfaces [7] of the system from 3 aspects:

(1) Distributed layout: the ENs are distributed at various locations on the edge of the network [8], making it difficult to unify all equipment for centralized management. The adversary can attack those ENs that have security flaws and use the nodes hijacked as a springboard to make an incursion to the entire system.

(2) Limited computing source: unlike cloud computing, the computational functionality of ENs is limited for the reason of the physical structure, which means that heavyweight security mechanisms are not suitable for ENs and large-scale centralized attacks such as the distributed denial of service (DDoS) attack will cause great damage to ENs.

(3) Heterogeneous environment: a wide range of technologies are applied in EC, including wireless sensor networks, mobile data collection, grid computing, and mobile data collection. Under this heterogeneous environment, it is difficult to design a unified security mechanism and achieve consistency of security policies between different security domains.

In order to make up for the safety hazards caused by the characteristics of edge computing, many security methods and algorithms come forth [9, 10]. Most of the current security mechanisms are based on the algorithms and models that follow a single pattern for intrusion detection, privacy preservation, or access control. With the continuous upgrade of attack techniques and methods, traditional defense mechanisms are often quickly eliminated. However, what is exciting is that the emergence and rise of artificial intelligence (AI) provide new solutions to security and privacy issues:

(1) Intrusion detection: common intrusive attacks are denial of service (DoS) attack and distributed denial of service (DDoS) attack. DoS makes frequent requests to the server, which increases the burden on the server and affects the server's response to normal requests, and DDoS refers to controlling the multiple compromised ENs to attack the server. The intrusion detection system (IDS) identifies attacks from the hijacked ENs by monitoring anomalous traffic on the network and cut off access from them. Machine learning (ML) extracts malicious access patterns through the training of the previous data sets, which can help IDS to quickly and accurately identify intrusions, greatly improving the detection efficiency compared with traditional recognition methods [11, 12].

(2) Privacy preservation: the IoT devices exist in every aspect of our lives, which contains much privacy-sensitive information as well [13]. Most existing privacy preservation methods encrypt the transmitted data to ensure data security, such as anonymization, cryptographic methods, and data obfuscation. Nonetheless, the above methods generally require high computational overhead, making it difficult to deploy on resource-constrained ENs. Compared to common encryption methods, distributed machine learning (DML) makes the ENs only need to pass the parameters to other ENs for cooperative learning after each training, instead of directly passing the original data, reducing the risk of data leakage and network burden during transmission [14].

(3) Access control: when multiple IoT devices work together in the same environment, access control becomes a key issue. Each authenticated node can only access the nodes and data within their authorities and cannot perform other operations beyond their access authorities [15, 16]. ENs need to be classified into different categories according to permissions, which coincides with the classification algorithm under ML [17]. The algorithm classifies the ENs connecting to the network to low-privileged IoT devices and high-privileged IoT devices. Access to those high-privileged devices will be strictly controlled to prevent potential attacks.

As the investigations of AI continue to advance, AI has gradually been applied to many fields of edge security [18, 19]. However, there are still many challenges in the realization of related theories on ENs. For instance, large amounts of clear data are important to the training efficiency of ML, but the premise of sufficient data is that the system has received mass attacks and can accurately identify these malicious behaviors [20]. Meanwhile, the attacks against the training set also need to be vigilant, which will reduce the performance of the model by tampering the parameters [21]. The lightweight AI algorithm is also needed because of the restricted computing resource and storage at ENs, but it will bring a drop in accuracy.

Although lots of investigations on the combination of AI and EC have been carried out, there is still little discussion and inquiry of AI in the security of IoT based on EC. Therefore, a comprehensive review which focuses on state-of-the-art technology and achievements about the above-mentioned field is presented.

The remaining parts of this paper are organized as follows. Section 2 introduces the basic definitions of IoT and EC. In Section 3, the IoT service framework with EC is discussed, followed by the survey of privacy preservation in EC enabled IoT with AI in Section 4. Section 5 presents the AI for blockchain in EC enabled IoT. Finally, Section 6 talks about the open issues and challenges of the application of AI in IoT security based on EC.

2. Basic Concepts and Definitions

2.1. IoT Service. Literally, IoT is to construct a global network of things where everything is connected to the Internet, thus realizing the interconnection of all objects using Internet technologies. With IoT technology, devices are able to transmit information to each other and several devices work together to complete a task without the intervention of humans. IoT can be applied in various industries by embedding sensors into objects such as medical equipment, home equipment, transports, implementing the integration of human society, and physical world.

IoT architecture is comprised of perceptual layer, network layer, and application layer [22], and each layer has its own specific function. The perceptual layer is employed to perceive the environment and obtain data by virtue of sensor technology, RFID, wireless communication technology, etc., acting as the indispensable foundation of IoT. The network layer is responsible for data transmission from the perceptual layer to the application layer. Besides, cloud platform serves as a vital component of this layer to store and analyse substantial perceived data. The application layer is the top layer of IoT architecture. This layer provides specific services for users based on processed and analysed data. Through the three layers, IoT devices can understand users' needs and accordingly give them the services they want, improving their living quality.

Next, we will illustrate three typical IoT services and their respective specific application scenarios which are introduced in Table 1 as follows:

(1) Remote monitoring and control: IoT allows users to control the devices connected to the Internet and monitor a scenario remotely, which brings generous convenience to our life. Users are enabled to monitor the condition of their babies anywhere with the help of the sensors installed at home that collect data on the baby's health status at any time. Furthermore, cameras can transfer baby's video to users timely. When it comes to logistics, customers can easily know about the condition of products in transit. Information about the quality statue and current location of goods they purchased online can be queried regardless of time.

(2) Smart home: smart home [27] has developed several years so that it is not a novel concept for us. However, what deserves our attention is that with the usage of IoT, smart home products contain a huge potential to become more intelligent and versatile, able to serve users better. Suppose that as soon as you enter your room from the outside, the air conditioner is turned on and adjusted to a comfortable temperature automatically for you. Many other products such as sweeping robots will free you from housework, and even lights can be switched on/off by themselves without any manual operation. Thus, it can be seen that smart home is one of the most direct manifestations of how IoT services make our lives easier and more comfortable.

(3) Natural disaster prediction: IoT plays an important role in the prediction of disasters such as earthquakes, floods, drought, and tsunami [28]. Sensors deployed outside are appointed to gather data from the ambient environment, and the processed data may reveal crucial information about the coming natural calamity, thus saving up enough time for us to remove people away from the disaster area and avoid property loss as much as possible.

So far, on the topic of benefits IoT brings about, we have only referred to the tip of the iceberg. Undeniably, IoT has served as a powerful engine driving revolutions in many traditional offline industries. Though IoT is still in its initial state, it has a wide application range which is just limited by humans' imagination and it is bound to influence almost every aspect of our life in the near future.

2.2. Edge Computing. EC is a new computing mode that processes and stores data at the edge of the network in close proximity to mobile devices and users [29]. In Table 2, we describe the definition of EC from two different angles.

With the advent of the IoT era, the scale of mobile devices is expanding incredibly and the high volume of data is produced by terminal devices every day [35–37]. It is unwise to transmit all data to the cloud center considering the excessive burden of bandwidth and massive energy consumption in the cloud. Besides, traditional cloud computing cannot process such a huge amount of data efficiently, which extends latency time and reduces response speed [38, 39]. At the same time, certain emerging technologies such as AR and VR [29] have higher requirements for low latency and fast response time. The contradiction between our growing need for higher computing efficiency as well as better privacy security and the limitations of cloud computing calls for a decentralized computing mode that can complement the cloud computing and push the future development of the IoT industry. Naturally, EC's advantages begin to be valued by humans under this circumstance.

