Smart Applications in Edge Computing: Overview on Authentication and Data Security

Xinghua Li, *Member, IEEE*, Ting Chen, Qingfeng Cheng, Siqi Ma, and Jianfeng Ma, *Member, IEEE*

***Abstract*—As a new computing paradigm, edge computing has appeared in the public field of vision recently. Owing to its advantages of low delay and fast response, edge computing has become an important assistant of cloud computing and has brought new opportunities for diverse smart applications like the smart grid, the smart home, and the smart transportation. However, the accompanying security issues, which have always been the focus of users' concern, still cannot be ignored. Therefore, we focus on the security issues in this overview. We first introduce some related definitions of edge computing and present the architecture for edge computing-based smart applications. After illustrating the smart applications, from the perspective of identity authentication and data security, we analyze the security protection requirements of these smart applications in the edge computing environment. Next, we review some state-of-the-art works on them. Furthermore, we present the extended discussions on the applicability of these current works in the edge computing environment. Finally, we briefly discuss the future work on authentication and data security of edge computing-based smart applications.**

***Index Terms*—Data security, edge computing, identity authentication, smart grid, smart home, smart transportation.**

I. Introduction

With the continuous advancement in the 5G technology and Internet of Things (IoT), more and more users join in the life of Internet. According to the 44th *Statistical Report on the Development of Internet in China*, the Internet users and Internet penetration rate of China are on the rise. They have reached 854 million and 61.2% by June 2019, respectively, [1]. Besides, network edge devices and the data are also growing explosively, which puts forward higher requirements to the cloud for data processing and storage. First, transmitting mass of data is a great pressure to the transmission bandwidth. Second, the centralized processing of a large amount of data cannot provide real-time response for users. In addition, the long-distance transmission and centralized storage of data are more vulnerable to the threat of privacy disclosure. However, traditional cloud computing fails to satisfy the higher requirements of user experience. To offset the weaknesses of cloud computing in the context of IoT, edge computing emerges as the time requires [2], [3]. Its wide application is an inevitable trend in the era of larger data. Recently, the *Guide to the Edge Computing Market of the Industrial IoT*, released by Gartner, predicted that more than 50% data generated by enterprises would be produced and processed outside the data center or cloud by 2022 [4]. Edge computing, which provides capabilities of computing and other services near the edge network, is just like a new tentacle of cloud computing extending to the edge.

Presently, various smart applications based on IoT are applying edge computing to achieve better utility, such as the smart grid [5], the smart home [6], and the smart transportation [7]. These smart applications bring convenience to our life, but there also exist some security issues that cannot be ignored. For example, the smart grid relies too much on the network infrastructure. Once the network exhibits weaknesses, the attacker is likely to damage the stability of the smart grid by manipulating system parameters or instrument measurement information [8]. Edge computing, a new computing paradigm, does bring new opportunities for these smart applications, but it is undeniable that its characteristics of distributed deployment and complex service mode may also bring some new security issues to the smart applications (brief explanations are presented in Section III-B). Moreover, there exist security issues in edge computing itself [9], [10]. For instance, Caprolu *et al.* [10] especially discussed some related scenario-driven attack identification. Consequently, the technologies originally used to solve the security issues of these smart applications cannot be directly applied in the edge computing environment. That is, they fail to consider the features of edge computing. By taking identity authentication for illustration, the trust model in the edge computing may be different from the assumed ones in some original schemes. For example in the smart home, terminals have trust relationship with the home gateway (edge node), as well as with the backend server (cloud), while there does not exist trust relationship between the edge node and cloud. This trust model is different from the 802.1X, where the authentication server has trust relationships with the access point and terminals. Therefore, the authentication schemes suitable for 802.1X cannot be directly used in the edge computing environment.

Manuscript received March 31, 2020; revised July 16, 2020; accepted August 19, 2020. Date of publication August 25, 2020; date of current version March 5, 2021. This work was supported by the National Natural Science Foundation of China under Grant U1708262, Grant U1736203, and Grant 61872449. *(Corresponding author: Qingfeng Cheng.)*

Xinghua Li, Ting Chen, and Jianfeng Ma are with the State Key Laboratory of Integrated Services Networks and School of Cyber Engineering, Xidian University, Xi'an 710071, China (e-mail: xhli1@mail.xidian.edu.cn; tingchen0127@163.com; jfma@mail.xidian.edu.cn).

Qingfeng Cheng is with the State Key Laboratory of Mathematical Engineering and Advanced Computing, Strategic Support Force Information Engineering University, Zhengzhou 450001, China (e-mail: qingfengc2008@sina.com).

Siqi Ma is with the School of Information Technology and Electrical Engineering, University of Queensland, Brisbane, QLD 4072, Australia (e-mail: slivia.ma@uq.edu.au).

Digital Object Identifier 10.1109/JIOT.2020.3019297

TABLE I
COMPARISON OF EXISTING OVERVIEWS WITH THEIR PRIMARY FOCUS

References	Smart applications	Edge computing	Focus on security	Identity authentication	Data security	Applicability discussion
Khan et al.[7]	smart city	√	×	√	×	×
Zhang et al.[8]	×	√	√	×	√	×
Mao et al.[11]	×	√	×	×	×	×
Wang et al.[12]	×	√	×	×	×	×
Tan et al.[13]	smart grid	×	√	×	√	×
Xiao et al.[14]	×	√	√	×	√	×
Li et al.[15]	smart transportation	√	×	√	×	×
Kuyucu et al.[16]	smart home	×	√	√	×	×
Caropreso et al.[17]	smart meters	×	√	×	√	×
Ghosal et al.[18]	smart grid	×	√	√	×	×
Our overview	smart grid, smart home, smart transportation	√	√	√	√	√

Consequently, the original schemes need improving based on the features of edge computing before they are applied to these edge computing-based systems.

Currently, there have existed some overviews on smart applications or edge computing, such as [7], [8], [11]–[18]. Among them, Khan *et al.* [11] surveyed on edge computing driven smart city and highlighted the role that edge computing played in smart city, but it did not focus on the security of specific applications in smart city. Although Zhang *et al.* [12] and Xiao *et al.* [15] highlighted the security in edge computing, but they did not combine specific smart applications. As [13] and [14], they only surveyed on edge computing, neither combining smart applications nor focusing on security. Tan *et al.* [8] and Kuyucu *et al.* [16] put emphasis on the security discussion in the smart grid and the smart home, respectively, but they did not take edge computing into account. Li *et al.* [7] surveyed on edge computing-based smart transportation, but their focus is not security. Caropreso *et al.* [17] and Ghosal and Conti [18] summarized the security issues and technologies related to smart metering facilities in the smart grid. Concretely, Caropreso *et al.* [17] put forward an open-source framework of smart meters from the perspective of communication security and data security, and realized the multiframe communication between the client and the server by TCP/IP protocol via wireless networks. Ghosal and Conti [18] emphasized the important role that key management system played in the advanced measurement infrastructure of the smart grid, and observed that its security was still a challenge. Although Caropreso *et al.* [17] and Ghosal and Conti [18] have made contributions to survey on the security of the smart grid, they still failed to consider edge computing. To indicate the difference between our article and the aforementioned overviews, the comparison of our overview with [7], [8], [11]–[18] is given in Table I. From the comparison, it is obvious that our overview is the first one to discuss the security of edge computing-based smart applications and the corresponding applicability in edge computing. Since the legality of entity and data security are two basic points to guarantee the better function of the system, we take the two aspects to discuss. Our main contributions are listed as follows.

1) We introduce the definition of edge computing from different research works. Associating with the definitions and related architectures of edge computing, we exhibit the edge computing-based architecture for smart applications.
2) We describe three typical smart applications and briefly illustrate how edge computing works in them. Then, we briefly summarize some security risks of them and present a security protection framework by taking identity authentication and data preserving for illustration.
3) Based on the proposed security protection framework, we overview and analyze the current related works, including briefly discussing their applicability after the participation of edge computing.
4) After summaries, analysis, and discussions, we briefly present the future security researches on authentication and data security of the edge computing-based smart applications.

The remaining of this article is sketched as follows. We briefly introduce the definitions of edge computing and exhibit the architecture of smart applications based on edge computing in Section II. Section III introduces three typical smart applications, analyzes the security protection requirements from the perspective of identity authentication and data security, and puts forward the security protection framework of these smart applications in the edge computing environment. Based on the proposed framework, some recent research reviews and corresponding analysis of the smart grid, the smart home, and the smart transportation are given in Sections IV–VI in order. Section VII presents brief extension that is interesting. Section VIII concludes this article. The last section presents the possible research works in the future.

II. EDGE COMPUTING: DEFINITION AND ARCHITECTURE

As [19] described, the requirement of edge computing were pushed from three aspects, i.e., cloud services, IoT, and data consumer to producer. Specifically, when various edge devices produce massive data that needs efficient processing in a network area, it is a challenge for the cloud to meet the high efficiency with limited resources. Moreover, in the IoT era, billions of devices participate in the data production. All the data transmitted to the cloud puts great pressure on the network bandwidth. To some extent, processing data on the edge of the

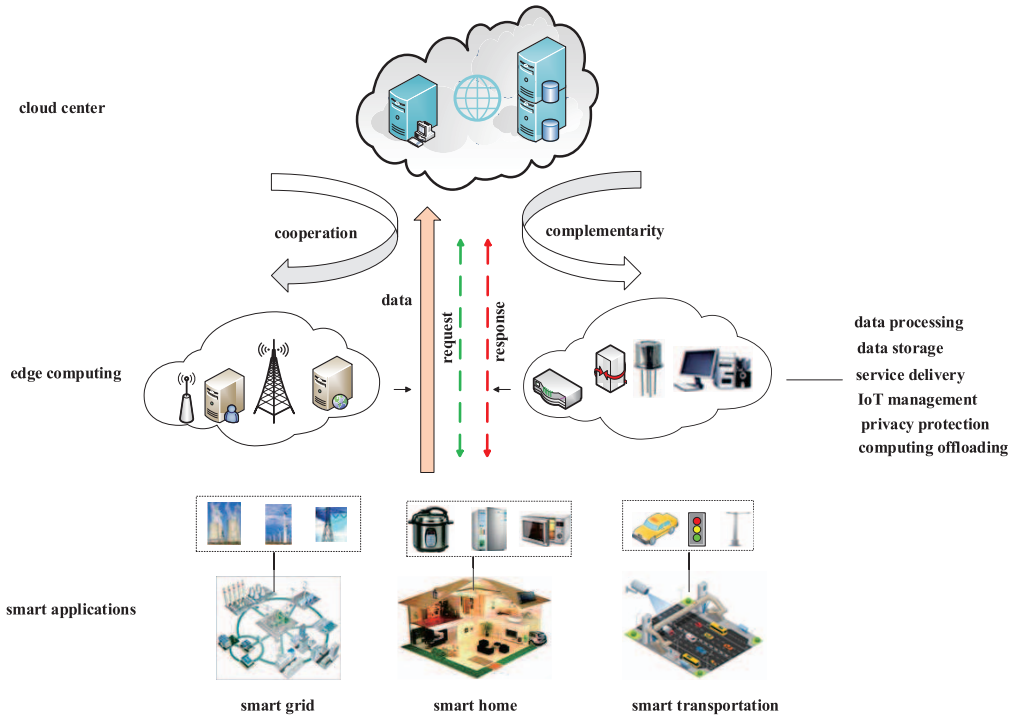


Fig. 1. Edge computing-based architecture for smart applications.

network can protect users' privacy better. Thus, the emergence of edge computing is inevitable, which plays a nonnegligible role in addressing the aforementioned issues.

