IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received February 7, 2018, accepted March 20, 2018, date of publication March 28, 2018, date of current version April 23, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2820162

Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues

JIALE ZHANG, BING CHEN, YANCHAO ZHAO, XIANG CHENG, AND FENG HU
College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China

Corresponding author: Bing Chen (cb_china@nuaa.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB0802303, in part by the National Natural Science Foundation of China under Grant 61672283 and Grant 61602238, and in part by the Natural Science Foundation of Jiangsu Province under Grant BK20160805.

ABSTRACT With the explosive growth of Internet of Things devices and massive data produced at the edge of the network, the traditional centralized cloud computing model has come to a bottleneck due to the bandwidth limitation and resources constraint. Therefore, edge computing, which enables storing and processing data at the edge of the network, has emerged as a promising technology in recent years. However, the unique features of edge computing, such as content perception, real-time computing, and parallel processing, has also introduced several new challenges in the field of data security and privacy-preserving, which are also the key concerns of the other prevailing computing paradigms, such as cloud computing, mobile cloud computing, and fog computing. Despites its importance, there still lacks a survey on the recent research advance of data security and privacy-preserving in the field of edge computing. In this paper, we present a comprehensive analysis of the data security and privacy threats, protection technologies, and countermeasures inherent in edge computing. Specifically, we first make an overview of edge computing, including forming factors, definition, architecture, and several essential applications. Next, a detailed analysis of data security and privacy requirements, challenges, and mechanisms in edge computing are presented. Then, the cryptography-based technologies for solving data security and privacy issues are summarized. The state-of-the-art data security and privacy solutions in edge-related paradigms are also surveyed. Finally, we propose several open research directions of data security in the field of edge computing.

INDEX TERMS Edge computing, data security, cryptography, authentication, access control, privacy.

I. INTRODUCTION

The proliferation of the IoT [1] and 5G network architecture [2] is boosting the arrival of new service models and essential applications, such as intelligent transportation, smart city, augmented reality, location services and etc. With IoT, there will be an explosive growth with a larger number of sensing devices, such as smart-phones, wearable devices, smart home appliances and etc., which will generate massive sensing data from the physical world. According to the estimation by Cisco Global Cloud Index (GCI) [3], the data produced by IoT devices, people, machines will exceed 500 Zettabytes (ZB) by 2020. However, the global data center IP traffic will only reach 15.3 ZB at that time [4], [5]. Such dilemma urges us to move forward to the era of the Internet of Everything (IoE) [6], [7], which not only produces but also processes the massive data at the edge of the network. Compared with IoT, the IoE focuses more on the intelligent connection of people, processes, data and things rather than communication between machines and IoT devices [8]. With the promotion of IoE, the devices at the edge of the network are changing from data consumers to data producers with big data processing capability, such as data acquisition, pattern recognition, and data mining. At the same time, these edge devices provide a rich service interface, providing collaborative computing services for users together with cloud computing centers.

In the era of IoE, by 2018, 50% of IoT network will be saturated due to the bandwidth limitation, and 40% of Edge-Created data will be analyzed, processed, and stored at the edge of the network, as estimated by Internet Data Center (IDC) [9]. In this case, the centralized cloud computing model has shown the inherent problems, which can be

2169-3536 © 2018 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

summarized as follows: 1) Linear growth computing capabilities of cloud computing cannot meet the multi-sources data processing requirements of massive data at the edge of network; 2) The network bandwidth and the transmission speed have come to a bottleneck because of the large scale of user access, while the long distance transmission between user and cloud center will lead to the high service latency and waste of computing resources; 3) User private data in edge devices is likely to be leaked during the outsourcing process. Therefore, the traditional cloud computing cannot efficiently support the IoE-based application services [10], and the edge computing arises at the historic moment [11], [12] to adapt to the era of IoE. Combined with existing cloud computing, edge computing can efficiently handle the edge big data processing problems.

In edge computing paradigm, the data can be processed close to, or at the edge of the network. Here, the edge of the network refers to the counterpart of the network core, where the connected entities directly produce the data. These entities could equip with the edge computing platforms which synthesis with network, storage, computation, and other core functions. These functions greatly offload the computation and communication burden of the network core. Meanwhile, processing data near the sources of data also provides better QoS for the delay sensitive services and better structure support for the user privacy and data security. At present, some related paradigms, such as mobile cloud computing [13], [14], fog computing [15]–[18], which is the predecessor or counterparts of edge computing, can provide the efficient solutions for massive data processing, and meanwhile improve the user experience.

Due to the distinct benefits and characteristics of edge computing paradigm, such as heterogeneity distributed architecture, massive data processing, parallel computation, location-awareness and requirement of mobility support, the traditional data security and privacy-preserving mechanisms in cloud computing are no longer suitable for protecting massive data security in edge computing. In particular, secure data storage, secure data computation, authentication, access control, and privacy protection issues are especially prominent. For example, edge computing is a distributed interactive computing system with multiple trust domains where coexistence of multiple functional entitles, the authentication mechanism not only requires the identity validating for each entity in one trust domain, but also needs all entitles to mutually authenticate each other among different trust domain. Moreover, for some resource-constrained end devices, it is impossible to store a large amount of data or to execute a high complexity security algorithm. In summary, the data security and privacy-preserving in edge computing mainly faced with the following new challenges:

- **Lightweight & Fine-grained:** New requirements for lightweight data encryption methods and fine-grained data sharing systems based on multiple authorized parties in edge computing.
- **Distributed access control:** Multi-sources heterogeneous data dissemination control and secure data management issues in distributed computing paradigm.
- **Resource-constrained:** Security challenges between large-scale edge services and resource-constrained edge devices.
- **Efficient privacy-preserving:** New requirements of efficient privacy-preserving mechanisms for various edge services and edge computing models faced with IoE.

The aforementioned data security and privacy-preserving challenges of edge computing paradigm motivate us to provide a comprehensive literature survey. The main contributions of this article are summarized as follows:

- A detailed analysis of the forming factors of edge computing is summarized from the holistic perspective. A comprehensively review of edge computing definition and architecture are presented. The promising applications for edge computing are also introduced.
- The data security and privacy requirements are summarized based on five critical metrics, including the confidentiality, availability, integrity, authentication and access control, and privacy requirements. Then, a comprehensive analysis of potential security and privacy challenges in edge computing is pointed out. In particular, the existing data security and privacy-preserving mechanisms are presented, and a research architecture of data security is proposed as well.
- A comprehensive summary of the cryptography-based technologies for solving data security and privacy issues are described, including identity-based encryption, attribute-based encryption, proxy re-encryption, homomorphic encryption, and searchable encryption. Furthermore, a detailed analysis and comparison of the state-of-art data security and privacy solutions are given, and the features of the solutions are pointed out.
- A discussion of open issues and future research directions is presented, including lightweight and distribute data encryption, cross-domain authentication, multi-authority access control system, dynamic data processing, fine-grained privacy-preserving and so on.

The rest of the paper is organized as follows. Section II gives a comprehensive overview of edge computing including the forming factors, definition, architecture and its applications. Section III summarizes the requirements and challenges of data security and privacy in edge computing, and also introduces the existing data security and privacy mechanisms and a research architecture is given. Then, the cryptography-based techniques for data security are explored in section IV. Section V presents a detailed analysis of the state-of-the-art data security and privacy-preserving solutions in edge-related paradigms with respect to data confidentiality, data integrity, authentication, access control and privacy-preserving. Section VI discusses the open research directions of edge computing. Finally, conclusions are drawn in section VII. To clearly illustrate the overall

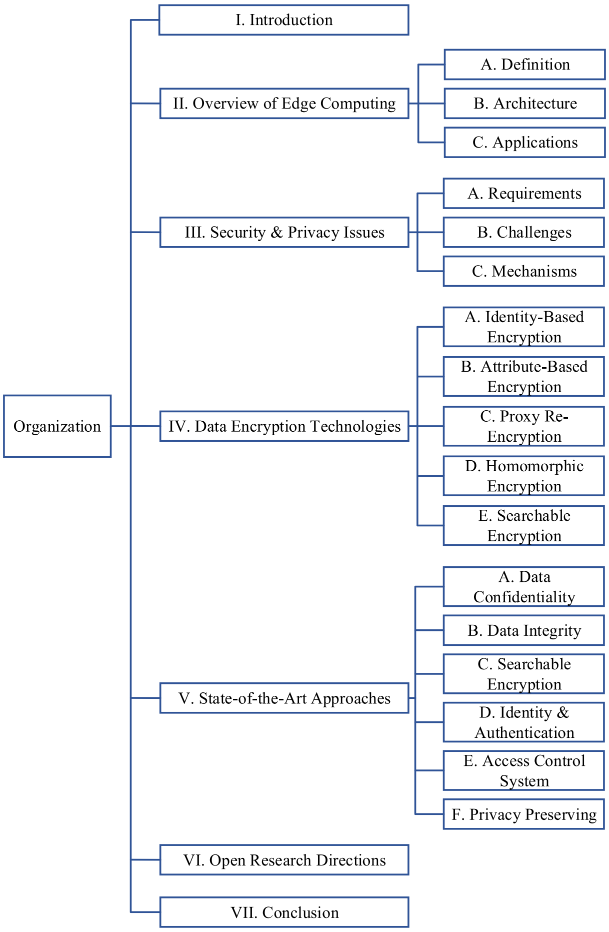


FIGURE 1. Organization of this paper.

structure, an organizational framework of this paper is shown in Fig. 1.

II. OVERVIEW OF EDGE COMPUTING

With the rapid development and extensive application of the IoT, big data and 5G network architecture, the massive data generated by the edge equipment of the network and the real-time service requirements are far beyond the capacity of the traditional cloud computing model. Previous work such as micro data center, [19], [20], mobile cloud computing [13], [14], fog computing [15], [16], cloudlet [21], and cloud-sea computing [22] have been introduced to reduce the storage and computation load in cloud computing. Recently, the mobile edge computing [17], [18] has been presented as a novel architecture to support the computation offloading process which extends the cloud computing services to the edge of the network. In this section, we briefly present an overview of edge computing. Firstly, we explain why we need edge computing so urgent by listing the forming factors. Then we give a definition and a four-layer architecture of edge computing. We also introduce some applications which have received extensive attention by academic and industrial areas, such as cloud offloading, video analytics, smart grid, Internet of vehicles and etc.

A. FORMING FACTORS OF EDGE COMPUTING

1) THE SHORTCOMING OF CLOUD COMPUTING

The traditional cloud computing paradigm is a centralized model to process the data at the remote data center. It would raise some drawbacks because of the proliferation of IoT and the massive data collected by the huge terminal devices [23]. Firstly, the perceptual layer data of IoT is in a massive level and there are frequent conflict and cooperation between data [24], which means the computation capabilities with linear growth of centralized cloud computing cannot meet the multi-sources data processing requirement of massive edge data. Secondly, the network bandwidth and the transportation speed have come to a bottleneck because of the large scale of user access and the long distance data transmission between user and cloud data center, this situation will leads to the high network latency and the waste of computing resources. Thirdly, most of the end users in the edge of the network are usually resource-constraint mobile devices, which have low storage and computation capability and limited battery life, so it is necessary to offload some computing tasks to the edge without long distance transmission to cloud data center. Lastly, data security and privacy-preserving are big challenges in cloud computing due to the long distance transmission and outsourcing features, so that processing data in the edge could reduce the risk of privacy leakage [25].

2) THE ERA OF INTERNET OF EVERYTHING

According to the estimation by Cisco Global Cloud Index (GCI) and Internet Business Solutions Group (IBSG), the data produced by IoT devices will exceed 500 Zettabytes (ZB) while the global data center IP traffic will only reach 15.3 ZB by 2020 [3], and there will be more than 50 billion devices connected to the Internet [4]. In addition, the concept of "sensing information" began to gradually extend to the IoT system which will speed up the arriving of the IoE era [6].

3) CHANGE FROM CONSUMER TO PROSUMER

In the traditional cloud computing paradigm, the end user usually plays a role as the data consumer, such as scanning images in a web browser, watching videos on YouTube or consulting documents in a file management system. However, the role of end user is changing from the data consumer to the data *Prosumer* (producer + consumer), which means people are also producing data on their IoT devices at the edge. For example, in every single minute, YouTube users upload nearly 100 hours video contents and Instagram users post 2430000 photos. In this case, processing data in the edge could improve the user experience with fast computation applications [18].

B. WHAT IS EDGE COMPUTING

The Pacific Northwest National Laboratory (PNNL) introduces the edge computing [26] as an approach to push the frontier of computing applications, data, and services away from centralized nodes to the logical extremes of a network, and it enables analytics and knowledge generation to occur at the source of the data. The Edge Computing Consortium (ECC) defines the edge computing [27] as an open platform deployed on the edge of the network that is close to the source of the data, and provides intelligent services to meet the requirements of real-time processing, data optimization, security and privacy by mobile edge network infrastructure [28]. Shi *et al.* [11] say in their article, the edge computing refers to the enabling technologies allowing computation to be performed at the edge of the network, where the downstream data on behalf of cloud services and upstream data on behalf of IoT service. In summary, we can say, *edge computing is a novel computing model that allowing storing and processing data at the edge of the network, and providing intelligent services near the source of the data by collaborating with cloud computing.*

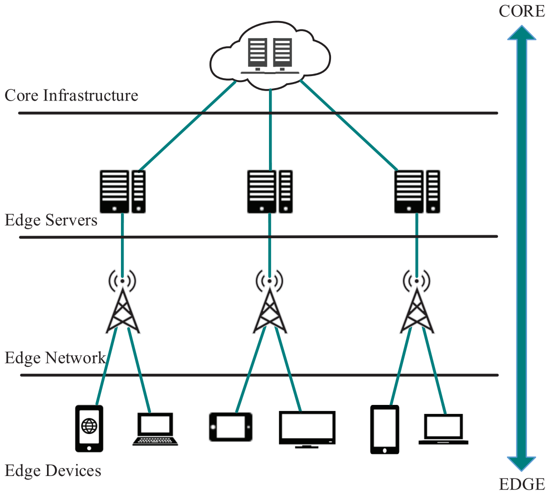


FIGURE 2. **Architecture of edge computing.**

Fig. 2 illustrates the general architecture of edge computing, which consists of a four-layer functional structure: core infrastructure, edge servers, edge network and edge devices. Firstly, core infrastructure provides the core network access (e.g. Internet, mobile core network) and centralized cloud computing services and management functions for mobile edge devices. Secondly, edge servers, which are owned and deployed by the infrastructure provider and equipped with multi-tenant virtualization infrastructure, are responsible for providing virtualized and multiple management services. Besides, the edge can deploy multiple edge data centers which cooperate with one another and will not disconnect from the traditional cloud. In addition, edge computing infrastructure realizes the connection between edge devices, edge servers and the core infrastructure with wireless network, data center network and the Internet. Finally, edge devices include all types of devices connected to the edge network (e.g. mobile terminals, IoT devices) which are not only play role as data consumers, but also data producers to participate in the distributed infrastructure for all four layers.

C. APPLICATIONS OF EDGE COMPUTING

Compared to traditional centralized cloud computing architecture, researchers found the edge computing has lots of promising applications in various aspects. Next, we will give several case of emerging application scenarios in detail.

1) CLOUD OFFLOADING

With the rapid increase of terminal devices (e.g. smartphones, wearable devices, laptops, and Internet TVs), lots of low-latency demand applications (e.g. self-driving car, virtual reality, and remote operation) for this devices require real-time processing to make correct decisions. In the traditional cloud computing paradigm, the data and requests produced by end users are usually processed in the cloud, which means longer latency would happen in such centralized computing paradigm because of long distance transmission. In edge computing, the edge entities usually have certain computation resources which could provide an opportunity to offload some or all workloads by caching data and operations at the edge of cloud. This offloading idea is somewhat similar to the traditional content delivery network (CDN) [29], but the difference is that the data and its processing operations are all needed to be cached in edge computing while only the data is cached in CDN. Numbers of researchers have addressed the improvement of user experience by offloading the computationally intensive workloads to the edge server in mobile edge computing environment [30]–[33]. By leveraging edge computing, the quality of computation efficiency and the user experience for time-sensitive applications could be improved significantly.

2) VIDEO ANALYTICS

Video analytics, as an emerging technology, can be loosely defined as an autonomous understanding of events occurring in a scene monitored by multiple video cameras. One potential application of video analytics that cloud benefit from edge computing is video surveillance system [34]. With the rapid increase of IoT devices, practical surveillance systems deployed today are not yet capable of autonomous analysis of complex events in massive cameras. Traditional cloud computing has a serious deficiency that the video feeds from millions of surveillance cameras cannot be analyzed in real time due to the high data transmission latency and privacy concerns. With the collaboration of edge computing, the results of video analytics can be generated from the cloud and distributed to the local edge servers in a specified area. Every user can perform operations with their requests in this local edge servers, and only need to report the operational results to the cloud. In this situation, video analytics can achieve real time and fast transmission of results, and meanwhile autonomous requests analysis in the cloud [35].