Three outstanding advantages of EC are introduced as follows:

(1) Low latency: instead of transmitting all data to cloud center, data computations are completed at the edge of the network closer to mobile devices, thus increasing the response speed and declining the latency [40].

(2) Privacy and security: thanks to EC, data are allowed to be stored locally or in ENs and privacy information does not have to be transmitted to cloud center so that the threat of privacy leakage has been effectively reduced [40].

(3) Decrease energy consumption in cloud center: in EC, part of computing tasks is offloaded to several ENs, which not only relieves the burden of bandwidth [29] but also helps reduce the energy consumption in the cloud center.

Table 1: Three typical IoT services and their specific application scenarios.

IoT services	Application scenarios
Application scenarios	(1) A greenhouse system based on IoT can monitor and control environmental parameters to facilitate plant growth and production [23]. (2) Cold chain logistics [24] can depend on IoT to maintain suitable storage and transportation temperature, ensuring the quality of goods.
Smart home	(1) Users can easily control devices inside the home via smart home systems to avoid unnecessary energy waste [25]. (2) With the usage of smart home and various devices connected to the Internet, users can enjoy the convenience of controlling the house at any time [25].
Disaster prevention	Disaster management systems based on IoT can be deployed in buildings of seismic areas to monitor the conditions of buildings of seismic areas, providing earthquake early warning [26].

Table 2: Two angles to define edge computing.

Definition of edge computing	Advantages	Related work
A distributed computing mode that offloads computation tasks to different edge nodes	Better privacy protection	A dispersed edge cloud infrastructure called Nebula [30] is presented.
	Relieve bandwidth burden	Cloudlet, an edge computing platform is introduced in [24, 31].
	Save energy in the cloud	A lightweight differential privacy-preserving mechanism used in edge computing is proposed in [32].
A new paradigm where computational resources are placed closer to data sources	Low latency	LAVEA [33] is a system designed to provide low-latency video analytics at places in close proximity to users.
	Fast response speed	The impact of both latencies in MEC architecture with regard to latency-sensitive services is researched in [34].

Today's IoT services are mostly cloud-based and centralized so that all data processing and analyses have to be completed in cloud [41]. With the prosper of IoT, more IoT devices demanding low latency and high response spring up [42]. However, cloud computing has encountered its bottleneck, unable to provide support for the sharp development of IoT continuously. Only making best of advantages of EC can IoT services be blessed with a bright outlook.

3. IoT Service Framework with EC

IoT service framework with EC can be divided into four major layers: device layer, network layer, edge layer, and cloud layer. Figure 1 shows the basic diagram of the IoT service framework with EC.

3.1. Device Layer. Various objects or electronic devices such as mobile phones, computers, cars, and even humans (in IoMT [43]) are equipped with different kinds of sensing devices such as RFID, intelligent sensors, and QR code. With them, 'things' in the IoT have the ability to provide context-based information about themselves or their surroundings in real-time, thus generating a large amount of real-time data. These data vary greatly due to different processing requirements, but most of them are fast, instantaneous, and frequent.

3.2. Network Layer. This layer can be seen as a channel among cloud, edge, and end. On the one hand, the layer is the transition between the device layer at the bottom and the edge layer at the upper end. It is the nervous system of the IoT service framework, connecting the sensing devices all over the IoT and undertaking the task of transmission. The data obtained from sensing devices are transmitted through different communication technologies [44] such as cellular networks composed of base stations, WiFi, ZigBee, Bluetooth, etc., which follow various IoT protocols or data transmission protocols, such as Hypertext Transfer Protocol and Message Queuing Telemetry Transport.

In order to adapt to the new computing model of EC and meet the requirements of establishing computing path and dynamically realizing computing services and data migration, named data networking (NDN [45]), a data network that names and addresses data and services, is applied to the context of edge computing. Besides, software-defined networking (SDN [46]), a programmable network that separates the control plane from the data plane and can perform simple network management, is paid attention to. As a result, through the combination of the two, data migration and transmission can be well-realized, and service organizations can be carried out quickly, so as to meet the requests of service discovery and rapid configuration in the network layer under the background of EC. On the other hand, the layer also links up the edge layer and cloud layer composed of cloud-data centers. It takes on the task of transmitting the data organized or concluded by the edge layer and transferring orders or feedback from the cloud layer to the edge layer.

Moreover, the safety of the network layer cannot be neglected. Physical isolation design and logical security design are two main approaches to securing the layer. Specifically, Air Gap that makes use of physical isolation technology and high-strength protocol analysis function to isolate the inside and outside network, routing attack protection design, and denial of service protection design is usually used.

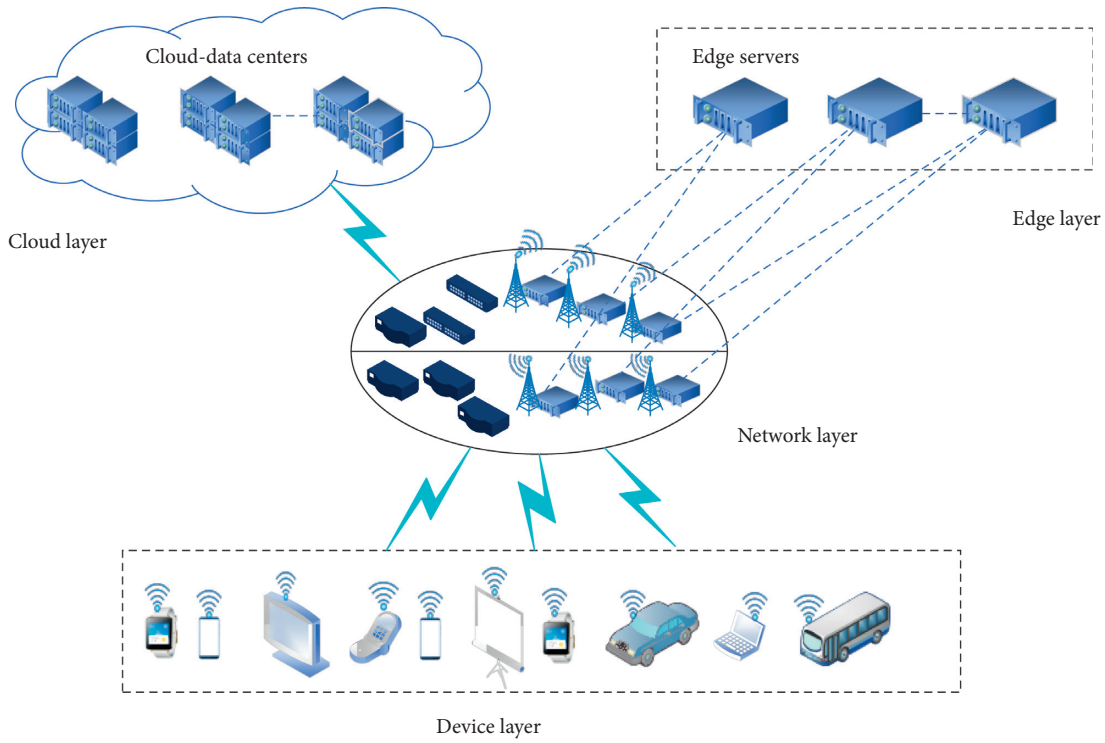

Figure 1: IoT service framework with edge computing.