The definitions of edge computing are various on versions. Specifically, Shi *et al.* [19] claimed that it referred to a technology, where the computing was permitted to be executed on the edge network. Moreover, the downstream and the upstream data represent cloud service and IoT services, respectively. The word "edge" can refer to any network and computing service existing from the data source to the cloud center. Edge computing consortium (ECC) also defined it in the white paper of *Edge Computing Reference Architecture 3.0*. Concretely, edge computing, a distributed architecture, integrates the computing, network, and other core capabilities on the edge network. Close to the objects or data sources, it provides smart services nearby and satisfies some key requirements, such as the industry digitalization in agile connection, real-time business, application intelligence, etc. Besides, it serves as a bridge that connects the physical and digital world, enabling smart assets, smart gateways, and smart services [20].

Associating with the aforementioned definitions, based on our understanding of edge computing and related descriptions in [21]–[23], we put forward an edge computing-based architecture for smart applications, seen in Fig. 1. The architecture consists of three layers, i.e., the cloud center, edge computing, and the smart applications. Edge computing, which interacts with both the cloud center and the smart applications, is in the middle layer, docking with the cloud upward and connecting with various smart devices downward. Edge computing is mainly composed of various hardware entity edge nodes. As described in [20], according to different hardware characteristics and business focus, edge nodes can be classified into edge gateway, edge controller, edge sensor, etc., where the edge gateway focuses on network protocol processing and conversion, the edge controller focuses on supporting real-time closed-loop control business, and the edge sensor mainly collects and processes low-power information. Specifically, when these smart applications upload data to the cloud center and interact with it, edge computing layer plays a significant role in data processing and storage, service delivery, the IoT management, privacy protection, and computing offloading by decreasing the time delay and lightening the pressure of the cloud center.

As Fig. 1 displays, cloud computing and edge computing are complementary and cooperative. They have their own advantages, but they are not separate. Otherwise, the system will not achieve the expected effect. As for cloud computing, it possesses a larger storage resource, while the storage resource of edge computing is limited. However, compared with cloud computing, edge computing closes to the data producer and costs shorter time to respond users. If the user requires a real-time response, then edge computing functioned as the data processor can satisfy the user by reducing the delay. In addition, to well make use of the storage of cloud computing, the edge node can also return the data result to the cloud if the user approves. In this case, if the edge node misses some data that the user requires, he/she can obtain them from the cloud. To exhibit a more comprehensive display of the differences and relations between cloud computing and edge computing, we summarize them in Table II.

III. Typical Smart Applications and Corresponding Security Requirements

Three typical smart applications, i.e., the smart grid, the smart home, and the smart transportation, are introduced in this

TABLE II
DIFFERENCE AND RELATION BETWEEN CLOUD COMPUTING AND EDGE COMPUTING

Difference	Cloud computing	Edge computing
Geo-distribution	Centralized	Distributed
Efficiency	Low	High
Storage space	Large	Small
Real-time	Low	High
Distance from user	Far	Close
Bandwidth requirement	High	Low
Mobility support	Limited, even no	Yes
Scalability support	At center	At center and edge
Personalization support	Limited, even no	Yes
Privacy disclosure risk	High	Low
Location of data processing	Close to data center	Close to edge or locally
Relation between cloud computing and edge computing	Edge computing is an extension and expansion of cloud computing. They cooperate and complement each other.	

section, including illustrating how edge computing is deployed in them at current research. Furthermore, we will summarize some security risks and security requirements of them in terms of authentication and data security. The details are shown as follows.

A. Brief Introduction of Typical Smart Applications

1) *Smart Grid:* As one of the IoT applications, the smart grid is a network physical system covering various smart devices. It perfectly combines modern information technology with traditional grid, and transmits not only current but also the data of advanced monitoring applications. It highly integrates flows of power, information, and business and improves the efficiency of power supply. Smart grid relies on some advanced technologies, such as data analysis, sensing, and measurement, to realize its efficient function with security and reliability. A variety of monitoring devices and measuring equipment are deployed in the smart grid system. In the earlier stage, it applies cloud computing for data processing and storage to guarantee efficiency. A related illustration can refer to [24]. In response to the high requirement of real time and meeting the challenges in communication and storage, researchers have introduced edge computing into the smart grid. Concretely, analyze and process the data collected by smart meters and other monitoring equipment on the edge or power devices terminal. There have already existed such cases in application. For instance, Tencent Cloud and Pengmai Energy Technology took edge computing into account and released the overall architecture of energy IoT solution in 2018 [25]. In the released Pengmai smart grid solution, the edge server acts as the core component. It connects with numerous monitoring devices and measuring equipment deployed in the smart grid, collects power information and analyzes them in real time.
2) *Smart Home:* Except for the smart grid, the smart home, which aims to improve the living environment of residents and remotely or automatically control different smart home appliances through computer and communication technologies, is also a hot application under the development of IoT. In the smart home scene, there are security monitoring devices, such as smart webcam that can identify hazards. Undoubtedly, smart appliances are indispensable in the smart home. They can implement some automatic functions for hosts' convenience. Moreover, smart energy and lighting are in great demand, such as smart doors and windows. One of the most important thing to realize smart home is sensing and speech recognition, which produce the amount of sensitive data locally. To better analyze and decide on these data in real time as well as preserving the privacy, edge node plays an essential role. In some proposed smart home edge computing architecture [26], there have introduced edge analysis engines like local speech recognition. Such engines, which are used to temporarily store sensitive data and further analyze them, are deployed on the edge and close to data resource.
3) *Smart Transportation:* The smart transportation can help solve the issues of urban residents' travel path. It integrates several technologies like information and communication technology, and applies them to the transportation, the vehicle manufacturing, and service control, realizing the improvement on the traffic environment and efficiency. Information collection, information analysis, and information release are three significant components of the smart transportation. For instance, if a vehicle accident happens somewhere, nearby monitors can collect such information, analyze causes of such accident, and release the accident information in the system to inform other vehicles and users. However, numerous vehicles and monitoring equipment are included in the system. Since the bandwidth is limited and the data resource is far from the data center, some urgent information may not be released in real time, resulting in serious consequence. To address such problem, researchers have tried to apply edge computing and realize cloud-edge collaboration. The edge nodes are deployed close to roadside infrastructure and vehicles, such as edge servers and edge sensors. In this way, the related information can be sent to the edge nodes close to the data source for analysis and processing in some emergency cases.

B. Summary of Security Requirements

No matter the smart grid, the smart home, or the smart transportation, the complexity of their own structure and the diversity of their participants will lead to many security threats. Edge computing also risks various security issues. For a clear display of the security problems existing in both edge computing and the described three smart applications, we briefly summarize and list them in Table III. There is no denying that the participation of edge computing will make them

TABLE III
BRIEF SUMMARY OF SECURITY WEAKNESSES EXISTING IN EDGE COMPUTING AND THOSE SMART APPLICATIONS

Applications	Security weaknesses
Edge computing	1)Malicious edge nodes masquerade as legitimate nodes to obtain user data. 2)The widely distributed edge nodes are the main targets of attackers and there is potential risk in data security stored in these edge nodes. 3)Easy to suffer from DDoS attack and Advanced Persistent Threat (APT) attack. 4)Attackers invade the edge data center and gain system control rights.
Smart grid	1)Smart meters can be unreliable. 2)Vulnerable to DDoS attacks, leading the attacked smart grid equipment to be not available. 3)False data injection (FDI) attack. 4)The potential leakage of meter data.
Smart home	1)Interfering with system information, such as generating false temperature information and sending it to the cloud. 2)Various network attacks, such as DoS attack and wormhole attack. 3)Unauthorized system access leads to privacy disclosure. 4)Home devices may be infected by third-party malware.
Smart transportation	1)Attackers eavesdrop on the message transmitted between entities in the system, resulting in information leakage of users or vehicles. 2)Blocking or tampering with the alarm information sent in the system, resulting in traffic accidents. 3)Controlling traffic signal and affecting normal traffic. 4)Attacking the roadside infrastructure and affecting the normal operation of the system.

become more complex, and the characteristics of edge computing also add new security threats to these smart applications. For instance, various edge nodes are distributed in the system, such as edge server and edge controller, so they are easier to become the target of attackers. Concretely, the attacker can disguise malicious edge nodes as legitimate edge nodes and then induce users to access them by giving some benefits. In this case, some important information of user may be leaked to the attacker, such as the account and password of some software used by users. Furthermore, as *Edge Computing Security White Paper* released [27], there exist 12 security challenges in edge computing, mainly reflecting in four aspects, i.e., edge network, edge dada, edge application, and edge infrastructure. In terms of attacks, they may occur in edge access, edge server, and edge management. For edge access, there exist insecure communication protocols and malicious edge nodes. For edge server, it occurs problems, such as Distributed Denial of Service (DDoS), insecure systems and components, and lack of data privacy preserving. For edge management, it exhibits challenges like malicious administrators that are difficult to supervise. Thus, if edge computing is applied in the smart application, it is inevitable to face these security problems.

Currently, most Internet scenes are open to people, including users and attackers. To guarantee the normal and secure function of the Internet system, identity authentication is the first defense line and the most significant basis. Identity authentication technology can confirm the validity of communication participants, preventing the attacker from impersonating as the legitimate users to spoof the server and consuming the computing, storage, and network sources of the server. Similarly, this technology prevents the attacker from impersonating as the legitimate servers to obtain the privacy information of users. In the edge computing environment, multiple trust domains coexist, and multiple user entities in the smart grid, the smart home, and the smart transportation participate in communication and interaction. Therefore, realizing the authentication of the application system is very necessary.

Additionally, any system will produce various data and the data plays an important part in these systems. The data is usually generated from the user terminal and there exists user's sensitive privacy in these data. Moreover, the data produced in the systems are encouraged to be shared and aggregated for better function of the systems, but the security needs to be guaranteed in these data operations. Thus, data security is another essential basis to guarantee the normal and even better functions of these systems. That is, apart from identity authentication, data security protection is also a top priority.

Similar to the smart grid, the smart home, and smart transportation, after edge computing is applied to them, although there involve threats of both edge computing and smart applications, the identity authentication of entities and data security are common issues. Besides, there exists a relationship between identity authentication and data security. By authentication, the user's legality is verified and then he/she can be authorized to access certain data. Moreover, in some proposed authentication schemes, after authentication, legal users can further negotiate a session key that can be utilized to protect the data transmitted between the entities, realizing data protection to a certain extent.

Different scenarios possess different architecture characteristics and the authentication objects are also not the same. Accordingly, the requirements of authentication and data security protection are naturally different. Consequently, there is no such common identity authentication scheme and data security protection mechanism for these smart application scenarios. We present the differences between them and summarize their respective security requirements on authentication and data preserving as follows.