3) SMART GRID

Smart grid, as the next-generation approach of delivering electricity to millions of households worldwide, is a combination of the electrical grid and power infrastructure, which supplemented by information and communication technology (ICT) [36]. Each smart grid infrastructure consists of several functional entities, such as unique operating center, communication gateways, and individual users, which is distributed connection with cloud computing. All the private information, such as power consumption data, collected by the smart meters can be used for grid analysis or pricing. With the edge computing paradigm, it is possible to store and process the power consumption data on the edge servers, e.g. micro grids [18] and smart meters, and balance the load of cloud data centers.

4) INTERNET OF VEHICLES

In the vehicular networks, Vehicles can connect with infrastructure (V2I) and other vehicular terminals (V2V) by the Road Side Units (RSUs), the RSUs need to provide the real-time vehicular services for a large number of mobility vehicles through distributing computation tasks [37]. Driven by the development of the Internet of Vehicles (IoV), there are more smart vehicles on the road now, and each of these vehicles is equipped with a computation unit to realize the intelligent traffic applications. In this paradigm, the vehicular network can achieve the two-way communication efficiently by deploying edge servers on the RSUs, and meanwhile push the cloud service to the edge of the RSUs by integrating of communication and computation mechanisms [38]. In addition, by leveraging edge computing, the advance Internet of vehicles applications, such as autonomous driving, real-time information processing, and mobility-aware computation, could be effectively promoted.

Some other smart applications, such as smart healthcare [39], smart home [40], smart city [41], big data analytics [42], and software-defined networks [43] also need a bridging point between cloud center and sensors to supporting the efficient services by edge computing.

III. DATA SECURITY AND PRIVACY ISSUES

Edge computing can offload some storage and computation tasks from cloud data centers to the edge of the network, and that could raise many challenges related to security and privacy concerns. In particular, data security and privacy protection are the most important services [11] in edge computing, which is our major concerning in this survey. This section summarizes the security and privacy requirements and challenges in edge computing. We also established a research architecture of data security in edge computing, including data confidentiality, data integrity, secure data search, authentication, access control and privacy-preserving.

A. DATA SECURITY AND PRIVACY REQUIREMENTS

No matter whether it is cloud computing or edge computing, the end user's privacy data needs to be partially or completely outsourced to third parties (such as cloud data center or edge data centers), and its ownership and control are separated, which will easily lead to data loss, data leakage, illegal data operations (replication, publishing, dissemination) and other data security issues, data confidentiality and integrity cannot be guaranteed. Therefore, the security of outsourcing data is still a fundamental problem of edge computing data security [25], [44].

- Confidentiality: The confidentiality is a fundamental requirement that ensures only data owner and user(s) could access the private information in the edge computing. It prevents unauthorized parties access to the data when the users' private data is transmitted and received in edge or core network infrastructure, and stored or processed in edge or cloud data center.
- Integrity: The integrity is under an obligation to ensure the correct and consistent delivery of data to the authorized user(s) without any undetected modification of the data. The absence of integrity auditing measures could affect the users' privacy.
- Availability: For edge computing, the availability ensures that all the authorized parties are able to access the edge and cloud services at any places as per users' requirements. In particular, it also means that the users' data which stored in edge or cloud data center with ciphertext form, can be processed under different operational requirements.
- Authentication and access control: The authentication ensures the identity of a user is authorized which means it is a process of establishing proof of user's identities. Furthermore, the access control acts like a bridging point of all the security and privacy requirements by the control strategy, it determines who can access the resources (authentication) and what kind of actions can perform such as reading (confidentiality) and writing (integrity).
- Privacy requirement: The security mechanisms are used to guarantee that all the outsourcing information of users, such as data, personal identity, and location, to be secret under the honest but curious adversaries. In addition, the data security mechanisms, like encryption, integrity auditing, authentication and access control, can preserve the privacy of the users directly or indirectly in edge computing.

B. DATA SECURITY AND PRIVACY CHALLENGES

Edge computing utilizes many recent technologies, such as offloading, virtualization, and outsourcing, to put the computing in the proximity of data sources. In this case, data security and privacy-preserving have become the basic requirements to protect end users in their business, economics, and daily life. Besides, we must admit that security and privacy should be addressed in every layer in designing edge computing systems. In this subsection, we point out the potential security and privacy challenges based on the four-layer architecture of edge computing. A summary of data security and privacy challenges classification can be noted in Table 1.

TABLE 1. Categorization of challenges in edge computing paradigm.

Asset	Core Infrastructure	Edge Servers	Edge Network	Mobile Edge Devices
Challenges	● Privacy leakage ● Data tampering ● Denial of service ● Service manipulation	● Privacy leakage ● Denial of service ● Privilege escalation ● Service manipulation ● Rogue data center ● Physical damage damage	● Denial of service ● Man-in-the-middle ● Rogue gateway	● Injection of information ● Service manipulation

1) CORE INFRASTRUCTURE SECURITY

It is worth mentioning that, all edge paradigms may be supported by several core infrastructures, such as centralized cloud service and the management systems, these core infrastructures may be managed by the same third party suppliers, such as mobile network operators. This would raise enormous challenges, such as privacy leakage, data tampering, denial of service attacks and service manipulation, because of these core infrastructure may be semi-trusted or completely untrusted. Firstly, the user's personal and sensitive information could be accessed or stolen by unauthorized entities or honest but curious adversaries. This will lead to the challenges of privacy leakage and data tampering. Besides, edge computing allows exchanging information directly between edge devices and edge data centers which may bypass the central systems. It is possible for core infrastructure to provide and exchange false information when the services are hijacked and jammed, which may cause the denial of services attacks. In addition, the information flow can be manipulated by an internal adversary who has sufficient access privileges, which will provide bogus information and false services to other entities. Due to the decentralized and distributed nature of edge computing, this type of security issue may not be able to affect the whole ecosystem, but this is still a security challenge that cannot be ignored.

2) EDGE SERVERS SECURITY

Edge servers (or edge data centers) are in charge of the virtualized services and several management services by deploying the edge data centers in a specific geographical location as same as a multi-cloud scenario. In this case, both internal and external adversaries can access the edge data center and may steal or tamper the sensitive information. If the adversaries have gained enough control privilege of the edge data center, then they can abuse their privileges as a legitimate administrator or can manipulate the services. As a consequence, the adversaries can execute several types of attack, such as man-in-the-middle attacks, denial of service attacks and etc. Moreover, there is an extreme situation that an adversary can control the entire edge server or can forge a false infrastructure, and the attacker can completely control all the services and direct the information flow to his rogue data center. Another security challenge is the physical attack of an edge data center. The main reason for this type of attack is possible that the physical protection of this edge infrastructure is careless or non-involved. It is worth mentioning that, this physical attack is limited to a specific local scope, and only the services in a particular geographical region will be disabled due to the distributed deployment of edge servers.

3) EDGE NETWORK SECURITY

As aforementioned, edge computing realizes the interconnection of IoT devices and sensors by the integration of multiple communication, such as mobile core network, wireless network and the Internet, which rise many network security challenges of these communication infrastructures. By employing the servers at the edge of the network, the traditional network attacks, such as denial of service (DOS) and distributed denial of service (DDOS) attacks, can be limited efficiently. Such attacks will only disrupt the vicinity of the edge networks and not much effect on the core network, also, the DOS or DDOS attacks occurred in core infrastructure might not seriously interfere with the security of the edge data centers. In addition, malicious adversaries can launch attacks such as eavesdropping or traffic injection attacks to control the communication network. Particularly, the man-in-the-middle attack highly possible to affect all the functional elements of edge network by hijacking the network stream information, such as information, network data flow, and virtual machines. Another edge network security challenge is rogue gateway which deployed by malicious adversaries. In this type of attack, the entire edge network infrastructure is injected with traffic, and the output the same result as the man-in-the-middle attack.

4) EDGE DEVICES SECURITY

In edge computing, the edge devices played as active participants in the distributed edge environment at different layers, so that even small portion compromised edge devices could lead to harmful results for the whole edge ecosystem. For example, any devices manipulated by an adversary can try to disrupt the services with the injection of false information or intrude the system with some malicious activities. In addition, malicious devices can manipulate services in some particular scenarios, where the malicious adversaries have gained the control privilege of one of these devices.

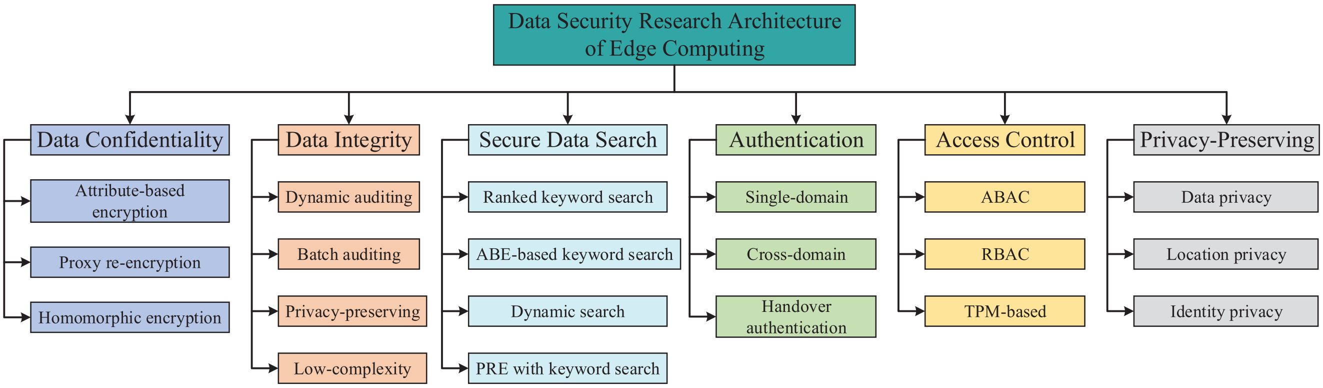


FIGURE 3. Data security research architecture of edge computing.

For example, an edge device connected in one trust domain can act as an edge data center of other devices.

C. DATA SECURITY AND PRIVACY MECHANISMS

In order to create a sustainable edge paradigm ecosystem with security and available services, it is crucial to implement various types of security and privacy mechanisms, and prevent any attraction from malicious adversaries. This subsection presents the existing security and privacy mechanisms that can be used in edge computing paradigm. Furthermore, we also built a data security research architecture for edge computing as is shown in Fig. 3.

1) DATA CONFIDENTIALITY

In edge computing, user private data is outsourced to the edge server and its ownership and control are separated, which causes users to lose their physical control over the outsourced data. Apart from that, the sensitive data in the outsource storage status are extremely giving rise to the data loss, data breach, illegal data operations (e.g. copy, delete and dissemination). To address these threats, suitable data confidentiality scheme should be proposed to protect the private data in the context of edge computing, which means the user sensitive data from edge devices has to be encrypted before outsourced to the edge servers. At present, data confidentiality and secure data sharing schemes are typically implemented using encryption techniques, the conventional process is that the data producer encrypts the outsourced data and uploads to the data center, and then decrypted by the data users when they required. The traditional encryption algorithm includes the symmetric encryption algorithm (e.g. AES, DES, and ADES) and the asymmetric encryption algorithm (e.g. RSA, Diffie-Hellman, and ECC), but the operability of the ciphertext data obtained by traditional encryption algorithm is usually low, that will be caused great obstacles to the subsequent data processing. In recent years, techniques such as identity-based encryption [45], attribute-based encryption [46], proxy re-encryption [47] and homomorphic encryption [48] are combined to build several data encryption methods for secure data storage system, and allows users to store its private data as ciphertext on untrusted edge servers.

2) DATA INTEGRITY

Data integrity is an important issue for the security of edge computing since the user data is outsourced to the edge servers while the data integrity could be compromised during this process. It refers to the process that data owners check the integrity and availability of outsourced data to make sure that there are no undetected modifications of data by any unauthorized users or systems. In edge computing, the research of data integrity should be focused on the following four functional aspects: batch auditing [49], dynamic auditing [50], privacy-preserving [51], and low complexity [52].

3) SECURE DATA COMPUTATION

Secure data computation is another crucial issue that needs to be addressed in edge computing. The sensitive data from end users are usually outsourced to edge computing servers with ciphertext form. In this case, the secure data search is the biggest challenge which means the user has to solve the problem of keyword search over the encrypted data files. With the efforts of researchers, several searchable encryption methods have been presented to support the securely search over encrypted data through keywords without decrypt operation. For example, secure ranked keyword search scheme [53] can obtain the correct search results through the certain relevant criteria and index. In addition, further implementation of various functions on the basis of secure data search is an important challenge, such as the attribute-based keyword search scheme [54] can support fine-grained data sharing, the dynamic search method [55] is able to achieve the dynamic updating, and the proxy re-encryption with keyword search approach [56] can realize the control of search privilege.

4) AUTHENTICATION

Edge computing is a distributed interactive computing system with multiple trust domains where coexistence of multiple functional actors, services and infrastructures. Without any authentication mechanisms, it is quite possible for external adversaries to access the sensitive resources of the service infrastructure, and the internal adversaries can erase the malicious access traces due to their legitimate access authority. In this context, it is necessary to explore authentication enforcement approaches in edge computing to protect users against existing security and privacy issues and minimize the internal and external threats. Moreover, the edge computing environment not only requires the identity validating for each entity in one trust domain, but also needs entities to mutually authenticate each other among different trust domain. At present, the appropriate authentication methods include the single-domain authentication [57], cross-domain authentication [58], and handover authentication [59].

5) ACCESS CONTROL

Due to the outsourcing feature of edge computing, if there are no efficient authentication mechanisms in that place, any malicious users without an authorized identity can abuse the service resources in edge or core infrastructure. This introduces a big security challenge for the secure access control system, for example, the virtualization resource of edge servers cloud be accessed, misused, and modified by edge devices if they hold any certain privileges. In addition, in distributed edge computing paradigm, there are multiple trust domains by different infrastructures coexisted in one edge ecosystem, so it is essential to develop the fine-grained access control system in every trust domain. However, most of the traditional access control mechanisms are usually addressed in one trust domain, and not suitable for multiple trust domains in edge computing. Several cryptography-based solutions, such as attribute-based encryption [60] and role-based encryption [61] methods, can be used to achieve flexible and fine-grained access control. Besides, there are some other security mechanisms like TPM-based access control [62] might be suitable for certain edge computing paradigm.

6) PRIVACY PRESERVING

Privacy is one of the major challenges in other computing paradigms as the end users' sensitive data and personal information are shifted from edge devices to the remote servers. In edge computing, privacy issue is more significant because there are a number of honest but curious adversaries, such as edge data centers, infrastructure providers, services providers, and even some users. These attackers are usually authorized entities whose secondary goal is to gain more sensitive information that can be used in various egoistic ways. In this situation, it is not possible to know whether a service provider is trustworthy in such open ecosystem with different trust domains. For example in smart grid, a lot of private information of a household can be disclosed from the reading of the smart meters or some other IoT devices, it means that no matter the house is vacant or not, if the smart meters were manipulated by a malicious adversary, the user's privacy is absolutely leaked.

In particular, the leakage of private information, such as data, identity and location, can lead to the very serious situations. Firstly, edge servers and sensor devices can collect sensitive data from the end devices, techniques such as data aggregation based on homomorphic encryption can provide a privacy-preserving data analysis without decryption. Probabilistic public key encryption [63] and pseudo-random permutation [64] can be used to design lightweight data privacy-preserving methods. Secondly, in the dynamic and distributed computing environment, it is necessary for users to protect their identity information during the authentication and management processes [65], [66]. Finally, the location information of users is quite predictable as they usually have a relatively fixed point of interests (POIs), which means users will probably make use of the same edge servers repeatedly. In this case, we should pay more attention to protecting our location privacy [67], [68].

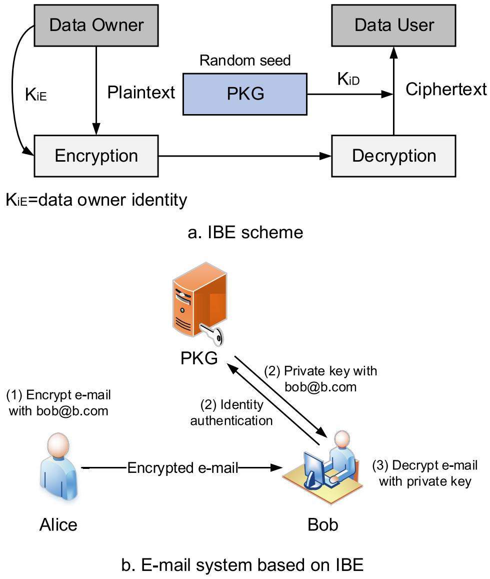
IV. DATA SECURITY TECHNOLOGIES: CRYPTOGRAPHY

In the edge computing paradigm, the edge devices are more reliable and powerful than cloud computing terminals, they are not only data consumers, but also play the role of data producers. For an edge user, the benefits from edge thing are as follows: computing offload, data caching, storage and processing, less maintenance cost, minimal transmission consumption and response time, as well as the distribute request and delivery service from edge things, results in a higher level of resource utilization, and therefore, imposes little electricity cost to service providers. Although the edge computing model has several benefits compared to traditional cloud computing paradigm, there are still security concerns that emerged as an obstacle to adoption of edge computing paradigm.

In this survey, we distinguish between the techniques and the solutions for data security and privacy-preserving. This section thoroughly explores the idea and the architecture of the five main cryptosystems, including identity-based encryption, attribute-based encryption, proxy re-encryption, homomorphic encryption, and searchable encryption. These crypto-systems are very useful to construct a secure and reliable data encryption techniques to ensure the confidentiality of outsourcing data in cloud, edge and distributed computing. Furthermore, a cryptography-based technique, called searchable encryption, which widely used in secure data computation is introduced.

