Distilling at the Edge: A Local Differential Privacy Obfuscation Framework for IoT Data Analytics

Chugui Xu, Ju Ren, Deyu Zhang, and Yaoxue Zhang

The authors propose a local differential privacy obfuscation (LDPO) framework for IoT data analytics to aggregate and distill the IoT data at the edge without disclosing users' sensitive data. They introduce the architecture and benefits of the LDPO framework, followed by some technical challenges in guaranteeing its performance. They present a preliminary implementation of the LDPO framework and validate its performance.

Abstract

Edge computing has emerged as a promising paradigm for delay-sensitive and context-aware IoT data analytics, through migrating data processing from the cloud to the edge of the network. However, traditional solutions adopting homomorphic encryption to achieve data protection and aggregation at edge servers are infeasible because of their heavy computational overhead. How to preserve data privacy while guaranteeing data utility in edge computing becomes an extremely important problem for IoT data analytics. In this article, we propose a local differential privacy obfuscation (LDPO) framework for IoT data analytics to aggregate and distill the IoT data at the edge without disclosing users' sensitive data. We first introduce the architecture and benefits of the LDPO framework, followed by some technical challenges in guaranteeing its performance. Then we present a preliminary implementation of the LDPO framework, and validate its performance in terms of privacy preservation level and data utility using real-world apps and datasets. Some future directions are finally envisioned for further research.

Introduction

The dramatic increase of wireless devices and services has fueled a data explosion in the era of the Internet of Things (IoT). According to the prediction of Cisco, nearly 850 ZB will be generated by all people, machines, and things by 2021 [1]. Moreover, as a growing number of IoT applications, such as e-healthcare systems, vehicle ad hoc networks (VANETs), and smart homes [2], are deployed for real-time data processing and context-aware missions, transmitting the huge amount of IoT data to the cloud for data processing incurs unpredictable delay and brings heavy burden to the Internet with limited capacity. Cloud computing is no longer a wise method for IoT data analytics, which also promotes the emergence and development of edge computing [3]. By leveraging the nearby devices/infrastructures and migrating data processing from the cloud to the edge of the network, edge computing has shown its great potential to support delay-sensitive and context-aware data analytics for IoT applications [4]. For example, in vehicular crowdsensing, vehicles on the road collect traffic information and report to edge servers, and a cloud server searches on the edge servers based on the crowdsensing tasks released by customers to retrieve the required data to generate crowdsensing results for the customers.

Despite the promising benefits of edge computing for IoT data analytics, data privacy is a critical issue in edge computing, which significantly impedes the development of the related applications. Since most IoT data is generated from cyber-physical systems and contains tremendous private data about human activity and physical environment (e.g., personal activities, health status, and personal data about individuals), preserving data privacy at the edge when edge servers become the center of local data storage and processing poses great challenges. Traditional solutions adopting homomorphic encryption to achieve data protection and aggregation at edge servers are infeasible because of their heavy computational overhead [5]. Therefore, how to achieve privacy preserving data aggregation at edge servers becomes appealing. Local differential privacy (LDP) [6] has been increasingly accepted as an effective way to process IoT data without disclosing private data in the research community. A basic approach to achieve LDP is to inject a Laplacian noise into original data for resisting data privacy leakage. However, it may increase the magnitude of noise that needs to be added and thus degrade the data utility. A better alternative for protecting IoT data is to build a compact, LDP-based data distillation model by limiting the collection of personal data to maximize the utility with the minimum amount of data.

Nowadays, there are a number of existing solutions to leverage local differential privacy mechanisms to address the data privacy issues in traditional device-to-cloud computing models [7]. However, with the introduction of edge computing for IoT data analytics, we are facing some new challenges in privacy protection mechanism design due to the distinct characteristics of this emerging computing paradigm. For example, since edge servers generally have limited capabilities, privacy preservation solutions should be lightweight enough to meet the constraint. Moreover, the efficiency of verifiable privacy computation, as well as the trade-off between privacy and utility, should be considered in designing a mechanism for distilling data at the edge with local differential privacy.

Digital Object Identifier:
10.1109/MCOM.2018.1701080

Chugui Xu, Ju Ren, Deyu Zhang, and Yaoxue Zhang are with Central South University; Chugui Xu is also with Sanming university.

