A Secure Edge-Cloud Computing Framework for IoT Applications

Yao Zhao, Zhenjiang Zhang, and Jian Li(✉)

School of Electronic and Information Engineering, Beijing Jiaotong University,
Beijing 100044, China
{16271208,zhjzhang1,lijian}@bjtu.edu.cn

Abstract. With the fast development of Internet of Things, more and more applications are deployed in this "connecting everything" network. Edge computing and cloud computing are two paradigms to implement the Internet of Things. To utilize the advantages of both these two computing forms, edge-cloud computing was proposed. In this paper, we construct a secure edge-cloud computing (SECC) framework. Sensor nodes and applications can interact with the framework through unified interfaces. We implement the edge server as a collection of services, including edge device orchestration, data processing and storage, communication management, authentication and authorization, environment sensing and situation analysis. Through a daisy-chain approach, our framework can be secured for heterogeneous security needs of different parts of the system. We also demonstrate the efficacy of the SECC framework through comprehensive analysis.

Keywords: Edge computing · Internet of Things · Edge-cloud collaboration

1 Introduction

In recent years, thanks to the characteristics of low construction and maintenance costs, the Internet of Things (IoT) and wireless sensor network technologies have become more and more widely used, especially in the monitoring of special environments. They have great advantages and application potential in fire alarm, geological exploration, and safe production. However, with the development of wireless communication technology, in general large-scale wireless sensor networks or large-scale IoT, especially in application scenarios that require extensive monitoring of the environment, the number of wireless sensor nodes and edge sensing devices is rapidly increased, so is the amount of data generated. Thus the backend cloud computing platforms need to undertake a large number of computing tasks and data storage tasks [1]. If all data generated by edge sensing devices are transmitted to the cloud computing platform for processing and analysis, it will bring great challenges to satisfy the bandwidth consumption and response time requirements of the IoT applications.

Y.-B. Lin and D.-J. Deng (Eds.): SGIoT 2020, LNICST 354, pp. 70–78, 2021.
https://doi.org/10.1007/978-3-030-69514-9_7

In this situation, the cloud computing has the following disadvantages: it is difficult to shorten the system response time, to reduce the communication bandwidth and to lower the energy consumption of data centers. Therefore, edge computing, a new computing model that performs computing at the edge of the network, is introduced into the IoT technology [2]. Once the edge computing model was proposed, it has been developed rapidly and widely used in the IoT technology.

Nevertheless, edge computing technology also has certain problems. Compared with cloud computing platforms, edge computing servers usually do not have enough memory and processors to process large amounts of data, so it cannot perform complex operations such as deep learning [3]. At the same time, with the continuous development of edge computing technology, we can consider assigning different tasks to each edge computing server to improve efficiency. So the edge-cloud collaboration technology is proposed and introduced into the IoT technology [4]. In the edge-cloud collaboration model, the cloud computing platform and the edge computing platform work together to give play to their respective characteristics and provide optimized services through data analysis of the IoT.

In this paper we propose to apply edge-cloud computing in an environment dynamic perception system characterized by large-scale IoT, and build a secure edge-cloud computing (SECC) framework for edge-cloud collaboration. Our proposed framework covers all the aspects of an IoT system, including the wireless sensor nodes, the edge computing server and the cloud computing platform. In the framework we propose unified interfaces to connect wireless sensors, applications and the services provided by the framework, including edge device orchestration, data processing and storage, communication management, authentication and authorization, environment sensing and situation analysis. Through the design of the framework, we can get a trade-off between computing capability and response delay in various IoT application scenarios. We also propose a Daisy-chain approach to meet different security requirements of the system.

The rest of this paper is organized as follows: in Sect. 2 we discuss related works. In Sect. 3 the overall system architecture and details of different components of the system are elaborated. In Sect. 4 system evaluation are presented. We conclude in Sect. 5.

2 Related Works

With the introduction of the concept of the Internet of Everything (IoE), business and industrial processes that can enrich people's lives are extended to the definition of IoT [5]. IoT has become a small part of IoE, and the latter depicts a world composed of trillions of smart devices, in which all sensors are connected through a network using a specific protocol [6]. According to Cisco Systems, market of devices would touch the value of 50 billion devices by 2020 [7]. The exponential increase of access devices has put tremendous pressure on the existing IoT architecture. Cloud computing technologies have been introduced into

IoT as the canonical data processing paradigm. Since 45% of the data generated by IoT will be processed at the edge of the network [7], a new computing model that performs computing at the edge of the network is proposed [9]. With the continuous development of edge computing technology, its problems are gradually revealed: Compared with cloud computing platforms, edge computing servers usually do not have enough memory and processors to process large amounts of data. Simultaneously, the communication between edge computing server and cloud computing platform puts huge pressure on bandwidth resources.