A. IDENTITY-BASED ENCRYPTION

The identity-based encryption was proposed by Shamir [69] as a simplification scheme of certificate management in e-mail systems. This scheme enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public key, without keeping key directories, and without utilizing the services of a third party. The IBE scheme allows users to select an arbitrary


Data Owner
Data User
Random seed
K_{IE}
Plaintext
PKG
K_{ID}
Ciphertext
Encryption
Decryption
K_{IE}=data owner identity
PKG
(2) Private key with bob@b.com
(1) Encrypt e-mail with bob@b.com
(2) Identity authentication
Encrypted e-mail
(3) Decrypt e-mail with private key
Alice
Bob

a. IBE scheme

b. E-mail system based on IBE

FIGURE 4. **Identity-based encryption scheme and application.**

string that provides a unique identity for him to the other party as a public key, compared with the traditional Public Key Infrastructure (PKI) technology, the users' private key in IBE is generated by using a Private Key Generator (PKG) instead of by a public Certificate Authority (CA) or users. The IBE scheme includes three main phases: 1) Encryption: When Alice sends an email to Bob, the email will be encrypted by Bob's email address (bob@b.com) as the public key, 2) Identity authentication: Upon Bob received the encrypted email, he needs to authentication himself and gets private key from the PKG, 3) Decryption: Bob decrypts the encrypted email and get the massages. Fig. 4 shows the identity-based encryption scheme and a general application in e-mail systems.

The basic IBE scheme proposed by Shamir exists two problems that cannot be ignored: 1) how can Bob prove his identity to multiple trusted third parties? 2) How can a trusted third party securely send Bob's private key to Bob's hand? To solving these two problems, a series of improved IBE schemes have been proposed. In 1984, Tanaka [70] proposed a modified IBE realization scheme based on the discrete logarithm and large integer decomposition problem, and then, the scheme introduces the concept of the threshold to solve the collusion attack problem in which the problem has not been considered in Shamir IBE scheme. In 1989, Tsuji and Itoh [71] improved the basic IBE scheme and proposed an ID-based cryptosystem based on ElGamal public key cryptosystem, this scheme also used the discrete logarithm problem to ensure the security. Until 2003, Boneh and Franklin [45] proposed a fully functional IBE scheme based on the bilinear maps between groups and the computational Diffie-Hellman assumption that can be widely used. The PKG in this scheme can be distributed by using a standard technique from threshold cryptography, so that the users can delegate the duty to third parties by giving one private key to each of them in accordance with their responsibility.

B. ATTRIBUTE-BASED ENCRYPTION

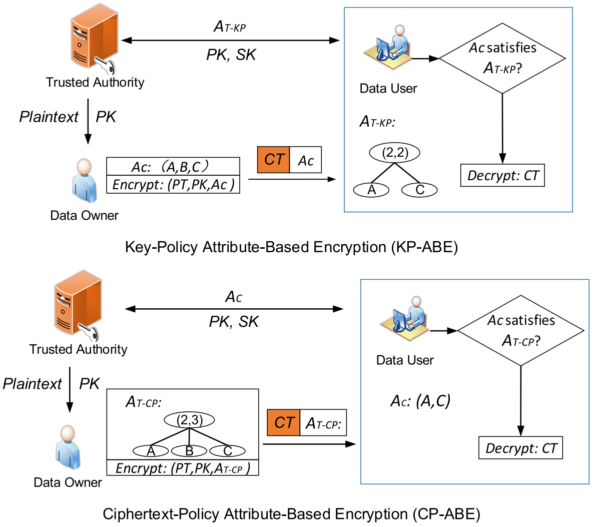
Attribute-based encryption (ABE) is a cryptographic primitive to control the decryption ability of the data owner over the encrypted data. An attribute-based access control system consists of two entities: 1) Trusted authority (TA) who is in charge of publishing attribute keys and managing users' attribute set, 2) The user includes the message sender and the receiver which correspond to the data owner and user. Sahai and Waters [72] proposed the basic Attribute-Based Encryption (fuzzy IBE) as a re-construction of IBE scheme in which the identities are replaced of a set attributes. In ABE scheme, each attribute of the user is mapped to the Z_p^* by the hash function, which the ciphertext and secret keys are related to the attributes. The ABE scheme also supports the threshold strategy based on the attributes, which means when the number of intersecting elements of users' and ciphertexts' attribute set reaches the threshold parameter specified by the system, the decryption operation can be executed. For example, an ABE mechanism defined an attribute set of data owner as (A, B, C, D) which related by private key and ciphertext, and let 2 be the threshold value by the ABE system, then a data user with attribute set (A, C, G) can access the ciphertext, while a data user with attribute set (B, H) cannot access the ciphertext. In another word, a data user can decrypt a ciphertext by his secret key w_1, if and only if at least t components of the ciphertext are matched with data owner's private key components w_2 $(|w_1 w_2| \geq t)$ where t shows the minimal overlap of two attribute sets.

The basic ABE scheme can only represent the "threshold" operation of the attribute, which the threshold parameter is set by the authority. As a result of this feature, the access control policy is totally determined by the third party, which may cause the privilege abused, service manipulation and privacy leakage. In many practical applications, they need flexible access control policies to support AND-OR-INVERT and threshold operations for attributes, so that the data sender can specify the access control policies when encrypting data. The basic ABE scheme was improved as two main types, as follows:

1) Key-Policy Attribute-Based Encryption (KP-ABE) was proposed by Goyal *et al.* [73] based on the monotonic access structure which consists only of AND, and OR gates. In KP-ABE cryptosystem, the ciphertext is labeled with sets of attributes and private keys are associated with access-tree structure that controls which ciphertext a user is able to decrypt. The interior nodes of the access tree (A_{T-KP}) are threshold policies, which are consisted of the number of leaf nodes x and a threshold value k where $0 < k \leq x$. A user is able to decrypt the ciphertext if and only if the access tree associated with a private key is satisfied by the attribute set associated with a ciphertext. As the Goyal's KP-ABE scheme cannot support the "INVERT" operation,

TABLE 2. Comparison basic ABE, KP-ABE and CP-ABE methods.

Cryptosystems	Access Structure	Applications	Assumption	Supported Policy
Basic ABE [72]	Trusted Authority	Simple	DBDH	Threshold
KP-ABE [73]	In Private Keys	Data Query	DBDH	AND, OR, Threshold
CP-ABE [74]	In Ciphertexts	Access Control	Group Model	AND, OR, Threshold



Key-Policy Attribute-Based Encryption (KP-ABE)

Ciphertext-Policy Attribute-Based Encryption (CP-ABE)

FIGURE 5. The encryption and decryption procedure of KP-ABE and CP-ABE.

Ostrovsky *et al.* [75] proposed a KP-ABE scheme with INVERT logic gate based on non-monotonic access structure and broadcast revocation mechanism. This approach makes the access strategy more flexible, but its ciphertext size and key length, encryption and decryption costs are doubled. To solve this problem, Lewko *et al.* [76] improved the Ostrovsky's scheme with shorter system public key length, but the ciphertext size is still large.

2) Ciphertext-Policy Attribute-Based Encryption (CP-ABE) was proposed under concrete and noninteractive cryptographic assumptions in the standard mode by Waters [74]. In CP-ABE cryptosystem, the ciphertexts are associated with the access-tree structure and private keys are labeled with sets of attributes that the data sender can determine the access control policies. A user is able to decrypt the ciphertext if and only if the access tree associated with ciphertext is satisfied by the attribute set associated with the private key. To solve the INVERT gate problem, Ostrovsky *et al.* [75] also constructed a CP-ABE scheme with INVERT operation by transferred any access structure to a Boolean formula. Fig. 5 illustrates the encryption and decryption procedure of KP-ABE and CP-ABE.

There are significant differences in complexity assumption, strategic flexibility and scope of application among three ABE schemes which mentioned above. The basic ABE [72] and the KP-ABE [73] cryptosystems are both constructed under Decisional Bilinear Diffie-Hellman (DBDH) assumption, while the CP-ABE [69] is designed with general group model. In terms of applicability, the basic ABE only represents the threshold strategy that applies to the applications with simple policy, while the KP-ABE and CP-ABE scheme are more suitable for the applications with fine-grained data sharing in storage systems because they support the complex access policy. Specifically, KP-ABE mechanism allows the data user to specify the requirements of massage, which is suitable for applications of query classes, such as pay TV system, VOD system, database access and etc., and in CP-ABE, the access policy requirements of ciphertext are determined by the data owner, which is more applicable to applications of access control classes, such as social networking sites, e-health systems and etc. The differences between basic ABE, KP-ABE, and CP-ABE cryptosystems are summarized in Table 2.

C. PROXY RE-ENCRYPTION

Blaze *et al.* [77] introduced Proxy Re-Encryption (PRE) as a ciphertext divertible protocol to converts the ciphertexts (messages or signature) for one key into ciphertexts for another by using a proxy. In another word, a semi-trusted proxy is able to turn a ciphertext encrypted under data owner's public key into an encryption of the same plaintext under data user's public key by using a re-encryption key, and PRE also can guarantee that the proxy cannot obtain any corresponding massages with plaintext. Therefore, the PRE method is widely used in cloud security applications such as data forwarding, document distribution and other multi-user sharing scenario.

Specifically, a general data sharing scheme using Blaze's PRE method is shown in Fig. 6. This scheme consists of four main phases: 1) Encryption: Alice encrypts the original data using her owner public key E_A, generates the first layer ciphertext C_1, and then transmits to the proxy. 2) Re-Encryption Key Generation: Alice obtains the Bob's public key E_B, encrypts E_A under E_B to generate the re-encryption key $E_{A\rightarrow B}$, and also transmits to the proxy. 3) Re-Encryption: Proxy encrypts the first layer ciphertext by using the re-encryption key when proxy gets C_1 and $E_{A\rightarrow B}$, and generates the second re-encrypted ciphertext C_2. 4) Decryption: Bob gets the re-encrypted ciphertext C_2 from the proxy, and decrypts it with his own private key S_B. The security of the scheme is any semi-trusted proxy or adversary

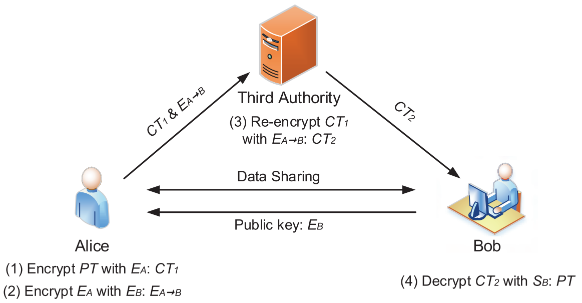

Third Authority
(3) Re-encrypt CT_1 with $E_{A\to B}$: CT_2
CT_1 & $E_{A\to B}$
CT_2
Data Sharing
Public key: E_B
Alice
(1) Encrypt PT with E_A: CT_1
(2) Encrypt E_A with E_B: $E_{A\to B}$
Bob
(4) Decrypt CT_2 with S_B: PT

FIGURE 6. **A PRE-based data sharing scheme.**

cannot decrypt the re-encrypted ciphertext because they do not have Bob's private key. Note that, although Blaze's PRE scheme is semantically secure under the Decisional Diffie-Hellman (DDH) assumption in group model, there are still two issues existing as follows [78]: 1) Bidirectionality: The proxy not only can divert the ciphertext from Alice to Bob, but also can be reversibly processed based on the computational properties of discrete logarithm without getting permission from Bob. 2) Collusion: The proxy and Alice can collude to deduce Bob's private key, then the proxy can decrypt the re-encrypted ciphertext, and get the message.

To solve these problems, a series of improved PRE schemes have been proposed [79]–[83], such as the Ivan and Dodis [79] presented a unidirectionality PRE by dividing Alice's secret key into two parts and distributed between Proxy and Bob, but this method has an obvious drawback that Bob requires to store the additional secret key for pre-secret sharing. Atenises *et al.* [80] addressed this problem and proposed another unidirectionality PRE scheme based on bilinear maps, this scheme introduced a master key security mechanism that can prevent any collusion attack without pre-secret sharing of secret keys. Green and Ateniese [81] proposed an Identity-Based Proxy Re-Encryption (IBPRE) scheme that realized the unidirectional encryption by using the user's identity information as the public key in re-encryption process, and then Wang *et al.* [82] extended the IBPRE scheme and presented an Indistinguishability Adaptive Chosen Ciphertext Attack (IND-CCA2) secure identity-based proxy re-encryption scheme which has several useful properties, including, multi-use, unidirectionality and etc. Weng *et al.* [83] proposed a Conditional Proxy Re-Encryption (C-PRE), whereby only ciphertext satisfying one conversion condition set by Alice can be transformed by the proxy and then decrypted by Bob, compared with the traditional PRE methods, the C-PRE is more suitable for practical application because the conversion permissions of proxy can be totally controlled.

D. HOMOMORPHIC ENCRYPTION

Homomorphic encryption, also called privacy homomorphism, is a cryptography technique that allows users to operate the ciphertext with arbitrary algebraic calculation directly. This is to say, if we choose one operation on the ciphertext and then decrypt, this decryption result is same as the result that we directly carry out the same operations on the plaintext. The advantage of this specific encryption form is that the user still can carry on the analysis and retrieval of encrypted data with specific circumstances, the encryption methods with this advantage can improve the efficiency of data processing, ensure the secure transmission of data, and data encryption right still can get the correct decryption results. This operation not only avoids the risk of data being intercepted, copied, tampered or forged in the process of transmission, but also avoids the risk of data leakage or data breach at the server end of data storage. From this special computing characteristic, the homomorphic encryption method can be widely used in data encryption, privacy-preserving, encrypted searching, and secure multi-party computation.

Rivest *et al.* [84] introduced the concept of homomorphic encryption firstly, and described the construction process in detail. The definition of homomorphic encryption can be simply illustrated as follow: Let $E_k(k, P)$ presents the encrypt of plaintext with an encryption algorithm E_k and a secret key k, and F be an arbitrary function of algebraic calculation. We called the encryption algorithm E_k is homomorphism for function F if and only if they satisfied the equation of $E_k(k, F(p_1, p_2, \ , p_n)) = G(k, F, (E(p_1), E(p_2), \ , E(p_n)))$, where G refers to an arbitrary efficient algorithm. According to the computational properties of the function, homomorphic encryption can be divided into three types as follows: 1) Additively Homomorphic Encryption (AHE) means the equation in the definition is only tenable for $F(p_1, p_2, \ , p_n) = \sum_{i=1}^{n} p_i$. 2) Multiplicatively Homomorphic Encryption (MHE) is similar to the AHE that the function F is only satisfies $F(p_1, p_2, \ , p_n) = \prod_{i=1}^{n} p_i$. 3) Synthetically, if the function F contains the mixed operations of addition and multiplication, then this encryption method is called Fully Homomorphic Encryption (FHE).

The security construction of homomorphic encryption is usually based on the following several computational difficulty problems which described as follows: 1) Integer Factorization Problem (IFP): Let n be any positive integer and (p_i, p_j) are mutually different prime numbers, the IFP refers to the problem of calculating factor expressions $n = (p_1^{(e_1)}, p_2^{(e_2)}, \ , p_k^{(e_k)})$ where $e_i \leq 1$. 2) Discrete Logarithm Problem (DLP): Let Z_p^* be a finite field of prime order p and let α be a generator of Z_p^*, then choose a integer $\beta \in Z_p^*$, the DLP problem represents to the difficult mathematical problem of finding the unique integer γ that satisfied the equation of $\alpha^\gamma \equiv \beta(modp)$. 3) Decisional Composite Residuosity Problem (DCRP): Let $N = pq$ where p and q are two primes, then choose a integer $y \in Z_{N^2}^*$ which subject to $z = y^N modN^2$, the DCRP refers to a determination of whether z is a N times residual. There are some other computational different problems such as Approximate GCD Problem (AGCDP), Spare Subset Sum Problem (SSSP) and Quadratic Residuosity Problem (QRP) that were widely used.