0163-6804/18/$25.00 © 2018 IEEE

In this article, we propose a local differential privacy obfuscation (LDPO) framework for IoT data analytics, in which IoT data is distilled in the edge servers, and these edge servers are limited in their ability to make inferences about users' sensitive data. The LDPO framework adopts a two-layer privacy strategy. In an IoT device, it leverages a feature distillation model to perform data minimization and limits the amount of data being shared. In the edge server, LDPO can obfuscate the learned features, thereby providing an additional protection layer against sensitive inference. Then we present a preliminary implementation of the LDPO framework, and validate its performance in terms of privacy preserving level and data utility using real-world apps and datasets.

The remainder of the article is organized as follows. We introduce the architecture and benefits of the LDPO framework for IoT data analytics. Then we discuss the new challenges arising from the LDPO framework, which cannot be adequately addressed by today's privacy enhancing technologies alone. We present a case study on the preliminary implementation of the LDPO framework for IoT data analytics, as well as a performance evaluation of our implementation. Finally, we outline some future research directions.

Local Differential Privacy Obfuscation Framework for IoT Data Analytics: Architecture and Benefits

In this section, we briefly introduce the concept and characteristics of edge computing and local differential privacy, and then present the LDPO framework as well as its benefits for IoT data analytics.

Edge Computing and Local Differential Privacy

Edge computing is a new computing paradigm in which substantial computing and storage resources are placed at the edge of the network. It can reduce the communication overhead between the central servers and network edge by performing data analysis and knowledge discovery at or near the data sources [3]. In edge computing, applications migrate to edge servers not only to avoid excessive processing in the cloud, but also to allow autonomous/local decisions, reducing response time by mitigating the need for data transfer [8]. However, edge computing does not intend to replace the cloud-based infrastructure but aims to extend it by increasing the processing of data and decision making rules early at the IoT physical layer. It enables edge servers to communicate more efficiently with intermediary nodes instead of the cloud.

Differential privacy has been recognized as a promising approach to preserve data privacy while guaranteeing the data utility for data analysis applications. The main idea of differential privacy is to perform random perturbations on the analysis data, such that any individual's presence in the data has negligible impact on the randomized data [9]. But recently, an increasing number of researchers have changed their focus to LDP [6], since LDP can enable devices to collect aggregated data while protecting each user's privacy, without relying on a trusted third party. A successful example can refer to RAPPOR, developed by the scientists from Google [20]. It enables Google to collect users' answers to questions, such as the default homepage of the browser and the default search engine, to understand the unwanted or malicious hijacking of user settings. When applying LDP to edge computing, edge servers are able to preserve data privacy without sacrificing data utility before sending it to cloud servers.

Architecture

With the development of edge computing, privacy is becoming one of the greatest challenges. The decentralized data processing at the edge has increased the risk of privacy disclosure, which has attracted increasing attention from both industry and academia. Some existing privacy preserving solutions in edge computing could address some privacy issues in IoT data analytics [11]. Similarly, edge computing could introduce many new privacy challenges due to its distinct characteristics. This consequently motivates us to design the LDPO framework in edge computing for IoT data analytics. Figure 1 illustrates an overview of the proposed architecture. In the following, we introduce each part of the proposed architecture in detail.

IoT devices. The IoT devices can not only sense and collect data from the cyber-physical space, but also conduct some computing tasks and request service from the edge servers.

Edge server. The edge server is an important part of the proposed architecture. It is responsible for distilling the IoT data by applying local differential privacy to preserve data privacy while maintaining the data utility as much as possible. In a sense, the edge server is a distillation device that controls the exchange of data between an IoT device and the cloud server.

Cloud server. The cloud server is composed of a cluster of computers with massive computing and storage resources, responsible for complex data processing, analysis, and large-scale data/service storage.

To better understand the procedure of data processing, we briefly describe the data flow in a typical IoT application with the LDPO framework. IoT data is collected by various IoT devices and then forwarded to edge servers. The edge servers aggregate and distill the received data by means of LDPO before sending it to cloud servers. Cloud servers conduct data analytics on the distilled data to make some decisions for IoT applications.

Benefits

By applying the LDPO framework, edge servers can aggregate and distill the data from IoT devices before sending it to a cloud server, and preserve data privacy while guaranteeing data utility. Besides, the LDPO framework can provide the following benefits.