1) First, according to the different security requirements and device characteristics of smart applications in these edge computing-based systems, it is necessary to design different authentication schemes, thus realizing the confidentiality of the communication process. Generally, the authentication in the smart grid occurs at the smart meter and service provider and requires properties of anonymity, unlinkability, and lightweight. While in the smart home, apart from the smart meter, there are other home devices that need to authenticate with users or home gateway. The authentication also requires relatively lightweight. In the smart transportation, we prefer to discuss authentication in the Internet of Vehicles (IoV), i.e., vehicle to vehicle and vehicle to roadside infrastructure. The authentication in such scene may

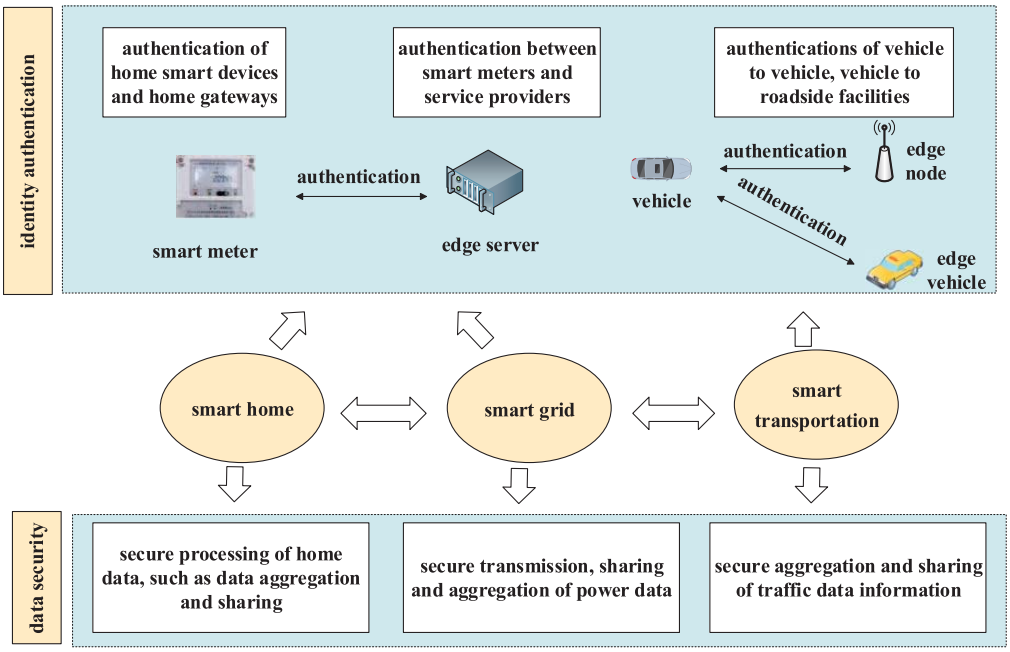


Fig. 2. Security protection framework of these smart applications in edge computing.

involve cross-domain authentication and need to realize real-time requirement.

2) Generally, data security protection includes confidentiality, integrity, availability, and so on. The data produced by different system varies in contents and usage. In the smart grid, the data is related with power and its consumption, and data interaction occurs between smart meters and substations or substations and data center. While in the smart home, the data consists of information of user and home equipment. If the owned information of the smart home devices is tampered, they will make incorrect decisions, further resulting in serious consequence. In the smart transportation system, the data involves information of traffic and road. Perfect data analysis and decision will contribute to the improvement of the traffic. To facilitate data analysis, the data usually needs to be aggregated and shared. In such process, the security requirements differ in smart applications for their different contents and usage. This article mainly discusses secure data sharing, aggregation, transmission, and storage.

Based on the above mentioned, we propose a security protection framework, shown in Fig. 2. As the framework displays, for instance, in the smart home, we will discuss the authentication between smart devices and home gateways and analyze the privacy processing and secure storage of home data. After applying edge computing in the smart grid and smart home, edge server participates in communication and authentication between it and the smart devices like smart meter should be taken into consideration. As for edge computing-based smart transportation, besides the authentications of vehicle to vehicle and vehicle to roadside facilities, considerations for the authentications of vehicle to edge node and vehicle to edge vehicle are necessary.

IV. Smart Grid

The scenario of the smart grid in the edge computing environment is presented in Fig. 3 [5], [24], [28]. After applying edge computing to the smart grid, part of the data can be directly processed on the edge nodes, and the smart meter and control center can communicate through the edge cloud. However, the structure and communication environment of the smart grid are complex and vulnerable to various network attacks, such as Denial-of-Service (DoS) attacks and eavesdropping attacks. In addition, a variety of smart devices participate in the system and the system targets a wide range of users. Meanwhile, users interact with the smart grid system frequently, which causes attackers to obtain the information transmitted through the public smart grid network, thus leading to the leakage of user's privacy.

A. Identity Authentication

To check the validity of entities in the smart grid, especially realizing the authentication between the smart meter and service provider, there have proposed many related schemes. Moreover, these schemes are developing and improving by adopting different cryptography methods, such as elliptic curve and hash functions. In this section, to show the recent research in this field, we overview some works, including some corresponding improvements.

During the authentication, the anonymity of smart meters can protect its privacy to a certain extent. To realize this feature, many related protocols have been presented [29]–[39]. Specifically, by adopting identity-based signature and encryption, Tsai and Lo [29] proposed a key distribution scheme with anonymity in the smart grid environment, where the smart meter could use a private key to access the service

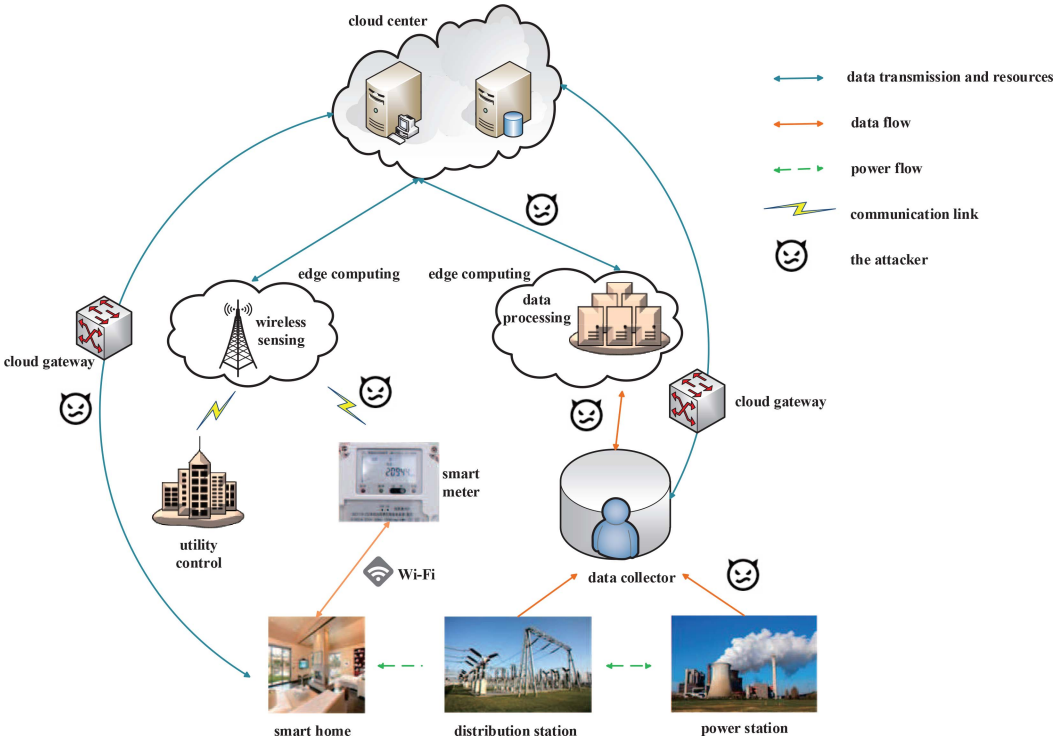


Fig. 3. Scene of the smart grid in the edge computing environment.

provider anonymously without the participation of third parties in the authentication. Additionally, only a small amount of calculation operation is needed at the smart meter. However, Odelu *et al.* [30] found that the scheme in [29] suffered from server impersonation attacks and failed to provide secure mutual authentication. Besides, when the ephemeral secret was inadvertently disclosed, Tsai *et al.*'s scheme could not guarantee the session key security and user certificate privacy. Consequently, Odelu *et al.* put forward an improvement and enhanced the security. However, both the protocols designed by Tsai *et al.* and Odelu *et al.* need high computation and communication costs, which cannot meet the resource constraints of smart meters. In 2018, Mahmood *et al.* [31] and Abbasinezhad-Mood and Nikooghadam [32] designed authentication protocols for smart grid based on bilinear pairing operation and elliptic curve cryptosystem, respectively, meeting the anonymity of smart meters. However, compared with Abbasinezhad-Mood *et al.*'s scheme, Mahmood *et al.*'s scheme costs more calculation and does not realize key escrow. Moreover, Chen *et al.* [33] pointed out that Mahmood *et al.*'s scheme failed to provide perfect forward security, suffered from impersonation attack and potentially vulnerable to ephemeral key compromise attack.

For the complexity and time delay sensitivity of the smart grid, Mahmood *et al.* [34] proposed a lightweight authentication scheme using the elliptic curve. After the effective session key is shared between the communication participants, the identity authentication is completed. However, Abbasinezhad-Mood *et al.*'s protocol [35] observed that their scheme still exhibited some drawbacks, such as the inability to provide forward security and resistance to ephemeral key disclosure attacks in the Canetti–Krawczyk (CK) threat model. Based on these analyses, Abbasinezhad-Mood and Nikooghadam [35] mended the drawbacks. In 2019, based on TinySet, Afianti *et al.* [36] designed a multiuser authentication scheme to improve efficiency and resist DoS attacks. Their scheme used RC5 encryption, partial recovery principle, and elliptic curve digital signature, which greatly increased the complexity of attack. Additionally, TinySet is regularized to simplify the administrator's task to setup initialization parameters. For the computing limitation of the smart measuring device, Abbasinezhad-Mood *et al.* [37] specifically designed a security protocol, which not only overcame the weakness of power service providers participating in the key protocol but also greatly reduced the communication cost. To overcome the weaknesses existing in the IEC 62351 standard, Moghadam *et al.* [38] used private key and hash function and proposed a secure protocol. By pointing out the failure of previous anonymous authentication schemes in identifying malicious users, Kong *et al.* [39] designed a group blind signature scheme, realizing conditional anonymity.

No matter what the application scenario, key agreement protocols to realize identity authentication usually use some common cryptography methods, such as elliptic curve, bilinear pairing, public-key encryption and symmetric encryption, etc. Thus, here we only take smart grid as an example to compare the involved protocols on the security and computation cost to present the advantages and disadvantages of these key agreement schemes. The compared literature involve [29]–[35], [37], [38], shown in Table IV. In the table, S_1–S_7 means user anonymity, perfect forward security, mutual authentication, anti-impersonation attack, anti-replay

TABLE IV
COMPARISON ON THE SECURITY AND COMPUTATION COST OF RELATED SCHEMES

Schemes	Year	S_1	S_2	S_3	S_4	S_5	S_6	S_7	Computation cost
[29]	2015	√	√	√	×	×	×	×	$7T_m + 2T_b + 2T_e + 10T_h$
[30]	2017	√	√	√	√	√	√	√	$5T_m + 2T_b + 2T_e + 12T_h$
[31]	2018	√	×	×	×	√	√	×	$4T_m + 3T_b + 2T_e + 7T_h$
[32]	2018	√	√	√	√	√	√	√	$8T_m + 10T_h$
[33]	2020	√	√	√	√	√	√	√	$8T_m + 2T_b + +4T_e + 14T_h$
[34]	2018	×	×	√	√	√	√	×	$10T_m + 8T_h$
[35]	2018	×	√	√	√	√	×	√	$8T_m + 8T_h$
[37]	2019	×	√	√	√	√	√	√	$4T_m + 2T_s + 12T_h$
[38]	2020	×	√	√	√	√	√	√	$4T_s + 17T_h$

attack, resistance to man-in-the-middle attack, and session key security. Additionally, the symbols T_m, T_b, T_e, T_h, and T_s denote time for performing scalar multiplication, bilinear pairing, modular exponentiation, hash function, and symmetric encryption in order. As the table shows, the key agreement schemes for the smart grid are improving. Besides, security and performance are relative, that is, high security requires a certain performance as a cost. The issue on how to balance the security and performance is a challenge.