3.3. Edge Layer. Compared to the conventional IoT service framework, this layer is the main characteristic of the IoT service framework with EC, which solves the problems of insufficient bandwidth and high delivery delay, to a certain extent. To processing a great number of data from IoT devices efficiently and accurately, partial computing resources are shifted from cloud to edge which is much closer to data sources.

As core compositions in edge layers, edge servers are principal undertakers of data processing, data management, and data storage. The results are transmitted to corresponding devices or uploaded to the cloud layer for further analysis or storage through the network layer. The deployment of edge servers which needs to satisfy the requirements of users under resource constraints has a significant impact on computing efficiency and computing resources utilization. Edge servers are usually deployed in cellular base stations' vicinity. Besides, they are often deployed in a single entity rather than multitenant [47]. In 2018, Zhao et al. proposed an innovative three-phase deployment way [48] that takes traffic diversity and wireless diversity of IoT into consideration in large-scale IoT, which greatly promotes the reduction of ENs.

To ensure the smooth and efficient operation of computing tasks, some core technologies such as edge operating systems, isolation techniques, and data processing platforms boost the development of the edge layer.

3.4. Cloud Layer. The layer is the brain of the IoT service framework with EC. It is usually composed of large cloud-data centers with extraordinary computing power. In the IoT service framework with EC, the cloud layer tends to be applied to further processing data from the edge layer, storing or updating significant information and carrying out advanced deployment.

Nonetheless, in some special situations, the importance of cloud-edge collaboration is highlighted. Cloud-edge collaboration includes resource collaboration, management collaboration, safety collaboration, and so forth, which think of cloud and edge as all in one to reinforce each other and schedule dynamically. Specifically, when computing resources in the edge layer are insufficient, the cloud layer can offer computing support with virtual machines and containers. When a certain edge layer appears malicious traffic, the relevant cloud layer which is equipped with better security policy has the ability to discover and block it so as to prevent it from continuing spreading. The establishment of cloud-edge collaboration has aroused wide concern. A few cloud-edge collaboration platforms such as KubeEdge, Edge Tunnel, and AWS Wavelength are pushing ahead with the prosperity of cloud-edge collaboration.

The application of IoT service with EC is booming and hot. Table 3 shows some typical examples of IoT service with EC.

4. Privacy Preservation for Edge-Enabled IoT Services with AI

The privacy protection methods in ML can be generally divided into two kinds, namely, training schemes and inference schemes in [54]. The privacy-preserving training schemes target to use encryption methods to ensure the security of sensitive privacy information during the

Table 3: Typical examples of IoT service with edge computing.

Reference	Application field	Author	Specific design
[49]	Smart cities	Sapienza et al.	Make use of mobile edge computing to monitor critical events (e.g., terrorist attack or disasters)
[50]	Smart farms	Caria et al.	Propose a smart farm animal welfare monitoring system based on edge computing (e.g., collecting and processing data from animals and surroundings)
[51]	Connected and autonomous vehicles	Liu et al.	Create an edge-based attack detection (e.g., detecting speech, video data, and driving behavior)
[52]	Smart home	Cao et al.	Implement a home operating system named EdgeOSH which includes various modules (e.g., data management, communication, and self-management)
[53]	Public safety	Zhang et al.	Present an AMBER alert assistant (A3) based on extended firework (e.g., following an illegal vehicle)

transmission. The privacy-preserving inference schemes focus on protecting the privacy data in the inference phase. Usually, in preserving inference schemes, a well-trained model receives the unclassified data sent by the EN for inference [54]. The common encryption methods include anonymization, cryptographic method, data obfuscation, and so on. However, the above methods for encryption always require different levels of computing overheads and communication overheads. It hinders the implementation of encryption methods on resource-limited ENs. As Figure 2 shows, the following parts of this section will talk about existing basic encryption approaches firstly and then furtherly discuss proper privacy-preserving methods for edge-enabled IoT service.

4.1. Existing Basic Encryption Methods

4.1.1. Anonymization. Anonymization techniques are applied to anonymize participants' identities in a group of people, by removing some obvious characteristics such as a user's name, sex, and ID number. Since the loss information is related to the user's specific identity, the most valuable data we need will not be ruined during the transmission. Many privacy preservation models using anonymization technology have been proposed, such as k-anonymity, l-diversity [55], and t-closeness [56] models. In the k-anonymity model, the participants' attributes are generally classified into three categories: explicit identifiers, the quasi-identifier attribute set, and sensitive attributes. Before the data are released, the explicit identifiers will be removed and the data in the quasi-identifier attribute set will be generalized to ensure that there are at least k records with the same quasi-identifier. However, the k-anonymity technique is flawed. The attacker can reidentify victims by linking or matching the data to other background data or by looking at unique attributes found in the released data [57]. Later, some researchers proposed I-diversity and t-closeness models based on the k-anonymity technique to defend against the above attacks. The I-diversity model requires that the diversity of sensitive attributes should not be less than I in each quasi-identifier class, thus reducing the matching probability between sensitive attributes and their owners. The t-closeness module requires that the distance between the distribution of sensitive attributes in each equivalence class and the general distribution of sensitive attributes do not exceed the upper limit t.

4.1.2. Cryptographic Method. Cryptographic methods encrypt the context of the data before uploading them to the cloud servers. However, cryptographic methods incur high compute overhead (millions of times higher than multiplicative projection) and require reliable and effective key management [58]. Homomorphic encryption (HE) can entrust third parties, such as various applications of cloud computing, to process the data without revealing the information. HE technology is secure in that they generate a key pair based on some mathematical problems which are difficult to be solved by the computer. The key pair includes a public key and a private key. The public key and some operation measures will be published to third parties. Then, the third parties carry out all the operations on the encrypted data and send back the results, which can only be decrypted by the private key; thus, the information is confidential throughout the whole process. The common homomorphic encryption algorithms include the RSA algorithm and the ECC algorithm. The later one has a lower computing overhead.

4.1.3. Data Obfuscation. Obfuscation methods perturb the data samples used for training a global module. The methods include additive perturbation and multiplicative perturbation. Additive perturbation is always related to differential privacy (DP), which is used to aggregate information without revealing any special entry [59]. Under the mechanism of DP, the adversary cannot tell the difference between the output of neighboring datasets, thus protecting the safety of different records of neighboring datasets. DP obfuscates the data by adding noises through some mechanisms such as Laplacian [60], exponential [61], and median mechanisms [62]. Laplacian mechanism realizes the DP protection by adding random noise with Laplacian distribution to the exact query outputs. Different from the Laplacian mechanism, the exponential mechanism selects the optimal output according to the probability after each query. The randomize multiplicative data perturbation technique is a type of multiplicative perturbation. The random projection scheme tries to create a new data representation with fewer dimensions through randomize multiplicative matrices [63]. Generally, data obfuscation has been widely applied in data mining to protect the users' privacy while obtaining high-quality data.

