Data Security and Privacy Challenges of Computing Offloading in FINs

Fei Wang, Boyu Diao, Tao Sun, and Yongjun Xu

Abstract

Recently, a variety of novel techniques (e.g. Internet-of-Things, cloud computing, edge/fog computing, big data, intelligence accelerating chip) make a great number of different devices connected for specific purposes. Based on the significant features of techniques, networking technologies have evolved into future intelligent networks (FINs), in which intelligence has been integrated into networks to help generate and optimize policies, freeing network administrators from management and configuration burdens, and improving the efficiency of self-learning from real-time network data. In FINs, low latency is achieved at the cost of computing-complexity which is beyond the capabilities of Internet of Things devices or users' devices. In order to achieve a new generation of computing-intensive, delay-sensitive and function-intelligent services, computing-intensive intelligence tasks are expected to be offloaded to more powerful edge devices with intelligent computing capabilities. However, because the data are copied or divided before being distributed to edge devices, and that the edge devices have heterogeneous computation resources and various purposes, there exist unknown types of security and privacy threats which would possibly crash the network system, break the data privacy of network entities, damage the data property or cause unfairness in incentives adjustment. In this article, we discuss the design issues for data security and privacy in FINs. We present the unique data security and privacy design challenges presented by computing offloading and highlight the reasons why the data protection techniques in current Internet-of-Things, cloud computing, edge/fog computing cannot be directly applied in FINs.

Introduction

Recently, a variety of novel techniques (e.g. Internet-of-Things, cloud computing, edge/fog computing, big data) make a great number of different devices connected for specific purposes. Internet of Things (IoT) is developing fast as billions of location beacons, cameras, smart meters, wireless sensors, connected vehicles, Unmanned Aerial Vehicles (UAVs) and other smart devices are immersed in our daily lives. Moreover, heterogeneous computing units have been equipped in devices such as, for example, smart phones, tablets, laptops and smart wireless routers [1], which gives them intelligent computing capabilities at the edge of the network. Meanwhile, cloud computing has developed dramatically and helps to reduce IT infrastructure costs on the user side. One obvious trend is that advanced cloud service providers like Amazon Cloud and Alibaba Cloud Computing begin to provide intelligent processing service and IoT device managing and computing service. However, in many scenarios of IoT, low latency is achieved at the cost of computing complexity which is beyond the capabilities of IoT devices and is with high delay if supported by cloud [2]. To meet the user's need for fluent experience and low delay, emerging computing paradigms include mobile transparent computing, edge computing and fog computing. [3]

Based on the significant features of techniques, networking technologies have evolved into FINs, in which intelligence has been integrated into networks. We can interpret it from three aspects. First, advanced intelligent algorithms could be applied to current different network scenarios, e.g., current Internet, IoT, and Vehicular Ad-hoc Networks (VANET) to improve the service optimization or network management. Second, both edge devices and cloud are capable of intelligent computation, which can help to complete the intelligent computing tasks from the cloud. Lastly, the offloaded intelligent computing task stream among heterogeneous edge devices would create new services of which the experience is fluent, the delay is low and the function is intelligent.

To explore the potential of FINs, offloading intelligent computing tasks from end users and cloud to proper edge devices is one of the most important issues. From the view of end users, intelligent function and low latency are achieved at the cost of computing complexity which is beyond the capabilities of IoT devices. By offloading the tasks from end users to advanced edge devices which are capable of intelligent computation, the FINs are expected to provide new generation computing-intensive and delay-sensitive service. From the view of network administrators, by offloading the tasks from cloud to edge devices, the FINs would help the network administrator to perform fine-grained, delay-sensitive, and self-learning diagnosis in a distributed manner. This will free network administrators from management and configuration burdens. The scenarios are shown in Figure 1.

In FINs, the cloud and the edge devices collaborate to accomplish the computing tasks from the end users or the network administrators. To achieve efficiency of intelligent computing task

Digital Object Identifier:
10.1109/MNET.001.1900140

Fei Wang, Boyu Diao, Tao Sun, and Yonjun Xu are with Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China.
Fei Wang is the corresponding author (wangfei@ict.ac.cn).

0890-8044/20/$25.00 © 2020 IEEE

stream, the data copies and divided data blocks are stored, prepared and processed on edge devices in a local way. However, the cloud always wants to achieve content of the data acquired form end users, and the edge devices from different providers might be malicious or greedy. All these characteristics make the security and privacy problems extremely critical.