B. Data Security

There are entities, such as substations, smart appliances, and control centers in the smart grid. Smart meter is used to help exchange information between the smart appliances and substations and transmit customer's requirements to the substation. Then, the substation forwards these requests to the corresponding control center, which further responds to incoming requests. Thus, there must exist data interaction among the above-mentioned entities. They are confidential information and need security protecting. According to the summarized security requirements, from the perspective of secure sharing, transmission, and aggregation of the power data, this subsection reviews some works and analyzes them.

Under the era of the IoT, smart meters in the smart grid will generate massive data. Users, however, are generally unwilling to share the data that they own because the privacy of their data cannot be guaranteed to be not leaked. To balance the personal privacy and the beneficial use of data in the smart grid, Yassine *et al.* [40] proposed a mechanism that could determine the value of privacy risk. Once a user decided to share data with a third-party service provider, this mechanism will function to determine the benefits of users. Moreover, Yassine *et al.*'s scheme used a negotiation mechanism based on game theory to study the fairness among entities involving a third party, consumers, and data aggregators, where the entities in the game aimed to maximize their own utility. Concretely, the consumers wanted to get the maximum return for allowance to access their data, the data aggregators wished to get more money from the third party by providing the consumers with less rewards, and the third party wanted to spend less money for the data. For the sake of encouraging users to share data, based on blockchain and differential privacy technology, Samuel *et al.* [41] proposed a mechanism of access control to fairly compensate users' contribution in sharing data. Meanwhile, in [41], PageRank mechanism was adopted to propose an authoritative proof consensus protocol, which aimed to get the credit score, so as to solve the existing computing problem of Ethereum blockchain.

Smart grid, the next power grid generation, can effectively monitor, control, and predict the production and consumption of the energy, but the transmission of power data fails to keep confidential. Besides, the fine-grained measurement data may leak the privacy of users. Therefore, Li *et al.* [42] designed a power data transmission protection scheme based on quantum cryptography combining with the one-time key mechanism. Additionally, they used quantum to generate random numbers, which fixed the weaknesses of the traditional generator, and put forward a key distribution scheme. For another thing, the research on secure data aggregation has been developing and improving [43]–[49], including various public-key-based data aggregation protocols, but the public-key technology is not recommended in this scenario due to the high costs of maintaining public-key infrastructure (PKI). Thus, by adopting the identity-based encryption and signature, Wang [43] proposed a protocol of data aggregation, which was suitable for the application in the smart grid. It can avoid fine-grained analysis as well as unauthorized reading, and resist unexpected faults and malicious tampering of message.

In 2018, Gope and Sikdar [44] put forward an effective data aggregation scheme, which avoided high computation cost and overcame the weakness of fixed price for the whole day (or even the whole month). Their scheme used symmetric key encryption primitives for privacy-aware and secure billing system, and promoted the generation of power and the requirement balance in the smart grid, relatively decreasing the computation cost and the time for data aggregation. Thus, it was suitable for smart grid devices with constrained resource. Liu *et al.* [45] proposed a practical scheme with privacy preserving used for data aggregation. In the scheme, a virtual aggregation region consisting of users with a certain degree of trust is constructed to hide single user's data, where the aggregation results have little impact on the data practicability of large-scale applications. Liu *et al.* [45] depended little on the third party, promoted the performance, and improved the practicability. In 2020, Gope and Sikdar [47] proposed a privacy-friendly scheme of data aggregation to prevent fine-grained data from being collected by smart meters and massive measurement results from being used to reconstruct the behavior of consumers. Aiming at the data integrity attacks for smart grid, Mohammadpourfard *et al.* [49] recommended to find the critical line outage contingencies.

TABLE V
KEY WORDS, ANALYSIS, AND THE APPLYING OF EDGE COMPUTING IN THE SMART GRID

References	Year	Key words	Applying edge computing	Technique used	Security analysis	Performance
Tsai et al.[29]	2015	identity-based encryption, identity-based signature, key distribution, privacy, smart grid.	No	bilinear pairing, hash function.	vulnerable to impers-onation attack, replay attack and man-in-the -middle attack.	high computation cost, low communication cost.
Odelu et al.[30]	2017	cloud computing, SK -security, credentials privacy, mutual authen -tication, user untrace -ability, AVISPA, NS2 simulation.	No	bilinear pairing, elliptic curve, signcryption, biometrics and fuzzy extractor.	realize user creden -tials' privacy and user untraceability.	high computation and communication cost.
Mahmood et al. [31]	2018	smart grid, authent -ication, anonymity, smart meter, edge computing, ProVerif.	Yes	bilinear pairing, hash function.	vulnerable to imper -sonation attack and ephemeral secrets leakage attack.	high computation cost, low communication cost.
Abbasinezhad-Mood et al.[37]	2019	anonymity, authenticat -ion, isolated smart meter, key establishm -ent, smart grid security.	No	elliptic curve, hash function.	realize anonymity and authentication without electricity service provider.	low computation and communication cost.
Kong et al. [39]	2020	smart grid, traceability, anonymous authenticat -ion, data integrity veri -fication, Industry 4.0/5.0 for security.	No	RSA algorithm, group blind signature, schnorr identification protocol.	realize anonymity, authenticatability and unforgeability.	low computation cost and efficiency.
Wang [43]	2017	data aggregation protocol, smart grid, identity-based, Edison platform.	No	bilinear pairing, identity-based encryption signature.	secure against some typical attacks, such as collector attack.	high computation cost.
Gope et al.[44]	2018	privacy, data aggregation, smart grids.	No	hash function, symmetric encryption.	realize security like forward secrecy and the confidentiality of usage data.	efficiency, low computation and communication cost.
Song et al.[46]	2019	data aggregation, data privacy, dynamic mem -bership, smart grid, virtual aggregation area.	No	bilinear map, ID-based signature.	realize security and privacy, especially secure against FDI attack.	high computation cost, low communication cost.
Mohammadp -ourfard et al. [49]	2020	smart grid, data integr -ity attacks, line outage, machine learning.	No	principal component analysis, two-sample kolmogorov-smirnov test, k-nearest neighbor.	withstand data integ -rity attacks like FDI attack under concept drift.	medium efficiency.

C. Applicability in Edge Computing Environment

For the sake of clearly presenting the consideration of edge computing in the smart grid, we summarize some literature mentioned above in Table V. Obviously, the table shows that a few schemes take edge computing into account when discussing the security in the smart grid. Among them, only [31] applies edge computing. However, [31] only introduces edge computing as a background, but it does not reflect in the authentication scheme. Edge nodes exhibits the characteristics of distributed deployment. Such deployment brings more threats to the secure communication of the smart grid, such as the DDoS attack, so the requirement of resistance to such attack should be taken into consideration when designing authentication protocols. Moreover, in the edge computing environment, massive smart devices are connected; thus, the efficiency of authentication is another challenge that cannot be ignored. These authentication protocols should realize lightweight and improve the performance. In addition, if the edge node is malicious or forcibly manipulated by the attacker, the data information it stores will also be disclosed. As far as the data sharing and aggregation are concerned, to ensure the data security or even the data privacy, the future researches should not only learn from the existing technologies, such as attribute encryption and homomorphic encryption but also shorten the time delay, being able to correctly and timely handle the data transmission among the smart grid devices, edge computing nodes, and the cloud centers.

V. SMART HOME

In the smart home system, the data collected by the sensor is transmitted to the decision-making unit, which calculates the appropriate control signals to achieve the predetermined goal [50]. The research works of deploying cloud computing, fog computing, and edge computing to the smart home have been put forward successively [51]–[54]. The scenario of the smart home in the edge computing environment is presented in Fig. 4 [55], [56]. Users can locally control kinds of smart home devices through Bluetooth, Wi-Fi, home LAN, etc. Additionally, users can also remotely operate home devices through Internet services provided by the edge computing layer. Therefore, the smart home system is also the intrusion target of hackers and other attackers. For instance, an attacker can launch a botnet attack [57] to control various smart home device, so as to achieve a large-scale DDoS attack.

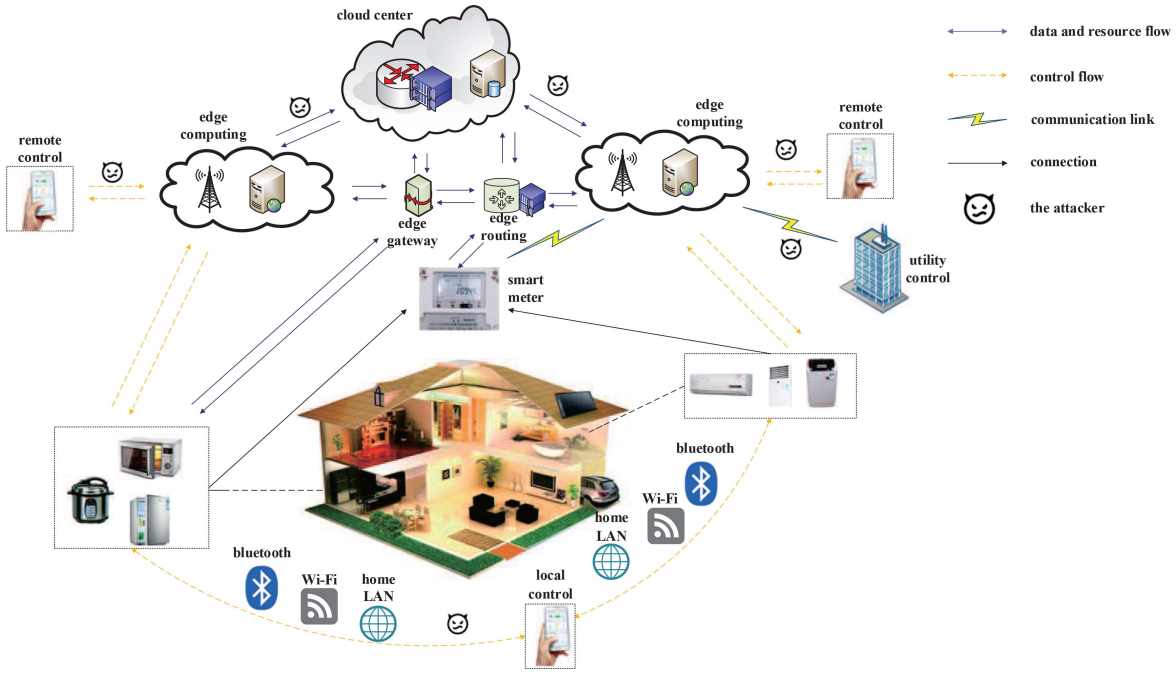


Fig. 4. Scene of the smart home in the edge computing environment.

A. Identity Authentication

As the summarized security requirements of the smart home describe, it is necessary to realize the authentication of user and smart home equipment. The entities in the smart home are able to use Bluetooth and other channels for communication, and these channels have their own unique parameters and features. The designed schemes will prefer to use physical-layer information for authentication. Such reviewing are illustrated as follows.

From the perspective of identity authentication in the smart home, there have been many related works available for reference [58]–[65]. The smart home enables individuals to control smart devices in their homes through the Internet. Internet services like IFTTT integrate different kinds of smart home devices, which allow users to customize smart home configuration through IFTTT. In view of the challenge that distributed malware based on features can harm users' IFTTT accounts, Baruah and Dhal [58] put forward a secure IFTTT-based framework for the smart home. It combined a one-time password authentication scheme using verification code. Adopting one-time password makes it resist to replay attack. Chifor *et al.* [59] presented an authorization stack that was lightweight in the cloud environment to provide digital identity for users and smart devices, where the cloud joint authentication for the smart home through the fast identity online (FIDO) authentication message was realized. In addition, they used a keep-alive online protocol for security, which was executed every time when a user requested for the authentication of FIDO. Additionally, to ensure the near real-time constraints, Chifor *et al.* implemented experiments based on the Kaa IoT cloud and further measured the delay time.