Privacy-preserving and efficient data aggregation: In IoT applications, each IoT device collects data from the cyber-physical world and distills it at edge servers to preserve data privacy before forwarding to cloud servers. The edge server transiently stores the received data or delivers it to the cloud. During these processes, privacy-preserving data aggregation is critical to prevent data leakage and reduce communication overhead. In this way, the communication overhead can be significantly reduced when compared to transmitting all the individual measurements separately.

Fine-grained data sharing: Since edge servers are generally connected to each other via wire-

The main idea of differential privacy is to perform random perturbations on the analysis data such that any individual's presence in the data has negligible impact on the randomized data. But recently, an increasing number of researchers have changed their focus to LDP, since LDP can enable devices to collect aggregated data while protecting each user's privacy, without relying on a trusted third party.

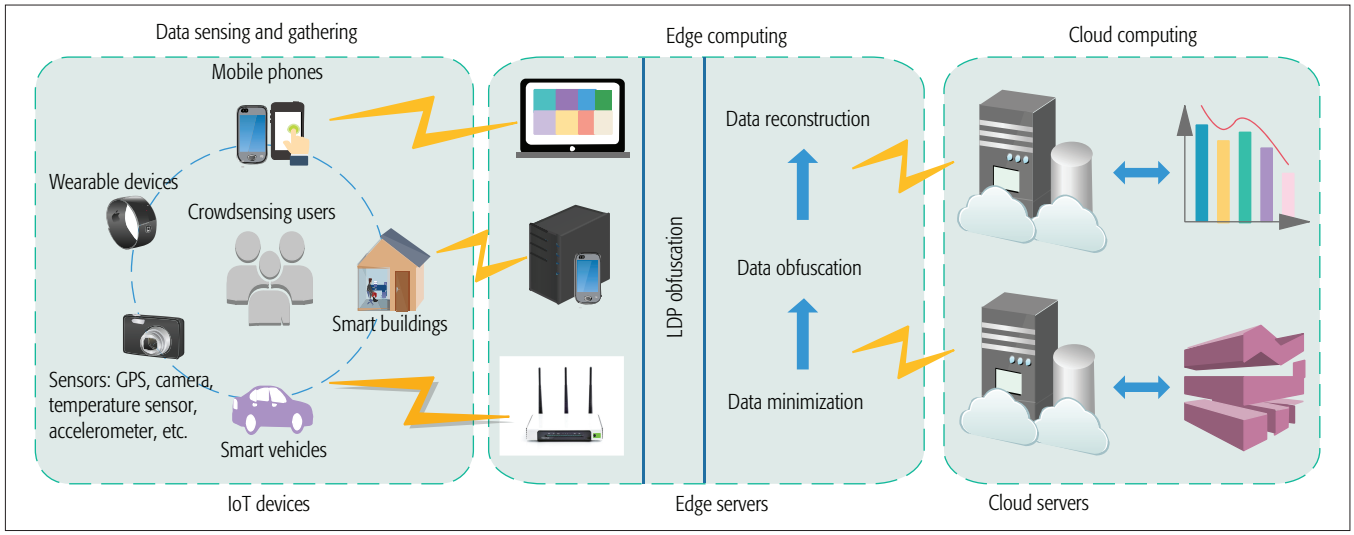

Figure 1. Local differential privacy obfuscation framework for IoT data analytics.

less or wired links, IoT data stored in edge servers may be shared among them [12]. This resolves the weak accessibility problem in traditional IoT systems, where applications cannot retrieve data from heterogeneous IoT devices because these devices may periodically sleep and suffer from intermittent wireless connections. LDPO can achieve fine-grained data sharing by leveraging LDP in edge computing and maximize the data utility for many real-time IoT applications.

Privacy-preserving content services: Edge servers with LDPO can provide local content distribution services to the users located in their coverage areas without disclosing sensitive data. Some contents are customized under the requests of users (e.g., navigation information and subscribed magazines); others may be diffused automatically. The diffused contents may contain plenty of sensitive information, such as preference, incentive, current location, and political inclination. The subscribed magazines may disclose preferences and political inclinations of subscribers. To prevent information leakage, edge servers with LDPO can define who can receive the diffused content and what kinds of contents should be obtained by a specific user.

Key Challenges

In order to fully exploit the benefits of the LDPO framework for IoT data analytics, we still face several challenges in its implementation, which significantly impede the flourishing of the related applications.