Compared with edge computing or cloud computing, the most important improvement in FINs is the integration of intelligence, which means that first the intelligent computing resources are integrated into both cloud and edge devices, and second, intelligent tasks form an efficient intelligent task stream among edge devices. Moreover, the three features of potential high mobility, decentralization and isolation, and fine-grained task allocation also make the computing offloading quite different than current edge computing. Many techniques which are able to solve the security and privacy issues in edge computing or cloud computing do not fit in the new environment [4]. In this article, from a set of applications, we will analyze the special data security and privacy challenges from the viewpoint of computing offloading in FINs. Moreover, we will highlight the reasons why the techniques in current Internet-of-Things, cloud computing and edge computing cannot be directly applied in FINs.

Features of Computing Offloading in FINs

There are four main features of computing offloading in FINs, which are summarized in Table 1.

Potential High Mobility: FINs are developing in the direction of interconnection with a growing number of IoT devices and edge devices. All the communication nodes in the network have potential relative mobility to each other. However, task offloading methods for current edge computing generally assume that each IoT device offloads tasks to one edge server on the base station. In contrast, computation tasks in FINs will result in IoT devices corresponding to multiple edge devices, such as multimedia entertainment over vehicle networks. When an IoT device is moving at a high speed, the tasks have to be switched between different base stations, which leads to a radical change in task offloading algorithms for current edge computing to FINs.

Decentralization and Isolation: As IoT devices correspond to multiple edge devices in FINs, not only the IoT devices but also edge devices involved in the computation task should be decentralized. There is a many-to-many relationship between the IoT devices and edge devices, which brings a series of new communication problems. To ensure the energy consumption and delay of IoT devices, edge devices are essential to achieve a higher bandwidth in order to satisfy real-time transferring and loading task context. At the same time, isolation technology must be used to ensure rapid migration and loading of task contexts.

Fine-grained Task Allocation: Most computing tasks of FINs are based on intelligent algorithms represented by CNNs or DNNs. Since the execution time is unacceptable for IoT devices, large-scale calculations are usually directly offloaded to the edge devices. This not only wastes communication resources, but also is not conducive to improving the throughput of service nodes. Fine-grained task scheduling based on neural network partition will be applied in a large number of FINs to achieve efficient collaboration of tasks between terminals and edge service nodes.

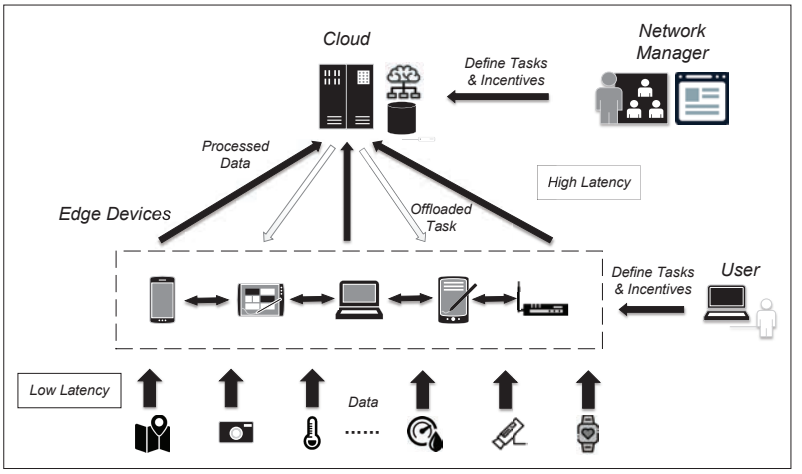

FIGURE 1. Computing offloading in FINs.

Technical Aspect	Current Edge Computing	FINs
IoT Device Mobility	Low to medium	Medium to high
Decentralization	IoT devices level	Edge server level
Task Allocation	Full task allocation	Fine-grained partial allocation
Computing Platform	ARM series/GPU	ARM/GPU/IPU/ DSP/FPGA
Local Computing Capability	300GOPS/W	Over 1TOPS/W

TABLE 1. Comparison of computing offloading between FINs and other networks.

Heterogeneous Computing Platform: The innovation of the computer architecture in the intelligent era has begun. There will be a large number of heterogeneous computing units applied to FINs, such as IPU, NPU, FPGA and other type of processors [1]. In order to make the heterogeneous computing platform transparent to the task offloading algorithms, an intermediate layer for task scheduling must be added between the hardware and software to ensure efficient coordination between heterogeneous computing units. With the application of heterogeneous computing, the computing capability of end-devices and edge servers will significantly increase in FINs.