Consequently, edge-cloud collaboration technology came into being and solve the problems mentioned above. SAT-IoT (an architectural model for a high-performance fog/edge/cloud IoT platform), which uses fog computing, edge computing, and cloud computing technology to improve the existing IoT platform and greatly improve its performance [8]. Multi-access edge computing (MEC), which can integrate telecommunications and IT services [10], and provide a cloud computing platform at the edge where radio access has been completed, involves edge-cloud collaboration technology. The collaboration between edge and cloud allows multiple access systems to have Sequence normal operation [11]. In addition, the application of deep learning in IoT edge cloud data analysis is also an application scenario of edge cloud collaboration technology [3]. For example, assigning a deep neural network (DNN) layer on an edge cloud environment can minimize the total delay of processing the DNN and solve the problem of least delay allocation (LMA). In this way, the response time of the application program can be shortened by effectively allocating deep learning tasks [12].

The rapid development of edge computing technology makes people largely ignore the security threats on the edge computing platform and the applications it supports. Distributed denial of service attacks, side channel attacks, malware injection attacks, and authentication and authorization attacks pose major challenges to edge computing security [13]. In this case, the academic community adopts a variety of methods to ensure its security. The security protection of edge computing through the perspective of classified protection of cyber security [14]. Through the popularity of containerization, many researches aim at identifying related vulnerabilities and possible security issues [15]. In this paper, we propose a secure framework that combines edge computing and cloud computing and can achieve the advantages of both the two computing paradigms.

3 Secure Edge-Cloud Computing (SECC) Framework Architecture

In this section, we will introduce the overall architecture of the proposed SECC framework and the details of all the components.

3.1 Overall Architecture

System architecture of the SECC framework is shown in Fig. 1. It is mainly composed of three components: wireless sensor nodes, edge computing server and cloud computing platform.

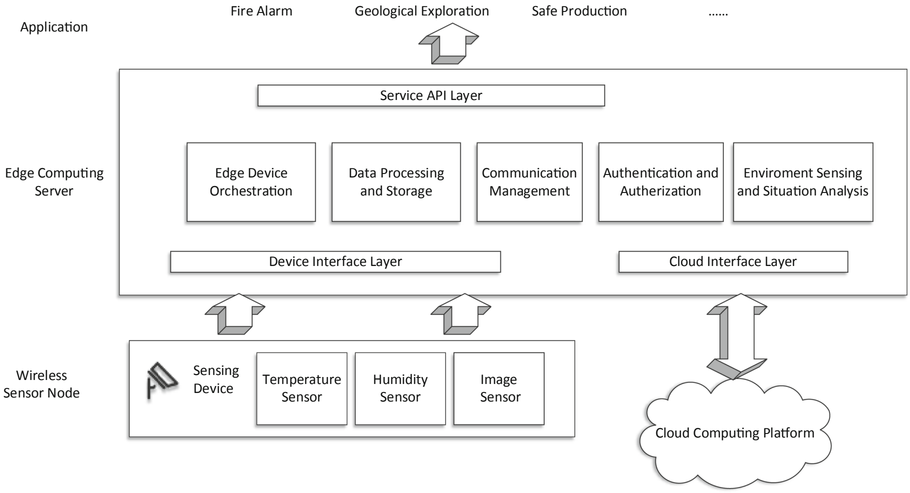

Fig. 1. System architecture of SECC framework

Sensing devices, such as temperature sensors, humidity sensors and image sensors, sense environmental changes and send these changes to the edge computing server. Then the edge computing server and the cloud computing platform collaborate and complete the tasks of the applications running on the framework. Different applications can be deployed according to application scenarios, such as fire monitoring, geological exploration, safe production, etc.

3.2 Wireless Sensor Nodes

The wireless sensor nodes are the most basic and important component of the system. As Fig. 2 shows, its role in this system is as follows: in some special environments that need to be monitored, sensing devices composed of temperature sensors, humidity sensors, and image sensors are put out randomly or according to a certain rule to form wireless sensor networks. These sensors can sense the dynamic changes of the environment in real time and collect some specific data in the environment.