To ensure the security of home LAN, it is necessary to implement a lightweight key extraction scheme on the physical layer to establish encryption key for smart home devices. However, the rate of key generation in most advanced schemes is low. To overcome this challenge and improve the key generation rate, by using the received signal strength (RSS), Zhao *et al.* [60] presented an adaptive key establishment scheme, where the two devices in the smart home were able to quantify the RSS measurements adaptively and got the key. Furthermore, to demonstrate the practicability, they carried out experimental implementation based on the Ralink Wi-Fi card of RT2870 chipset and evaluated the randomness of the key generation through the test experiment of NIST randomness. In some cases, devices used in the smart home are made by various factories, so it is a big challenge to use the secret loaded in advance by different factories to securely establish the communication key. In this case, Zhang *et al.* [61] presented a key agreement protocol suitable for the smart home. Their scheme adopted the problem of secret mismatch existing in the schemes of secret extraction on the physical layer. That is, two smart home devices used mismatched bitstreams to generate highly correlated blocks and then used these blocks to mask the transmitted message between the devices in the smart home, so as to guarantee the secure establishment of the communication key between them. Although this key protocol can address some issues existing in some related works, it also increases some extra communication cost. Considering the group communication, Mughal *et al.* [63] presented a mobile management scheme using logical tree, which could effectively solve the problem of frequent key updates. Based on transaction history and physical context awareness, Fakroon *et al.* [65] proposed a scheme for authenticating the user remotely, which avoided the problems of clock synchronization and maintaining a verification table.

B. Data Security

Similar to the smart grid, this subsection overviews related work in terms of the security protection on data sharing, data aggregation, and data uploading. However, the designing is different from the smart grid and they are suitable for the environment of the smart home.

There is no doubt that numerous devices are connected in the smart home, thereby massive data is generated simultaneously. Data sharing can promote the optimization of the system, but the generated data usually contains the privacy of home users. Therefore, to ensure the privacy protection of these shared data, the numbers of schemes in this field have been proposed. For instance, Mollah *et al.* [66] used edge computing and presented a secure scheme of data sharing at the edge of smart devices connected to the IoT by cloud. Their scheme adopted encryption technologies like public-key encryption. Moreover, all the security executions are transferred to operate in edge servers nearby, which have greatly reduced the smart devices' burdens on processing. In 2019, Yang *et al.* [67] put forward a random access memory architecture, which realized efficiency and security, achieving preserving data privacy and saving server resource when sharing data. Their scheme combined the double chain circular information table with obfuscation operation and used the technology of proxy re-encryption to realize the secure sharing of data among multiple users.

In the process of data aggregation and upload, data security needs to be considered as well. Therefore, based on blockchain, Guan *et al.* [68] put forward an efficient scheme of data aggregation with privacy preserving. In their scheme, users were divided into different groups, where the member data was recorded by a private blockchain in the group. Moreover, they used pseudonyms to hide the real identity of users, so as to preserve users' privacy. The users were allowed to generate multiple pseudonyms, which were used to associate with their data. For issues in some existing home LAN data protection schemes, such as the absolute monitoring and modification of the data by the home gateway and the cloud's inability to check the uploaded data's integrity, Shen *et al.* [69] presented a secure data upload scheme that addressed these mentioned issues. In the scheme, they designed a tag for verifying data's integrity using a hash tree, where the tag allowed the service provider to possess the function of data integrity checking. Additionally, through the structure of hash tree, partial local computing can be offloaded to the home gateway. Considering the authentication and the secure data storage and query of the smart home system, Poh *et al.* [70] presented a scheme with privacy protection for the smart home. Their scheme provided data confidentiality and authentication of entities to prevent external person modifying and learning the communication data among devices, gateways, service providers, and users. Besides, Poh *et al.*'s scheme provided queries that preserved privacy, realizing that both gateways and service providers failed to know the specific data. Liu *et al.* [71] used the physical-layer method to design a protocol that ensured the security of data exchange.

C. Applicability in Edge Computing Environment

The smart home deploys various networking devices, controllers, and wireless sensors to every corner. The data storage and processing of the smart home gateway or cloud alone may fail to achieve better experience effect. The emergence of edge computing provides a solution to some extent. Variety of devices in the smart home need to apply different protocols for communication, such as Bluetooth, LAN, Wi-Fi, etc. Therefore, the identity authentication of the smart home in the edge computing environment should not only be designed to be lightweight enough but also be combined with the characteristics of Bluetooth, Wi-Fi and other network environments where the device is located, as well as the application characteristics of edge computing. Additionally, to preserve the security and privacy of the home data transmission, processing sensitive data within the home is expected to realize, such as using the edge home gateway to process some data. To better present those involved literature, we summarize several aforementioned literature in Table VI. However, we observe that these schemes all fail to consider edge computing in the smart home.

VI. SMART TRANSPORTATION

The scene of the smart transportation in edge computing is presented in Fig. 5 [72]–[75], where the edge nodes can be deployed to the roadside monitor, traffic lights, roadside servers, etc. Similar to other smart applications, the smart transportation system also faces various privacy disclosure and security attack issues, which can refer to Table III and [76]–[78]. For example, during the process of collecting road state information, the system may inadvertently collect the users' private information and further disclose them. Attackers can attack the sensors or monitoring cameras installed on the roadside for information collection, resulting in the destruction of the correct operation of the smart transportation system.

A. Identity Authentication

As mentioned in Section III-B, we prefer to research on the authentication of the IoV. As an important research of the smart transportation, the IoV also faces many security threats. In the IoV, vehicles possess the capability of broadcasting some special message like traffic accidents and emergencies. To achieve the communication security, vehicles need to be certified to verify the legality of them and researchers have presented lots of works in this field [79]–[86].

Specifically, based on the tamper-proof device (TPD) and roadside unit (RSU), Pournaghi *et al.* [79] proposed an authentication scheme, where the TPD of RSU was responsible to store the main system parameters and the keys. Since there exists a secure and fast communication channel between the registration center and RSU, it is much more effective to insert TPD into RSU. Moreover, their scheme needed a relatively low cost because it did not need to establish online RSU on the whole road. However, there are many vehicles in the IoV, so the efficiency of single authentication

TABLE VI
KEY WORDS, ANALYSIS, AND THE APPLYING OF EDGE COMPUTING IN THE SMART HOME

References	Year	Key words	Applying edge computing	Technique used	Security analysis	Performance
Chiforet et al.[58]	2018	identity, smart home, security, embedded, cloud computing, Internet of Things.	No	federated authorization mechanism, ciphertext policy attribute based encryption (CP-ABE), FIDO model.	provide user anony -mity.	the additional intro -duced delay only has a little influence.
Zhao et al.[60]	2019	self-adaptive, quanti -zation, key generation, smart home devices.	No	RSS measurements.	the security of the secret key relies on the distance between the attacker and two devices.	bit mismatch rate increases when α increses. The incre -ased RSS measure -ments results in sli -ghtly secret bit rate.
Zhang et al. [61]	2019	key agreement, secu -rity, secret mismatch problem, smart homes.	No	the secret mismatch problem.	withstand the passive attacks.	high communication cost.
Lu et al.[62]	2019	key agreement, secu -rity, secret mismatch problem, smart homes.	No	symmetric encryption and decryption, hash function.	withstand common attacks and realize properties like unlink -ability.	slightly higher computation cost.
Fakroon et al. [65]	2020	smart home, Internet of Things, user authen -tication, AVISPA.	No	message authentica -tion code of keyed -hash (HMAC), key encryption.	withstand common attacks, such as smart-phone device loss attack.	medium communica -tion cost and low computation overhead.
Guan et al.[68]	2018	privacy-preserving, data aggregation, pseudonyms, block -chain, bloom flter.	No	virtual ring, bloom filter, RSA algorithm, zero knowledge proof, blockchain.	preserve personal data privacy and secure against pse -udonym forgery.	has lower authentica -tion time complexity and computation over -head.
Shen et al.[69]	2018	secure data uploading, smart home system, home area networks.	No	elliptic curve, hash tree structure.	secure against the common attacks and adversarial smart dev -ices and home gate -way.	low computation over -head.
Poh et al.[70]	2019	smart home privacy, encrypted query, searchable encryption.	No	symmetric encryption, pseudorandom function.	realize data privacy and privacy-preserving query.	has lower computation overhead.
Liu et al.[71]	2020	smart home, group data exchange, nested lattice code, physical layer secu -rity.	No	nested lattice code.	withstand attacks like external eavesdropping attack.	has lower time slots overhead.

is not very high. Meanwhile, it is necessary to ensure the anonymity of the vehicle, so as to prevent the vehicle from being tracked by the attacker and preserve the privacy of the owner. In 2018, for some problems existing in the related works, such as the high cost of initial authentication may lead to serious DoS attacks, Liu *et al.* [80] put forward a cooperative authentication scheme applied in VANET. Their scheme designs a computing problem using the real-time information like the expected receiver and location, so as to reduce DoS attacks against anonymous authentication. Additionally, the trust cluster was constructed by adopting the trust relationships among vehicles and the connected component theory that effectively helped construct the trust cluster. After establishing the trust clusters among the legal vehicles, they can conduct authentications through the trust cluster to improve the efficiency.

Furthermore, vehicles in the IoV come from different domains and the mobility of vehicles is high. Therefore, in addition to the authentication of vehicles in the single domain, cross-domain authentication of vehicles is also needed consideration. In 2019, Li *et al.* [81] presented a cross-domain authentication scheme using blockchain. Their scheme authenticated servers and users anonymously, solving a single point of failure problems and realizing privacy preserving. Through the mutual authentication and distributed agreement mechanism, Li *et al.*'s scheme exhibits high fault tolerance and can well handle the attacked servers. To overcome the weaknesses of the low performance and the strong hypothesis of ideal TPD, Zhong *et al.* [83] proposed a completely converged privacy-preserving authentication scheme in vehicle *ad hoc* network. They used the aggregation signature without certificate, realizing the secure communication of vehicle to infrastructure and greatly saving the resources of computing and bandwidth. Furthermore, they adopted pseudonyms, conditionally achieving privacy protection, and when necessary, the tracking agencies were able to identify the vehicle's real identity. Since the length is constant in the aggregation signature, the overhead of storage and communication are reduced. Based on bilinear pairing and one-way hash operation, Ali and Li [84] presented an efficient signature scheme called ID-CPPA, which was used for the communication between vehicles and infrastructure and was allowed to