Applications

Before digging into the challenges in security and privacy issues of computing offloading in FINs, we will give three scenarios in which computing offloading will improve the intelligent capabilities, which include UAV special express, connected smart home networks and self-driving vehicular networks.

UAV Special Express: Special express such as medical express through unmanned aerial vehicles will gradually become a reality in the era of FINs. UAVs may be equipped with high-definition cameras, GPS modules, cellular communication

Data Processing	Differences of FINs	Security and Privacy Requirements
Task Data Storage	The data is copied or divided into blocks, and stored among edge devices.	Data confidentiality
		Integrity verification
		Lightweight auditing
		Public challenge
		Dynamic support
Task Data Preparing	Keywords of data might change after copied or divided. Edge device might retrieve data from both end user, cloud and other edge devices for one task.	Fine-grained access control
		Authorization revocation
		Robust secure search ability
		Dynamics support
		Queried result refining
Task Computation	The task are usually intelligent tasks. One task might rely on early task. A group of edge devices will exchange data to accelerate the tasks.	Task integrity verification
		Denial of service resistance
		Edge device anonymity
		Conditional traceability

TABLE 2. Security and privacy requirements of computing offloading in FINs.

modules and powerful computing processors. In addition to path planning through sensors such as GPS, UAVs will also collect real-time ground information through high-definition image sensors for fine-grained path analysis, such as dropping goods in a particular window of a building. When the computing load exceeds the capability of UAVs, UAVs will offload tasks to edge devices on base stations nearby. However, an adversary might try to eavesdrop the offloaded tasks to acquire privacy information of the express or even the customers. It can also impersonate as a powerful edge device and give back the wrong results, which would crash the UAV special express facilities.

Connected Smart Home Networks: The advances in domains such as sensor networks, electronic and ambient intelligence allow to create "smart homes" and "smart cities" [5]. A smart home is an augmented environment with miniaturized processors and software agents communicating between each other [6]. In a smart home environment, multi-modal sensors are embedded in any kind of common everyday objects to make themselves effectively invisible to the residents. The sensors of a smart home can capture temperature, humidity, brightness and act automatically on several elements to satisfy a service requirement [7].

A smart home network mainly includes a smart wireless gateway and connected end devices. The end devices such as smart meters and security cameras collect large quantities of private information of the house owners who are reluctant to upload data to cloud. FINs make it possible to process those data in the smart wireless gateway equipped with powerful intelligent processors, which can act as an edge device. However, that gateway is possible to be compromised by adversaries or implanted into loopholes by manufactures, which would leak the privacy of house owners, or even more terrifying, would be used to control the house devices illegally [8].

Self-Driving Vehicular Networks: With the development of intelligent on-board computers, vehicular networks are not only transportation systems enhanced by inter-vehicle commutation technology, but also a cooperative driving system which provides passengers with an automatic driving experience. A self-driving system basically contains sensing, perception and decision-making components. A self-driving vehicle generates large quantities of data every day using advanced sensors, and needs to accomplish tasks like data processing, route perception and decision-making. Other advanced vehicles or road-side units may act as edge devices to support the work due to the limited bandwidth with cloud. Once the privacy information such as current locations, trip destination and so on is known, the adversaries may track and commit a crime such as theft and robbery [9, 10]. It is more dangerous when the impersonated edge devices forge or modify the results of offloaded tasks, which might cause accidents and threaten passengers' safety.

Data Security and Privacy in Computing Offloading of FINs

Through the aforementioned applications, we can conclude that FINs can not only improve service strategy, network management automation and real-time processing, but also provide an evolved type of network in which the cloud and the edge devices collaborate to accomplish the computing tasks from the end users or the network administrator. Due to the mismatch of different intelligent computing tasks and different intelligent computing resources on edge devices or cloud, computing offloading needs to adjust to the new environment, in which unique data security and privacy requirements arise. We will talk about these requirements from the aspects of task data storage, task data querying and task computation in computing offloading, which are summarized in Table 2.

Computing Offloading Framework and Threat Model

In this paragraph, the framework of computing offloading and corresponding threat model is given.