Rivest *et al.* [85] were the first to propose RSA scheme as a public-key cryptosystems based on the discrete

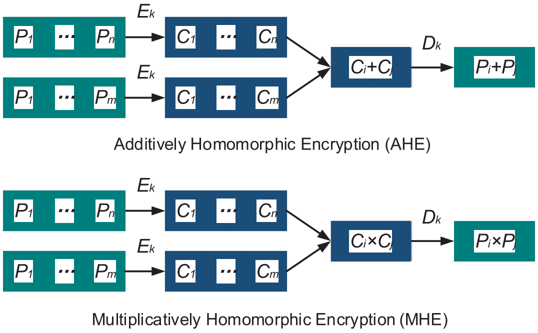


FIGURE 7. Characteristic of AHE and MHE.

logarithm problem (DLP) in 1978. The RSA encryption algorithm can well satisfy the multiplicative homomorphism property which can be described as follows: 1) KeyGen: Let $n = pq$ where p and q are two random big primes, choose a random integer e that satisfied the inequality of $1 < e < \varphi(n)$ where $\varphi(n) = (p-1)(q-1)$ and $gcd((n), e) = 1$. Then we can calculate the public key $pk = (n, e)$ and the private key $sk = d$ where $d \times e \equiv 1mod(\varphi(n))$. 2) Encryption: $C = E_{pk}(P) = P^e(modn)$, where P and C are the plaintext and ciphertext, respectively. 3) Decryption: $P = D_{sk}(C) = C^d(modn)$. 4) Homomorphic property: Suppose there are two plaintexts (P_1, P_2), using the RSA algorithm to encrypt the plaintexts and gets $E(P_1) = P_1^e(modn)$,$E(P_2) = P_2^e(modn)$ where $E(P_1)$ and $E(P_2)$ are the ciphertexts C_1 and C_2 after encryption. Then we can get the following equations based on the multiplication operation: $E(P_1) \times E(P_2) = (P_1^e \times P_2^e)modn$, where $E(P_1 \times P_2) = (P_1^e \times P_2^e)modn$, and we can get the same result that $E(P_1) \times E(P_2) = E(P_1 \times P_2)$, so the RSA algorithm satisfies multiplicative homomorphism. Similarly, the ElGamal algorithm [86] is also satisfied the multiplicative homomorphism property, and the Paillier [87] scheme is satisfied the additive homomorphism because it put the plaintext in the exponential position and the exponential operation will transfer multiplication into exponential addition. Fig. 7 illustrates the operation property in AHE and MHE.

The application scope of partial homomorphic encryption is very limited in the practical data encryption scenario. The full homomorphic encryption technology must be used to completely solve the main security problems in edge computing. Therefore, constructing fully homomorphic encryption algorithm becomes a central open problem in cryptography. In 2009, Gentry [88] was the first to propose FHE scheme based on the ideal lattice in polynomial ring that allows one to evaluate circuits over encrypted data without being able to decrypt, this scheme gives the basic concept of boots-trappable which supports the additive homomorphism and multiplication homomorphism in arbitrary polynomial time. The shortcoming of Gentry'09 scheme is the high calculation complexity and low efficiency of encryption and decryption. In 2010, Van Dijk *et al.* [89] introduced a simple FHE method based on the approximate greatest common divisor (GCD) problem, the boots-trappable encryption process was using only elementary modular arithmetic over the integers instead of ideal lattices in Gentry'09. The biggest advantage of the Dijk'10 method is the conceptual simplicity, but the drawback is that the length of the public key is still very long. In 2011, Brakerski and Vaikuntanathan [90] presented a FHE scheme based on the (standard) learning with errors (LWE) assumption, this scheme can shorten the ciphertexts and reduces the decryption complexity without introducing additional assumptions by the combination of re-linearization technique and dimension-modulus reduction technique. In 2013, Gentry *et al.* [91] described an improved the Brakerski's FHE scheme based on the approximate eigenvector method, the advantage of this scheme is that the homomorphic addition and multiplication are just matrix addition and multiplication, which greatly improves the efficiency of the algorithm.

E. SEARCHABLE ENCRYPTION

The problem of searching on encrypted data searching problem is derived from the Song's definition [92]: "It is desirable to store data on data storage servers such as mail servers and file servers in encrypted form to reduce security and privacy risks. But this usually implies that one has to sacrifice functionality for security. For example, if a client wishes to retrieve only documents containing certain words, it was not previously known how to let the data storage server perform the search and answer the query without loss of data confidentiality". The most direct solutions are as follows: 1) One method is to download all the ciphertext data to the local and decryption, then search in plaintext with keywords, but this operation will also download the unnecessary documents that do not contain the certain keywords which may cause the resource wasting of network and storage. Moreover, the decryption and searching operation of unnecessary documents will cost the huge computational overhead, and this method is not suitable for low broadband network environments. 2) Another extreme solution is sending the private key and keywords to the storage server, then decrypt the encrypted documents and search on the server. An obvious drawback to this approach is that the user's private data is re-exposed to the server which will be a serious threat to data security and personal privacy.

In order to solve these problems, the Searchable Encryption (SE) technology emerges as the times require which can guarantee the privacy and availability of data, and also supports query and retrieval operations of ciphertext data. Searchable encryption scheme in single user data sharing scenario consists of four main phase as shown in Fig. 8: 1) Encryption: The user encrypts the plaintext file with the secret key and generates the index structure, and then uploads the ciphertext and index to the server. 2) Trapdoor: The user with retrieval ability generates the trapdoor of keywords using the secret key which requiring trapdoor to not disclose any information of keywords. 3) Search: The server executes a searching algorithm with the keyword trapdoor as input, and returns all ciphertext files that contain the keyword

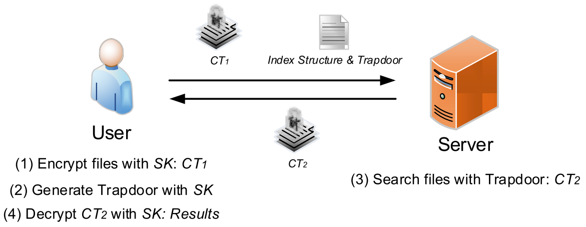

CT_1
Index Structure & Trapdoor
User
Server
CT_2
(1) Encrypt files with *SK*: CT_1
(2) Generate Trapdoor with *SK*
(4) Decrypt CT_2 with *SK: Results*
(3) Search files with Trapdoor: CT_2

FIGURE 8. Searchable encryption in single user scenario.

corresponding to the trapdoor which requiring the server cannot obtain more information except for the keyword information in the ciphertext. 4) Decryption: The user decrypts the encrypted documents returned by the server with a secret key and obtain the search results.

Searchable encryption schemes could be classified into two main types, as follows:

1) Searchable Symmetric Encryption (SSE): SSE is an efficient ciphertext retrieval scheme based on symmetric encryption method in which data owner and users shared the same secret key information, and the secret key is not only used for encryption and decryption, but also for trapdoor generation. The typical construction method of SSE includes the SWP scheme [92], Z-IDX scheme [93] and SSE-1 scheme [94] which are based on pseudo random function, bloom filter, and pseudo random permutation, respectively. The construction strategy of above SSE scheme can be divided into two categories which called the sequential scanning construction strategy and the index-based construction strategy. In SWP scheme, each word is encrypted one by one and then scan all the ciphertext sequentially to find out the ciphertext word which matched with the keyword during the searching operations. But the shortcoming of the sequential scanning is the searching efficiency will be very low. On the contrary, the index-based construction strategy used in Z-INX and SSE-1 schemes can reduce more computation resources which widely used in encrypted data searching methods. This strategy divides the structure of SSE into two sub-processes includes the index built and file encryption which encrypted files can protect the privacy of user's data on untrustworthy servers and built index can implement efficient keyword searching for ciphertext files. Recently, research points of SSE are focused on the functional expansion and security optimization, which will be detailed description in Section V.
2) Searchable Asymmetric Encryption (SAE): SAE is also called Public key Encryption with Keyword Search (PEKS) which is suitable for one-to-many data sharing scenarios. The PEKS schemes are mostly built on the bilinear pairs [95], and its security is based on different assumptions such as Discrete Diffie-Hellman problem [96] (DDH), Bilinear Diffie-Hellman problem [95], [97] (BDH), and so on. PEKS uses two secret keys when encryption: the public key is used for the encryption of plaintexts and the retrieval of the target ciphertexts, while the private key is used to decrypt the ciphertext files and generate the trapdoor of keywords. The PEKS schemes usually have low efficiency because it was constructed on the operation of bilinear pairs which caused the higher algorithm complexity. However, the characteristics of the separation of public and private key make it still very suitable for multi-user data sharing system.

The application model for searchable encryption technology has been explored for several years in data sharing scenarios that can be illustrated as shown in Fig. 9.

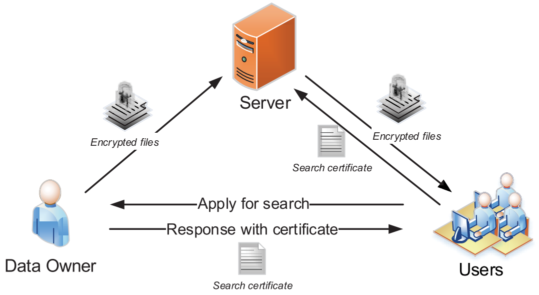


FIGURE 9. Searchable encryption in data sharing scenario.

V. STATE-OF-THE-ART SOLUTIONS

In the previous sections, we have analyzed the security and privacy challenges and countermeasures, and we have provided a detailed analysis of five cryptographic technologies that could be applied to edge computing paradigms and security mechanisms that should be used to protect them. At present, the research of data security in edge computing is still in the exploring stage, there are very few research works that have analyzed how to ensure data security and privacy in the context of edge computing. Yet it might be possible to look for the solution methods in other related fields, such as mobile cloud computing (MCC) [25], [98], fog computing [99], [100], and peer-to-peer computing [101]. Therefore, one of the main research ideas of data security in edge computing is to transplant the security mechanisms from other computing paradigms into edge computing paradigm, and finally realized the lightweight and distributed data security protection system with consideration of the features in edge computing.

In this section, we provide a taxonomy and analysis of the state-of-the-art data security and privacy-preserving solutions in edge-related paradigms, the specific taxonomy section includes the solutions of data confidentiality, data integrity, secure data computation, authentication, access control system and privacy-preserving. Moreover, a summary of related work is listed as the tabular format in Tables 3-8.

A. DATA CONFIDENTIALITY

In edge computing, users' private data is outsourced to the edge server and the ownership and control over data are

TABLE 3. Comparison of related works towards data confidentiality.

Work Area	Proposed Schemes	Technical Approaches	Security Features	Scalability
ABE-based Schemes	File hierarchy CP-ABE scheme [46]	CP-ABE Hierarchy access structure	Data confidentiality Data sharing	High
	Extended proxy-assisted approach [102]	CP-ABE All-or-Nothing principle	Data confidentiality	Moderate
	ABE with outsourced decryption [103]	Attribute-based encryption	Data confidentiality	High
PRE-based Methods	Secure and efficient CP-ABPRE [47]	PRE CP-ABE	Data sharing	High
	Fine-grained PRE scheme [104]	Condition-PRE CP-ABE	Data sharing User revocation	Moderate
	Bidirectional PRE scheme [105]	Proxy re-encryption	Data confidentiality Data sharing	High
	Cloud-manager-based re-encryption scheme [106]	Proxy re-encryption	Data confidentiality	Medium
	Workload distribution model based on PRE [107]	Proxy re-encryption	Data confidentiality	High
HE-based Approaches	Lightweight homomorphic encryption [48]	Homomorphic encryption	Data confidentiality	High

separated. This character result in the outsourced data must be in ciphertext form to prevent the private information cannot be leaked. In another word, data confidentiality is a fundamental requirement that refers to keep users' data secret in the edge data center. At present, data confidentiality and secure data sharing schemes are typically implemented using encryption techniques, the conventional process is that the data producer encrypts the outsourced data and upload to the data center, and then decrypted by the data users when they required.

1) ABE-BASED SCHEMES

The attribute-based encryption method is widely used in cloud data storage and sharing systems, the traditional CP-ABE presents the access policy that the users' attribute set satisfying the access tree corresponding to the threshold, in which the access policy is usually constructed by a Monotone Boolean structure. However, in the practical data storage scenario, the shared data file usually has multi-layer features, which will cause the access policy with monotone structure cannot meet the fine-grained access and sharing of multi-layer file data.

To solve this problem, Wang *et al.* [46] proposed an efficient encryption scheme based on a layered model of the access structure, named file hierarchy CP-ABE (FH-CP-ABE), which is extending the typical CP-ABE with a hierarchical structure of access policy. In FH-CP-ABE, hierarchical files are encrypted with an integrated access structure and the ciphertext components related to attributes could be shared by the files. Moreover, the overhead of ciphertext storage and encryption complexity can be reduced greatly by adding the transport nodes to the access structure, and the scheme is proved to be secure under DBDH assumption. User revocation problem is a very prominent problem in the file storage system. Yang *et al.* [102] presented an extended proxy-assisted approach, in order to overcome the limitation of needing to trust the cloud server not to disclose users' proxy keys inherent in proxy/mediator assisted user revocation approaches. To discourage the colluding between cloud server and third party, this approach binds the cloud server's private key to the data decryption operation, which requires the cloud server to reveal its private key should be the cloud server decide to collude with revoked users. Recently, Zuo *et al.* [103] constructed an attribute decryption method with outsourcing decryption in fog computing environment (OD-ABE), and is proved to be secure under the Chosen Ciphertext Attack (CCA).

2) PRE-BASED METHODS

Proxy re-encryption method is usually used in combination with other encryption mechanisms due to its features of ciphertext conversion and privilege control.

In 2015, Liang *et al.* [47] proposed a secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption (CP-ABPRE) scheme with combination of CP-ABE and PRE methods, in this way, the third party is able to turn a ciphertext encrypted under one access structure into an encryption of the same plaintext under different access structure. Furthermore, the authors also presented a novel single-hop unidirectional CP-ABPRE system by integrating the dual system encryption technology with the selective proof technique and proven to be adaptively Chosen Ciphertext Attacks (CCA2) secure in

TABLE 4. Comparison of presented approaches dealing with data integrity solutions.

Works	Proposed Schemes	Technical Approaches	Security Features	Scalability
(Wang et al., 2010) [49]	Privacy-preserving public auditing system	Homomorphic authenticator Random masking	Batch auditing Privacy-preserving	High
(Wang et al., 2011) [50]	Dynamic public auditing scheme	Merkle hash tree Bilinear aggregation signature	Dynamic auditing Secure storage	High
(Yang et al., 2013) [51]	Efficient dynamic auditing protocol	Cryptography method Bilinearity property	Dynamic auditing privacy-preserving	High
(Sookhak et al., 2017) [110]	Remote data auditing for secure data storage	Algebraic signature Divide and conquer table	Dynamic auditing Low-complexity	Moderate
(Li et al., 2016) [111]	Lightweight privacy-preserving auditing	Online/offline signatures Merkle hash tree	Batch auditing Privacy-preserving	High
(Lin et al., 2017) [52]	Mobile provable data possession scheme	Provable data possession BLS short signature	Dynamic auditing low-complexity	Moderate

the standard model. In the same year, Yang *et al*. [104] firstly proposed a ciphertext-policy attribute-based CPRE scheme for fine-grained data sharing by a combination of conditional proxy re-encryption and CP-ABE methods, which achieve user revocation operation. This scheme also realized the high user-side efficiency feature of the application, which makes it more suitable for the mobile computing scenarios.

In 2016, Shao *et al*. [105] designed a bidirectional proxy re-encryption scheme with constant ciphertext size in dynamic cloud storage scenario, which the ciphertext size is unrelated to the conversion times. The authors also proved that the scheme is master secret secure and Replayable Chosen Ciphertext Attacks (RCCA) secure in the random oracle model. Khan *et al*. [106] proposed a Cloud-Manager-based Re-encryption Scheme (CMReS) that combines the characteristics of manager-based re-encryption and cloud-based re-encryption for outsourcing the computation-intensive task to the cloud center and realized the minimum processing burden on the mobile device. Recently, Khan *et al.* [107] made a further expansion of CMReS, aiming at the task migration problem between mobile devices and trusted entities and further proposed a comparative study and workload distribution model for re-encryption schemes in mobile cloud computing environment, which improved the overall performance.

3) HE-BASED APPROACHES

The Homomorphic Encryption is one of the suitable and strong techniques to ensure data storage security and provide a necessary support for ciphertext processing, but this technique comes later, with little research achievements and imperfect theory, so its application is limited.

Louk and Lim [108] discussed and evaluated the several homomorphic encryption methods in mobile multi-cloud computing, and provide a good theoretical support for the subsequent research work. Baharon *et al*. [48] proposed a Lightweight Homomorphic Encryption (LHE) scheme for mobile users by HE which minimizes the use of computation power of encryption and key generation. The main contribution of this paper is to have a lightweight scheme with improved efficiency while enabling homomorphism under both addition and multiplication.

B. DATA INTEGRITY

As the data storage and processing are rely on the edge server, this will introduces some problems as it is in cloud computing, for example, outsourced data cloud be lost or incorrectly modified by unauthorized parties or systems. The data integrity needs to ensure the accuracy and consistency of users' data, in other words, the integrity prevents undetected modification of data by any unauthorized users or systems. At present, the research on data integrity is mainly focused on the following four functional aspects [109]:

1) *Dynamic Auditing*: The data integrity auditing scheme should have the dynamic auditing function because the data is usually dynamically updated in outsourcing server.
2) *Batch Auditing*: The data integrity auditing scheme should support the batch operation when a large number of users simultaneously send audit requests or data are stored in multiple edge data centers.
3) *Privacy-Preserving*: The integrity auditing is usually implemented by a Third Party Auditing (TPA) platform because the data storage servers and the data owners cannot provide an unbiased and honest auditing result. In this case, it is hard to ensure data privacy when the TPA is semi-trusted or untrusted, and it is necessary to protect the data privacy in the integrity auditing project.

TABLE 5. Comparison of proposed schemes for secure data search.