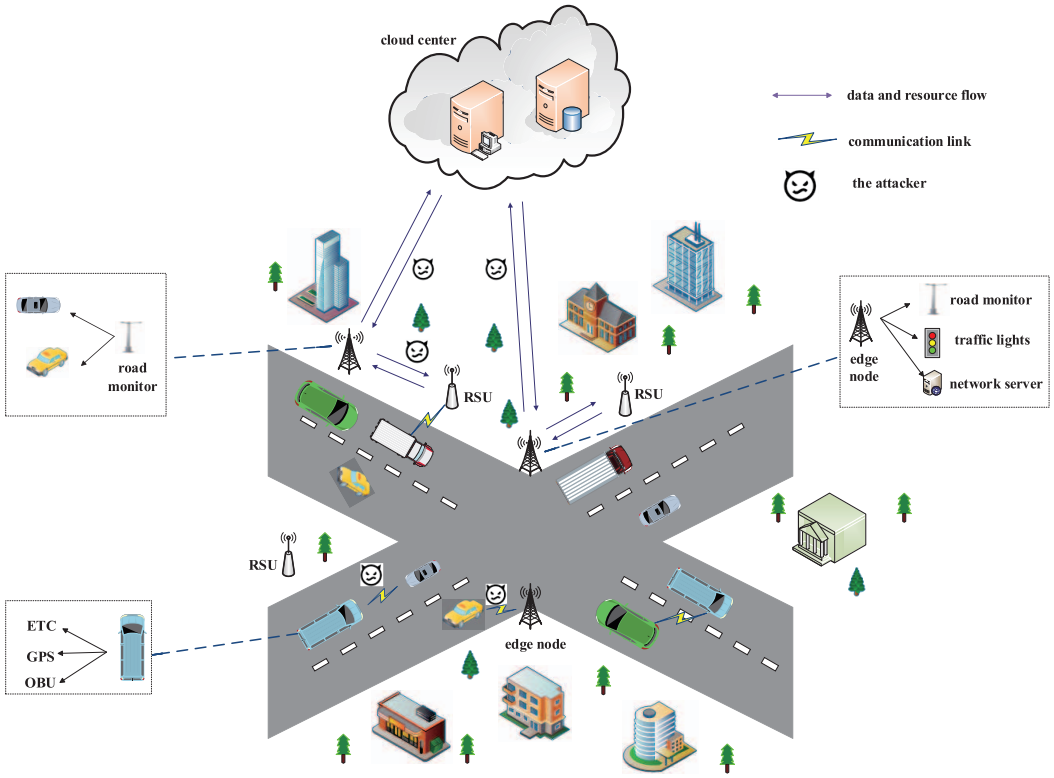


Fig. 5. Scene of the smart transportation in the edge computing environment.

authenticate massive traffic-related messages. Facing the application of cloud-assisted autonomous vehicles, Jiang *et al.* [86] presented a three-factor authentication scheme, involving smart card, biometrics and password. Their scheme provides privacy preserving, especially user's biometric privacy preserving.

B. Data Security

Various privacy data will be generated in the smart transportation system, such as the location data produced by vehicle users, road information data collected by surveillance cameras, etc. To enjoy better service, some personal data is encouraged to share in the system. For better deciding on the data, sometimes they need aggregating. All these data operation should be secure and even privacy preserving. To realize the above mentioned, researchers have presented plenty of schemes and some of them [87]–[93] are illustrated as follows.

Zhang and Chen [87] proposed a new scheme to ensure the privacy protection of real-time location data. In this scheme, a vehicle can dynamically generate virtual location according to the surroundings and provide misleading information of driving route, so as to achieve the privacy preserving. Also, based on the alliance chain, Zhang *et al.* [88] put forward a secure system of data storage and data sharing. The technology of digital signature adopted in [88] follows the elliptic curve's feature of bilinear pairing, which guarantees the reliability and integrity of data transmission. Besides, the adopted blockchain provides a decentralized database that is reliable and secure. In addition, the smart contracts are utilized to be the constraint triggering conditions of the preselected nodes when they transmit and store data, and allocate rewards to the vehicles participating in data sharing. Based on blockchain, Fan *et al.* [90] presented a scheme of data sharing that realized one to many, where the blockchain was responsible for recording the access policy to achieve the cloud nonrepudiation and user self-certification.

The rapid advancement in the IoT technology contributes to massive smart devices with specific perception ability accessing to the network and getting data. To guarantee the security and privacy of data aggregation, Li *et al.* [91] put forward a scheme of data aggregation for IoT applications assisted by mobile-edge computing in 2018. In their scheme, Boneh–Goh–Nissim cryptosystem is adopted to ensure user privacy. Through edge computing, the public cloud center can use the sensing function of the IoT terminal equipment (TE) to obtain specific parameters and the data collected by TE is summarized by the edge server. In 2019, based on fog computing, Guan *et al.* [92] designed a device-oriented scheme with privacy protection, which provided security for the data aggregation application. It supported multiauthority management of local smart devices and fog nodes. Moreover, Guan *et al.* used pseudonym and the corresponding pseudonym certificate to ensure the validity and anonymity for the devices and deployed the local certification authority to transfer the management of pseudonyms to the professional edge fog network, so as to offer real-time services for the registration and corresponding update of devices. Besides, they used Paillier algorithm to ensure the data confidentiality in the process of data aggregation. Based on the feature of message recovery signature (MRS), Shen *et al.* [93] proposed a secure scheme of traffic data aggregation with real-time service for vehicle cloud in

TABLE VII
KEY WORDS, ANALYSIS, AND THE APPLYING OF EDGE COMPUTING IN THE SMART TRANSPORTATION

References	Year	Key words	Applying edge computing	Technique used	Security analysis	Performance
Pournaghi et al. [79]	2018	VANETs, authentication, conditional privacy pres -erving, security, formal proof, ProVerif analysis.	No	elliptic curve, bilinear pairing.	meet the security pro -perties like condition -al privacy and revoca -bility.	high computation overhead.
Liu et al. [80]	2018	denial of service, pseudo -nymous authentication, VANET, puzzles, 5G, co-authentication.	No	hash puzzle, trust clusters.	realize the enhancement on the capacity of resis -tance to DoS attack.	effective and effi -cient.
Tangade et al. [82]	2018	security, public key infra -structure, identity-based cryptography, hybrid cry -ptography, VANETs.	No	asymmetric ID-based cryptography, symmetric HMAC.	realize security and privacy-preserving.	relatively efficient and has further im -provement.
Zhong et al. [83]	2019	certificateless aggregate signature, privacy preser -ving, full aggregation, VANET.	No	elliptic curve, bilinear maps.	meet the common security requirement.	medium comput -ation overhead.
Ali et al. [84]	2020	vehicle, public key infra -structure, identity-based signature, privacy, trace -ability, random oracle model.	No	elliptic curve, bilinear maps, hash function.	resist various attacks and collision.	relatively low compu -tation overhead and relatively high comm -unication overhead.
Zhang et al. [88]	2019	Internet of Vehicles, secu -rity and privacy, data sha -ring, blockchain.	No	fair blind signa -ture, threshold secret sharing.	withstand rogue key attack and realize conditional privacy.	the performance is influenced by the v -ehicles' number.
Fan et al. [90]	2020	vehicular social networks, blockchain, CP-ABE, pol -icy hiding, data revocation.	No	CP-ABE, linear secret sharing access structure, bilinear maps, blockchain, prac -tical byzantine fault tolerance.	resist cloud sever pro -vider attack and coll -usion.	relatively efficient.
Li et al. [91]	2018	cloud computing, mobile edge computing, Internet of Things, data aggregati -on, privacy.	Yes	Boneh-Goh-Nissim cryptosystem, bilin -ear maps.	realize integrity, priv -acy preserving and source authentication.	relatively high com -munication cost and relatively low comm -unication overhead.
Shen et al. [93]	2019	vehicular cloud, VANETs, traffic data aggregation, m -essage recovery signature, batch verification.	No	bilinear pairing, message recovery signature.	realize confidentiality and privacy protection.	relatively high communication cost.

vehicle *ad hoc* network. The scheme first verified the validity of the signature of vehicles and then extracted the original data of traffic from it. Because of the advantages of MRS, Shen *et al.*'s scheme owns the common data security attributes, such as the confidentiality, privacy protection, and anti-replay attacks.

C. Applicability in Edge Computing Environment

The smart transportation system consists of vehicles, various roadside infrastructure, monitoring cameras, etc. There exist interactions between not only vehicles and the roadside infrastructure but also the edge node and the roadside infrastructure, as well as the cloud and the edge nodes; thus, different authentication protocols need to be designed to adapt to the corresponding communication entities. In addition, vehicles and edge nodes are dynamic, and the mobility of vehicles is high and fast. Therefore, in the designed authentication protocols, the edge server or cloud should be able to cope with the dynamic changes, ensure high efficiency, and do not increase complex computing operations. To show the consideration on edge computing of the literature discussed above, we summarize some of them in Table VII. From the table, we observe that the existing authentication protocols and data protection schemes in the IoV still lacks of consideration on edge computing scenario. For authentication, the scheme in [94], which realizes anonymous authentication for mobile-edge computing, may be a good reference. Additionally, because of the participation of the edge sensors, the format of the generated data may be different. While realizing security and privacy protection, how to well integrate these multisource heterogeneous data should be paid more attention, and the corresponding processing strategy with privacy preserving should be chosen according to the data characteristics, so that they can be better used in the analysis.

VII. EXTENSION

Most of the aforementioned authentication schemes are high-layer protocols based on cryptography without using the inherent properties of the wireless channel. They may resist various attacks, but they commonly cost high computation or communication overhead. In recent years, PHY-layer authentication based on physical-layer channel features

is a hot authentication technology. It enhances the security of high-layer with the help of transmission features of the channel, such as spatiotemporal uniqueness. Due to its advantages of low computation and communication cost, low delay and power consumption, and unnecessary distribution of secret keys, PHY-layer authentication is promising to serve as a complementary solution for the conventional high-layer authentication.

There is no doubt that PHY-layer authentication can be applied in these smart applications, as described in the smart home scenario, such as [60] and [61]. Moreover, in the smart city scenario, by using tag embedding and verification, Zhang *et al.* [95] presented a PHY-layer authentication framework that was lightweight. PHY-layer authentication is also a useful aid in edge computing. For instance, Liao *et al.* [96] used PHY-layer authentication to enhance the security of mobile-edge computing. In their designed method, multiple legal edge nodes can be distinguished from attackers and malicious nodes. Recently, Liao *et al.* [97], Zhang *et al.* [98], and Zhang *et al.* [99] have also investigated on PHY-layer authentication. For edge computing-based smart application scenarios, PHY-layer authentication may also be a good boost in identity authentication and there has presented such work. For instance, to overcome rogue edge attacks in mobile-edge computing-based VANETs, an important part of smart transportation scenario, Lu *et al.* [100] proposed a PHY authentication scheme by exploiting mobile device's serving edge and the related channel information. Unfortunately, PHY-layer authentication may be not suitable for the mobile communication system with fast mobility, and to achieve higher efficiency, it needs to be combined with cryptography. In a word, applying PHY-layer authentication in edge computing-based smart application scenarios will be an interesting research direction in the future.

VIII. Conclusion

The trend of the large-scale deployment of edge computing is inevitable, especially in IoT-based smart applications. From the viewpoint of cybersecurity, this article especially investigates on the issues of authentication and data security existing in edge computing-based smart applications. To provide a comprehensive understanding, we briefly describe some definitions of edge computing in current works and compare it with cloud computing. From the comparison, it can be seen that edge computing does have its obvious advantages, such as fast response. Moreover, we introduce three typical applications that apply edge computing and analyze some security weaknesses existing in these smart applications as well as edge computing. We observe that their common challenge is to ensure the identity legality of system entity, which is also the most basic problem to be solved in ensuring system security. Besides, data protection is indispensable because it is an important component of these smart applications. Thus, based on authentication and data security, we summarize some related works of these smart applications and briefly illustrate the adaptability after edge computing is introduced to them. Moreover, we give the future research direction for the security in the edge computing environment.

Future Work

Based on the aforementioned summaries and discussions, we look forward to future researches in this field as follows.