As an example, in the forest monitoring system GreenOrbs deployed in Wuxi City, Jiangsu Province, wireless sensor nodes are placed on trees, including temperature sensors, humidity sensors, light intensity sensors, carbon dioxide concentration sensors, etc. These nodes can monitor and real-time detect the forest environment to prevent forest fires.

3.3 Edge Computing Server

In the SECC framework, the edge computing server belongs to the middle layer of the system. As shown in Fig. 3, the main functions of the edge computing server are as follows.

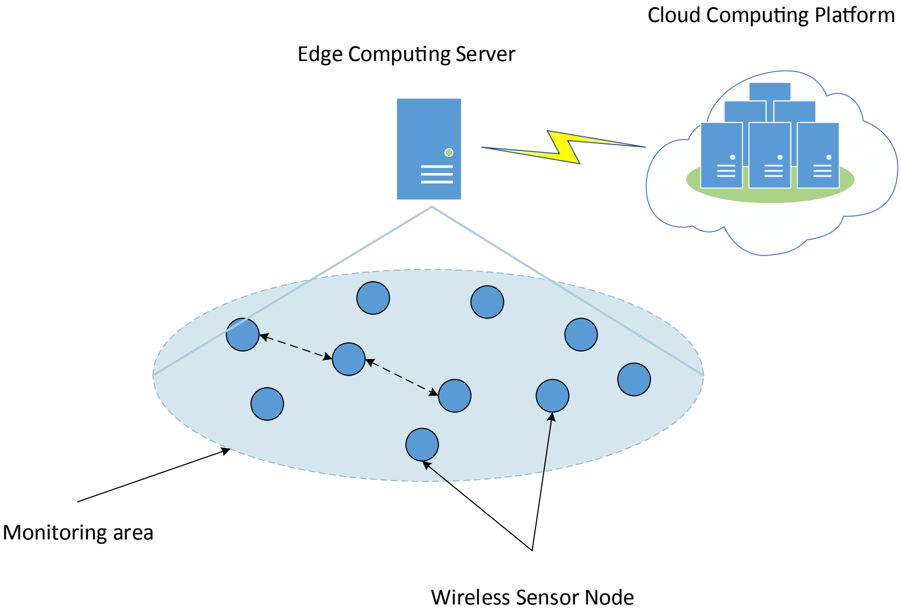

Fig. 2. Wireless sensor nodes

- In system initialization phase, various monitoring data in the environment collected by the wireless sensor nodes and corresponding initialization parameters are uploaded to the cloud computing platform through the relay of the edge computing server. The edge computing server is also in charge of the setting up of wireless sensor nodes on its behalf and on the behalf of the cloud computing platform.
- In the system operation stage, preliminary processing is performed on the various monitoring data collected in the environment to detect abnormal situations in time. Once an abnormality of a certain item or items of data is detected, the cloud computing platform will immediately receive an abnormal report from the edge computing server. At the same time, the controller at the bottom will be driven by the edge computing server to provide emergency solutions for the abnormal situation.
- The edge computing server also provide basic common services such as edge device orchestration, data storage and processing, communication management, authentication and authorization, environment sensing and situation evaluation and so on. Based on the common services, applications can be developed and deployed in a timely manner.

During system deployment, small base stations can be deployed on the side close to the wireless sensor nodes as a small edge computing server. It is also possible to use special equipment, such as drones, in areas where it is difficult to deploy