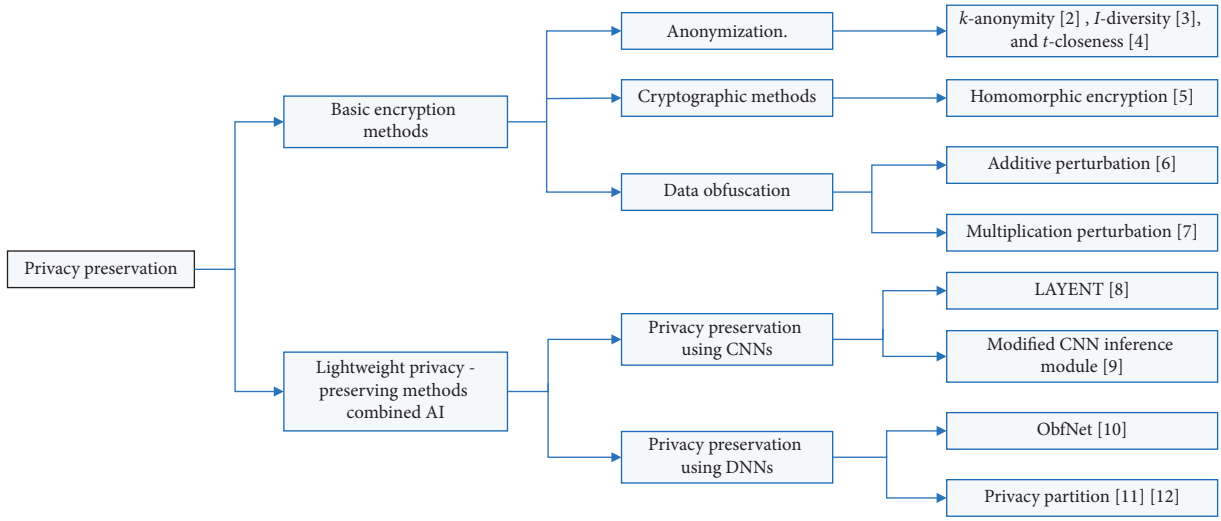

Figure 2: Structure of this section.

4.2. Lightweight AI Privacy-Preserving Methods in ENs. The booming development of IoT encourages a new computing paradigm "edge computing," which leverages the computing and storage capability of device nodes between the cloud center and terminal devices. Compared with traditional cloud computing, EC pushes the process of data close to the data sources, reducing the data required to be sent to the data center originally. It provides real-time services with low latency and reduces communication bandwidth usage. The attention has concentrated on the privacy problems not only in the training of the module but also in tasks offloading schemes [64]. Conventional encryption methods such as anonymization, cryptographic method, and data obfuscation have been requested in computing power and they are originally implemented in the cloud center. Thus, it is hard for conventional encryption methods to work effectively on the resource-constrained ENs. Recently, some research studies have focused on creating lightweight privacy preservation methods combined with AI technologies such as convolutional neural network (CNN) and deep neural network (DNN) models and other ML technologies to optimize the traditional encryption methods.

4.2.1. Privacy Preservation Using CNNs. The following context will introduce two schemes: LAYENT and the modified CNN inference module. The former scheme optimizes the basic framework to make the module privacy-aware and the later uses the trained module for privacy preservation.

(1) LAYNET. LAYENT is a new privacy-preserving algorithm in machine learning. Compared with most related algorithms based on cloud computing's processing power, LAYRNT not only has a very high accuracy up to 91% but also well protects the privacy incurring a low computing overhead [61]. Before the data are transmitted to the potential unsafe third party, the data will be perturbed. To achieve this function, the algorithm LAYENT improves the original CNN framework, by adding a new layer—the randomization layer between convolution layers and full connected layers. Moreover, the randomization layer employs a new unary encoding protocol to enhance the flexibility of randomization when encoding the context.

(2) Modified CNN Inference Module. An energy theft detection scheme is proposed to detect the unusual behavior of the smart meters in the smart grid. The scheme combines the modified convolutional neural network (CNN) module in the framework. The data generated by the smart meter are used to train the CNN module, and then the trained module can detect the abnormal data by making reasonable inferences after training. The scheme combined the modified CNN module has excellent behavior in the experiment in that the accuracy of the inference has reached up to 92.67% [62].

4.2.2. Privacy Preservation Using DNNs. Deep neural network is a framework in deep learning, and it has been widely applied in many areas such as the understanding of natural language, speech recognition, and image recognition. The training of DNN modules needs to consume large computing power. The following context is two lightweight schemes:

(1) ObfNet. An obfuscation neural network (ObfNet) approach is proposed to obfuscate the inference data before being transmitted to the backend [63]. ObfNet is an approach that realizes lightweight and unobtrusive data obfuscation for remote inference. The lightweight and unobtrusive characters refer that the ENs only need to implement a small neural network and do not need to indicate whether the data are obfuscated.

There are two issues in the implementation of the edge-enable IoT. One of them is the separation of information sources and computer power, and the other is the privacy

preservation of inference models. Remote inference can overcome the above issues. In remote inference, the collected data will be sent to the backend and then the inference results will be returned.

ObfNet is a light neural network suitable to be deployed in ENs. The training process is designed as follows. The backend connects the untrained ObfNet with the trained in-service inference model (named InfNet) in the center, forming a concentrated DNN module. In the DNN module, the output of ObfNet is the input of InfNet. The backend uses the part random data which are used for the training of InfNet to train ObfNet. Meanwhile, only the ObfNet's weights are sent to the backend until convergence. Repeating the procedure, the backend can generate a group of ObfNets. Due to the random data sources and random original weights of ObfNets, all the ObfNets are different from each other. Finally, EN chooses an ObfNet randomly and dynamically.

(2) Privacy Partition. A practical method named privacy partition for privacy preservation in ML is presented in [65, 66]. Privacy partition is a privacy-preservation framework for deep neural networks, and the basic structure of the framework is made up of a bipartite topology network and an interactive adversarial network [65].

A bipartite deep network topology is made up of two partitions: a trusted local computing context and the untrusted remote computing context, forming a neural network. The output of the last transformation in a trusted local computing context will be processed by a learning module. After that, the processed information will be the input of the first transformation layer in remote computing context [65]. Under the architecture of the edge network, privacy partition provides an optional choice to some centralized deep learning frameworks. Users can limit access to the sensitive data stream for privacy preservation.

The interactive adversarial network provides a practical solution when the ENs need to use remote services and computing. It can attenuate the capacity of the adversary who has access to deep network intermediate state to learn privacy-sensitive input.

5. Blockchain for Edge-Enabled IoT Services with AI

Blockchain is a distributed computing and storage paradigm with a variety of existing technologies. The distributed consensus algorithm is used to generate and update data, transmits data between nodes by a peer-to-peer network and keeps the stored data immutable by a distributed ledger. It also uses an automated script code or smart contracts to implement upper-layer application logic [67]. In short, blockchain provides a new approach to preserve and transmit data safely against attack or bug and gives a decentered environment.

Part 1 includes the method of most urgent security problems in IoT services by blockchain. Part 2 discusses the sharing of data resources which is from one mechanical device to another mechanical device and provides many communication facilities. Part 3 includes the improvement of efficiency in the environment based on the IoT networks. Besides, the hierarchical taxonomy of the section is shown in Figure 3 and the research studies we discuss are listed in Table 4.