1) When designing the protocol for realizing the identity authentication in the edge computing-based smart grid system, we should not only consider the anonymity of smart devices but also consider the ability to resist DDoS attacks under edge computing. When designing the data security protection scheme, we should not only learn from the existing data security technology of the smart grid but also reduce the time delay and ensure the data availability.
2) After edge computing is deployed in the smart home, based on the existing authentication technology, we need to combine with the network environment of the home equipments and the application characteristics of edge computing and design the lightweight authentication protocols with high security. For the data security and privacy preserving, the existing task offloading technologies need to be improved, enabling them to offload part or all of the sensitive data in the smart home to the edge for execution.
3) After the combination of smart transportation and edge computing, it is necessary to design the corresponding security protocols with low cost and high efficiency under the condition of knowing the characteristics of mutual authentication entities, as well as considering the dynamic and mobility. Moreover, in the environment of edge computing, according to the multisource heterogeneity of the data generated by the smart transportation system, it is necessary to design secure aggregation and sharing schemes with privacy preserving.
4) The smart grid and the smart home, the smart grid and the smart transportation are also closely related. For example, the smart grid can provide power for the smart home, and electric vehicles in the smart transportation can help the smart grid in case of power shortage when they are idle. Therefore, how to design appropriate security protection technologies while ensuring mutual promotion among them is another possible future research direction.

References

[1] "The 44th China statistical report on Internet development," in *Office of the Central Leading Group for Cyberspace Affairs*, China Internet Netw. Inf. Center, Beijing, China, 2019.
[2] W. Shi and S. Dustdar, "The promise of edge computing," *Computer*, vol. 49, no. 5, pp. 78–81, May 2016.
[3] M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, Jan. 2017.
[4] (2018). *Gartner Inc.* [Online]. Available: https://www.gartner.com/technology/home.jsp
[5] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019.

[6] R. Trimananda, A. Younis, B. Wang, B. Xu, B. Demsky, and G. Xu, "Vigilia: Securing smart home edge computing," in *Proc. IEEE/ACM Symp. Edge Comput. (SEC)*, Seattle, WA, USA, 2018, pp. 74–89.

[7] Q. Li, P. Chen, and R. Wang, "Edge computing for intelligent transportation system: A review," in *Cyberspace Data and Intelligence, and Cyber-Living, Syndrome, and Health*. Singapore: Springer, 2019, pp. 130–137.

[8] S. Tan, D. De, W. Z. Song, J. Yang, and S. K. Das, "Survey of security advances in smart grid: A data driven approach," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 397–422, 1st Quart., 2017.

[9] D. Liu, Z. Yan, W. Ding, and M. Atiquzzaman, "A survey on secure data analytics in edge computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4946–4967, Jun. 2019.

[10] M. Caprolu, R. Di Pietro, F. Lombardi, and S. Raponi, "Edge computing perspectives: Architectures, technologies, and open security issues," in *Proc. IEEE Int. Conf. Edge Comput. (EDGE)*, Milan, Italy, 2019, pp. 116–123.

[11] L. U. Khan, I. Yaqoob, N. H. Tran, S. Kazmi, T. N. Dang, and C. S. Hong, "Edge computing enabled smart cities: A comprehensive survey," *IEEE Internet Things J.*, early access, Apr. 10, 2020, doi: 10.1109/JIOT.2020.2987070.

[12] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18209–18237, 2018.

[13] 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.

[14] X. Wang, Y. Han, V. C. Leung, D. Niyato, X. Yan, and X. Chen, "Convergence of edge computing and deep learning: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 869–904, 2nd Quart., 2020, doi: 10.1109/COMST.2020.2970550.

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

[16] M. K. Kuyucu, Ş. Bahtiyar, and G. İnce, "Security and privacy in the smart home: A survey of issues and mitigation strategies," in *Proc. IEEE 4th Int. Conf. Comput. Sci. Eng. (UBMK)*, Samsun, Turkey, 2019, pp. 113–118.

[17] R. D. T. Caropreso, R. A. Fernandes, D. P. Osorio, and I. N. Silva, "An open-source framework for smart meters: Data communication and security traffic analysis," *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1638–1647, Feb. 2019.

[18] A. Ghosal and M. Conti, "Key management systems for smart grid advanced metering infrastructure: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2831–2848, 3rd Quart., 2019.

[19] 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.

[20] (2018). *Edge Computing Consortium*. [Online]. Available: http://www.ecconsortium.org/Lists/show/id/334.html

[21] S. Raponi, M. Caprolu, and R. Di Pietro, "Intrusion detection at the network edge: Solutions, limitations, and future directions," in *Proc. Int. Conf. Edge Comput.*, 2019, pp. 59–75.

[22] T. M. Mengistu, A. Albuali, A. Alahmadi, and D. Che, "Volunteer cloud as an edge computing enabler," in *Proc. Int. Conf. Edge Comput.*, 2019, pp. 76–84.

[23] T. Suganuma, T. Oide, S. Kitagami, K. Sugawara, and N. Shiratori, "Multiagent-based flexible edge computing architecture for IoT," *IEEE Netw.*, vol. 32, no. 1, pp. 16–23, Jan./Feb. 2018.

[24] Z. Guan, J. Li, L. Wu, Y. Zhang, J. Wu, and X. Du, "Achieving efficient and secure data acquisition for cloud-supported Internet of Things in smart grid," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1934–1944, Dec. 2017.

[25] (2018). *Cloud Tencent and Energy IoT Pengmai*. [Online]. Available: https://cloud.tencent.com/solution/energy_iot

[26] N. Gupta, K. Anantharaj, and K. Subramani, "Containerized architecture for edge computing in smart home: A consistent architecture for model deployment," in *Proc. IEEE Int. Conf. Comput. Commun. Informat. (ICCCI)*, Coimbatore, India, 2020, pp. 1–8.

[27] (2019). *Edge Computing Consortium*. [Online]. Available: http://www.ecconsortium.org/Lists/show/id/374.html

[28] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. Rodrigues, "Fog computing for smart grid systems in the 5G environment: Challenges and solutions," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 47–53, Jun. 2019.

[29] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, Mar. 2016.

[30] V. Odelu, A. K. Das, S. Kumari, X. Huang, and M. Wazid, "Provably secure authenticated key agreement scheme for distributed mobile cloud computing services," *Future Gener. Comput. Syst.*, vol. 68, pp. 74–88, Mar. 2017.

[31] K. Mahmood *et al.*, "Pairing based anonymous and secure key agreement protocol for smart grid edge computing infrastructure," *Future Gener. Comput. Syst.*, vol. 88, pp. 491–500, Nov. 2018.

[32] D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ECC-based self-certified key distribution scheme for the smart grid," *IEEE Trans. Ind. Electron.*, vol. 65, no. 10, pp. 7996–8004, Oct. 2018.

[33] T. Chen, Q. Cheng, and X. Li, "An anonymous key agreement protocol with robust authentication for smart grid infrastructure," *Sci. China Inf. Sci.*, early access. [Online]. Available: http://engine.scichina.com/doi/10.1007/s11432-019-2736-5

[34] 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 Gener. Comput. Syst.*, vol. 81, pp. 557–565, Apr. 2018.

[35] D. Abbasinezhad-Mood and M. Nikooghadam, "Design and hardware implementation of a security-enhanced elliptic curve cryptography based lightweight authentication scheme for smart grid communications," *Future Gener. Comput. Syst.*, vol. 84, pp. 47–57, Jul. 2018.

[36] F. Afianti, T. Suryani, and I. Wirawan, "Lightweight and DoS resistant multiuser authentication in wireless sensor networks for smart grid environments," *IEEE Access*, vol. 7, pp. 67107–67122, 2019.

[37] D. Abbasinezhad-Mood, A. Ostad-Sharif, and M. Nikooghadam, "Novel anonymous key establishment protocol for isolated smart meters," *IEEE Trans. Ind. Electron.*, vol. 67, no. 4, pp. 2844–2851, Apr. 2020.

[38] M. F. Moghadam, M. Nikooghadam, A. H. Mohajerzadeh, and B. Movali, "A lightweight key management protocol for secure communication in smart grids," *Elect. Power Syst. Res.*, vol. 178, Jan. 2020, Art. no. 106024.

[39] W. Kong, J. Shen, P. Vijayakumar, Y. Cho, and V. Chang, "A practical group blind signature scheme for privacy protection in smart grid," *J. Parallel Distrib. Comput.*, vol. 136, pp. 29–39, Feb. 2020.

[40] A. Yassine, A. A. N. Shirehjini, and S. Shirmohammadi, "Smart meters big data: Game theoretic model for fair data sharing in deregulated smart grids," *IEEE Access*, vol. 3, pp. 2743–2754, 2015.

[41] O. Samuel, N. Javaid, M. Awais, Z. Ahmed, M. Imran, and M. Guizani, "A blockchain model for fair data sharing in deregulated smart grids," in *Proc. IEEE Global Commun. Conf. (GLOBCOM)*, Waikoloa, HI, USA, 2019, pp. 1–7.

[42] Y. Li, P. Zhang, and R. Huang, "Lightweight quantum encryption for secure transmission of power data in smart grid," *IEEE Access*, vol. 7, pp. 36285–36293, 2019.

[43] Z. Wang, "An identity-based data aggregation protocol for the smart grid," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2428–2435, Oct. 2017.

[44] P. Gope and B. Sikdar, "An efficient data aggregation scheme for privacy-friendly dynamic pricing-based billing and demand-response management in smart grids," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 3126–3135, Aug. 2018.

[45] Y. Liu, W. Guo, C. I. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3PDA) scheme for smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1767–1774, Mar. 2019.

[46] J. Song, Y. Liu, J. Shao, and C. Tang, "A dynamic membership data aggregation (DMDA) protocol for smart grid," *IEEE Syst. J.*, vol. 14, no. 1, pp. 900–908, Mar. 2020, doi: 10.1109/JSYST.2019.2912415.

[47] P. Gope and B. Sikdar, "An efficient privacy-friendly hop-by-hop data aggregation scheme for smart grids," *IEEE Syst. J.*, vol. 14, no. 1, pp. 343–352, Mar. 2020, doi: 10.1109/JSYST.2019.2899986.

[48] H. Shen, Y. Liu, Z. Xia, and M. Zhang, "An efficient aggregation scheme resisting on malicious data mining attacks for smart grid," *Inf. Sci.*, vol. 526, pp. 289–300, Jul. 2020, doi: 10.1016/j.ins.2020.03.107.

[49] M. Mohammadpourfard, Y. Weng, M. Pechenizkiy, M. Tajdinian, and B. Mohammadi-Ivatloo, "Ensuring cybersecurity of smart grid against data integrity attacks under concept drift," *Int. J. Elect. Power Energy Syst.*, vol. 119, Jul. 2020, Art. no. 105947.

[50] S. Feng, P. Setoodeh, and S. Haykin, "Smart home: Cognitive interactive people-centric Internet of Things," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 34–39, Feb. 2017.

[51] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Gener. Comput. Syst.*, vol. 78, pp. 1040–1051, Jan. 2018.

[52] A. Yassine, S. Singh, M. S. Hossain, and G. Muhammad, "IoT big data analytics for smart homes with fog and cloud computing," *Future Gener. Comput. Syst.*, vol. 91, pp. 563–573, Feb. 2019.

[53] C. S. M. Babou, D. Fall, S. Kashihara, I. Niang, and Y. Kadobayashi, "Home edge computing (HEC): Design of a new edge computing technology for achieving ultra-low latency," in *Proc. Int. Conf. Edge Comput.*, 2018, pp. 3–17.

[54] J. M. Batalla and F. Gonciarz, "Deployment of smart home management system at the edge: Mechanisms and protocols," *Neural Comput. Appl.*, vol. 31, no. 5, pp. 1301–1315, 2019.

[55] K. Xu, Y. Wan, and G. Xue, "Powering smart homes with information-centric networking," *IEEE Commun. Mag.*, vol. 57, no. 6, pp. 40–46, Jun. 2019.