Lightweight Privacy Algorithms for Real-Time Services

In edge computing, IoT devices generally communicate with edge servers in one or two hops. This short-range communication makes real-time services feasible. Nevertheless, the delay of service response not only depends on the communication range and bandwidth, but also relies on the processing delay on edge servers. It means that the response delay will be significantly large if the edge servers have to perform complex computational operations to respond to users. In addition, due to the low computational capability of edge devices, they have no capability to perform complicated computation tasks. Therefore, it is crucial to design lightweight privacy preservation algorithms to support real-time services for edge computing systems.

Heavy Overhead for Verifiable Privacy Computation

Most differential privacy algorithms are generally constructed on verifiable privacy computation, which introduces theoretical approaches to achieve privately verifiable computation. In edge computing, edge servers cooperatively perform the computation tasks for users in a distributed way. The errors made by one edge server can spread to other edge servers and lead to incorrect final data. Besides, all the intermediate data and the final data should be verified to guarantee the correctness and privacy of data, which would cause heavy overhead. In addition, local differential privacy has its inherent drawback on computational overhead, which is intolerable for resource-restricted IoT devices in data distillation and for the edge server in function evaluation, especially on large volumes of datasets. Therefore, how to design practical verifiable privacy computation schemes suitable for resource-restricted IoT devices is necessary and crucial in edge computing.

Trade-off of Privacy and Utility of IoT Data

In the LDPO framework, distilling data at the edge can preserve the data privacy by minimizing the sensitive data that needs to be transmitted to the cloud for data analysis. However, this new model introduces some challenges such as decreasing the utility of IoT data. Existing local differential privacy schemes are usually designed for centralized data storage and analysis. They are no longer suitable for the decentralized architecture of edge computing where the data may come from various services and heterogeneous IoT devices. Therefore, how to tune the trade-off between privacy and utility becomes an important and challenging problem in the implementation of the LDPO framework.

Case Study: An Implementation of the LDPO Framework for IoT Data Analytics

In this section, we present a case study to introduce a preliminary implementation of the LDPO framework for IoT data analytics.

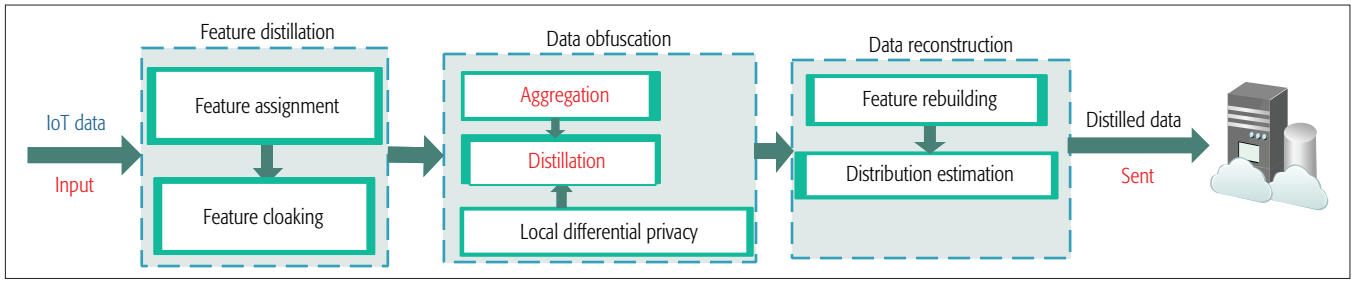

Figure 2. The implementation of LDPO framework for IoT data analytics.

Overview

The implementation of the LDPO framework for IoT data analytics is shown in Fig. 2. It consists of three components:

- Feature-distillation-based data minimization to learn a compact feature representation that is specific to useful inferences
- Data obfuscation with LDP to perturb features and provide provable privacy guarantees
- Data reconstruction to generate obfuscated IoT data from perturbed features for data analytics

The three components are joined together to make the LDPO framework capable of preserving the privacy of IoT data while maximizing the accuracy of data analytics at edge servers. These servers extract features from raw IoT data and perform data minimization to guarantee that only features related to useful inferences are retained for further processing. Specifically, we modify an autoencoder to explore the inherent structural characteristics of the IoT data, and learn a sparse feature representation of the data that is specific to the useful inferences. However, some of these extracted features might still have some correlation with sensitive inferences. To address this issue, we exploit local differential privacy to obfuscate the extracted features. Finally, we reconstruct obfuscated IoT data from the perturbed features without changing the existing interfaces. The implementation details of the LDPO framework are described in the following sections.