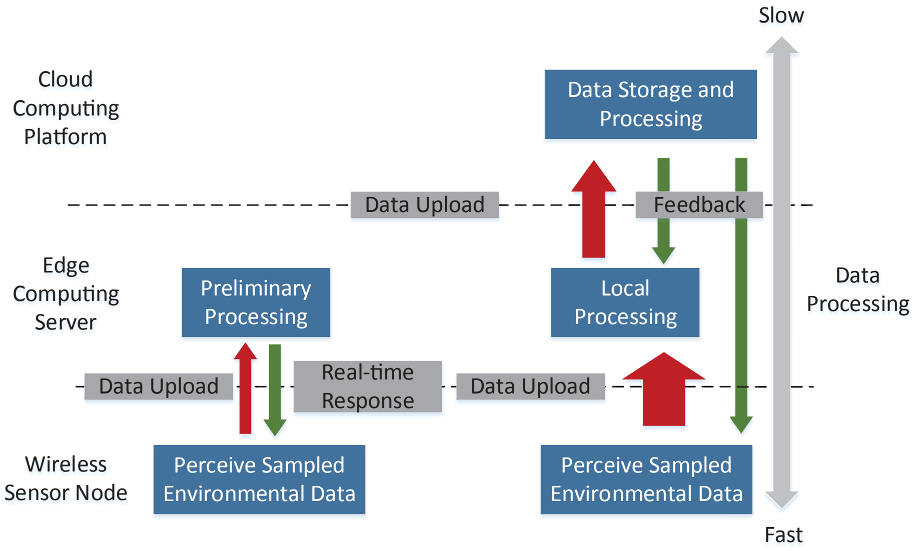

Fig. 3. The functionality of edge computing server

small base stations, as edge computing servers that can be deployed on mobile, to provide edge computing services for the system on the edge of the data.

3.4 Cloud Computing Platform

In the SECC framework, the cloud computing platform's functions are mainly as follows.

- It has the characteristics of large storage space and strong computing power. Therefore, it plays the role of remote data and control center in the system, and its role is mainly to store data and process highly complex data.
- In some application scenarios, the edge computing server and wireless sensor nodes may not be able to provide the corresponding computing power required by the system, and cannot afford the resource loss caused by complex calculations. Therefore, using cloud computing platforms for various complex tasks is also an embodiment of collaborative processing between the edge computing server and cloud computing platform.

As an example, in an IoT detection system based on edge computing that uses an autoencoder neural network to realize anomaly detection, the autoencoder has high complexity in training model parameters as an artificial neural network model for feature extraction. It is difficult for the wireless sensor nodes and edge computing server to provide corresponding computing capabilities and resource consumption caused by complex computing. Therefore, the model training process is deployed on a cloud computing platform. The generated model parameters are sent back to the edge computing server for real-time anomaly detection.

3.5 Daisy-Chain Approach to Ensure the System Security

As a complex framework consisting of wireless sensor nodes, edge computing server and cloud computing platform, the whole system has heterogeneous security needs. Sensor nodes have to ensure the authenticity of messages transmitted while the edge computing server and cloud computing platform have to authenticate legal sensor nodes to join in the network and manage the correct access rights of users and applications. Different computing capabilities and resource limitations make it difficult to adopt a single security approach in the whole system.

In the SECC framework, we propose to apply the daisy-chain approach to satisfy different security needs of the system. In the system initialization phase, the cloud computing platform will first authenticate the edge computing server and establish security parameters used in the following cryptographic operations. Then the edge computing server will in turn authenticate sensors nodes, initializing security parameters used in light-weight message authentication algorithms. Through the daisy-chain approach, each part of the system can get a corresponding security level on-demand.

4 System Evaluation

At the system architecture level, the SECC framework uses edge computing technology and edge-cloud collaboration technology to realize the development and deployment of IoT applications. Compared with the traditional IoT infrastructure, it has the following advantages.

From the Perspective of Wireless Sensor Node
In this system framework, the wireless sensor nodes communicate with the edge computing server, and at the same time, the edge computing server acts as a relay to communicate with the cloud computing platform. First, the requirements for the communication capabilities of wireless sensor nodes are greatly reduced. Second, the edge computing server's advantage in data processing capabilities on the data edge side has been more embodied.

From the Perspective of Edge Computing Server
Compared with the IoT system based on wireless sensor network technology, the edge computing server is deployed on the edge of the network. The data is close to the preprocessing unit for data analysis, protocol conversion, and data collection to ensure the low latency of the system. It generally uses dedicated GPUs, DSP chips or general-purpose CPUs, and has strong computing capabilities in data storage, network security, and data transmission. Moreover, edge computing server can be embedded with artificial intelligence technology

and machine learning to bring higher service efficiency through edge intelligence, thereby enhancing service capabilities.

The edge server stores the sensitive data collected or generated in the wireless sensor nodes in a local device, which greatly improves security and privacy. In some application scenarios, such as smart homes, smart cities, etc., wireless sensor nodes will get some private data of users for intermediate processing purpose. The data do not need to be stored on the local device, or to be uploaded to the cloud computing platform. This greatly reduces the risk of data leakage and provides strong protection for user data security and user privacy.For private data that must be transmitted to the cloud computing platform, it can adopt necessary ways such as authentication, desensitization, and encryption to ensure the security of the data without revealing privacy.