Figure 2 shows data flows and threat flows of computing offloading in FINs. There exist three kinds of entities: end users, the cloud and edge devices. The end users might be smart meters, smart wearable devices, wireless routers, roadside cameras, vehicular onboard units and so on. The cloud is responsible for the computing offloading control like user/edge registration, resource status gathering, computing offloading strategy making and execution. The edge devices could cache the dataset copies and divided data blocks [11] from end users, cloud or other edge devices. They will receive offloaded tasks and prepare task data as efficiently as possible through data sharing and data query. Some task data might also be the result of early tasks by other edge devices. After all the offloaded tasks are done, the cloud or some powerful edge device will integrate the results and return to end users or administrators.

Figure 3 shows the operation procedure of computing offloading processes, which consists of six steps. We need to focus on the following steps especially. In the second step, edge devic-

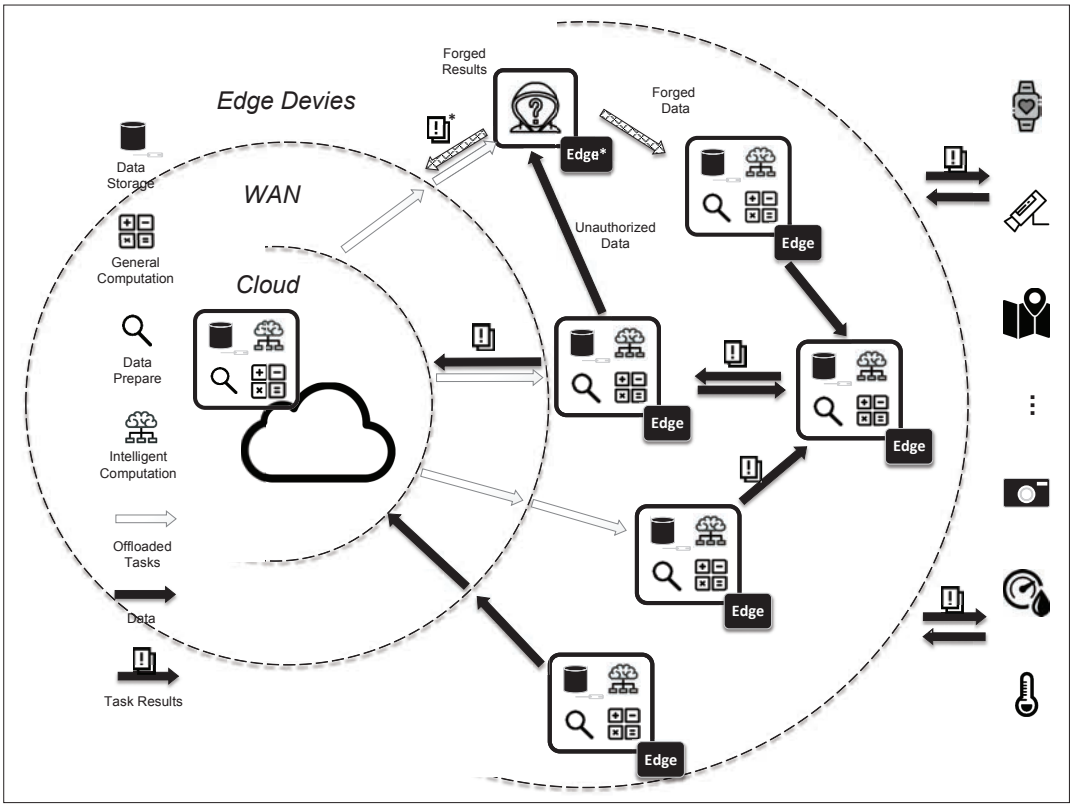

FIGURE 2. Data and threat flows in computing offloading in FINs.

es update its mobility information, data storage status, available resources and history credit. In the third step, after end users or network administrators send application requests to the network, the computing offloading controller would make task offloading and resource allocation strategies based on the data storage status and available resources. In the fifth step, each edge device tries to prepare task data based on some indexing mechanism. After it acquires data blocks from the end user via requesting, its local storage via querying, other edge devices and cloud via ad-hoc communication, it combines the data blocks and executes the computing tasks one by one. After the last step, the computing offloading controller performs incentive adjustment and updates the credit of edge devices.

The cloud is assumed semi-trusted which means the cloud would execute the relevant protocols but will try to achieve the unauthorized secret information. The edge devices are assumed malicious or greedy, which means they might launch attacks to break the FINs, pry to get unauthorized data or forge task results for more incentives than fair adjustment. There also exist adversaries who are able to control all communicating channels and have nearly unlimited computing powers. They would try to access data illegally, forge task results and impersonate as legal edge devices to acquire more privacy or credits.