Feature-Distillation-Based Data Minimization

IoT data is usually high-dimensional in nature, which typically exhibits both structure and redundancy. These features allow us to minimize the amount of data. Data minimization [13] is a fundamental legal instrument that protects privacy by limiting the collection of personal data to the minimum extent for attaining legitimate goals.

Constructing the Data Minimization Model: Feature distillation models learn multi-layer transformations from the input data to the output representations, which is more efficient for feature extraction than hand-crafted shallow models. Among the building blocks of these models, autoencoders extract features in an unsupervised manner by minimizing the reconstruction error between the input and output. Using a nonlinear encoding function, an autoencoder can typically extract better features than linear transformation methods. However, the learned features may not be specific to the useful inferences. To handle this issue, we modify the autoencoder models by incorporating the useful inference and other associated constraints.

Incorporating Useful Inference: To the best of our knowledge, we are the first to modify the distillation models through incorporating the useful inferences. The objective for our data minimization model is to maximize the utility with the minimum amount of data. Therefore, it is important to combine the useful inferences with the autoencoder models to automatically extract features in a supervised manner. Specifically, we incorporate the minimization of cost function corresponding to the useful inferences to the objective function of existing autoencoders.

Local Differential Privacy Distribution Estimation

A common framework of locally private distribution estimation is that each edge server applies the LDPO framework on the data for privacy protection and then sends the distilled data to a cloud server. To achieve LDP distribution estimation, the LDPO design includes two key steps: one is distilling with minimax filters, and the other is adding randomness [14]. Particularly, a minimax filter with multiple hash functions can hash all the variables in the domain into a predefined space. Thus, the unique bit strings are the representative features of the original report. Then, after privacy preserving by randomized responses, many samples with various levels of noise are generated by edge servers. After distillation, an edge server obtains a large sample space with random noises. As a result, the edge server may estimate the distribution from the noised sample space by taking advantage of machine learning techniques such as regression analysis [15].

In an IoT device, the feature abstraction of IoT data consists of two phases.

Feature Assignment: In this phase, a dataset has one attribute with the domain. For each candidate value, several hash functions are used to transform it into a k-bit string. Once k and the number of hash functions are well chosen, this transformation can maximize the uniqueness of a bit string to represent any attribute value.

Feature Cloaking: After the minimax filter F is obtained, each bit in F will be randomized to 0 or 1 with a certain probability. This randomness is important as the original data may be sensitive.

On the edge server, we adopt randomized minimax filters to distill data from different IoT devices, and then estimate the univariate distribution as follows.

Distillation-Based Local Differential Privacy: After distillation by the edge server, all the bit strings will be transformed bitwise. Then the count of each bit can be estimated based on the randomness of the bit strings. The privacy guarantees of the edge server come from its distillation. Let m denote the number of edge servers in our task. The label count for a given sensor data $j \in [m]$ and an input x_t is the

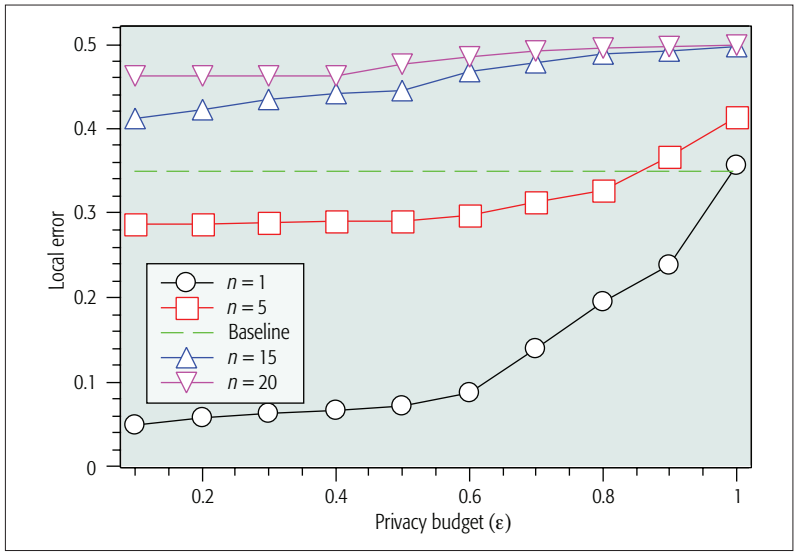

Figure 3. Local error for the given privacy budget.