From the Perspective of Cloud Computing Platform
Compared with the sole use of edge computing technology or cloud computing technology, the edge computing server in SECC framework can perform preliminary data processing, thereby reducing the amount of computing on the cloud computing platform, reducing the amount of data uploaded in the cloud computing platform, and cooperating with the cloud computing platform to reduce the backbone link bandwidth usage.

The edge computing server adopts a layered processing mechanism and works with the cloud computing platform. In order to improve the data processing efficiency of the cloud computing platform, only some complicated tasks that do not require low latency and require centralized control are placed on the cloud computing platform. It brings higher efficiency to the services provided by the system.

5 Conclusion

In this paper we propose a secure edge-cloud computing (SECC) framework for the Internet of Things. We divide the framework into three components: wireless sensor nodes, the edge computing server and the cloud computing platform. Through the collaboration of the edge computing server and the cloud computing platform, we can achieve a trade-off between computing capability and response delay. We further implement the edge computing server as a common basic service provider, including unified interfaces to connect wireless sensors and applications to the framework, basic services such as edge device orchestration, data processing and storage, communication management, authentication and authorization, environment sensing and situation analysis. To achieve the security in the framework, we propose a daisy-chain approach to meet the heterogeneous security requirements of the system. We demonstrate the efficacy of the SECC framework through comprehensive analysis.

Acknowledgement. This work was in part supported by the National Natural Science Foundation of China under Grant 61701019.

References

1. Liu, A., Cai, R.: Architecting cloud computing applications and systems. In: 2011 Ninth Working IEEE/IFIP Conference on Software Architecture, Boulder, CO, pp. 310–311 (2011)
2. Naveen, S., Kounte, M.R.: Key technologies and challenges in IoT edge computing. In: 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, pp. 61–65 (2019)
3. Ghosh, A.M., Grolinger, K.: Deep learning: edge-cloud data analytics for IoT. In: 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, pp. 1–7 (2019)
4. Xu, J., Wang, S., Zhou, A., Yang, F.: Edgence: a blockchain-enabled edge-computing platform for intelligent IoT-based dApps. China Commun. **17**(4), 78–87 (2020)
5. Miraz, M.H., Ali, M., Excell, P.S., Picking, R.: A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). In: 2015 Internet Technologies and Applications (ITA), Wrexham, pp. 219–224 (2015)
6. Raj, A., Prakash, S.: Internet of Everything: a survey based on architecture, issues and challenges. In: 2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Gorakhpur, pp. 1–6 (2018)
7. Evans, D.: The Internet of Things: how the next evolution of the internet is changing everything. In: Cisco White Paper, pp. 3–4 (2011)
8. Lpez Pea, M.A., Muoz Fernndez, I.: SAT-IoT: an architectural model for a high-performance fog/edge/cloud IoT platform. In: 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, pp. 633–638 (2019)
9. Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L.: Edge computing: vision and challenges. IEEE Internet Things J. **3**(5), 637–646 (2016)
10. Zhao, P., Zhao, W., Bao, H., Li, B.: Security energy efficiency maximization for untrusted relay assisted NOMA-MEC network with WPT. IEEE Access **8**, 147387–147398 (2020)
11. Taleb, T., Samdanis, K., Mada, B., Flinck, H., Dutta, S., Sabella, D.: On multi-access edge computing: a survey of the emerging 5G network edge cloud architecture and orchestration. IEEE Commun. Surv. Tutor. **19**(3), 1657–1681 (2017)
12. Hu, L., Sun, G., Ren, Y.: CoEdge: exploiting the edge-cloud collaboration for faster deep learning. IEEE Access **8**, 100533–100541 (2020)
13. Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., Lv, W.: Edge computing security: state of the art and challenges. Proc. IEEE **107**(8), 1608–1631 (2019)
14. Wu, W., Zhang, Q., Wang, H.J.: Edge computing security protection from the perspective of classified protection of cybersecurity. In: 2019 6th International Conference on Information Science and Control Engineering (ICISCE), Shanghai, China, pp. 278–281 (2019)
15. Caprolu, M., Di Pietro, R., Lombardi, F., Raponi, S.: Edge computing perspectives: architectures, technologies, and open security issues. In: 2019 IEEE International Conference on Edge Computing (EDGE), Milan, Italy, pp. 116–123 (2019)