Task Data Storage

Data storage is the fundamental service of cloud computing, fog/edge computing and big data. Through outsourcing the data to the remote powerful devices or cloud, the data owner can alleviate the burden of local data storage and maintenance.

When we consider the scenarios of FINs, large quantities of data are acquired from IoT devices. Cloud and edge devices are supposed to collaborate to provide the storage service due to the following reasons. First, although the bandwidth between IoT devices and edge devices or cloud is limited, the cloud still needs to acquire task data for applications like service police optimization. Second, to support offloaded task computation efficiently on edge devices in delay-sensitive applications, it is the best way that the edge devices acquire designated data from storage locally or on edge devices as near as possible. Lastly, the edge devices have the potential to provide more reliable and efficient storage service than cloud, especially in adverse weather conditions and electromagnetic interference.

However, when the data is outsourced, the adversary might try to change the data because of monetary reasons or inside attacks. The auditable secure cloud data is proposed to solve the problem in cloud computing. It cannot be adopted in for network with edge devices, because the relationship between the divided data blocks and corresponding homomorphic authenticators may disappear. To achieve the auditability in FINs, the data to be audited include the data processed in cloud and data processed by edge devices. Therefore, the follow properties are needed.

Data Confidentiality: In IoT, some key management schemes for heterogeneous networks can help guarantee data confidentiality between IoT devices [12-14]. However, the circumstances are more complex in FINs due to the fusing architecture. In order to guarantee data confidentiality,

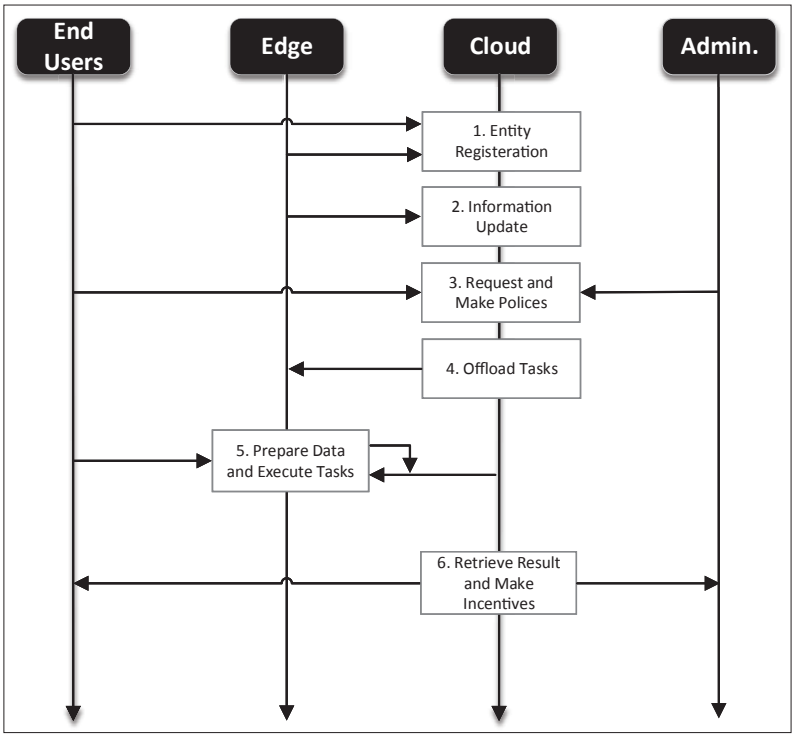

FIGURE 3. Operation procedure in computing offloading in FINs.

the key management scheme should include all of the end users, edge devices and cloud.

Integrity Verification: In FINs, the end users are bonded to the IoT devices. Hence, they should have the ability to verify the integrity of data stored in edge devices or cloud. However, if the adversary modifies or forges data in the transmission, the consensus between end users and edge devices or cloud will be broken. The integrity verification on the received data would never succeed. Hence, the verification capability should allow the edge devices and cloud to check the integrity and validity of the data mutually without knowledge about the data sources.

Lightweight Auditing: FINs are supposed to support real-time network applications and provide time-sensitive services in some applications. The training of CNNs and DNNs on cloud and the possible incremental learning computation on edge devices both meet the computation resource challenge. Compared to cloud computing, FINs request additional computation resources of the end users, the edge devices and the cloud to achieve verification capability. The cost of secure data auditing should be as lightweight as possible. Ideally, the data owner could enjoy the data storage as in cloud computing without worrying about the auditing of the data stored in FINs.