5.1. Blockchain for IoT Services' Security. In order to build an IoT network that can be in use, massive terminal devices will be set and any device in IoT network can get the data from the whole IoT network. Due to the number of devices, the weakness of a single device cannot be avoided. If the device is hacked into, massive data in IoT services will be leaked out which may result in disastrous consequences [80]. Therefore, improving the security of IoT services becomes unavoidable.

The connection of these IoT devices is not safe due to the quantity of the devices. As a result, it is easy for ill-disposed people to steal the data which are transmitted between devices. Although there are some ways to solve the unsafety such as CAPTCHAs, it still has the limitation in the protection of data. So, blockchain technology and AI technology are introduced to solve them. There are two aspects which will be introduced below: (1) access control and authentication management and (2) confidentiality and reliability of data.

5.1.1. Access Control and Authentication Management. Access control is to provide a set of methods to identify, organize, and host all functions in the system, organizing and identifying all data, and then provide a simple and unique interface [81]. Authentication is to identify the access by verification tools such as passwords and decide whether to give the interface of the system.

In the traditional IoT service which is without AI or blockchain, the way of identity authentication is to authenticate the combination of the user name and password for each device. This way will cost a lot of energy and have difficulty in extension, so it can be used in IP cameras. Single sign-on protocols can simplify identity authentication, which is to provide a reliable third-party organization to give the user access to multiple devices by authenticate identity for a single device. Although it can accelerate the authentication, it will result in a horrible consequence to the whole IoT system if the account of users is destroyed or one device is broken down.

To solve these problems, a new design has been proposed in the article [68]. In this design, the users only need to authenticate identity to the blockchain (such as Ethereum) once then use the smart contract token to access the system. Smart contact will broadcast the token and the Ethereum address when authenticating identity, and the IoT service will receive the package which includes the user's public key, IP, and token to authenticate the package. Besides, fingerprint information collection, storage, and verification can be completed by blockchain to solve the falsify problem in the access authentication technology at present [69].

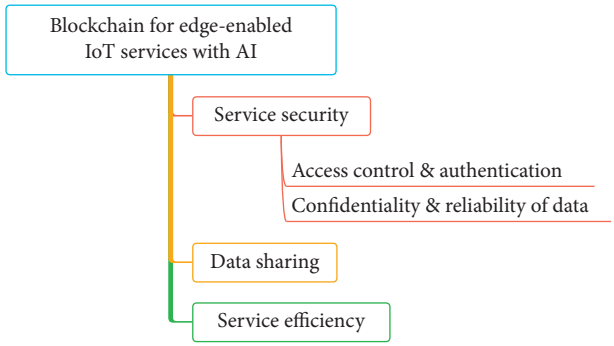

Figure 3: Hierarchical taxonomy of blockchain for edge-enabled IoT services with AI.

5.1.2. Confidentiality and Reliability of Data. The application of the IoT continues to grow in various fields such as healthcare, finance, and agriculture. In the field of health care, with the application of IoT, different kinds of physical sensors are be in use to record the body data, which can help the doctors to improve the methods of medical treatment for patients. These personal data need to be protected safely.

Rui et al. [70] propose a method which realizes distributed storage and tampers resistance of data in data blockchain and improves the utility Byzantine fault-tolerant (PBFT) mechanism consensus algorithm to store IoT data safely. Xu et al. [71] propose a blockchain-powered crowdsourcing method. They design a mobile crowdsourcing architecture based on blockchain to keep players' data private and complete. They generate service policies by density-based spatial clustering of applications with noise and improved dynamic programming. Besides, they judge the polices by using simple additive weighting and multiple criteria decision making.

5.2. Blockchain for Edge-Enabled IoT Data Sharing. Data are the basis of the IoT network, more data can be collected, and the research results and the improvement of the application are more accurate. At present, IoT data are collected by lots of different types of ways in many fields such as agriculture, industry, healthcare, and automatic drive. This shows that the sensors collecting different kinds of data are heterogeneous, and the database is owned by different companies, organizations, or governments. The isolation of data costs a large cost of energy and time because of collecting repetitive data. Therefore, sharing data from the IoT services in the database can assign the resource properly and reduce the avoidable cost.

However, massive data, heterogeneous devices, lack of trust, security problem, and some other problems become barriers to safe data sharing. In order to build a platform which can share data safely, blockchain becomes a good choice. We can build a distributed platform with trust way without central support by blockchain technology.

Zheng et al. [72] propose an architecture called MicrothingsChain. In this architecture, they proposed an EC network based on blockchain and every point's data are untamable and traceable. By designing Proof-of-Edge Computing Node which is based on Proof-of-Authority, data can be shared fairly. Besides, Truong et al. [73] propose an architect called Sash which transmits more data to the back end of blockchain to avoid malicious action by its own resilience. They also use smart contact to put Policy Decision Point into blockchain and analyse requests by access control which can both benefit the owners and the costumers to share data. In the field of Industry Internet of Things (IIoT), Liu et al. [74] propose an architecture which can collect and share data by blockchain and deep reinforcement learning. It divides points in private blockchain networks into computing and sharing and uses DRL to collect distributed data in IIoT.

Moreover, knowledge just as data in IoT networks can be shared safely and equally. Lin et al. [75] propose a market based on edge-enabled IoT with AI by blockchain. Consortium blockchain and smart contract from blockchain are used to keep knowledge such as data trading fairly, efficiently, and safely. They design a new consensus mechanism called Proof-of-Trading which can reduce the cost of computing resources.

5.3. Blockchain for Edge-Enabled IoT Services' Efficiency. Application of blockchain for IoT can effectively ensure the safety of IoT services' data just as mentioned in part 1 and 2 before, but with the expansion of IoT services, the demand for computing sources will easily exceed the resources that the Internet can provide which impact the efficiency of IoT service. If this kind of situation happens, it may result in data overflow, service delay, and so on. However, it is impractical for now to solve the fundamental problem by only updating the computing ability of IoT devices. We introduce some research studies from different aspects below which help improve the efficiency of IoT services.

Khanji et al. [76] discuss the balance between cache capacity and computing ability to improve the efficiency of the whole system. They desired a mechanism by Geometric Programming which combines each data point of IoT networks to exchange data which can disperse a single device's cache to others. Fu et al. [77] introduce a method to solve the problem by cooperative computing which virtualizes the servers of data points into computation-intensive virtual machines and design a three-level cache to assign the computing properly. Chen et al. [78] design an algorithm based on game theory to solve the multihop computing offloading problems with normal and mining tasks in blockchain IoT services.

When discussing the offloading problem in edge IoT, Xu et al. [79] design an algorithm called BeCome which is monitoring EC devices' resource by blockchain ledgers and allocating computing resources by nondominated sorting genetic algorithm III (NSGA-III).

6. Open Issues and Challenges

Though the application of AI is expected to enhance the security of IoT services in EC, many serious problems should be wiped out before AI can finally be used to secure IoT.

Table 4: Current research studies in blockchain for edge-enabled IoT services with AI.