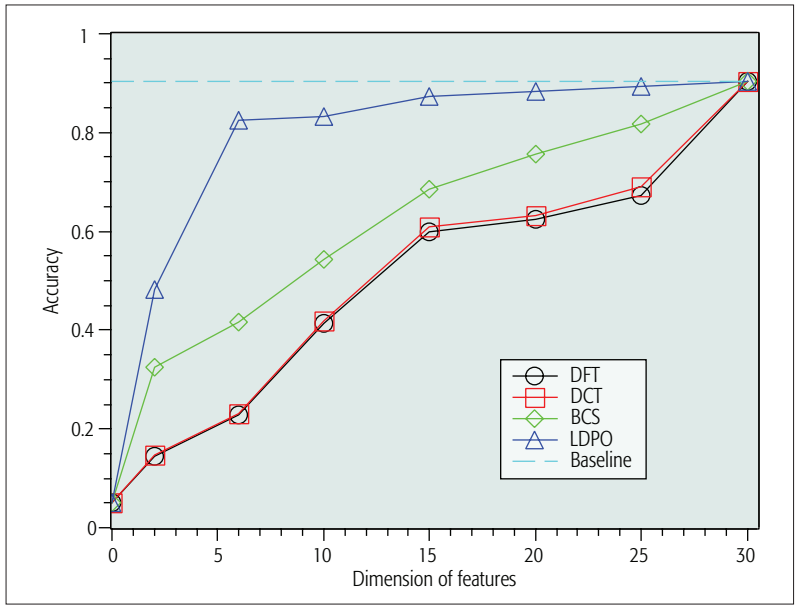

Figure 4. The utility after data distillation.

number of IoT devices that assign sensor data j to input x_t. If we simply apply the label with the largest count, the ensemble's decision may depend on the crowdsource data from the IoT devices. Indeed, the distilled output changes if an edge server makes a different decision. We add random noise to the data from connected IoT devices to introduce obfuscation. However, the obfuscation parameter influences the level of privacy guarantee. Intuitively, the large obfuscation parameter leads to a strong privacy guarantee, but can degrade the accuracy of the labels, as the noisy maximum output can obfuscate the raw data form IoT devices.

Feature Rebuilding: The hash functions used on the IoT devices are replayed on the edge servers to reconstruct the minimax filters.

Distribution Estimation: Taking the minimax filters as the feature variables, the edge server can estimate the univariate distribution of the single attribute via linear regression.

Under the above framework, if features are mutually independent, we can easily conclude that the combinations of features from different candidate sets are also mutually independent. Therefore, with mutually independent features of minimax filters, existing machine learning techniques like Lasso regression are effective for the multivariate distribution estimation [15].

Performance Evaluation

In this subsection, we evaluate the performance of LDPO for IoT data analytics in terms of privacy and utility guarantees.

Privacy and Utility Guarantees: To evaluate the performance of LDPO in terms of privacy and utility guarantees, we experimentally evaluate our distilling-based data minimization model, using the ECBT dataset[1] for a case study. To show the advantage of our method, we further compare it with the state-of-the-art feature extraction approaches. The discrete Fourier transform (DFT) and discrete cosine transform (DCT) are two basic transformation techniques in the signal processing community, and form the basis of the fundamental wavelet transformation (BCS) for time-frequency signal analysis.

Figure 3 shows that the number of IoT devices n has a positive effect on individual privacy, independent of the individual choices of privacy budget: the larger the privacy budget, the higher the local error. Therefore, it is feasible to incentivize IoT devices to extract the data at lower privacy budget by means of LDPO, but the parameters of LDPO depend on the characteristics of the data.

From Fig. 4, we can observe that:

- More features would be beneficial for improving the utility performance since the combination of multiple features would be more accurate to represent the input data.
- LDPO can achieve higher accuracy than the state-of-the-art approaches with large improvement. Seven features are enough for LDPO to provide good utility performance with 87.27 percent accuracy, while the accuracy using all 30 features is 90.45 percent.
- The proposed feature-distillation-based data minimization model significantly benefits from the automatic learning process, which incorporates the useful inference data into distillation models.