Public Challenge: The edge devices want to achieve incentives through offering their resources. They might have doubts about the fairness of incentive adjustment, which is computed based on many types of information about edge resource, offloaded task, task result completion and so on. This information might be stored in the computing offloading controller or devices for bandwidth saving purposes. To encourage more edge devices to participate, it is quite necessary for public auditing like in cloud computing, especially public verification capability of the data sent from edge devices to cloud, task offloading and resource allocation strategies and the incentive adjustment log.

Dynamic Support: In cloud computing, the data owner only needs to care about the dynamic data update inside cloud. When it comes to the scenarios of FINs, new challenges arise that first the end users will dynamically change which make the data sent to edge devices change. Second, the edge devices participating in FINs might dynamically change, which would affect the datasets for intelligence algorithms stored on them. Finally, one original dataset might have multiple copies or be divided into multiple blocks to improve efficiency. These make the synchronization of data auditing difficult. Hence, auditability design in FINs should include this crucial characteristic into consideration.

Task Data Preparing

After the data is stored in FINs, the end users, edge devices and the cloud would try to prepare different data for computing offloading. Compared with cloud computing or Internet of Things, the situations in FINs are different. As for edge devices, they require the task data from other edge devices or cloud. As for cloud, in order to train intelligent models for network management and configuration burdens, they require the task data from distributed edge devices or sometimes indirectly from end users. The preparing processes include data sharing and data query. The former enables the end users to store the data in FINs and share the data with legitimate edge devices authorized by the network, while the latter enables the edge devices or cloud to retrieve a designated part of the data.

Data should be encrypted to resist malicious edge devices, offline device thieves or insider attacks. Attribute-Based Encryption (ABE) is proposed to realize access control of the shared data, which allows the end users make access policies and encrypt the data correspondingly before outsourcing the data to FINs. Only edge devices whose attributes satisfy the access policies are able to retrieve the plaintext. Searchable encryption is proposed to solve the data query problem, which would make the search on the encrypted data without leaking privacy keywords possible. However, due to the complex data distribution, data division of computing offloading, and dependent task computation in FINs, the powerful primitives cannot be applied in FINs directly.

Fine-Grained Access Control: Fine-grained access control of task data is required. However, it is very hard than that in cloud computing. On one hand the access control mechanism in FINs is supposed to guarantee that access policy still works after the encrypted data is copied or divided; on the other, it is best that the expression of the access policy could comply with the task offloading and resource allocation strategies. Only such a mechanism can guarantee that the proper data is shared to satisfy edge devices.

Authorization Revocation: The end users and cloud should have the ability to revoke the access rights. The first reason is that in the application like UAV cooperative operation, participating edge devices may change dramatical-

ly and leaving one should not access the data anymore. The second reason is that once the malicious edge devices which perform an inside attack or misbehave to cheat for incentives are conditionally traced, which will be talked about later, also should be excluded from the FINs immediately.

Robust Secure Search Ability: The edge devices and the cloud have different data search requirements. There are two secure search ability properties which are confidentiality of task data and confidentiality of the underlying keywords in an offloaded task. The secure search ability could be achieved by Symmetric Searchable Encryption (SSE) or Public Key Encryption with Keyword Search (PEKS). Because the data related to offloaded tasks are stored both in the cloud and the edge devices, the secure search is challenging. First, the end users cannot insert keywords into the cipher text efficiently for later secure search. Second, the cloud can hardly decide which keyword to insert after the data is copied or divided. Third, severe security risks will happen when several edge devices conspire to launch a specific search request from the edge devices and acquire an encrypted underlying keyword. The possible solution is to let the edge controller define a dictionary for the whole FIN and let edge devices use an encrypted fuzzy keyword set instead.

Dynamics Support: As mentioned above, the changeable end users, participating edge devices and data copying or division might change the data. Moreover, due to that one offloaded task might depend on the results of another offloaded task, the edge devices can also hardly decide which keyword to insert into or supplement after the data changes in early offloaded tasks. Therefore, secure search ability should also adjust to this crucial characteristic of the dynamics of FINs.

Queried Result Refining: It is possible that after the end users, the edge devices or the cloud perform the search query, large quantities of search results would return from multiple other edge devices and the cloud. The network entity which launches the query would prefer to receive a refined result in which the redundant copies are excluded and the data records are sorted. This will not only help cloud accomplish the model training like CNNs and DNNs but also help edge devices accomplish the model training like incremental learning. This is quite challenging in FINs because the end users or the edge devices lack the knowledge of processed data output by other edge devices. The sorting rule cannot be applied to the processed data directly if no new supplemental information is inserted into it.