Reference	Problem addressed	Technique used
[68]	Access control, authentication management	Blockchain
[69]	Authentication management	Blockchain, HTTPS protocol, and HMAC technology
[70]	Confidentiality and reliability of IoT data	ECC asymmetric encryption, DH key exchange, RAF consensus protocol, blockchain
[71]	Integrality and confidentiality of IoT data	Crowdsourcing, blockchain, DBSCAN
[72]	IoT data sharing	Blockchain, edge computing
[73]	IoT data sharing	Smart contact
[74]	Collection and share of IIoT data	Blockchain, deep reinforcement learning
[75]	Knowledge sharing	P2P networks, smart contact, consortium blockchain
[76]	The balance between cache capacity and computing ability	Blockchain
[77]	IoT cache offloading and computing	Cooperative computing, blockchain
[78]	Multihop computing offloading	Game theory, blockchain
[79]	Edge computing offloading	Blockchain ledger, NSGA-III

6.1. ML-Based Security Schemes. ML is an advisable choice to secure IoT services because of its ability to augment the analytical capabilities of IoT devices and there actually exist security schemes based on ML. However, most of these schemes have fatal defects that make it impractical to adopt them into IoT systems at present.

6.1.1. High Computation and Communication Cost. Many ML-based security schemes have an obvious deficiency that a flood of training data is required by machines in order to deduce a feasible model to tackle practical issues and the feature-extraction [82] process is very complicated as well. Worse still, its computation and communication cost [82] is very high. So, it is an urgency for us to devise a new ML-based security scheme with low computation and communication costs.

6.1.2. Backup Security Solutions. Deep learning (DL) and reinforcement learning (RL) are two different types of ML and they have shortcomings, respectively. DL may fail to detect attacks precisely due to overfitting or insufficient training data. Hence, a suitable training dataset is a key for DL to reducing error rates. Then, let us talk about RL. Existing RL-based schemes are feasible merely on the premise that the intelligent agent knows the accurate state and is capable of evaluating the feedback of each action timely [82]. However, in fact, RL usually learns from scratch so that security schemes based on RL often lack the capability to handle attacks at the very beginning of the learning process, which increases the risk of IoT being attacked. So, to further secure IoT services, reliable backup security solutions should be designed in case of failures of ML-based schemes.

6.2. Adopt ML in Blockchain Technology. IoT is maturing rapidly, and IoT services are gradually infiltrating into every aspect of our life. However, IoT is doomed to encounter cyber-attacks and undergo a security threat in its developing process. Moreover, trust problems hindering the information exchange among different IoT devices also act as obstacles to IoT's future advancement. Fortunately, blockchain technology can be used in IoT to facilitate security and resolve trust problems thanks to its nature of decentralization [83], ultimately optimizing IoT services.

Meanwhile, new security problems such as double spending and majority attack [28] come with the application of blockchain. Therefore, the help of ML technologies is instrumental in preventing underlying attacks to blockchains, but there is still much work to be done before we can successfully integrate ML and blockchain to enhance the security of IoT.

In view of the fact that data stored in the blockchain can be accessed by all blockchain nodes, privacy problems are worthy of our great attention. Private blockchains [27] and encryption have been utilized to solve privacy problems, but paradoxically, this will inevitably lead to limited and even insufficient training data for ML, making it difficult to acquire a satisfactory model for privacy protection [28]. When used in real scenarios, chances are that the performance of these models may fail to live up to our expectations and finally let us down.

7. Conclusions

As a new computational paradigm which provides the various solutions to the challenges of traditional cloud faces, EC will greatly promote the development of the IoT field and enrich the diversity of the IoT application ecosystem. Reliable privacy protection and security mechanisms are indispensable for high-quality IoT services, putting strict requirements on the privacy and security of EC. In this paper, the survey of the combination of AI and EC in IoT security is presented. Firstly, the basic concepts and definitions are introduced. Then, the IoT service framework with EC is summarized. Afterward, conventional and AI-driven privacy preservation of edge-based IoT are compared and the latter are elaborated. The collaboration of blockchain and AI on IoT security is also discussed. Finally, the paper talks about the open challenges and issues on AI for securing IoT services in EC.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This research is supported by the Financial and Science Technology Plan Project of Xinjiang Production and Construction Corps under grant no. 2020DB005. Also, the research was supported by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) fund.

References

[1] F. X. Ming, R. A. A. Habeeb, F. H. B. Md Nasaruddin, and A. B. Gani, "Real-time carbon dioxide monitoring based on iot & cloud technologies," in *Proceedings of the 2019 8th International Conference on Software and Computer Applications*, pp. 517–521, Cairo, Egypt, April 2019.

[2] S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. Imran, "Securing IoTs in distributed blockchain: analysis, requirements and open issues," *Future Generation Computer Systems*, vol. 100, pp. 325–343, 2019.

[3] F. Chu, S. Yuan, and Z. Peng, "Using machine learning techniques to identify botnet traffic," *Encyclopedia of Structural Health Monitoring*, pp. 967–974, Wiley, Hoboken, NJ, USA, 2006.

[4] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: state of the art and challenges," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1608–1631, 2019.

[5] W. Shi and S. Dustdar, "The promise of edge computing," *Computer*, vol. 49, no. 5, pp. 78–81, 2016.

[6] X. Xia, F. Chen, Q. He, J. Grundy, M. Abdelrazek, and H. Jin, "Cost-effective app data distribution in edge computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 1, pp. 31–44, 2020.

[7] P. K. Manadhata and J. M. Wing, "A formal model for a system's attack surface," in *Moving Target Defense*, pp. 1–28, Springer, Berlin, Germany, 2011.

[8] P. Lai, Q. He, M. Abdelrazek et al., "Optimal edge user allocation in edge computing with variable sized vector bin packing," in *Proceedings of the International Con-Ference on Service-Oriented Computing*, pp. 230–245, Springer, Hangzhou, China, November 2018.

[9] 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.

[10] 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, pp. 637–646, 2016.

[11] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin et al., "Deep learning and big data technologies for IoT security," *Computer Communications*, vol. 151, pp. 495–517, 2020.

[12] X. Chi, C. Yan, H. Wang, W. Rafique, and L. Qi, "Amplified locality-sensitive hashing-based recommender systems with privacy protection," *Concurrency and Computation: Practice and Experience*, 2020.

[13] W. Zhong, X. Yin, X. Zhang et al., "Multi-dimensional quality-driven service recommendation with privacy-preservation in mobile edge environment," *Computer Communications*, vol. 157, pp. 116–123, 2020.

[14] G. Song and W. Chai, "Collaborative learning for deep neural net-works," in *Proceedings of the Advances in Neural Information Processing Sys-Tems*, pp. 1832–1841, Montreal, Canada, December 2018.

[15] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in internet of things," *Future Generation Computer Systems*, vol. 100, pp. 144–164, 2019.

[16] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in *proceedings of the IEEE World Congress on Services*, pp. 21–28, IEEE, New York, NY, USA, June 2015.

[17] L. Li, T.-T. Goh, and D. Jin, "How textual quality of online reviews affect classification performance: a case of deep learning sentiment analysis," *Neural Computing and Applications*, vol. 32, no. 9, pp. 4387–4415, 2020.

[18] X. Xu, X. Zhang, X. Liu, J. Jiang, L. Qi, and M. Z. A. Bhuiyan, "Adaptive computation offloading with edge for 5G-envisioned internet of connected vehicles," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2020.

[19] X. Xu, X. Liu, Z. Xu, F. Dai, X. Zhang, and L. Qi, "Trust-oriented IoT service placement for smart cities in edge computing," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4084–4091, 2019.

[20] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): a survey," *Journal of Network and Computer Applications*, vol. 161, Article ID 102630, 2020.

[21] F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, "Machine learning for security and the internet of things: the good, the bad, and the ugly," *IEEE Access*, vol. 7, pp. 158126–158147, 2019.