Future Directions

Despite the great potential of the LDPO framework for IoT data analytics, the emerging technology still requires continuous research efforts to promote its development. In this section, we summarize some future directions to attract further studies.

Privacy Exposure in Data Fusion

In IoT applications, the devices act as data producers to generate and process data of various levels of sensitivity. Some may be inherently sensitive, such as the data generated by a blood glucose sensor. However, even the collected data seems to be non-sensitive, so the application of data fusion can trigger serious privacy concerns. This problem is exacerbated by the use of edge computing for IoT application, as one of the motivations for edge computing is to explicitly enable the fusion among edge servers that can aggregate and process the data across a large number of IoT devices. Therefore, some levels of privacy preservation in data fusion need to be defined, and efficient and effective privacy-preserving mechanisms must be designed to protect users' privacy in edge computing.

[1] ECBT (2012). CER Smart Metering Project-Electricity Customer Behaviour Trial; www.ucd.ie/issda/CER-electricity.

Decentralized and Scalable Security

Generally, distributed systems are more vulnerable to attacks than centralized systems. Edge computing often needs to operate in more vulnerable environments where they can best satisfy users' requirements. Additionally, proximity to IoT devices and locality on the edge enable it to help address certain new IoT security challenges. Specifically, edge servers can serve as distillation points for sensitive data before sending it to a cloud server, provide contextual integrity and isolation, and conduct selected security functions for IoT data analytics. Nevertheless, a large number of edge servers may not have enough resources to protect themselves. Furthermore, each edge server may not have the global capability to detect threats. In summary, how to design a scalable, efficient, and decentralized security mechanism is challenging but important for the healthy development of edge computing.

Detection of Malicious Edge Servers and IoT Devices

As the architecture of edge computing is vulnerable to a large variety of cyber attacks, both edge servers and IoT devices may be at risk of being compromised. Malicious edge servers and IoT devices may pretend to be legitimate and inveigle users to connect to them. Some malicious IoT devices may collude to manipulate the results of mobile crowdsensing. Compromised or malicious edge servers and IoT devices would be large threats to the security and privacy of users' data. Unfortunately, it is difficult to detect them in edge computing. Therefore, study on the mechanism to detect malicious and corrupted edge servers and IoT devices in edge computing is worthy of attention.

Conclusion

Edge computing is a new computing paradigm that revolutionizes cloud computing by extending storage, computing, and networking resources to edge servers for supporting extremely large-scale IoT applications. However, it is also confronted with traditional privacy leakage risks, which raise various new privacy challenges for IoT data analytics. In this article, we have proposed an LDPO framework for IoT data analytics to aggregate and distill the IoT data at the edge without disclosing users' sensitive data. We have also introduced the architecture and benefits of the LDPO framework, followed by some key technical challenges in guaranteeing its performance. Then we have presented a preliminary implementation of the LDPO framework, and validated its performance in terms of privacy preservation level and data utility using real-world apps and datasets. Finally, some future directions are outlined to attract continued research focus in this emerging and evolving field of study.

Acknowledgment

This work was supported by the Natural Science Foundation Project of the Fujian Province of China (No. 2015J01271), the Young, Middle-Aged Scientific Research Project in the Department of Education of Fujian (No. JAT160469/B201618), the Natural Science Foundation of China (Nos. 61702562 and 61702561), and the Innovation-Driven Project of Central South University (No. 2016CXS013).