Task Computation

Computing offloading allows the data owner to outsource the computing tasks and corresponding data to FINs to achieve computation intensive and delay-sensitive services. It also allows the edge devices to achieve incentives from the FINs through offering capabilities like data storage, data query and data computation, especially intelligence computation powered by IPU. Moreover, it is possible to allow a group of edge devices to keep and exchanges selective data copies or data blocks to assist in acceleration of the offloaded tasks. However, new challenges arise in confidentiality or verifiability of the data and computing offloading relevant information, and also arise in resistance to denial of services.

Computing offloading allows the data owner to outsource the computing tasks and corresponding data to FINs to achieve computation intensive and delay-sensitive services. It also allows the edge devices to achieve incentives from the FINs through offering capabilities like data storage, data query and data computation, especially intelligence computation powered by IPU.

Integrity Verification: Besides integrity verification of stored data mentioned above, information about the edge resource status, offloaded tasks, task result and incentive adjustment are vulnerable to outside adversaries or inside misbehaved participants. For example, an adversary might try to change the result of one offloaded task, which will make all relevant tasks fail. Traditional techniques could not help the FINs directly obtain the confidentiality and verifiability of computing tasks, task relevant data, results of offloaded tasks and adjusted incentives. Flexible authentication protocols are needed to handle this crucial situation.

Denial of Service Resistance: Because intelligent algorithms usually cost incredible computing resources, the Denial of Service (DoS) prevention requirement is more critical in FINs. The main reason is that edge devices are also supposed to accomplish the computation of intelligent algorithms. Therefore, the adversary could select and launch specific tasks which cost large computation resources, or change the offloaded tasks before edge devices receive them, which both might dry the resources of edge devices and crash the network. To resist these types of attacks, on one hand the integrity verification of offloaded tasks is necessary; on the other hand an excitation perdition scheme which is able the detect abnormal tasks might be the solution.

Edge Device Anonymity: Generally, edge devices need to update real-time location, resource status, and task status through beacon messages to support optimization of task offloading and resource allocation strategies. However, even when identities or resource status are encrypted, the adversary is still able to track the edge device based on the common information of the encrypted messages, then perform network breaking crimes. In VANET, the privacy preserving authentication technique is used to provide message integrity protection without leaking vehicles' identity and location privacy [15]. However, there are more correlations in edge device beacon messages, therefore privacy preserving authentication should also adjust to this crucial characteristic of distributed cooperation in FINs.

Conditional Traceability: After abnormal network events happen, for example network services crash, the results of tasks are not correct, the task data is polluted, or incentive adjustment is not fair. Even if the data confidentiality, data integrity and edge device privacy are guaranteed, in order to find malicious inside attackers, get evidence of improper behavior or diagnose the flaws of network management, FINs should allow the computing offloading controller to conditionally reveal the true identities by the important messages which describe task data, computing tasks, task results and incentives.

Even if the data confidentiality, data integrity and edge device privacy are guaranteed, in order to find malicious inside attackers, get evidence of improper behavior or diagnose the flaws of network management, FINs should allow the computing offloading controller to conditionally reveal the true identities by the important messages which describe task data, computing tasks, task results and incentives.

Conclusions

In this article, we have discussed the critical challenges in the security and privacy issues of computing offloading in FINs. We analyze the features of FINs and propose the possible evolved intelligent network architecture which is based on offloading intelligent tasks to IPU-enhanced edge devices. Also, we pointed out the reasons why the current security and privacy preserving techniques cannot adjust to FINs directly. This article is intended to give vision for the new generation services of FINs and begin the development of secure computing offloading design of FINs.

Acknowledgment

This work is partially supported by NSFC No. 61902376 and NSFC No. 61602447. This work is also financially supported by the National Key Research and Development Program of China No. 2018YFC1407400.