[22] H. Haddadpajouh, R. Khayami, A. Dehghantanha, K. R. Choo, and R. M. Parizi, "AI4SAFE-IoT: an AI-powered secure archi-tecture for edge layer of internet of things," *Neural Comput-Ing and Applications*, 2020.

[23] P. Vimal and K. Shivaprakasha, "IoT based greenhouse environ-ment monitoring and controlling system using arduino plat-form," in *Proceedings of the International Conference on Intelligent Com-Puting, Instrumentation and Control Technologies (ICICICT)*, pp. 1514–1519, IEEE, Kannur, India, July 2017.

[24] A. Mohsin and S. S. Yellampalli, "IoT based cold chain logistics monitoring," in *Proceedings of the IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, pp. 1971–1974, IEEE, Chennai, India, September 2017.

[25] T. Adiono, B. A. Manangkalangi, R. Muttaqin, S. Harimurti, and W. Adijarto, "Intelligent and secured software application for iot based smart home," in *Proceedings of the IEEE 6th Global Conference on Consumer Electronics (GCCE)*, pp. 1-2, IEEE, Nagoya, Japan, October 2017.

[26] F. Franchi, A. Marotta, C. Rinaldi, F. Graziosi, and L. D'Errico, "IoT-based disaster management system on 5G uRLLC network," in *Proceedings of the International Conference on Information and Commu-Nication Technologies for Disaster Management (ICT-DM)*, pp. 1–4, IEEE, Paris, France, December 2019.

[27] T. Malche and P. Maheshwary, "Internet of things (IoT) for build-ing smart home system," in *Proceedings of the*

International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), IEEE, Coimbatore, India, pp. 65–70, February 2017.

[28] S. Chaudhary, R. Johari, R. Bhatia, K. Gupta, and A. Bhatnagar, "CRAIoT: concept, review and application(s) of IoT," in *Proceedings of the 4th International Conference on Internet of Things: Smart In-Novation and Usages (IoT-SIU)*, pp. 1–4, IEEE, Ghaziabad, India, April 2019.

[29] W. Shi, X. Zhang, Y. Wang, and Q. Zhang, "Edge computing: state-of-the-art and future directions," *Journal of Computer Research and Development*, vol. 56, no. 1, pp. 69–89, 2019.

[30] A. Jonathan, M. Ryden, K. Oh, A. Chandra, and J. Weissman, "Nebula: distributed edge cloud for data intensive comput-ing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 28, no. 11, pp. 3229–3242, 2017.

[31] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017.

[32] X. Zhang, Q. Chen, X. Peng, and X. Jiang, "Diffierential privacy-based indoor localization privacy protection in edge com-puting," in *Proceedings of the IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scal-Able Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pp. 491–496, IEEE, Leicester, UK, August 2019.

[33] S. Yi, Z. Hao, Q. Zhang, Q. Zhang, W. Shi, and Q. Li, "Lavea: latency-aware video analytics on edge computing platform," in *Proceedings of the Second ACM/IEEE Symposium on Edge Computing*, pp. 1–13, San Jose, CA, USA, October 2017.

[34] K. Intharawijitr, K. Iida, H. Koga, and K. Yamaoka, "Practical en-hancement and evaluation of a low-latency network model us-ing mobile edge computing,"vol. 1, pp. 567–574, in *Proceedings of the IEEE 41st Annual Com-puter Software and Applications Conference (COMPSAC)*, vol. 1, pp. 567–574, IEEE, Turin, Italy, July 2017.

[35] T. Cai, J. Li, A. S. Mian, R. Li, T. Sellis, and J. X. Yu, "Target-aware holistic influence maximization in spatial social networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 4347, p. 1, 2020.

[36] J. Li, T. Cai, K. Deng, X. Wang, T. Sellis, and F. Xia, "Community-diversified influence maximization in social networks," *Information Systems*, vol. 92, Article ID 101522, 2020.

[37] H. Liu, H. Kou, C. Yan, and L. Qi, "Keywords-driven and popularity-aware paper recommendation based on undirected paper citation graph," *Complexity*, vol. 2020, Article ID 2085638, 15 pages, 2020.

[38] Y. Chen, N. Zhang, Y. Zhang, X. Chen, W. Wu, and X. S. Shen, "TOFFEE: task offloading and frequency scaling for energy efficiency of mobile devices in mobile edge computing," *IEEE Transactions on Cloud Computing*, p. 1, 2019.

[39] L. Wang, X. Zhang, R. Wang, C. Yan, H. Kou, and L. Qi, "Diversified service recommendation with high accuracy and efficiency," *Knowledge-Based Systems*, vol. 204, Article ID 106196, 2020.

[40] Z. Ziming, L. Fang, C. Zhiping, and X. Nong, "Edge computing: platforms, applications and challenges," *Journal of Computer Research and Development*, vol. 55, no. 2, p. 327, 2018.

[41] C. Avasalcai, C. Tsigkanos, and S. Dustdar, "Decentralized resource auctioning for latency-sensitive edge computing," in *Proceedings of the IEEE International Conference on Edge Computing (EDGE)*, pp. 72–76, IEEE, Milan, Italy, July 2019.

[42] Q. He, G. Cui, X. Zhang et al., "A game-theoretical approach for user allocation in edge computing environment," *IEEE Transactions on Parallel and Distributed Systems*, vol. 31, no. 3, pp. 515–529, 2019.

[43] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdic, "Internet of medical things: a review of recent contributions dealing with cyber-physical systems in medicine," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3810–3822, 2018.

[44] M. Capra, R. Peloso, G. Masera, M. R. Roch, and M. Martina, "Edge computing: a survey on the hardware requirements in the internet of things world," *Future Internet*, vol. 11, no. 4, p. 100, 2019.

[45] L. Zhang, A. Afanasyev, J. Burke et al., "Named data networking," *ACM Sigcomm Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[46] A. C. Baktir, A. Ozgovde, and C. Ersoy, "How can edge comput-ing benefit from software-defined networking: a survey, use cases & future directions," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, p. 1, 2017.

[47] S. A. Noghabi, L. Cox, S. Agarwal, and G. Ananthanarayanan, "The emerging landscape of edge computing," *GetMobile: Mobile Computing and Communications*, vol. 23, no. 4, pp. 11–20, 2020.

[48] Z. Zhao, G. Min, W. Gao, Y. Wu, H. Duan, and Q. Ni, "Deploying edge computing nodes for large-scale iot: a diversity aware approach," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3606–3614, 2018.

[49] M. Sapienza, E. Guardo, M. Cavallo, G. La Torre, G. Leombruno, and O. Tomarchio, "Solving critical events through mo-bile edge computing: an approach for smart cities," in *Proceedings of the IEEE International Conference on Smart Computing (SMARTCOMP)*, pp. 1–5, IEEE, St. Louis, MO, USA, May 2016.

[50] M. Caria, J. Schudrowitz, A. Jukan, and N. Kemper, "Smart farm computing systems for animal welfare monitoring," in *Proceedings of the 40th International Convention on Information and Com-Munication Technology, Electronics and Microelectronics (MIPRO)*, pp. 152–157, IEEE, Opatija, Croatia, May 2017.

[51] L. Liu, X. Zhang, M. Qiao, and W. Shi, "Safeshareride: edge-based attack detection in ridesharing services," in *Proceedings of the IEEE/ACM Symposium on Edge Computing (SEC)*, pp. 17–29, IEEE, Seattle, WA, USA, October 2018.