[56] L. Zhu, M. Li, Z. Zhang, X. Du, and M. Guizani, "Big data mining of users' energy consumption patterns in the wireless smart grid," *IEEE Wireless Commun.*, vol. 25, no. 1, pp. 84–89, Feb. 2018.

[57] Y. Meidan *et al.*, "N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders," *IEEE Pervasive Comput.*, vol. 17, no. 3, pp. 12–22, Jul./Sep. 2018.

[58] B. Baruah and S. Dhal, "A two-factor authentication scheme against FDM attack in IFTTT based smart home system," *Comput. Security*, vol. 77, pp. 21–35, Aug. 2018.

[59] B. C. Chifor, I. Bica, V. V. Patriciu, and F. Pop, "A security authorization scheme for smart home Internet of Things devices," *Future Gener. Comput. Syst.*, vol. 86, pp. 740–749, Sep. 2018.

[60] H. Zhao, Y. Zhang, X. Huang, and Y. Xiang, "An adaptive secret key establishment scheme in smart home environments," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Shanghai, China, 2019, pp. 1–6.

[61] Y. Zhang, H. Zhao, Y. Xiang, X. Huang, and X. Chen, "A key agreement scheme for smart homes using the secret mismatch problem," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10251–10260, Dec. 2019.

[62] Y. Lu, G. Xu, L. Li, and Y. Yang, "Robust privacy-preserving mutual authenticated key agreement scheme in roaming service for global mobility networks," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1454–1465, Jun. 2019.

[63] M. A. Mughal, P. Shi, A. Ullah, K. Mahmood, M. Abid, and X. Luo, "Logical tree based secure rekeying management for smart devices groups in IoT enabled WSN," *IEEE Access*, vol. 7, pp. 76699–76711, 2019.

[64] Q. Jiang, Z. Chen, J. Ma, X. Ma, J. Shen, and D. Wu, "Optimized fuzzy commitment based key agreement protocol for wireless body area network," *IEEE Trans. Emerg. Topics Comput.*, early access, Oct. 23, 2019, doi: 10.1109/TETC.2019.2949137.

[65] M. Fakroon, M. Alshahrani, F. Gebali, and I. Traore, "Secure remote anonymous user authentication scheme for smart home environment," *Internet Things*, vol. 9, Mar. 2020, Art. no. 100158, doi: 10.1016/j.iot.2020.100158.

[66] M. B. Mollah, M. A. K. Azad, and A. Vasilakos, "Secure data sharing and searching at the edge of cloud-assisted Internet of Things," *IEEE Cloud Comput.*, vol. 4, no. 1, pp. 34–42, Jan./Feb. 2017.

[67] H. Yang, W. Zheng, T. Zhou, X. Jin, and A. Wang, "A privacy-protecting and resource-saving scheme for data sharing in smart home," *J. Internet Technol.*, vol. 20, no. 2, pp. 607–615, 2019.

[68] Z. Guan *et al.*, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.

[69] J. Shen, C. Wang, T. Li, X. Chen, X. Huang, and Z.-H. Zhan, "Secure data uploading scheme for a smart home system," *Inf. Sci.*, vol. 453, pp. 186–197, Jul. 2018.

[70] G. S. Poh, P. Gope, and J. Ning, "PrivHome: Privacy-preserving authenticated communication in smart home environment," *IEEE Trans. Depend. Secure Comput.*, early access, May 3, 2019, doi: 10.1109/TDSC.2019.2914911.

[71] Q. Liu, W. Zhang, S. Ding, H. Li, and Y. Wang, "Novel secure group data exchange protocol in smart home with physical layer network coding," *Sensors*, vol. 20, no. 4, p. 1138, 2020.

[72] S. Garg, A. Singh, S. Batra, N. Kumar, and L. T. Yang, "UAV-empowered edge computing environment for cyber-threat detection in smart vehicles," *IEEE Netw.*, vol. 32, no. 3, pp. 42–51, May/Jun. 2018.

[73] T. S. Darwish and K. A. Bakar, "Fog based intelligent transportation big data analytics in the Internet of Vehicles environment: Motivations, architecture, challenges, and critical issues," *IEEE Access*, vol. 6, pp. 15679–15701, 2018.

[74] H. A. Khattak, S. U. Islam, I. U. Din, and M. Guizani, "Integrating fog computing with VANETs: A consumer perspective," *IEEE Commun. Stand. Mag.*, vol. 3, no. 1, pp. 19–25, Mar. 2019.

[75] S. Garg *et al.*, "Edge computing-based security framework for big data analytics in VANETs," *IEEE Netw.*, vol. 33, no. 2, pp. 72–81, Mar./Apr. 2019.

[76] A. Mahmood, H. Zen, and S. Hilles, "Big data and privacy issues for connected vehicles in intelligent transportation systems," 2018. [Online]. Available: arXiv:1806.02944. doi: 10.1007/978-3-319-63962-8_234-1.

[77] A. Nanda, D. Puthal, J. J. Rodrigues, and S. A. Kozlov, "Internet of autonomous vehicles communications security: Overview, issues, and directions," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 60–65, Aug. 2019.

[78] D. A. Hahn, A. Munir, and V. Behzadan, "Security and privacy issues in intelligent transportation systems: Classification and challenges," *IEEE Intell. Transp. Syst. Mag.*, early access, Apr. 11, 2019, doi: 10.1109/MITS.2019.2898973.

[79] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, "NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET," *Comput. Netw.*, vol. 134, pp. 78–92, Apr. 2018.

[80] P. Liu, B. Liu, Y. Sun, B. Zhao, and I. You, "Mitigating DoS attacks against pseudonymous authentication through puzzle-based co-authentication in 5G-VANET," *IEEE Access*, vol. 6, pp. 20795–20806, 2018.

[81] C. Li, Q. Wu, H. Li, and J. Liu, "Trustroam: A novel blockchain-based cross-domain authentication scheme for Wi-Fi access," in *Proc. Int. Conf. Wireless Algorithms Syst. Appl.*, 2019, pp. 149–161.

[82] S. Tangade, S. S. Manvi, and P. Lorenz, "Decentralized and scalable privacy-preserving authentication scheme in VANETs," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8647–8655, Sep. 2018.

[83] H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving authentication scheme with full aggregation in VANET," *Inf. Sci.*, vol. 476, pp. 211–221, Fev. 2019.

[84] I. Ali and F. Li, "An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in VANETs," *Veh. Commun.*, vol. 22, Apr. 2020, Art. no. 100228.

[85] T. Chen, X. Li, and Q. Cheng, "An enhanced key exchange protocol exhibiting key compromise impersonation attacks resistance in mobile commerce environment," *Sci. China Inf. Sci.*, 2019. [Online]. Available: http://engine.scichina.com/doi/10.1007/s11432-019-2645-x

[86] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K.-K. R. Choo, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Trans. Veh. Technol.*, early access, Feb. 3, 2020, doi: 10.1109/TVT.2020.2971254.

[87] X. Zhang and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019.

[88] L. Zhang *et al.*, "Blockchain based secure data sharing system for Internet of Vehicles: A position paper," *Veh. Commun.*, vol. 16, pp. 85–93, Apr. 2019.

[89] J. Shen, T. Zhou, J. F. Lai, P. Li, and S. Moh, "Secure and efficient data sharing in dynamic vehicular networks," *IEEE Internet Things J.*, early access, Apr. 29, 2020, doi: 10.1109/JIOT.2020.2985324.

[90] K. Fan *et al.*, "A secure and verifiable data sharing scheme based on blockchain in vehicular social networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5826–5835, Jun. 2020, doi: 10.1109/TVT.2020.2968094.

[91] X. Li, S. Liu, F. Wu, S. Kumari, and J. J. Rodrigues, "Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4755–4763, Jun. 2019.

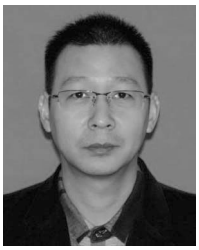
[92] Z. Guan *et al.*, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, Jan. 2019.

[93] J. Shen, D. Liu, X. Chen, J. Li, N. Kumar, and P. Vijayakumar, "Secure real-time traffic data aggregation with batch verification for vehicular cloud in VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 807–817, Jan. 2020, doi: 10.1109/TVT.2019.2946935.

[94] Y. Li, Q. Cheng, X. Liu, and X. Li, "A secure anonymous identity-based scheme in new authentication architecture for mobile edge computing," *IEEE Syst. J.*, early access, Mar. 19, 2020, doi: 10.1109/JSYST.2020.2979006.

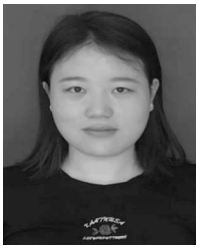
[95] P. Zhang, J. Liu, Y. Shen, H. Li, and X. Jiang, "Lightweight tag-based PHY-layer authentication for IoT devices in smart cities," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3977–3990, May 2020.

[96] R. Liao *et al.*, "Security enhancement for mobile edge computing through physical layer authentication," *IEEE Access*, vol. 7, pp. 116390–116401, 2019.
[97] R. F. Liao *et al.*, "Multiuser physical layer authentication in Internet of Things with data augmentation," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 2077–2088, Mar. 2020.
[98] N. Zhang *et al.*, "Physical layer authentication for Internet of Things via WFRFT-based Gaussian tag embedding," *IEEE Internet Things J.*, early access, Jun. 11, 2020, doi: 10.1109/JIOT.2020.3001597.
[99] P. Zhang, Y. Shen, X. Jiang, and B. Wu, "Physical layer authentication jointly utilizing channel and phase noise in MIMO systems," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2446–2458, Apr. 2020.
[100] X. Lu, L. Xiao, T. Xu, Y. Zhao, Y. Tang, and W. Zhuang, "Reinforcement learning based PHY authentication for VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 3068–3079, Mar. 2020.



Xinghua Li (Member, IEEE) received the M.E. and Ph.D. degrees in computer science from Xidian University, Xi'an, China, in 2004 and 2007, respectively.

He is currently a Professor with the School of Cyber Engineering, Xidian University. His research interests include wireless networks security, privacy protection, cloud computing, and security protocol formal methodology.



Ting Chen received the B.S. degree in Internet of Things Engineering from East China Jiaotong University, Nanchang, China, in 2018. She is currently pursuing the M.S. degree in security of cyberspace with Xidian University, Xi'an, China.

Her research interests include authentication and security protocol.

Qingfeng Cheng received the M.S. degree from the National University of Defense Technology, Changsha, China, in 2004, and the Ph.D. degree from Information Engineering University, Zhengzhou, China, in 2011.

He is currently an Associate Professor with the State Key Laboratory of Mathematical Engineering and Advanced Computing, Strategic Support Force Information Engineering University, Zhengzhou. His research interests include cryptography and information security.

Siqi Ma received the B.S. degree in computer science from Xidian University, Xi'an, China, in 2013, and the Ph.D. degree in information system from Singapore Management University, Singapore, in 2018.

She is currently a Lecturer with the School of Information Technology and Electrical Engineering, University of Queensland, Brisbane, QLD, Australia, and was a Research Fellow with Distinguished System Security Group, CSIRO, Canberra, ACT, Australia. Her research interests include IoT security, mobile security, and software security.

Jianfeng Ma (Member, IEEE) received the M.E. and Ph.D. degrees in computer software and communications engineering from Xidian University, Xi'an, China, in 1988 and 1995, respectively.

He is currently a Professor with the School of Cyber Engineering, Xidian University, China. His research interests include information and network security, coding theory, and cryptography.