Work Area	Proposed Schemes	Taxonomy	Technical Approaches	Search Function	Scalability
Ranked Keyword Search	Ranked searchable symmetric encryption [53]	SSE	One-to-many mapping, order preserving symmetric encryption	Ranked keyword search	Moderate
	Multi-keyword ranked search scheme [112]	SSE	Coordinate matching, inner product similarity	Multi-keyword search	Moderate
	Efficient multi-keyword ranked search scheme [113]	SSE	k nearest neighbor , blind storage system	Multi-keyword search	High
	Traffic and energy saving encrypted search [114]	SSE	Computation offloading technique	Efficient keyword search	High
Attribute-based Keyword Search	Ciphertext-policy attribute-based encryption scheme with keyword search function [54]	PEKS	Ciphertext-policy ABE	Search authority control	High
	Verifiable attribute-based keyword search [115]	PEKS	Ciphertext-policy ABE	Search authority control	High
	Key-policy attribute-based keyword search [116]	PEKS	Key-policy ABE	Verifiable search	Moderate
	Attribute-based keyword search scheme with efficient user revocation [117]	PEKS	ABE, PRE, lazy PRE	Search authorization	High
Dynamic Search	Dynamic searchable symmetric encryption [55]	SSE	Compact index structure, random masking	Dynamic search	Moderate
	Parallel and dynamic SSE scheme [118]	SSE	Keyword red-black tree	Parallel and dynamic search	High
	Verifiable conjunctive keyword search scheme [119]	PEKS	Bilinear-map accumulator	Conjunctive keyword search	High
	Dynamic multi-keyword ranked search scheme [120]	PEKS	Greedy depth-first search, TF×IF	Dynamic multi-keyword search	High
	Dynamic attribute-based keyword search [121]	PEKS	ABE, PRE, secret sharing scheme	Dynamic search	Moderate
Proxy Re-Encryption with Keyword Search	Proxy re-encryption with keyword search [56]	PEKS	PRE, PEKS	Proxy keyword search	High
	Constrained single-hop unidirectional proxy re-encryption with conjunctive keyword search [122]	PEKS	PRE,PEKS	Conjunctive keyword search	Moderate
	Conditional proxy re-encryption with keyword search [123]	PEKS	C-PRE, PEKS	Proxy keyword search	High
	Attribute-based proxy re-encryption with keyword search [124]	PEKS	PRE, ABE, CP-ABE, KP-ABE	Proxy keyword search	High

4) *Low-Complexity*: Low complexity is an important performance criterion in the design of data integrity auditing protocols, it includes the low storage overhead, low communication cost, and low computational complexity.

According to the above four design requirements, the researchers finished a series of work. In 2010, Wang *et al.* [49] proposed a privacy-preserving public auditing system for data storage in cloud computing by utilizing the homomorphic authenticator and random masking technical which can guarantee that the TPA would not know any information about the outsourcing data. Furthermore, considering TPA can simultaneously handle multiple audit sessions, the authors further improved the system into a multi-user setting based on the bilinear aggregation signature method, where the TPA can process the batch auditing tasks in a distributed manner.

In 2011, Wang *et al.* [50] further improved the auditing scheme in [49], and achieved efficient dynamic auditing by manipulating the traditional Merkle Hash Tree (MHT) construction for block tag authentication. To support more efficient operation of batch auditing, the authors also improved the scheme into a multi-user setting by further explored the bilinear aggregation signature.

In 2013, Yang and Jia [51] first designed an efficient and inherently secure dynamic auditing protocol by the combination of the cryptography method and the bilinearity property of bilinear paring for data storage in cloud computing, and further extended the protocol to support the data dynamic operations, which is proved secure in the random oracle

TABLE 6. Comparison of related works counting authentication issues.

Work Area	Proposed Schemes	Technical Approaches	Security Features	Scalability
Single-Domain Authentication	Shared authority based privacy-preserving authentication protocol [57]	Anonymous request matching CP-ABE PRE	Privacy-preserving Anonymous authentication	High
	Privacy-aware authentication scheme [125]	Bilinear pairing cryptosystem Dynamic nonce generation	Privacy-preserving Anonymous authentication	Moderate
	New privacy-aware authentication scheme [126]	Bilinear pairing cryptosystem Identity-based signature	Privacy-preserving Anonymous authentication	High
	Conditional privacy-preserving authentication scheme for VSN [127]	Identity-based signature ECC	Privacy-preserving Batch verification	High
	Lightweight authentication scheme [128]	Elliptic curve cryptography	Lightweight authentication	High
Cross-Domain Authentication	Attribute-based authorization framework [58]	Attribute Certificates Revocation system	Privacy-preserving Certificate revocation	Moderate
	Cross-domain dynamic anonymous authenticated group key management System [129]	Elliptic curve cryptography Hierarchical tree structure	Anonymous authentication Privacy-preserving Key revocation	Medium
Handover Authentication	Efficient handover authentication protocol [59]	Elliptic curve cryptography Identity-based authentication	Anonymous authentication Privacy-preserving Untraceability	High

model. Recently, Sookhak *et al.* [110] proposed an efficient Remote Data Auditing (RDA) method based on algebraic signature properties to verify the integrity of big data storage in cloud computing, which the auditor can check user's data possession in the cloud. Furthermore, to improve this method, the authors also presented a new data structure, called Divide and Conquer Table (DCT), which efficiently supports dynamic data operation such as update, insert, modify and delete.

In 2016, Li *et al.* [111] proposed two lightweight privacy-preserving public auditing protocols based on online/offline signatures. The basic auditing protocol allows offline signature process before outsourcing data, which an end device only needs to perform lightweight computing when a file to be outsourced is available. The extended auditing protocol supports batch auditing and data dynamics by using the Merkle hash tree authentication structure to guarantee the correctness of the partial signatures. The Provable Data Possession (PDP) is another integrity auditing method that provides probability guarantee for data possession, but this method has high computational complexity and larger storage space because of the auditor needs to access all the data block during the auditing process. To solve this problem, Lin *et al.* [52] developed a comprehensive mobile provable data possession schemes (MPDP) based on the hash tree structure and a Boneh-Lynn-Shacham (BLS) short signature scheme that supports the dynamic verification outsourcing, blockless and stateless verification, and dynamic data operations.

C. SECURE DATA SEARCH

In edge computing, users usually outsourcing their sensitive data to the edge server with ciphertext form through some encryption methods to protect data privacy. In this case, the biggest problem is the keyword search from encrypted data which means the user will encounter the problem of how to search the keywords on the ciphertexts. The researchers have developed several searchable encryption methods that support a user to securely search over encrypted data through keywords without decrypt operation. These searchable encryption methods can be classified as follows: ranked keyword search, attribute-based keyword search, dynamic search and proxy re-encryption with keyword search.

1) RANKED KEYWORD SEARCH

Secure ranked keyword search refers to the system returns the search results correctly according to certain relevance criteria such as the frequency of keyword occurrence, which improves the applicability of the system, and conforms to the actual needs of privacy data protection in the edge computing environment.

In 2012, Wang *et al.* [53] defined the problem of secure ranked keyword search over encrypted data for the

TABLE 7. Comparison of proposed access control schemes.

Work Area	Proposed Schemes	Technical Approaches	Application Scenarios	Scalability
Attribute-based AC	Fine-grained attribute-based access control scheme [60]	ABE, PRE, LRE	Cloud computing	Moderate
	Robust and auditable access control scheme [135]	CP-ABE	Public cloud storage	High
	Secure and lightweight data access control scheme [136]	CP-ABE	Mobile cloud computing	High
	First efficient access control scheme [137]	CP-ABE	Fog computing	High
	Secure and fine-grained access control with ciphertext update and computation outsourcing [138]	CP-ABE, ABS	Fog computing	Moderate
Role-based AC	Secure role-based access control scheme [61]	Role-based encryption Identity-based signature	Cloud storage	High
	Hierarchical virtual role assignment for negotiation-based RBAC scheme [139]	Hierarchical cryptographic assignment, Negotiation function	Large scale information system	High
	Distributed role-based access control architecture [140]	Role-based encryption	Distributed cloud computing	High
TPM-based AC	Direct anonymous attestation protocol with attributes [62]	ECC Zero-knowledge proof	Edge computing	High

first time, and proposed the Ranked Searchable Symmetric Encryption (RSSE) scheme with little relevance score information leakage against keyword privacy. To achieve the effectively ranked search over encrypted file collection, the authors also designed a new cryptographic primitive called Order Preserving Symmetric Encryption (OPSE) which used the one-to-many order-preserving mapping to protect the user's privacy and verify the search results at the same time.

In 2014, Cao *et al.* [112] firstly defined and solved the problem of privacy-preserving multi-keyword ranked search over encrypted storage data, and proposed a Multi-keyword Ranked Search (MRSE) scheme by construction the coordinate matching mechanism to capture the relevance of data documents to the search query. Furthermore, the authors also quantitatively evaluated the relevance similarity measure by using the inner product similarity. It is worth to mention that the above two schemes all face with the problem of low search efficiency. The search efficiency of the system will greatly reduce when the number of users in the system increased.

To solve the search efficiency problem in keyword search system, in 2015, Li *et al.* [24] proposed an Efficient Multi-keyword Ranked Search (EMRS) scheme based on the MRSE scheme and k nearest neighbor technique in mobile cloud computing environment which can return the ranked keyword search results based on the accuracy. In addition, to achieve the privacy-preserving feature, the authors designed the blind storage system to hide the search mode of users. Finally, the simulation results show that EMRS scheme can achieve a more efficient multi-keyword ranked search than MRSE scheme.

In 2017, Li *et al.* [114] presented a Traffic and Energy saving Encrypted Search (TEES) framework in mobile cloud that can offloads a big part of computation task from mobile devices to the cloud, and the experiment results show that TEES can reduce the computation time by 23 to 46 percent, and the energy consumption decreased by 35 to 55 percent per file retrieval, which means this scheme is suitable for the mobile devices with limited resources.

2) ATTRIBUTE-BASED KEYWORD SEARCH

Attribute-based searchable encryption supports fine-grained data sharing while achieving efficient search operations.

In 2013, Wang *et al.* [54] proposed a new cryptographic primitive called Ciphertext-Policy Attribute-Based Encryption scheme with Keyword Search Function (KSF-CP-ABE) to achieve efficient search processing and fine-grained data sharing. This scheme can realize the search authority control by constructing the same access policy between keyword retrieval system and data encryption system. In addition, the authors further presented a concrete KSF-CP-ABE construction based on bilinear pairings and proved that the scheme is secure against both outer and inner attacks.

In 2014, Zheng *et al.* [115] proposed a novel cryptographic scheme called Verifiable Attribute-Based Keyword Search (VABKS) to further defined the search authority problem, this scheme allows the data owner to control the search and use of their outsourced encrypted data according to the access control strategy, while authorized data users can outsource the search operations to the third party. In the same year, Liu *et al.* [116] pointed out the practicability problem of the VABKS scheme which the construction of VABKS

TABLE 8. Comparison of presented schemes counting privacy issues.

Work Area	Proposed Schemes	Technical Approaches	Application Scenarios	Scalability
Data Privacy	A privacy preserving data utilization method [146]	Probabilistic public-key encryption Trusted proxy server	Hybrid clouds	High
	Light-weight data privacy preserving method [63]	Pseudo-random permutation	Mobile cloud computing	Moderate
	Efficient and secure privacy-preserving approach [64]	Probabilistic public-key encryption Ranked keyword searching	Mobile devices in cloud	High
Identity Privacy	Identity privacy preserving approach [147]	Dynamic credential generations	Mobile cloud computing	High
	Improved identity management protocol [65]	Pretty good privacy	Mobile cloud computing	High
	Consolidated identity management system [66]	Trusted third party managers Authentication	Mobile cloud computing	Moderate
Location Privacy	Privacy-preserving location sharing system [148]	Dummy location updates	Mobile online social networks	Moderate
	Location privacy preservation scheme [67]	Distributed cache proxy servers	Location-based services	High
	Caching-aware dummy selection algorithm [68]	Creating fake locations Privacy metrics	Location-based services	High
	Location privacy preserving for mobile applications [149]	Trusted manager and analyzers	Mobile location-based services	High

relies on the secure channel between the communication parties. To solve this problem, the authors proposed a new scheme without secure channel and also constructed a novel method for verifying the searched results based on Key-Policy Attribute-Based Keyword Search (KP-ABKS). The simulation results show that the KP-ABKS scheme is more practical than VANKS.

In 2016, Sun *et al.* [117] presented the first Attribute-Based Keyword Search scheme with efficient User Revocation (ABKS-UR) that enables scalable fine-grained search authorization. The ABKS-UR scheme was fully considered the scenario where the outsourced data were contributed by multiple owners and were searchable by multiple users, which called multi-user multi-contributor case. Furthermore, the authors improved this scheme to migrate the system upload work into the third party during user revocation by using the proxy re-encryption and lazy re-encryption techniques. Finally, it is proved that the scheme is selectively secure against chosen keyword attacks.

3) DYNAMIC SEARCH

As aforementioned, the data is usually dynamically updated in edge computing servers, which means the traditional static searchable encryption methods cannot perform well enough in this situation. On the contrary, dynamic searchable encryption schemes can support varies operation of ciphertext data, and can return the correct search results without reconstructing the search index.

In 2012, Kamara *et al.* [55] proposed the first searchable symmetric encryption scheme to support the dynamic operation of ciphertext data, called Dynamic Searchable Symmetric Encryption (DSSE), which achieved optimal search time. This scheme supports efficient data updating by constructing a compact index structure, including deletion, insertion, and modification. In addition, the authors also presented a formal security definition for DSSE, adaptive security against chosen-keyword attacks (CKA2), and proved the scheme is secure in the random oracle model. Although the DSSE scheme can achieve the dynamic search with CKA2 security, the computation complexity of this scheme is very high, and it is difficult to implement in a practical application.

To solve this problem, in 2013, Kamara *et al.* [55] further proposed the parallel and dynamic searchable symmetric encryption method [118] based on a new tree-based multi-map data structure which called Keyword Red-Black (KRB) tree. This KRB-based data structure can index a document collection in such a way that keyword search can be performed in $O(rlogn)$ sequential time and $O(\frac{r}{p}logn)$ parallel time, and greatly improved the efficiency of data searching and updating time.

In 2015, Sun *et al.* [119] proposed an efficient and Verifiable Conjunctive Keyword Search (VCKS) that enables users to conduct the secure conjunctive keyword search, update outsourced file dynamically and verify the authenticity of the search results. The proposed verification mechanism allows a user to delegate the task to a public Trusted Authority (TA) or executed privately by data users through a bilinear-map accumulator. In 2016, Xia *et al.* [120] presented a secure multi-keyword ranked search scheme based on a special tree-based index structure and Greedy Depth-first search algorithm, which simultaneously support dynamic operations of files. In particular, the proposed special tree-based index structure is effective for the phase of index construction and query generation by using the vector space model and Term Frequency (TF)×Inverse Document Frequency (IDF) model, and the search time can be sub-linear level.

Recently, Hu *et al.* [121] pointed out that the existing Attribute-Based Keyword Search (ABKS) scheme only addressing the fine-grained search authorization problem while ignoring the problem of efficiently updating. To solve this problem, the authors proposed a Dynamic Attribute-Based Keyword Search (DABKS) scheme that incorporates proxy re-encryption and a secret sharing scheme into ABKS and meanwhile achieved fine-grained search authorization and efficient updating of access policies. But the drawback of DABKS scheme is that only the single keyword search is supported.

4) PROXY RE-ENCRYPTION WITH KEYWORD SEARCH

In 2010, Shao *et al.* [56] proposed the first proxy re-encryption with keyword search (PRES) as a new cryptographic primitive by combining the Proxy Re-Encryption (PRE) with Public Key Encryption with Keyword Search (PEKS). In addition, the authors further improved the PRES scheme to a bidirectional PRES scheme, which is proven secure in the random oracle model, based on the modified Decisional Bilinear Diffie-Hellman (DBDH) assumption. Finally, two application examples of PRES scheme in cloud computing and sensor network are given.

In 2012, Wang *et al.* [122] further extended PRES scheme and introduced a new primitive with Constrained single-hop unidirectional Proxy Re-Encryption supporting Conjunctive Keyword Search (CPRE-CKS). Compared with Shao's PRES scheme, the proxy in CPRE-CKS scheme can only re-encrypt the second level ciphertext which contains the corresponding keywords, while the proxy in Shao's PRES scheme needs to re-encrypt all the second level ciphertext. In this case, the CPRE-CKS scheme can simultaneously support efficient and conjunctive keyword search. Furthermore, the authors also presented a bilinear pairing-based construction method of CPRE-CKS and proved secure in the random oracle model. However, the shortcoming of this scheme is that it can only achieve the weak Chosen Ciphertext Attack (wCCA) secure.

To solve this weak security problem, Fang *et al.* [123] proposed a new cryptographic primitive called Conditional Proxy Re-Encryption with keyword Search (C-PRES), which combines the Conditional Proxy Re-Encryption (C-PRE) and the PEKS, and proved secure against Chosen Ciphertext Attacks (CCA) for C-PRES scheme by keyword anonymity method. In 2014, Shi *et al.* [124] proposed an Attribute-Based Proxy re-encryption with Keyword Search (ABRKS) by combining attribute-based encryption with proxy re-encryption which supports keyword search with fine-grained access control. In addition, the authors also proposed two concrete constructions for ABRKS based on CP-ABE and KP-ABE, and proved the KP-ABRKS scheme has achieved the selective security against chosen-keyword attacks (CKA1) in the random oracle model.