[52] J. Cao, L. Xu, R. Abdallah, and W. Shi, "EdgeOS_H: a home op-erating system for internet of everything," in *Proceedings of the IEEE 37th International Conference on Distributed Computing Sys-Tems (ICDCS)*, pp. 1756–1764, IEEE, Atlanta, GA, USA, June 2017.

[53] Q. Zhang, Q. Zhang, W. Shi, and H. Zhong, "Distributed collaborative execution on the edges and its application to AMBER alerts," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3580–3593, 2018.

[54] M. Zheng, D. Xu, L. Jiang, C. Gu, R. Tan, and P. Cheng, "Challenges of privacy-preserving machine learning in IoT," in *Proceedings of the First International Workshop on Challenges in Artificial Intelligence and Machine Learning for Internet of Things*, pp. 1–7, New York, NY, USA, November 2019.

[55] B. Zhou and J. Pei, "The k-anonymity and l-diversity approaches for privacy preservation in social networks against neighborhood attacks," *Knowledge and Information Systems*, vol. 28, no. 1, pp. 47–77, 2011.

[56] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: privacy be-yond k-anonymity and l-diversity," in *Proceedings of the*

IEEE 23rd International Conference on Data Engineering, pp. 106–115, IEEE, Istanbul, Turkey, April 2007.

[57] L. Sweeney, "*k*-anonymity: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[58] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pp. 41–47, Washington, DC USA, November 2002.

[59] R. Kalaivani and S. Chidambaram, "Additive Gaussian noise based data perturbation in multi-level trust privacy preserving data mining," *International Journal of Data Mining & Knowledge Management Process*, vol. 4, no. 3, pp. 21–29, 2014.

[60] K. Liu, H. Kargupta, and J. Ryan, "Random projection-based mul-tiplicative data perturbation for privacy preserving distributed data mining," *IEEE Transactions on Knowledge and Data En-Gineering*, vol. 18, no. 1, pp. 92–106, 2005.

[61] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "Local diffierential privacy for deep learn-ing," *IEEE Internet of Things Journal*, vol. 7, pp. 5827–5842, 2020.

[62] Y. Donghuan, M. Wen, X. Liang, Z. Fu, K. Zhang, and B. Yang, "Energy theft detection with energy privacy preservation in the smart grid," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7659–7669, 2019.

[63] D. Xu, M. Zheng, L. Jiang, C. Gu, R. Tan, and P. Cheng, "Lightweight and unobtrusive privacy preservation for remote inference via edge data obfuscation," 2019, https://arxiv.org/abs/1912.09859.

[64] X. Xu, X. Liu, X. Yin, S. Wang, Q. Qi, and L. Qi, "Privacy-aware offloading for training tasks of generative adversarial network in edge computing," *Information Sciences*, vol. 532, pp. 1–15, 2020.

[65] J. Chi, E. Owusu, X. Yin et al., "Privacy partition: a privacy-preserving framework for deep neural networks in edge networks," in *Proceedings of the IEEE/ACM Symposium on Edge Computing (SEC)*, IEEE, Seattle, WA, USA, pp. 378–380, October, 2018.

[66] J. Chi, E. Owusu, X. Yin et al., "Privacy partitioning: protecting user data during the deep learning inference phase," 2018, https://arxiv.org/abs/1812.02863.

[67] H. Gamage, H. Weerasinghe, and N. Dias, "A survey on blockchain technology concepts, applications, and issues," *SN Computer Science*, vol. 1, pp. 1–15, 2020.

[68] A. Z. Ourad, B. Belgacem, and K. Salah, "Using blockchain for iot access control and authentication management," in *Proceedings of the Interna-tional Conference on Internet of Things*, pp. 150–164, Springer, Santa Barbara, CA, USA, October 2018.

[69] Y. Cheng, M. Lei, S. Chen, Z. Fang, and S. Yang, "IoT security ac-cess authentication method based on blockchain," in *Proceedings of the Interna-tional Conference on Advanced Hybrid Information Process-Ing*, pp. 229–238, Springer, Nanjing, China, September 2019.

[70] H. Rui, L. Huan, H. Yang, and Z. YunHao, "Research on secure transmission and storage of energy IoT Informa-tion based on blockchain," *Peer-to-Peer Networking and Applications*, vol. 13, no. 4, pp. 1225–1235, 2019.

[71] X. Xu, Q. Liu, X. Zhang, J. Zhang, L. Qi, and W. Dou, "A blockchain-powered crowdsourcing method with privacy preservation in mobile environment," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1407–1419, 2019.

[72] J. Zheng, X. Dong, T. Zhang, J. Chen, W. Tong, and X. Yang, "Mi-crothingschain: edge computing and decentralized IoT archi-tecture based on blockchain for cross-domain data shareing," in *Proceedings of the International Conference on Networking and Net-Work Applications (NaNA)*, pp. 350–355, IEEE, Xi'an, China, October 2018.

[73] H. T. T. Truong, M. Almeida, G. Karame, and C. Soriente, "To-wards secure and decentralized sharing of IoT data," in *Proceedings of the IEEE International Conference on Blockchain (Blockchain)*, pp. 176–183, IEEE, Seoul, Korea, May 2019.

[74] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learn-ing," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3516–3526, 2018.

[75] X. Lin, J. Li, J. Wu, H. Liang, and W. Yang, "Making knowledge tradable in edge-ai enabled iot: a consortium blockchain-based efficient and incentive approach," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6367–6378, 2019.

[76] S. Khanji, F. Iqbal, Z. Maamar, and H. Hacid, "Boosting iot efficiency and security through blockchain: blockchain-based car insurance process-a case study," in *Proceedings of the 4th International Conference on System Reliability and Safety (ICSRS)*, pp. 86–93, IEEE, Rome, Italy, November 2019.

[77] S. Fu, L. Zhao, X. Ling, and H. Zhang, "Maximizing the system energy efficiency in the blockchain based internet of things," in *Proceedings of the ICC 2019-IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, Shanghai, China, May 2019.

[78] W. Chen, Z. Zhang, Z. Hong et al., "Cooperative and distributed computation offloading for blockchain-empowered industrial internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8433–8446, 2019.

[79] X. Xu, X. Zhang, H. Gao, Y. Xue, L. Qi, and W. Dou, "Become: blockchain-enabled computation offloading for iot in mobile edge computing," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4187–4195, 2019.

[80] M. Singh, A. Singh, and S. Kim, "Blockchain: a game changer for securing IoT data," in *Proceedings of the IEEE 4th World Forum on Internet of Things (WF-IoT)*, pp. 51–55, IEEE, Singapore, February 2018.

[81] S. H. Hashemi, F. Faghri, P. Rausch, and R. H. Campbell, "World of empowered IoT users," in *Proceedings of the IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp. 13–24, IEEE, Berlin, Germany, April 2016.

[82] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: how do IoT devices use AI to enhance security?" *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41–49, 2018.

[83] H. Desai, M. Kantarcioglu, and L. Kagal, "A hybrid blockchain architecture for privacy-enabled and accountable auctions," in *Proceedings of the IEEE International Conference on Blockchain (Blockchain)*, pp. 34–43, IEEE, Atlanta, GA, USA, July 2019.