References

[1] Networking, Cisco Visual, "Cisco Global Cloud Index: Forecast and Methodology, 2016–2021"; https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html#Toc503317525, 02-19-2018.
[2] Y. Zhang *et al.*, "Home m2m Networks: Architectures, Standards, and QoS Improvement," *IEEE Commun. Mag.*, vol. 49, no. 4, Apr. 2011.
[3] N. Abbas *et al.*, "Mobile Edge Computing: A Survey," *IEEE Internet of Things J.*, vol. 5, no. 1, 2018, pp. 450–65.
[4] J. Ren *et al.*, "Serving at the Edge: A Scalable IoT Architecture Based on Transparent Computing," *IEEE Network*, vol. 31, no. 5, Sept./Oct. 2017, pp. 96–105.
[5] G. Zhuo *et al.*, "Privacy-Preserving Verifiable Data Aggregation and Analysis for Cloud-Assisted Mobile Crowdsourcing," *Proc. 35th Annual IEEE INFOCOM*, 2016, pp. 1–9.
[6] Z. Qin *et al.*, "Heavy Hitter Estimation Over Set-Valued Data with Local Differential Privacy," *Proc. ACM SIGSAC Conf. Computer and Commun. Security*, 2016, pp. 192–203.
[7] M. Akter and T. Hashem, "Computing Aggregates Over Numeric Data with Personalized Local Differential Privacy," *Proc. Australasian Conf. Info. Security and Privacy*, 2017, pp. 249–60.
[8] T. G. Rodrigues *et al.*, "Hybrid Method for Minimizing Service Delay in Edge Cloud Computing Through VM Migration and Transmission Power Control," *IEEE Trans. Computers*, vol. 66, no. 5, 2017, pp. 810–19.
[9] C. Xu *et al.*, "DPPro: Differentially Private High-Dimensional Data Release Via Random Projection," *IEEE Trans. Info. Forensics and Security*, vol. 12, no. 12, 2017, pp. 3081–93.
[10] Ú. Erlingsson, V. Pihur, and A. Korolova, "Rappor: Randomized Aggregatable Privacy-Preserving Ordinal Response," *Proc. 2014 ACM SIGSAC Conf. Computer and Commun. Security*, 2014, pp. 1054–67.
[11] R. Lu *et al.*, "A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT," *IEEE Access*, vol. 5, 2017, pp. 3302–12.
[12] H. Zhu *et al.*, "You Can Jam But You Cannot Hide: Defending Against Jamming Attacks for Geolocation Database Driven Spectrum Sharing," *IEEE JSAC*, vol. 34, no. 10, 2016, pp. 2723–37.
[13] S. Li, L. Da Xu, and X. Wang, "Compressed Sensing Signal and Data Acquisition in Wireless Sensor Networks and Internet of Things," *IEEE Trans. Industrial Informatics*, vol. 9, no. 4, 2013, pp. 2177–86.
[14] J. Hamm, "Enhancing Utility and Privacy with Noisy Minimax Filters," *Proc. IEEE Int'l. Conf. Acoustics, Speech and Signal Processing*, 2017, pp. 6389–93.
[15] J. Zhang *et al.*, "Functional Mechanism: Regression Analysis Under Differential Privacy," *Proc. VLDB Endowment*, vol. 5, no. 11, 2012, pp. 1364–75.

Biographies

Chugui Xu [S'16] (chuguixu@csu.edu.cn) is a Ph.D student at Central South University, China. He received his B.S. in physics (2005) from Hunan Normal University, China, and his M.S. in computer science (2010) from Hunan University of Technology, China. He is also a lecturer at Sanming University, China. His research interests include the Internet of Things, data privacy, and security.

Ju Ren [S'13, M'16] (renju@csu.edu.cn) received his B.Sc., M.Sc., and Ph.D. degrees, all in computer science, from Central South University (CSU), China, in 2009, 2012, and 2016, respectively. Currently, he is a professor with the School of Information Science and Engineering, CSU. He serves as an Associate Editor for *IEEE Transactions on Vehicular Techonology* and *Peer-to-Peer Networking and Applications*. His research interests include the Internet of Things, transparent computing, and edge computing.

Deyu Zhang [S'13, M'17] received his B.S. degree from PLA Information Engineering University in 2005 and his M.S. degree from CSU in 2012, both in communication engineering. He received his Ph.D. degree in computer science from CSU in 2016. He is now an assistant professor with the School of Software, CSU. His research interests include stochastic resource allocation, edge computing, and IoT.

Yaoxue Zhang (zyx@csu.edu.cn) received his B.Sc. degree from Northwest Institute of Telecommunication Engineering, China, in 1982, and his Ph.D. degree in computer networking from Tohoku University, Japan, in 1989. Currently, he is a professor with the Department of Computer Science, CSU. His research interests include computer networking, operating systems, and transparent computing. He is a Fellow of the Chinese Academy of Engineering and the Editor-in-Chief of the *Chinese Journal of Electronics*.

Edge computing is a new computing paradigm that revolutionizes cloud computing by extending storage, computing, and networking resources to edge servers for supporting extremely large-scale IoT applications. However, it is also confronted with traditional privacy leakage risks, which raise various new privacy challenges for IoT data analytics.