D. AUTHENTICATION

In edge computing paradigms, there are multiple functional roles (end users, service providers, infrastructure providers), services (virtual machine, data container), and infrastructures (edge devices, edge data center, core infrastructure) coexistence and interaction in an ecosystem. In this complex environment, we not only need to assign an identity to each entity in one trust domain, but also have to let the entities to mutually authenticate each other among different trust domains. At the same time, considering the high mobility of the edge devices, the handover authentication technology is also an important research point in the authentication protocol.

1) SINGLE-DOMAIN AUTHENTICATION

Authentication in a single trust domain is mainly used to solve the identity allocation problem of each entity. The entities in edge computing must authenticate from the authorization center before they obtain the services.

In 2015, Liu *et al.* [57] proposed a Shared Authority based Privacy-preserving Authentication (SAPA) protocol to enhance a user's access request related privacy in which the shared access authority is achieved by anonymous access request matching mechanism. With the use of ciphertext-policy attribute-based access control mechanism, a user can only reliably access its own data filed, and data sharing among multiple users was achieved by proxy re-encryption method. In the same year, Tsai and Lo [125] proposed a new anonymous authentication scheme for the distributed mobile cloud computing environment, which provides security and convenience for mobile users to access multiple mobile cloud services from multiple service providers using only one private key. The proposed scheme also supports mutual authentication, key exchange, user anonymity, and user untraceability, and the security strength is based on bilinear pairing cryptosystem and dynamic nonce generation.

In 2016, Jiang *et al.* [130] pointed out that the authentication scheme in [125] is failing to achieve mutual authentication, because it is vulnerable to the service provider impersonation attack. This is to say, the adversary can impersonate any service provider to do the authentication for users. To address this problem, He *et al.* [126] constructed a new privacy-aware authentication (PAA) scheme for MCC services based on the identity-based signature method that can solve the serious problems existing in Tsai and Lo's PAA scheme.

In 2016, Lo and Tsai [127] proposed a novel conditional privacy-preserving authentication scheme based on the batch ID-based signature to support secure communication and driver privacy for vehicles in a Vehicular Sensor Network (VSN). This new batch ID-based signature is constructed based on the Elliptic Curve Cryptosystem

(ECC) and the traditional identity-based signature method. Furthermore, to enhance scheme efficiency, there is no bilinear pairing operation and MapToPoint operation in both vehicles and Roadside Units (RSUs) during the signature process. Recently, Mahmood *et al.* [128] proposed an ECC based lightweight authentication scheme for smart grid system that provides mutual authentication with protection against all known security attacks. The performance analysis results show that this scheme is quite suitable for the smart grid system due to its lightweight operations.

2) CROSS-DOMAIN AUTHENTICATION

At present, there are few research results on authentication mechanisms among different trust domain entities of interconnected edge servers and has not yet formed a complete research context and theoretical methods. In this case, a feasible research idea is to looking for the solutions to this problem from other related fields to edge computing environment, such as the authentication among multiple cloud services providers in cloud computing can be seen as a form of cross-domain authentication in edge computing, which makes the authentication standards (such as SAML, OpenID) in multi-cloud may pursue the creation of the research of cross-domain authentication [131].

In 2015, Touceda *et al.* [58] designed a completely new attribute-based authentication framework for authorization in structured Peer-to-Peer (P2P) networks. The proposed authorization framework is constructed by Attribute Certificates (ACs) and a fully distributed certificate revocation system to achieve the flexible and efficient allocation of privileges without any trusted third parties, which instead of the Public Key Certificates (PKCs) and Access Control Lists (ACLs) in traditional identity-based authorization models.

Recently, Yang *et al.* [129] proposed a Cross-Domain dynamic anonymous Authenticated Group Key Management System with symptom-matching (CD-AGKMS) in Electronic health (e-health) social system that allows a group of patients from different healthcare domains to securely establish a group session key to protect the group disease discussion. The proposed system achieves the cross-domain group key agreement by setting up a hierarchical tree structure with the Key Generation Center (KGC) is on the top layer. In the aspect of group key management, this system provides a time controlled key revocation mechanism that user's secret key is revoked when the pre-assigned validity time expires. In addition, the CD-AGKMS system does not require bilinear pairing calculation, which improves the feasibility and efficiency of the system. As the design of these methods is compatible with the underlying infrastructure in edge computing, these methods potentially might be applied to the authentication of edge data centers belonging to different trust domains.

3) HANDOVER AUTHENTICATION

In edge computing, the geographical location of mobile users often changes because of the high mobility of the edge devices, which makes the traditionally centralized authentication protocol unsuitable for such situations. Handover authentication is kind of useful authentication transfer technology to solve high mobility user authentication.

In 2016, Yang *et al.* [59] proposed a new efficient design of handover authentication for heterogeneous mobile cloud networks, which allow a mobile client to migrate from one region to another with anonymity and intractability. The proposed authentication protocol using the elliptic curve algorithm cryptography on identity authentication to keep clients' identities and location is hidden in authentication transfer process. However, the protocol usually needs to access to the authentication server located in the centralized cloud infrastructure, so there is still room for improvement. It is worth mentioning that some mechanisms, such as the OPENi framework [132], have great potential to apply for edge computing paradigm because the certain edge paradigms (such as cloudlet) allow users to deploy their own personal data centers. The OPENi framework provides the authentication protocol to external users of OpenID connect authentication layer, which allows the owner of cloudlet can decide which cloud authentication servers he trust and what users are allowed to access the cloudlet resources.

Recently, He *et al.* [133] introduced the handover authentication for Mobile Wireless Network (MWN) and presented a handover authentication protocol using the Identity-based Public Key Cryptography (ID-based PKC) which has a high level of security assurance after a detail discussion of the security and privacy requirements of handover authentication in MWN. In addition, the authors also implemented and compared the communication and computation costs associated with these protocols on a specific mobile device. Lately, Alizadeh *et al.* [134] have done another comprehensive survey of authentication methods in mobile cloud computing environment, which analyzed the security and performance of authentication mechanisms for MCC based on five critical metrics, and in our review, we will no longer repeat the introducing of related authentication works.

E. ACCESS CONTROL SYSTEM

Data confidentiality and access control have been a key technology and reliable tool to ensure the security of the system and protect the privacy of the users. Most of the traditional access control schemes are usually assumed that users and entities are in the same trust domain, while are not suitable for the trusted infrastructure based on multiple trust domains in edge computing. Due to the outsourcing nature of edge computing, the access control system is usually cryptographically implemented for outsourced data. There are two typical access control systems are widely used in cloud computing environment, which respectively called Attribute-Based Access Control (ABAC) and Role-Based Access Control (RBAC).

1) ATTRIBUTE-BASED ACCESS CONTROL

Attribute-based encryption is one of the preeminent technologies to control data access in cloud computing, which can be well applied to the distributed architecture and achieved fine-grained data access control by establishing the decryption ability on the basis of a user's attributes [78].

In 2010, Yu *et al.* [60] firstly proposed a secure, scalable, and fine-grained data access control scheme in cloud computing by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption (PRE) and lazy re-encryption (LRE). This access control scheme achieves, on the one hand, the fine-grained access policies based on data attributes, and, on the other hand, the delegation of most computation tasks to semi-trusted third party without disclosing any information of data contents and user access privileges. In addition, the proposed scheme is provably secure under standard security model, which laid a theoretical foundation for the research of ABAC methods. Most of the traditional ABAC schemes were constructed by a single attribute authorization way, the drawback of this construction is that the authentication of users and key distribution must be performed while access control method is carried out, users may be stuck in the waiting queue for a long period to obtain their secret keys, thereby resulting in the single-point performance bottleneck problem in a large-scale distributed computing model. To solve this problem, recently, Xue *et al.* [135] proposed a Robust and Auditable Access Control scheme (RAAC) with multiple attribute authorities for public cloud storage based on ciphertext-policy attribute-based encryption. This scheme is aiming at the solution of single-point performance bottleneck problem with the heterogeneous framework and provides an efficient access control with an auditing mechanism. The innovation of RAAC scheme lies in the design of multiple attribute authorities to share the load of user legitimate verification and each authority can independently manage the whole attribute.

In 2015, with the in-depth research of mobile cloud computing and fog computing, a lot of secure, efficient and lightweight access control schemes have been put forward. In 2015, Jin *et al.* [136] designed a Secure and Lightweight data access control scheme based on Ciphertext-Policy Attribute-Based Encryption algorithm (SL-CP-ABE), which can protect the confidentiality of outsourced data and provide fine-grained data access control in mobile cloud computing. The proposed SL-CP-ABE scheme can obviously reduce the computation overhead by greatly decreasing the encryption and decryption operations and meanwhile improve the overall system performance.

Recently, Zhang *et al.* [137] proposed the first efficient access control (CP-ABE) scheme with outsourcing capability and attribute update for fog computing based on Jin's work [136]. This scheme achieves the fine-grained access control strategy by the CP-ABE method and simultaneously outsourcing heavy computation operations of encryption and decryption to fog nodes where the encryption and decryption operations are irrelevant to the access structure and secret keys. Finally, the proposed scheme is proven secure under the DBDH assumption. Lately, Huang *et al.* [138] proposed a secure and fine-grained data access control scheme with ciphertext update and computation outsourcing in fog computing. The ciphertext updating mechanism was designed based on Attribute-Based Signature (ABS) which authorized user whose attributes integrated with the signature satisfies the update policy can renew the ciphertext. The computation outsourcing mechanism in this paper is the same as Zhang's work [137] that most encryption, decryption, and signing operations related bilinear computations are outsourced to fog node to minimize the computation cost of the IoT devices.

2) ROLE-BASED ACCESS CONTROL

Role-Based Access Control (RBAC) can provide a flexible access control and privilege management by users-to-roles and roles-to-objects authority mapping mechanism which means the RBAC can regulate the access of users to resources and applications based on identifying roles and activities of users in the system [141], [142].

In 2013, Zhou *et al.* [61] firstly proposed a Role-Based Encryption (RBE) scheme with efficient user revocation that combines the cryptographic techniques with RBAC policies, which allow executing the RBAC policies in the encrypted data. The proposed RBE scheme has a superior feature that it can always keep the constant size ciphertext and decryption key. In addition, the authors also presented a hybrid cloud storage architecture based on the RBE which allows the users to store data in a public cloud while maintaining the sensitive data in a private cloud. In 2015, Chen *et al.* [139] proposed a hierarchical virtual role assignment for negotiation-based RBAC scheme which allows huge users in a hierarchy can highly get the role to access resources with lots of multiple cooperation servers or agents.

In 2010, Kuhn *et al.* [143] firstly realized the dynamic role assignment and distributed access control by adding attributes to role-based access control scheme, and also gives an appropriate trade-off for attribute-centric and role-centric. This distributed access control architecture meets the design requirements of edge computing, and most of the researches on distributed access control are focused on other computing paradigms [144] that can be a useful guidance of edge computing. In 2012, Almutairi *et al.* [140] proposed a distributed role-based access control architecture for cloud computing based on the principles of security management and software engineering that provide the role mapping and constraint verification of multi-domain. It is worth mentioning that this distributed access control architecture is quite suitable for constructing the cross-domain access control strategy among multiple entities in edge computing.

Besides, there are some other security mechanisms that might be suitable for certain edge computing paradigm. For example, Chen and Urian [62] proposed the Direct Anonymous Attestation protocol with Attributes (DAA-A) based on elliptic curve cryptosystem. The proposed DAA-A protocol allows users to prove that which attributes should be verified and which attributes he will hide by implementing the protocol on the Trusted Platform Module 2.0 (TPM 2.0), and meanwhile using the zero-knowledge proof method to verify the authenticity of the hidden attributes. Therefore, this scheme can be applied to edge computing paradigm, where multiple edge data centers can use the DAA-A protocol to prove the certain attributes they have and without disclosing their owner's private information [145].

F. PRIVACY PRESERVING

The protection of private information like data, identity, and location from leakage, is constantly drawing wide attention in other computing paradigms, comparing to which there are more significant privacy challenges in edge computing, because there are many honest but curious adversaries which are usually authorized entities, such as edge data centers, infrastructure providers, services providers, and even some users. In this case, it is not possible to know whether a service provider is trustworthy in such open ecosystem with different trust domains. Therefore, preserving the users' privacy is a big challenge that must be carefully considered.

1) DATA PRIVACY

Data privacy is one of the major challenges as the users' private data is processed and shifted from edge devices to the heterogeneously distributed edge data servers or cloud servers.

In 2014, Li *et al.* [100] considered a practical hybrid data utilization architecture which consisting of a public cloud and a private cloud based on the probabilistic public key encryption method. The main purpose of the proposed architecture is to realize the fine-grained access control and keyword search without any leakage of private data. Here, the private cloud is introduced as a proxy or an access interface to support private data processing in public cloud.

In 2015, Bahrami and Singhal [63] proposed a light-weight cryptographic method for mobile clients to store data on one or multiple clouds by using Pseudo-Random Permutation (PRP) method in mobile cloud computing environment. The proposed method can be directly used in mobile devices and efficiently run on a smart-phone with low computation overheads by splitting files into multiple blocks based on chaos system.

In 2016, Pasupuleti *et al.* [64] proposed an Efficient and Secure Privacy-Preserving Approach (ESPPA) for mobile devices based on probabilistic public key encryption technique and ranked keyword searching algorithm. The proposed ESPPA consists of four phases: firstly, the data owner builds an index for multiple keywords from file collection, and then encrypt both the data and index to ensure the privacy of the index and data files. Next, in the retrieval phase, the data owner generates trapdoor for keyword and sends to the cloud server, and when the cloud receives the trapdoor, the server starts to search for the matched files and their corresponding relevance scores based on the trapdoor. Later, the server ranks the matched files and sends to the user based on the relevance scores. Finally, the user can retrieve the plaintext by decrypting the files using the private key.

2) IDENTITY PRIVACY

In 2013, Khan *et al.* [147] proposed a light-weight identity protection scheme for mobile users in cloud environment based on dynamic credential generation instead of the digital credential method. The proposed scheme can minimize the computational overhead of mobile devices by offloading the frequently dynamic credential generation operations to a trusted third party entity. Furthermore, to improve the performance of security and reliability of this scheme, dynamic credential information is generated on the basis of mobile-cloud packets exchange that can update frequently to ensure better protection against credential faking or stealing attacks. Finally, this scheme can also reduce the possibility of the Man-in-the-Middle attack according to the participant of the nonce in generating the cloud and mobile secrets. In the same year, Park *et al.* [65] introduce an Improved Identity Management Protocol (I2DM) by using Pretty Good Privacy (PGP) that based on Public Key Infrastructure (PKI) for secure mobile cloud computing. This protocol can reduce the network cost by maximizing load balancing at the weakest point, which allows mutual dependence communication via mobile operator process and easy identity management for the mobile user.

In 2014, Khalil *et al.* [66] pointed out the three possible vulnerabilities, namely-Identity Management (IDM) server compromise, mobile device compromise, and network traffic interception, and presented a novel IDM architecture named Consolidated Identity Management (CIDM) system to countermeasure the three above attacks. The proposed CIDM system makes use of the third-party server of IDM to manage the digital identities of mobile users which instead of the services provider. Firstly, the third party separates the authorization credentials and distributes them among all the IDM parties to prevent the illegal access. Secondly, the vulnerable of mobile device compromise can be solved by adding a layer of authentication using human-based challenge-response. Finally, consolidation the security of the communication link between the CIDM and the cloud services provider to decrease the probability of successful compromise of that link.

3) LOCATION PRIVACY

Location-Based Services (LBSs) have been more and more popular in recent years, the users can obtain varies services from location-based services provider (LBSP) by submitting their request and location information to the server. In this case, the private location information might be leakage because of the users cannot know whether the LBSP server is trusted or not, and that will be raising a big privacy challenge to preserve such location information that widely used in our daily life.

In 2012, Wei *et al.* [148] presented a flexible privacy-preserving location sharing system dubbed MobiShare in mobile online social networks. This system can realize the location sharing between both trusted social relations and untrusted strangers, and it also supports query locations within a certain range and user-defined access control. In the MobiShare system, user identities and anonymous location information are separately stored in two entities, the user' location privacy can be protected even if one entity is attacked by the adversary.

In 2014, Chen *et al*. [67] proposed a Location Privacy Preservation Scheme (LPPS) to protect the location privacy of mobile user by using a distributed cache pushing which is based on Markov Chain. The distributed cache proxies can store the most frequent location-related data after divided them into groups and push them from group to the mobile user. In this case, users can receive the location-based data from the cache proxies without sending out their real locations to location services server, which means the users' location privacy is well preserved.