References

[1] J. Dean, D. Patterson, and C. Young, "A New Golden Age in Computer Architecture: Empowering the Machine-Learning Revolution," *IEEE Micro*, vol. 38, no. 2, 2018, pp. 21–29.
[2] M. Shen *et al.*, "Cloud-Based Approximate Constrained Shortest Distance Queries over Encrypted Graphs with Privacy Protection," *IEEE Trans. Inf. Forensics and Security*, vol. 13, no.4, 2018, pp. 940–53.
[3] W. Shi *et al.*, "Edge Computing: State-of-the-Art and Future Directions," *J. Computer Research and Development*, vol. 56, no.1, 2019, pp. 69–89.
[4] F. Wang *et al.*, "LAMANCO: A Lightweight Anonymous Mutual Authentication Scheme for N-times Computing Offloading in IoT," *IEEE Internet of Things J.*, 2018. DOI: 10.1109/JIOT.2018.2888636.
[5] M. Shen *et al.*, "Privacy-Preserving Support Vector Machine Training over Blockchain-Based Encrypted IoT Data in Smart Cities," *IEEE Internet of Things J.*, 2019. DOI: 10.1109/JIOT.2019.2901840.
[6] Y. Xiao *et al.*, "Internet Protocol Television (IPTV): The Killer Application for the Next Generation Internet," *IEEE Commun. Mag.*, vol. 45, no. 11, 2007, pp. 126–34.
[7] X. Du *et al.*, "Security in Wireless Sensor Networks," *IEEE Wireless Commun. Mag.*, vol. 15, no. 4, 2008, pp. 60–66.
[8] L. Zhu *et al.*, "Privacy-preserving DDoS Attack Detection Using Cross-domain Traffic in Software Defined Networks," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 3, 2018, pp. 628–43.
[9] L. Zhu *et al.*, "ASAP: An Anonymous Smart-parking and Payment Scheme in Vehicular Networks," *IEEE Trans. Dependable and Secure Computing*, 2018. DOI: 10.1109/TDSC.2018.2850780.
[10] L. Zhu *et al.*, "PRIF: A Privacy-preserving Interest-based Forwarding Scheme for Social Internet of Vehicles," *IEEE Internet of Things J.*, vol. 5, no. 4, 2018, pp. 2457–66.
[11] D. Zhang *et al.*, "A Real-Time and Non-Cooperative Task Allocation Framework for Social Sensing Applications in Edge Computing Systems," *2018 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS)*, Porto, Portugal, 2018, pp. 316–26. DOI: 10.1109/RTAS.2018.00039.
[12] X. Du *et al.*, "A Routing-Driven Elliptic Curve Cryptography based Key Management Scheme for Heterogeneous Sensor Networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, 2009, pp. 1223–29.
[13] Y. Xiao *et al.*, "A Survey of Key Management Schemes in Wireless Sensor Networks," *J. Computer Commun.*, vol. 30, no. 11–12, 2007, pp. 2314–41.
[14] X. Du *et al.*, "An Effective Key Management Scheme for Heterogeneous Sensor Networks," *Ad Hoc Networks*, vol. 5, no. 1, 2007, pp 24–34.
[15] F. Wang *et al.*, "2FLIP: A Two-Factor Lightweight Privacy-Preserving Authentication Scheme for VANET," *IEEE Trans. Vehicular Technol.*, vol. 65, no. 2, Feb. 2016, pp. 896–911. DOI: 10.1109/TVT.2015.2402166.

Biographies

Fei Wang [M'12] (wangfei@ict.ac.cn) received his Ph.D. degree in computer architecture from the University of Chinese Academy of Sciences, Beijing, China, in 2017. From 2011 to 2017, he was a research assistant with the Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China. Since 2017, he has been an assistant professor with the Institute of Computing Technology, Chinese Academy of Sciences. His research interests include security and privacy protection in Internet of Things, cyber-physical system architecture and multi-sensor data fusion.

Boyu Diao (diaoboyu2012@ict.ac.cn) received his Ph.D. degree in computer architecture from the University of Chinese Academy of Sciences, Beijing, China, in 2018. From 2012 to 2018, he was a research assistant with the Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China. Since 2018, he has been an assistant professor with the Institute of Computing Technology, Chinese Academy of Sciences. His research interests include edge computing, heterogeneous computing and multi-sensor data fusion.

Tao Sun (suntao@ict.ac.cn) is a Ph.D. student at the Chinese Academy of Sciences, Beijing, China. His research interests include trajectory data mining, edge computing and multi-sensor data fusion.

Yongjun Xu [M'06] (xyj@ict.ac.cn) received a Ph.D. degree in computer architecture from the University of Chinese Academy of Sciences, Beijing, China, in 2006. He is currently a professor at the Institute of Computing Technology, Chinese Academy of Sciences. His current research interests include cyber-physical systems an multi-sensor data fusion.