In 2015, Niu *et al*. [68] proposed a Caching-aware Dummy Selection Algorithm (CaDSA) to protect location privacy in LBSs based on Chen's scheme [67]. The proposed CaDSA achieves k-anonymity effectively by sending some fake location with real location information as a query parameter to LBSP. Thus, the LBSP cannot find the real location information among fake ones which realize the location privacy-preserving. In addition, the authors also introduced a privacy metric based on entropy which can quantitatively describe the privacy relation between cache hit ratio and the privacy level. In the same year, Kassem *et al*. [149] proposed a fine-grained location access control tool, named LP-doctor, to prevent the location-privacy threats posed by mobile applications. This LP-doctor is an Android-based mobile device tool that can realize user-level location access control based on the operating system (OS) without any modification of application layer and OS. The specific functional components defined by LP-doctor include application session manager, policy manager, place detector, mobility manager, histogram manager, threat analyzer, and anonymization actuator. The functionality of the several components are described as follows: the application session manager is responsible for monitoring application launch and exit events to anonymous location when a location-based application is running; the policy manager fetches the privacy policy, such as block, allow, and protect, for the currently visited place and launched applications; the place detector monitors the user's real location, and the mobility manager updates the location information when the user's location changed; the histogram manager maintains the histogram of the locations visited ass observed by each application; the threat analyzer decides whatever to allow the protection of the current location according to the privacy policy made in policy manager. If the threat analyzer decided to protect the location information, then the anonymization actuator computes a fake location by adding a Laplacian noise to ensure the location anonymity.

VI. OPEN RESEARCH ISSUES

As analyzed in previous sections, data security and privacy-preserving are two of the most important issues in each computing paradigm, especially in edge computing since the data storage and processing scenarios become more complex with an outsourcing situation. In this section, we will further summarize some open research issues of data security and privacy-preserving that need to be addressed before specific deployment of edge computing.

Firstly, the open features of edge computing, such as parallel computing, resource constraint, big data processing, and coexistence of multiple trust domains, should be fully considered in the design of encryption mechanisms, to achieve *lightweight and distributed data encryption systems*. Moreover, in edge computing, there is multiple trust domains coexistence of multiple functional entities, the authentication mechanism not only needs to *assign an identity to every entity* but also needs to support *mutual authentication each other in all entities*. In addition, *access control of multiple entities between different trust domains* is a very important issue. It is necessary to build a *fine-grained, dynamic, and lightweight multi-domain access control system* with full consideration of cross domain and inter group hierarchical access control method in edge computing. At last, the users will generate massive data at the edge of the network, and this data will be calculated partially or completely in the edge devices. Most of the existing privacy-preserving methods do not have the dynamic update function, so the *fine-grained data security and privacy-preserving will be a major challenge in the dynamic data update process*. This four future research aspects of data security and privacy-preserving can be described as follows in detail.

A. DATA SECURITY

1) DATA CONFIDENTIALITY

Most of edge devices are resource constrained, so the current data security method might not be able to be deployed on these devices. Moreover, the highly dynamic environment in edge computing also makes the network become vulnerable. Thus, it is an important research idea to design lightweight, dynamic, and distributed secure data storage system based on several functional encryption methods as mentioned in section IV. In addition, the collaboration between edge data centers and cloud data centers could be utilized to decrease the complexity of the cryptographic algorithm.

2) DATA INTEGRITY

A major research goal of data integrity is to increase the auditing efficiency and to reduce the verification overhead when auditing functions are implemented. Moreover, designing privacy-preserving integrity auditing scheme in the multi-source heterogeneous computing environment that supports dynamic data updates is promising to be the focus of future research.

B. SECURE DATA COMPUTATION

1) SECURE DATA SEARCH

To protect data privacy, the user's sensitive data need to be encrypted before outsourced to the edge servers. In this case, the users are confronting the problem of how to search the keywords on the ciphertexts among encrypted data files. In distributed and multi-domain coexistence edge computing environment, the secure data search issues can be described as follows:

- How to build a secure keyword search scheme in distributed storage service model and further expand to the edge computing environment is needed.
- It is necessary to implement fine-grained search authority control in secure multi-party sharing environment with highly searching speed and accuracy, which can be applied to the multi-user search scenario with different trust domains.
- How to efficiently construct security index to make it suitable for resource constraint edge devices, and design distributed searchable encryption algorithm is an urgent problem that needs to solve.

2) VERIFIABLE COMPUTING

In edge computing, the verifiable computing strategy allows one edge server to offload some computation tasks to other edge servers among different trust domain, whatever other edge servers are trusted or not. This edge server has only one thing to perform that is to verify the computation results through the given function. Therefore, the verifiable computing mechanism should be considered to verify the computational accuracy and also to improve the collaborative computational ability of the edge servers.

C. AUTHENTICATION AND ACCESS CONTROL

Edge computing incorporates multiple functional entities, such as end users, service providers, and infrastructure providers. These actors coexistence and interaction in an ecosystem where multiple trust domain coexist. In such open environment, appropriate authentication and access control mechanisms are required to protect data privacy.

1) AUTHENTICATION

- Cross-domain authentication and handover authentication mechanisms between the same entities in different trust domain.
- Identification and mutual authentication methods of different entities in the same trust domain.
- It is also an important research issue to consider the functions of anonymity, integrity, traceability, and batch authentication while implementing lightweight authentication.

2) ACCESS CONTROL

- An important research direction of the access control system is to realize the cross domain, inter group, and hierarchical fine-grained access control system which supporting the extension from a single domain to multi domains.
- There are many urgently problems in cross-domain access control processes that needed to focus, such as unauthorized access, access conflict, key management, policy management, attribute management and etc.

D. PRIVACY PRESERVING

- In edge computing, there will be massive real-time dynamic data generated by edge devices in a real network, which would provide the opportunities to perform data association, integration analysis and privacy mining for attackers. Thus, it is very important to build the dynamic and fine-grained privacy-preserving scheme from the perspective of users' identity, behavior, interest and location.
- While ensuring the privacy of users is under protected, various data security functions (such as auditing, searching and updating), and the privacy issue in the process of cooperative inter-operation among users should be deserved widely attention.
- The privacy-preserving solutions provide advantages to both edge devices and service providers, but they introduce computational and communicational overhead. Hence, proposed privacy-preserving methods should encounter both privacy requirements as well as performance.

VII. CONCLUSION

In this survey, we analyze and summarize the data security and privacy-preserving challenges and countermeasures in edge computing paradigm from a holistic perspective. Firstly, forming factors of edge computing are given including the shortcomings of cloud computing, the coming era of IoE, and the change from data consumer to data prosumer, then we present the definition, architecture and several essential applications of edge computing. Secondly, we analyze the potential data security and privacy-preserving challenges, and the possible security mechanisms are given. Besides, cryptography-based technologies for solving data security and privacy issues are summarized, and a detailed study regarding the state-of-the-art security mechanisms are extensively surveyed and classified. Lastly, we point out the open research directions of data security and privacy issues in edge computing.

REFERENCES

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[2] P. K. Agyapong, M. Iwamura, D. Staehle, W. Kiess, and A. Benjebbour, "Design considerations for a 5G network architecture," *IEEE Commun. Mag.*, vol. 52, no. 11, pp. 65–75, Nov. 2014.

[3] GC Idex, "Cisco global cloud index: Forecast and methodology, 2016–2021," Cisco, San Jose, CA, USA, White Paper C11-738085-02, Feb. 2018.

[4] T. Snyder and G. Byrd, "The Internet of everything," *Computer*, vol. 50, no. 5, pp. 8–9, Jun. 2017.

[5] H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelfflé, "Vision and challenges for realising the Internet of Things," *Cluster Eur. Res. Projects Internet Things, Eur. Commision*, vol. 3, no. 3, pp. 34–36, Mar. 2010.

[6] D. E. Culler, "The once and future Internet of everything," *GetMobile: Mobile Comput. Commun.*, vol. 20, no. 3, pp. 5–11, Jul. 2016.

[7] P. G. Lopez *et al.*, "Edge-centric computing: Vision and challenges," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 45, no. 5, pp. 37–42, 2015.

[8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[9] V. Turner, J .F. Gantz, D. Reinsel, and S. Minton, "The digital universe of opportunities: Rich data and the increasing value of the Internet of Things," IDC, Framingham, MA, USA, White Paper IDC-1678, Apr. 2014.

[10] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, "A survey on mobile edge computing: The communication perspective," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2322–2358, 4th Quart., 2017.

[11] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.

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

[13] N. Fernando, S. W. Loke, and W. Rahayu, "Mobile cloud computing: A survey," *Future Generat. Comput. Syst.*, vol. 29, no. 1, pp. 84–106, 2013.

[14] A. R. Khan, M. Othman, S. A. Madani, and S. U. Khan, "A survey of mobile cloud computing application models," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 393–413, 1st Quart., 2014.

[15] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," presented at the 1st Ed. MCC Workshop Mobile Cloud Comput., Helsinki, Finland, Aug. 2012, pp. 13–16.

[16] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues," in *Proc. Workshop Mobile Big Data (Mobidata)*, Hangzhou, China, Jun. 2015, pp. 37–42.

[17] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing—A key technology towards 5G," ETSI, Sophia Antipolis, France, White Paper 11, Sep. 2015, pp. 1–16.

[18] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, Feb. 2018.

[19] A. Greenberg, J. Hamilton, D. A. Maltz, and P. Patel, "The cost of a cloud: Research problems in data center networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 1, pp. 68–73, 2009.

[20] M. Armbrust *et al.*, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[21] K. Gai, M. Qiu, H. Zhao, L. Tao, and Z. Zong, "Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing," *J. Netw. Comput. Appl.*, vol. 59, pp. 46–54, Jan. 2016.

[22] Z.-W. Xu, "Cloud-sea computing systems: Towards thousand-fold improvement in performance per watt for the coming zettabyte era," *J. Comput. Sci. Technol.*, vol. 29, no. 2, pp. 177–181, Jan. 2014.

[23] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generat. Comput. Syst.*, vol. 25, no. 6, pp. 599–616, 2009.

[24] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, Jun. 2015.

[25] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *J. Netw. Comput. Appl.*, vol. 84, pp. 38–54, Apr. 2017.

[26] "Edge computing," Pacific Northwest Nat. Lab, Richland, WA, USA, White Paper, Jan. 2013.

[27] ECC, "White paper of edge computing consortium," ECC, Beijing, China, White Paper, Nov. 2016.

[28] S. Wang, X. Zhang, Y. Zhang, L. Wang, J. Yang, and W. Wang, "A survey on mobile edge networks: Convergence of computing, caching and communications," *IEEE Access*, vol. 5, pp. 6757–6779, 2017.

[29] A. Vakali and G. Pallis, "Content delivery networks: Status and trends," *IEEE Internet Comput.*, vol. 7, no. 6, pp. 68–74, Nov. 2003.

[30] Y. Mao, J. Zhang, Z. Chen, and K. B. Letaief, "Dynamic computation offloading for mobile-edge computing with energy harvesting devices," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 3590–3605, Dec. 2016.

[31] X. Chen, L. Jiao, W. Li, and X. Fu, "Efficient multi-user computation offloading for mobile-edge cloud computing," *IEEE/ACM Trans. Netw.*, vol. 24, no. 5, pp. 2795–2808, Oct. 2016.

[32] S. Sardellitti, G. Scutari, and S. Barbarossa, "Joint optimization of radio and computational resources for multicell mobile-edge computing," *IEEE Trans. Signal Inf. Process. Over Netw.*, vol. 1, no. 2, pp. 89–103, Jun. 2015.

[33] K. Zhang *et al.*, "Energy-efficient offloading for mobile edge computing in 5G heterogeneous networks," *IEEE Access*, vol. 4, pp. 5896–5907, 2016.

[34] C. Regazzoni, A. Cavallaro, Y. Wu, J. Konrad, and A. Hampapur, "Video analytics for surveillance: Theory and practice," *IEEE Signal Process. Mag.*, vol. 27, no. 5, pp. 16–17, Sep. 2010.

[35] K. Hong, D. Lillethun, U. Ramachandran, B. Ottenwälder, and B. Koldehofe, "Mobile fog: A programming model for large-scale applications on the Internet of Things," in *Proc. 2nd ACM SIGCOMM Workshop Mobile Cloud Comput. (MCC SIGCOMM)*, Hong Kong, Aug. 2013, pp. 15–20.

[36] F. Li *et al.*, "Smart transmission grid: Vision and framework," *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 168–177, Sep. 2010.

[37] K. Zhang, Y. Mao, S. Leng, Y. He, and Y. Zhang, "Mobile-edge computing for vehicular networks: A promising network paradigm with predictive off-loading," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 36–44, Jun. 2017.

[38] K. Zhang, Y. Mao, S. Leng, S. Maharjan, and Y. Zhang, "Optimal delay constrained offloading for vehicular edge computing networks," in *Proc. IEEE 17th Int. Conf. Communs. (ICC)*, Paris, France, May 2017, pp. 1–6.

[39] L. Catarinucci *et al.*, "An IoT-aware architecture for smart healthcare systems," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 515–526, Dec. 2015.

[40] M. Aazam and E.-N. Huh, "Fog computing and smart gateway based communication for cloud of things," in *Proc. 2nd Int. Conf. Future Internet Things Cloud (FiCloud)*, Barcelona, Spain, Aug. 2014, pp. 464–470.

[41] P. Neirotti, A. De Marco, A. C. Cagliano, G. Mangano, and F. Scorrano, "Current trends in Smart City initiatives: Some stylised facts," *Cities*, vol. 38, pp. 25–36, Jun. 2014.

[42] A. Taherkordi, F. Eliassen, and G. Horn, "From IoT big data to IoT big services," in *Proc. 32th SIGAPP Symp. Appl. Comput. (SAC)*, Marrakech, Morocco, Apr. 2017, pp. 485–491.

[43] R. Jain and S. Paul, "Network virtualization and software defined networking for cloud computing: A survey," *IEEE Commun. Mag.*, vol. 51, no. 11, pp. 24–31, Nov. 2013.

[44] T. Bhatia and A. K. Verma, "Data security in mobile cloud computing paradigm: A survey, taxonomy and open research issues," *J. Supercomput.*, vol. 73, no. 6, pp. 2558–2631, Jun. 2017.

[45] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, 2003.

[46] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1265–1277, Jun. 2016.

[47] K. Liang *et al.*, "A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing," *Future Generat. Comput. Syst.*, vol. 52, pp. 95–108, Nov. 2015.

[48] M. R. Baharon, Q. Shi, and D. Llewellyn-Jones, "A new lightweight homomorphic encryption scheme for mobile cloud computing," in *Proc. 15th Int. Conf. Comput. Inf. Technol. (CIT)*, Liverpool, U.K., Oct. 2015, pp. 618–625.

[49] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *Proc. 29th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, San Diego, CA, USA, Mar. 2010, pp. 1–9.

[50] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 5, pp. 847–859, May 2011.

[51] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 9, pp. 1717–1726, Sep. 2013.

[52] C. Lin, Z. Shen, Q. Chen, and F. T. Sheldon, "A data integrity verification scheme in mobile cloud computing," *J. Netw. Comput. Appl.*, vol. 77, pp. 146–151, Jan. 2017.

[53] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 8, pp. 1467–1479, Aug. 2012.

[54] C. Wang, W. Li, Y. Li, and X. L. Xu, "A ciphertext-policy attribute-based encryption scheme supporting keyword search function," in *Proc. 5th Int. Symp. Cyberspace Safety Secur. (CSS)*, Zhangjiajie, China, Nov. 2013, pp. 377–386.

[55] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic searchable symmetric encryption," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, Raleigh, NC, USA, Oct. 2012, pp. 965–976.

[56] J. Shao, Z. Cao, X. Liang, and H. Lin, "Proxy re-encryption with keyword search," *Inf. Sci.*, vol. 180, no. 13, pp. 2576–2587, 2010.

[57] H. Liu, H. Ning, Q. Xiong, and L. T. Yang, "Shared authority based privacy-preserving authentication protocol in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 1, pp. 241–251, Jan. 2015.

[58] D. S. Touceda, J. M. S. Cámara, S. Zeadally, and M. Soriano, "Attribute-based authorization for structured peer-to-peer (P2P) networks," *Comput. Standards Interfaces*, vol. 42, pp. 71–83, Nov. 2015.

[59] X. Yang, X. Huang, and J. K. Liu, "Efficient handover authentication with user anonymity and untraceability for mobile cloud computing," *Future Generat. Comput. Syst.*, vol. 62, pp. 190–195, Sep. 2016.

[60] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. 29th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, San Diego, CA, USA, Mar. 2010, pp. 1–9.

[61] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1947–1960, Dec. 2013.

[62] L. Chen and R. Urian, "DAA-A: Direct anonymous attestation with attributes," in *Proc. 8th Int. Conf. Trust Trustworthy Comput. (TRUST)*, Heraklion, Greece, Aug. 2015, pp. 228–245.

[63] M. Bahrami and M. Singhal, "A light-weight permutation based method for data privacy in mobile cloud computing," in *Proc. 3th IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud)*, San Francisco, CA, USA, Mar./Apr. 2015, pp. 189–198.

[64] S. K. Pasupuleti, S. Ramalingam, and R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," *J. Netw. Comput. Appl.*, vol. 64, pp. 12–22, Apr. 2016.

[65] I. Park, Y. Lee, and J. Jeong, "Improved identity management protocol for secure mobile cloud computing," in *Proc. 46th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Maui, HI, USA, Jan. 2013, pp. 4958–4965.

[66] I. Khalil, A. Khreishah, and M. Azeem, "Consolidated identity management system for secure mobile cloud computing," *Comput. Netw.*, vol. 65, no. 2, pp. 99–110, Jun. 2014.

[67] M. Chen, W. Li, Z. Li, S. Lu, and D. Chen, "Preserving location privacy based on distributed cache pushing," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Istanbul, Turkey, Apr. 2014, pp. 3456–3461.

[68] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Enhancing privacy through caching in location-based services," in *Proc. 34th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Hong Kong, Apr. 2015, pp. 1017–1025.

[69] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 196. Santa Barbara, CA, USA: Springer, 1984, pp. 47–53.

[70] H. Tanaka, "A realization scheme for the identity-based cryptosystem," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 293. Santa Barbara, CA, USA: Springer, 1984, pp. 340–349.

[71] S. Tsujii and T. Itoh, "An ID-based cryptosystem based on the discrete logarithm problem," *IEEE J. Sel. Areas Commun.*, vol. 7, no. 4, pp. 467–473, May 1989.

[72] A. Sahai and B. Waters. "Fuzzy identity-based encryption," in *Proc. Proc. 24th Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Aarhus, Denmark, May 2005, pp. 457–473.

[73] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, Alexandria, VA, USA, Nov. 2006, pp. 89–98.

[74] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. 14th Int. Conf. Pract. Theory Public Key Cryptography (PKC)*, Taormina, Italy, Mar. 2011, pp. 53–70.

[75] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-based encryption with non-monotonic access structures," in *Proc. 14th ACM Conf. Comput, Commun. Secur. (CCS)*, Alexandria, VA, USA, Oct. 2007, pp. 195–203.

[76] A. Lewko, A. Sahai, and B. Waters, "Revocation systems with very small private keys," in *Proc. IEEE Symp. Secur. Privacy*, Oakland, CA, USA, May 2010, pp. 273–285.

[77] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Proc. 17th Int. Conf. Theory Appl. Cryptograph Techn. (EUROCRYPT)*, Espoo, Finland, May 1998, pp. 127–144.

[78] M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang, and R. Buyya, "Attribute-based data access control in mobile cloud computing: Taxonomy and open issues," *Future Generat. Comput. Syst.*, vol. 72, pp. 273–287, Jul. 2017.

[79] A. A. Ivan and Y. Dodis, "Proxy cryptography revisited," in *Proc. 10th Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, San Diego, CA, USA, Feb. 2003, pp. 1–20.

[80] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Trans. Inf. Syst. Secur.*, vol. 9, no. 1, pp. 1–30, 2006.

[81] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in *Proc. 5th Int. Conf. Appl. Cryptography Netw. Secur. (ACNS)*, Zhuhai, China, Jun. 2007, pp. 288–306.

[82] H. Wang, Z. Cao, and L. Wang, "Multi-use and unidirectional identity-based proxy re-encryption schemes," *Inf. Sci.*, vol. 180, no. 20, pp. 4042–4059, Oct. 2010.

[83] J. Weng, R. H. Deng, X. Ding, C.-K. Chu, and J. Lai, "Conditional proxy re-encryption secure against chosen-ciphertext attack," in *Proc. 4th ACM Symp. Inf., Comput., Commun. Secur. (ASIACCS)*, Sydney, NSW, Australia, Mar. 2009, pp. 322–332.

[84] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Found. Secure Comput.*, vol. 4, no. 11, pp. 169–180, 1978.

[85] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[86] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[87] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Adv. Cryptol.—EUROCRYPT*, Prague, Czech Republic, May 1999, pp. 223–238.

[88] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. 41st ACM Symp. Theory Comput. (STOC)*, Bethesda, Maryland, May 2009, pp. 169–178.

[89] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in *Proc. 29th Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*, Riviera, French, May 2010, pp. 24–43.

[90] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," *SIAM J. Comput.*, vol. 43, no. 2, pp. 831–871, 2014.

[91] C. Gentry, A. Sahai, and B. Waters, "Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based," in *Proc. 33rd Annu. Cryptol. Conf. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 2013, pp. 75–92.

[92] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE Symp. Secur. Privacy*, Oakland, CA, USA, May 2000, pp. 44–55.

[93] B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters, "Building an encrypted and searchable audit log," in *Proc. 11th Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS)*, San Diego, CA, USA, Feb. 2004, p. 1.

[94] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," *J. Comput. Secur.*, vol. 19, no. 5, pp. 895–934, Jan. 2011.

[95] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 3027, C. Cachin and J. Camenisch, Eds. Berlin, Germany: Springer-Verlag, 2004, pp. 506–522.

[96] P. Golle, J. Staddon, and B. Waters, "Secure conjunctive keyword search over encrypted data," in *Applied Cryptography and Network Security* (Lecture Notes in Computer Science), vol. 3089. Berlin, Germany: Springer, 2004, pp. 31–45.

[97] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Theory of Cryptography*. vol. 4392. Amsterdam, Netherlands: Springer, 2007, pp. 535–554.

[98] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Commun. Mobile Comput.*, vol. 13, no. 18, pp. 1587–1611, Dec. 2013.

[99] J. A. González-Martínez, M. L. Bote-Lorenzo, E. Gómez-Sánchez, and R. Cano-Parra, "Cloud computing and education: A state-of-the-art survey," *Comput. Edu.*, vol. 80, pp. 132–151, Jan. 2015.

[100] I. Stojmenovic and S. Wen, "The Fog computing paradigm: Scenarios and security issues," in *Proc. Federated Conf. Comput. Sci. Inf. Syst. (FedCSIS)*, Warsaw, Poland, Sep. 2014, pp. 1–8.

[101] D. S. Milojicic *et al.*, "Peer-to-peer computing," HP Labs, Palo Alto, CA, USA, Tech. Rep. HPL-2002-57, 2002.

[102] Y. Yang, J. K. Liu, K. Liang, K.-K. R. Choo, and J. Zhou, "Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data," in *Proc. 20th Eur. Symp. Res. Comput. Secur. (ESORICS)*, Vienna, Austria, Sep. 2015, pp. 146–166.

[103] C. Zuo, J. Shao, G. Wei, M. Xie, and M. Ji, "CCA-secure ABE with outsourced decryption for fog computing," *Future Generat. Comput. Syst.*, vol. 78, pp. 730–738, Jan. 2018.

[104] Y. Yang, H. Zhu, H. Lu, J. Weng, Y. Zhang, and K.-K. R. Choo, "Cloud based data sharing with fine-grained proxy re-encryption," *Pervasive Mobile Comput.*, vol. 28, pp. 122–134, Jun. 2016.

[105] J. Shao, R. Lu, X. Lin, and K. Liang, "Secure bidirectional proxy re-encryption for cryptographic cloud storage," *Pervasive Mobile Comput.*, vol. 28, pp. 113–121, Jun. 2016.

[106] A. N. Khan, M. L. M. Kiah, M. Ali, S. Shamshirband, and A. ur Rehman Khan, "A cloud-manager-based re-encryption scheme for mobile users in cloud environment: A hybrid approach," *J. Grid Comput.*, vol. 13, no. 4, pp. 651–675, Dec. 2015.

[107] A. N. Khan *et al.*, "A comparative study and workload distribution model for re-encryption schemes in a mobile cloud computing environment," *Int. J. Commun. Syst.*, vol. 30, no. 16, p. e3308, Nov. 2017.

[108] M. Louk and H. Lim, "Homomorphic encryption in mobile multi cloud computing," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Siem Reap, Cambodia, Jan. 2015, pp. 493–497.

[109] K. Yang and X. Jia, "Data storage auditing service in cloud computing: Challenges, methods and opportunities," *World Wide Web*, vol. 15, no. 4, pp. 409–428, 2012.

[110] M. Sookhak, A. Gani, M. K. Khan, and R. Buyya, "Dynamic remote data auditing for securing big data storage in cloud computing," *Inf. Sci.*, vol. 380, pp. 101–116, Feb. 2017.

[111] J. Li, L. Zhang, J. K. Liu, H. Qian, and Z. Dong, "Privacy-preserving public auditing protocol for low-performance end devices in cloud," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2572–2583, Nov. 2016.

[112] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 222–233, Jan. 2014.

[113] H. Li, D. Liu, Y. Dai, T. H. Luan, and X. S. Shen, "Enabling efficient multi-keyword ranked search over encrypted mobile cloud data through blind storage," *IEEE Trans. Emerg. Topics Comput.*, vol. 3, no. 1, pp. 127–138, Mar. 2015.

[114] J. Li, R. Ma, and H. Guan, "TEES: An efficient search scheme over encrypted data on mobile cloud," *IEEE Trans. Cloud Comput.*, vol. 5, no. 1, pp. 126–139, Jan/Mar. 2017.

[115] Q. Zheng, S. Xu, and G. Ateniese, "VABKS: Verifiable attribute-based keyword search over outsourced encrypted data," in *Proc. 33th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Toronto, ON, Canada, Apr./May 2014, pp. 522–530.

[116] P. Liu, J. Wang, H. Ma, and H. Nie, "Efficient verifiable public key encryption with keyword search based on KP-ABE," in *Proc. IEEE 9th Int. Conf. Broadband Wireless Comput., Commun. Appl. (BWCCA)*, Guangdong, China, Nov. 2014, pp. 584–589.

[117] W. Sun, S. Yu, W. Lou, Y. T. Hou, and H. Li, "Protecting your right: Verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 4, pp. 1187–1198, Apr. 2016.

[118] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption," in *Proc. 17th Int. Conf. Financial Cryptography Data Secur. (FC)*, Okinawa, Japan, Apr. 2013, pp. 258–274.

[119] W. Sun, X. Liu, W. Lou, Y. T. Hou, and H. Li, "Catch you if you lie to me: Efficient verifiable conjunctive keyword search over large dynamic encrypted cloud data," in *Proc. 34th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Hong Kong, Apr. 2015, pp. 2110–2118.

[120] Z. Xia, X. Wang, X. Sun, and Q. Wang, "A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 2, pp. 340–352, Jan. 2016.

[121] B. Hu, Q. Liu, X. Liu, T. Peng, G. Wang, and J. Wu, "DABKS: Dynamic attribute-based keyword search in cloud computing," in *Proc. IEEE 17th Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–6.

[122] X. A. Wang, X. Huang, X. Yang, L. Liu, and X. Wu, "Further observation on proxy re-encryption with keyword search," *J. Syst. Softw.*, vol. 85, no. 3, pp. 643–654, 2012.

[123] L. Fang, W. Susilo, C. Ge, and J. Wang, "Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search," *Theor. Comput. Sci.*, vol. 462, pp. 39–58, Nov. 2012.

[124] Y. Shi, J. Liu, Z. Han, Q. Zheng, R. Zhang, and S. Qiu, "Attribute-based proxy re-encryption with keyword search," *PLoS ONE*, vol. 9, no. 12, p. e116325, Dec. 2014.

[125] J.-L. Tsai and N.-W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," *IEEE Syst. J.*, vol. 9, no. 3, pp. 805–815, Sep. 2015.

[126] D. He, N. Kumar, M. K Khan, L. Wang, and J. Shen, "Efficient privacy-aware authentication scheme for mobile cloud computing services," *IEEE Syst. J.*, to be published.

[127] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 5, pp. 1319–1328, May 2016.

[128] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Generat. Comput. Syst.*, vol. 81, pp. 557–565, Apr. 2018.

[129] Y. Yang, X. Zheng, X. Liu, S. Zhong, and V. Chang, "Cross-domain dynamic anonymous authenticated group key management with symptom-matching for e-health social system," *Future Generat. Comput. Syst.*, to be published. [Online]. Available: https://doi.org/10.1016/j.future.2017.06.025

[130] Q. Jiang, J. Ma, and F. Wei, "On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services," *IEEE Syst. J.*, to be published.

[131] A. N. Toosi, R. N. Calheiros, and R. Buyya, "Interconnected cloud computing environments: Challenges, taxonomy, and survey," *ACM Comput. Surv.*, vol. 47, no. 1, Jul. 2014, Art. no. 7.

[132] D. McCarthy *et al.*, "Personal cloudlets: Implementing a user-centric datastore with privacy aware access control for cloud-based data platforms," in *Proc. IEEE/ACM 1st Int. Workshop Techn. Legal Aspects Data Privacy Secur. (TELERISE)*, Florence, Italy, May 2015, pp. 38–43.

[133] D. He, S. Zeadally, L. Wu, and H. Wang, "Analysis of handover authentication protocols for mobile wireless networks using identity-based public key cryptography," *Comput. Netw.*, vol. 128, pp. 154–163, Dec. 2017.

[134] M. Alizadeh, S. Abolfazli, M. Zamani, S. Baharun, and K. Sakurai, "Authentication in mobile cloud computing: A survey," *J. Netw. Comput. Appl.*, vol. 61, pp. 59–80, Feb. 2016.

[135] K. Xue *et al.*, "RAAC: Robust and auditable access control with multiple attribute authorities for public cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 4, pp. 953–967, Apr. 2017.

[136] Y. Jin, C. Tian, H. He, and F. Wang, "A secure and lightweight data access control scheme for mobile cloud computing," in *Proc. 5th IEEE Int. Conf. Big Data Cloud Computing. (BDCloud)*, Dalian, China, Aug. 2015, pp. 172–179.

[137] P. Zhang, Z. Chen, J. K. Liu, K. Liang, and H. Liu, "An efficient access control scheme with outsourcing capability and attribute update for fog computing," *Future Generat. Comput. Syst.*, vol. 78, pp. 753–762, Jan. 2018.

[138] Q. Huang, Y. Yang, and L. Wang, "Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things," *IEEE Access*, vol. 5, pp. 12941–12950, Jul. 2017.

[139] H.-C. Chen, "A hierarchical virtual role assignment for negotiation-based RBAC scheme," in *Proc. 10th Int. Conf. Broadband Wireless Comput., Commun. Appl. (BWCCA)*, Krakow, Poland, Nov. 2015, pp. 538–543.

[140] A. Almutairi, M. Sarfraz, S. Basalamah, W. Aref, and A. Ghafoor, "A distributed access control architecture for cloud computing," *IEEE Softw.*, vol. 29, no. 2, pp. 36–44, Mar/Apr. 2012.

[141] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[142] G. J. Ahn and R. Sandhu, "Role-based authorization constraints specification," *ACM Trans. Inf. Syst. Secur.*, vol. 3, no. 4, pp. 207–226, Nov. 2000.

[143] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," *IEEE Comput.*, vol. 43, no. 6, pp. 79–81, Jun. 2010.

[144] H. Li, S. Wang, X. Tian, W. Wei, and C. Sun, "A survey of extended role-based access control in cloud computing," in *Proc. 4th Int. Conf. Comput. Eng. Netw. (CENeT)*, Shanghai, China, Jul. 2015, pp. 821–831.

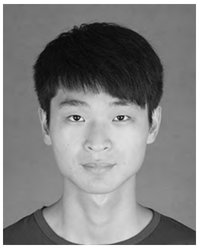
[145] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges," *Future Generat. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018.

[146] J. Li, J. Li, X. Chen, Z. Liu, and C. Jia, "Privacy-preserving data utilization in hybrid clouds," *Future Generat. Comput. Syst.*, vol. 30, pp. 98–106, Jan. 2014.

[147] A. N. Khan, M. L. M. Kiah, S. A. Madani, A. ur Rehman Khan, and M. Ali, "Enhanced dynamic credential generation scheme for protection of user identity in mobile-cloud computing," *J. Supercomput.*, vol. 66, no. 3, pp. 1687–1706, Dec. 2013.

[148] W. Wei, F. Xu, and Q. Li, "MobiShare: Flexible privacy-preserving location sharing in mobile online social networks," in *Proc. 31th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Orlando, FL, USA, Mar. 2012, pp. 2616–2620.

[149] F. Kassem, F. Huan, and K. G. Shin, "Anatomization and protection of mobile apps' location privacy threats," in *Proc. 24th USENIX Conf. Secur. Symp. (USENIX)*, Washington, DC, USA, Aug. 2015, pp. 753–768.

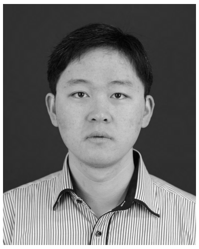


JIALE ZHANG received the M.E. degree in computer technology from Tianjin Polytechnic University, Tianjin, China, in 2017. He is currently pursuing the Ph.D. degree with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China. His research interests are mainly edge computing, network security, privacy preserving, and applied cryptography.

BING CHEN received the B.S. and M.S. degrees in computer engineering from the Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China, in 1992 and 1995, respectively, and the Ph.D. degree from the College of Information Science and Technology, NUAA, in 2008. He has been with NUAA since 1998, where he is currently a Professor with the Computer Science and Technology Department. His main research interests include cloud computing, wireless communications, and cognitive radio networks.

YANCHAO ZHAO received the B.S. degree and the Ph.D. degree in computer science from Nanjing University in 2007 and 2015, respectively. In 2011, he was a Visiting Student with the Department of Computer and Information Sciences, Temple University, Philadelphia, USA. He is currently an Associate Professor with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China. His research interests include wireless network, mobile computing, edge computing, and device-free sensing.

XIANG CHENG received the M.E. degree in computer technology from the Civil Aviation University of China, Tianjin, China, in 2016. He is currently pursuing the Ph.D. degree with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China. His research interests are mainly edge computing, network security, risk assessment, and big data analysis.



FENG HU received the M.E. degree in computer science from the Anhui University of Science and Technology, Anhui, China, in 2014. He is currently pursuing the Ph.D. degree with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China. His research interests are mainly cognitive radio networks, mobile networks, SDN, and 5G.